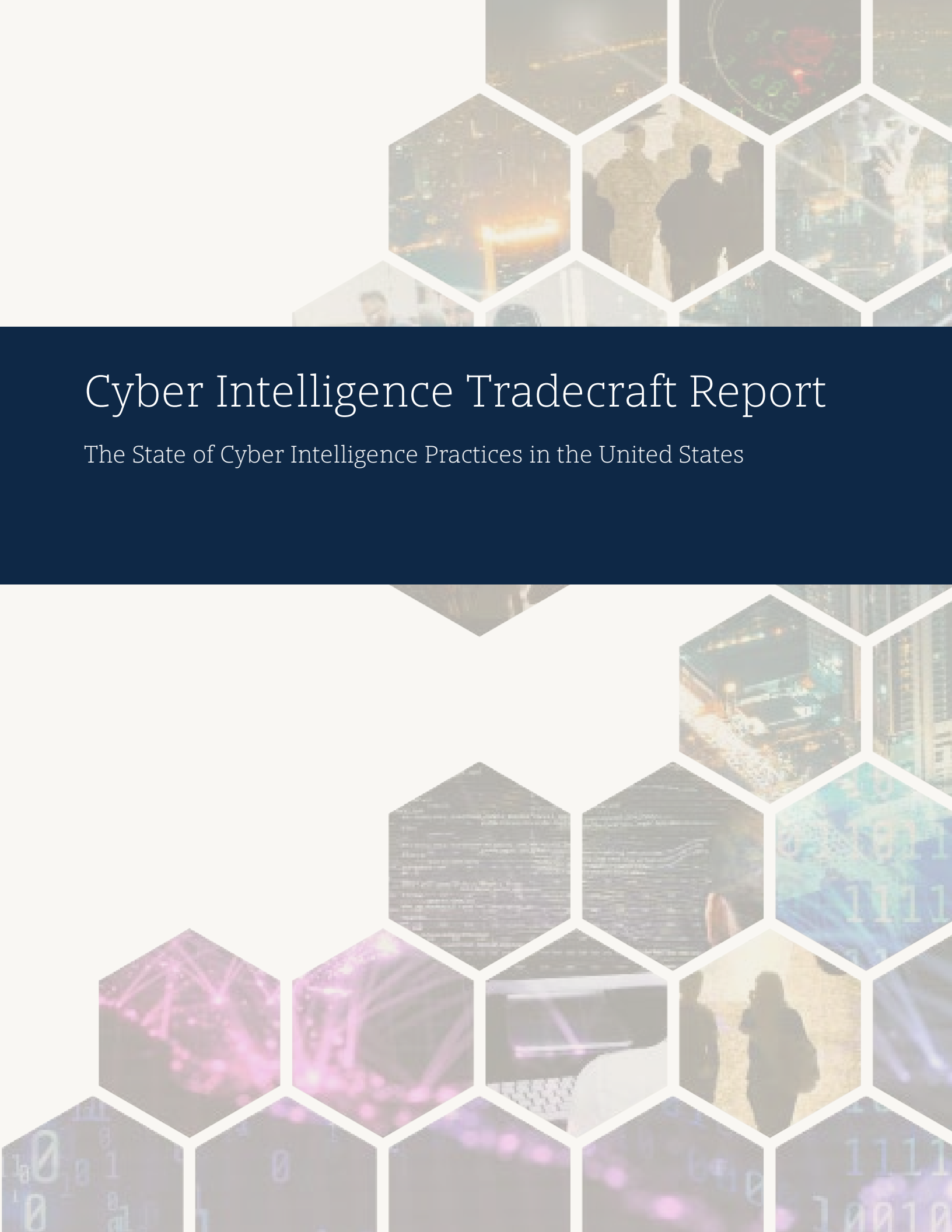


Cyber Intelligence Tradecraft Report

The State of Cyber Intelligence Practices in the United States

Cyber Intelligence Tradecraft Report:
The State of Cyber Intelligence
Practices in the United States

By
Jared Ettinger

Contributors
Hollen Barmer
Jennifer Kane
Heather Evans
Erica Brandon
Ritwik Gupta
Daniel Decapria
Andrew Mellinger

Implementation Guides

Artificial Intelligence and Cyber Intelligence
April Galyardt, Ritwik Gupta, Dan DeCapria, Eliezer Kanal, Jared Ettinger

The Internet of Things and Cyber Intelligence
Dan Klinedinst, Deana Shick, Jared Ettinger

Public Cyber Threat Frameworks and Cyber Intelligence
Samuel Perl, Geoffrey Dobson, Geoffrey Sanders, Daniel Costa, Lawrence Rogers, Jared Ettinger

Graphics Team
David Biber, Alex Van Deusen, Todd Loizes

Biber format author lists and legal language

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0447

Contents

Executive Summary 1

Cyber Intelligence Tradecraft Framework Report 3

Environmental Context 11

Data Gathering 35

ThreatAnalysis 54

Strategic CyberIntelligence Analysis 66

Reporting and Feedback 81

The Future of Cyber andCyber Intelligence 99

Conclusion 101

Glossary & Appendix 103

Executive Summary

Strengthening Cyber Intelligence

Intelligence dates to ancient times when early civilizations used it to protect their assets and gain an advantage over their adversaries. Although the ways we perform the work of intelligence have changed, it remains as critical as ever. And this can be no truer than in the cyber domain. In performing cyber intelligence, we collect, compare, analyze, and disseminate information about threats and threat actors seeking to disrupt the cyber ecosystem[1], [2] one of our most critical assets. Through cyber intelligence, we know ourselves and our adversaries better. And with that knowledge, we can proactively take steps to better understand risks, protect against threats, and seize opportunities.

In 2013, the Software Engineering Institute (SEI) at Carnegie Mellon University conducted a study on behalf of the U.S. Office of the Director of National Intelligence to understand the state of cyber intelligence practices at organizations throughout the country. We conducted a similar study in 2018, and this report details our findings.

Two important outcomes from the 2013 study formed the foundation for our 2018 work. First, we defined cyber intelligence as acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making. Second, we defined a framework for cyber intelligence; based on the intelligence cycle, its components provide for environmental context, data gathering, threat analysis, strategic analysis, and reporting and feedback.

During the 2018 study, we interviewed 32 organizations representing a variety of sectors to understand their best practices and biggest challenges in cyber intelligence. During conversations guided by questions designed to elicit descriptive answers, we noted organizations' successes and struggles and how they approached each component of the cyber intelligence framework. We also provided an informal assessment of how well each organization was performing for certain factors within each component. We aggregated and analyzed these answers, grouping what participants told us into themes. This report moves through the cyber intelligence framework, detailing our findings for each component. The final aspects of the report includes three implementation guides on machine learning for cyber intelligence, IoT for cyber intelligence and cyber threat frameworks.

1 https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

There are a number of areas where organizations can take action to improve their cyber intelligence practices. They include differentiating between cyber intelligence and cybersecurity, establishing repeatable workflows, breaking down silos that fragment data and expertise, enabling leadership to understand and become more engage in cyber intelligence, establishing consistent intelligence requirement and data validation processes, and harnessing the power of emerging technologies.

Since 2013, the practice of cyber intelligence has gotten stronger. Yet it is not strong enough. In the coming years, data and compute power will continue to increase, and artificial intelligence will enable us to make sense of threats while also making threats themselves more complex. Organizations of any size can learn from and apply the best practices and performance improvement suggestions outlined in this report. Together we can achieve higher levels of performance in understanding our environment, gathering and analyzing data, and creating intelligence for decision makers.

Cyber Intelligence Tradecraft Framework Report

Introduction

ABOUT THIS REPORT: IMPROVING THE PRACTICE OF CYBER INTELLIGENCE

This report details the findings of a study the Software Engineering Institute (SEI) at Carnegie Mellon University conducted at the request of the United States Office of the Director of National Intelligence (ODNI). Our mission was simple: understand how organizations across sectors conduct the work of cyber intelligence and share our findings.

In this report, we describe the practices of organizations that are performing well and the areas where many organizations struggle, and we identify the models, frameworks, and innovative technologies driving cyber intelligence today. We believe this report can provide a starting point to enable organizations across the country to adopt best practices, work together to fix common challenges, and reduce the risk of cyber threats to the broader cyber community.

WHO SHOULD READ THIS REPORT?

We have designed this report to be informative for anyone concerned with cyber threats. The following readers will find this report useful:

- Organizational Decision Makers: understanding where to direct funding and resources
- Cyber Intelligence Team Managers: understanding best practices for your team, including hiring, workflow, and leveraging data
- Cyber Intelligence Analysts: understanding best practices, tools for analysis, and what your peers are doing

Whether your organization has a robust cyber intelligence program or is just getting started, the actionable recommendations provided in each section of this report can serve as guideposts for helping you achieve high performance.

THE IMPORTANCE OF CYBER INTELLIGENCE

Cyber intelligence: acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making.

CYBER INTELLIGENCE DEFINED

Cyber intelligence is a strategic approach to cyber threats that can enable your organization to anticipate, plan, and make decisions about risks and opportunities, not merely react to incidents or specific threats. Your organization may protect the confidentiality, integrity, and availability of data and computer systems. Such practices

are part of cybersecurity.[2] However, do you know which threat actors have the intent and capability to target your organization now and in the future? Do you track malware campaigns? Do you know which of your technologies are at risk? Do you know how certain attacks would affect your organization? Do you perform supply chain analysis, produce targeting packages for your pen-testing team, or provide assessments on the impact/opportunity of emerging technologies? Are you able to produce threat priority and vulnerability lists or industry threat assessments? Do you know if your organization should open a line of business in a foreign country? Cyber intelligence can provide strategic insight to protect your organization.

DIFFERENTIATING CYBERSECURITY FROM CYBER INTELLIGENCE

Improving your organization's security involves both cybersecurity and cyber intelligence, two important and distinct activities. Cybersecurity is the security actions or measures taken to ensure a state of inviolability of the confidentiality, integrity, and availability of data and computer systems from hostile acts or influences. We have seen the term Cyber hygiene be referred to as both cybersecurity and as actions to improve cybersecurity. A) Cyber Hygiene: Actions could be: protecting network infrastructure, inventorying hardware and software assets; configuring firewalls and other products; vulnerability scanning; patching systems; ensuring compliance, and conducting technical analysis for incident response purposes involving specific threats to the organization. Another important and separate concept is this thing called cyber intelligence 2). Cyber Intelligence: Acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making. (Modified CITP 2013 Definition)

---

2 The NIST Framework for Improving Critical Infrastructure Cybersecurity defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." The DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 defines cybersecurity as "actions or measures taken to ensure a state of inviolability of the confidentiality, integrity, and availability of data and computer systems from hostile acts or influences."

CYBER INTELLIGENCE FRAMEWORK

ENVIRONMENTAL CONTEXT

A deep understanding of your organization, including your organization's entire attack surface; threats, risks, and opportunities targeting your organization and industry; and your organization's internal and external network and operations. Gaining this understanding is a continuous process and influences what data is needed to perform cyber intelligence.

DATA GATHERING

Data Gathering: Through automated and labor -intensive means, data and information is collected from multiple internal and external sources for analysts to analyze to answer organizational intelligence requirements.

THREAT ANALYSIS

Assessing technical telemetry and non-technical data pertaining to specific threats to your organization and industry to inform cybersecurity operations/actions and strategic analysis. Threat analysis is built on operational and tactical analysis and enhances CSO/CISO and other mid- to senior-level decision making.

STRATEGIC ANALYSIS

Holistically assessing threats, risks and opportunities to enhance executive decision making pertaining to organization-wide vital interests such as financial health, brand, stature and reputation.

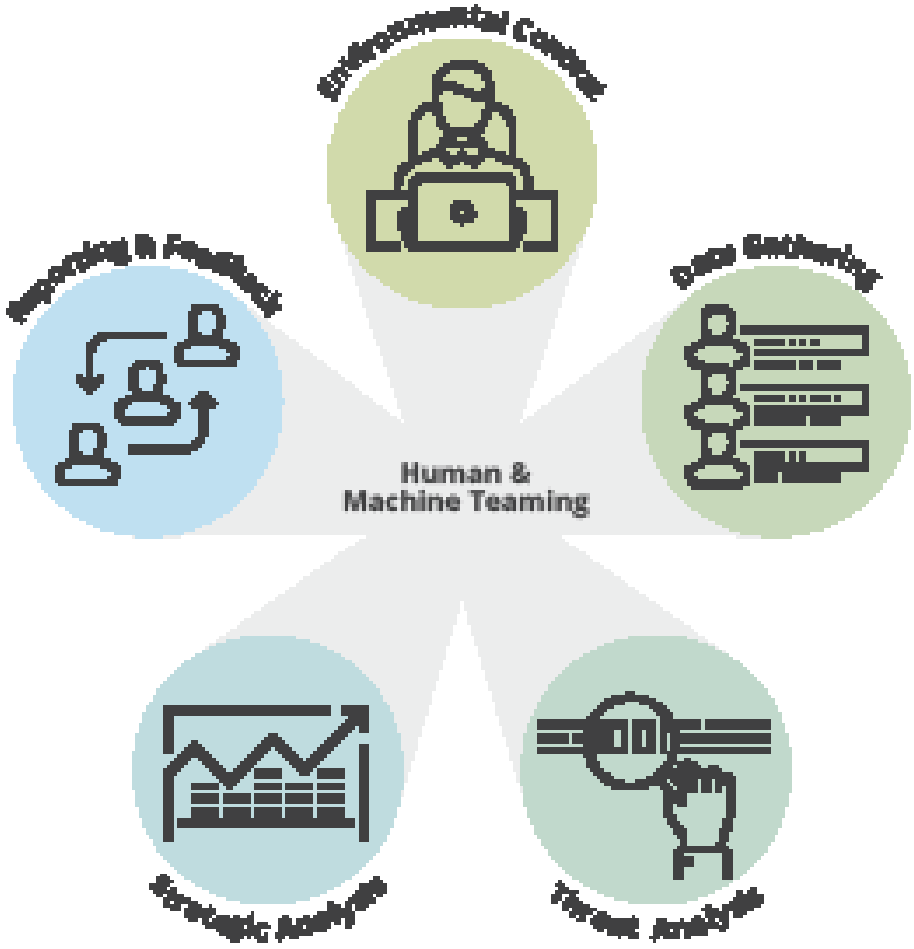
REPORTING AND FEEDBACK

Communication between analysts and decision makers, peers, and other intelligence consumers regarding their products and work performance. Reporting and feedback help identify intelligence requirements and intelligence gaps.

HUMAN-MACHINE TEAMING

At the center of the cyber intelligence framework, human analysts use their analytical acumen alongside the computational power and speed of machines—computers able to automate processes and, increasingly, to learn through artificial intelligence—to produce timely, actionable, and accurate intelligence, depending on the cyber issue being analyzed.

CYBER INTELLIGENCE FRAMEWORK



the concepts in this study.

BACKGROUND: 2013 CYBER INTELLIGENCE STUDY

This study is a follow-up to a similar cyber intelligence study we conducted at the request of ODNI in 2013. The Cyber Intelligence Tradecraft Project (CITP 2013) Key Findings Report highlights cyber intelligence best practices and biggest challenges we observed several years ago. We used our 2013 findings as a foundation for the most recent study, and as a baseline to understand changes in cyber intelligence practices over the years. In this report, we point out areas where cyber intelligence practices are improving rapidly and areas where progress has been almost glacial.

HOW WE CONDUCTED THE STUDY

The Cyber Intelligence Tradecraft Study was conducted on behalf of the US Office of the Director of National Intelligence by the Software Engineering Institute at Carnegie Mellon University

Purpose

- Understand how organizations conduct cyber intelligence activities
- Identify common challenges and best practices

WE INTERVIEWED

To understand the state of cyber intelligence practices nationwide, we set out to interview companies and organizations about their cyber intelligence practices. Using our 2013 report as a foundation, we developed updated interview questions rooted in the five components of our 2013 cyber intelligence framework: Environmental Context, Data Gathering, Threat Analysis, Strategic Analysis, and Reporting and Feedback. We asked conversational questions that helped us determine how well organizations were doing in relation to 33 assessment factors.

Our SEI team interviewed 32 U.S. organizations during sessions that ranged from 2-4 hours. We performed both onsite and virtual interviews of small, large, new, and established organizations representing a variety of critical infrastructure sectors: Finance, Health and Public Health, Information Technology, Communications, Food and Agriculture, Commercial Facilities, Government Facilities, Energy, Defense Industrial Base, Transportation, and Academia. We interacted with representatives from these organizations' cyber intelligence and cyber security teams and leadership.

After completing all of the interviews, our team benchmarked the data we collected against the 33 assessment factors within the five components of the cyber intelligence framework; the levels of performance we observed are shown in the performance snapshots in each chapter of this report. We compiled an exhaustive list of the challenges and best practices we noted from interview participants (a total of 2,268 items) and grouped them by themes. The 78 resulting themes drive the content of this report.

HOW WE UNDERSTOOD HIGH PERFORMANCE

Using information from our 2013 study, we developed some baseline criteria for high performance. We refined and adjusted these criteria based on information from interviews we conducted during the current study to define the methodologies, technologies, and processes that constitute high performance in cyber intelligence today. We then scored performance according to the following scale:

High-Performing: Organization meets all high-performing criteria.
Almost High-Performing: Organization generally meets all high-performing criteria, except one.
Getting Started / Doing a Few Things: Organization generally meets one or two high-performing criteria.
Low Performing: Organization meets no high-performing criteria.
Insufficient Information: Insufficient information to make an assessment.

WHAT HAS CHANGED SINCE THE 2013 STUDY? WHAT HAS STAYED THE SAME?

THE CYBER INTELLIGENCE FRAMEWORK

We changed some terminology within the cyber intelligence framework. We first introduced the cyber intelligence framework, rooted in the traditional intelligence cycle, in 2013, with the components Environment, Data Gathering, Functional Analysis, Strategic Analysis, and Decision Maker Reporting and Feedback. To reflect terminology we heard from participants, we changed Functional Analysis to Threat analysis. Because we heard time and again from participants whose reporting and feedback practices involved a variety of individuals, especially at the peer level, we changed Decision Maker Reporting and Feedback to simply Reporting and Feedback.

TRADITIONAL INTELLIGENCE CYCLE

Our recent research showed some high performing organizations using frameworks that are modeled on the traditional intelligence cycle and that successfully incorporate cutting edge technology into their cyber intelligence programs. These high performing organizations have long established cyber intelligence programs and foster a complete people, processes, and technologies approach to cyber intelligence. In contrast to our 2013 report, which described the traditional intelligence cycle as limited by its linear format, we now assess the traditional intelligence cycle as an interrelated and non-linear process. The success and failure of one or more steps in the cycle may spawn a rippling effect on the entire cycle. The traditional intelligence cycle is therefore an acceptable way for organizations to approach cyber intelligence; our cyber intelligence framework is ideal because it addresses the intersection and pervasiveness of cyber and technology.

GAP BETWEEN TECHNICAL AND ANALYTICAL EXPERTISE

A gap remains and is widening between individuals experienced in intelligence analysis and operations and those experienced in information security, computing fundamentals, and artificial intelligence. Some organizations have only technical people on their team with zero to little understanding, background or training in intelligence analysis. Other organizations that employ individuals experienced in intelligence analysis and information security encounter stark cross-team communication challenges. Words mean different things to different people, often shaped by our own unique experiences and backgrounds. While getting different perspectives is encouraged, the lack of a common lexicon and framework makes it challenging for teams and organizations across sectors to arrive at common ground for solving complex problems. Shared lexicon and frameworks increase collaboration and build trust.

INCREASED ADOPTION OF AUTOMATION AND ARTIFICIAL INTELLIGENCE

Computing hardware and software is changing and improving every day; machines, with their computational power and speed, have the potential to transform cyber intelligence. As organizations create and have access to more and more data, these organizations are increasingly adopting automation and artificial intelligence. Specifically, many are using machine learning to assist human analysts with understanding their environment, data collection, analysis, and report generation.

“Knowing yourself is the beginning of all wisdom.”

—Aristotle

Environmental Context

Understanding Your Organization Inside and Out

INTRODUCTION

A cyber intelligence team should have a deep understanding of its organization's entire attack surface; threats, risks, and opportunities relevant to the organization and industry; and the impact of those threats, risks, and opportunities. Environmental Context refers to this understanding, which requires a knowledge of your organization's internal and external network and operations, including services, operating systems, endpoints, mission and culture, processes and policies, business partners, suppliers, geopolitics, emerging technologies, and position in industry relative to competitors. Because your environment is constantly changing, gaining and maintaining this understanding is a continuous process.

ENVIRONMENTAL CONTEXT ASSESSMENT FACTORS

In evaluating the state of the practice of cyber intelligence in terms of Environmental Context, we considered the following factors:

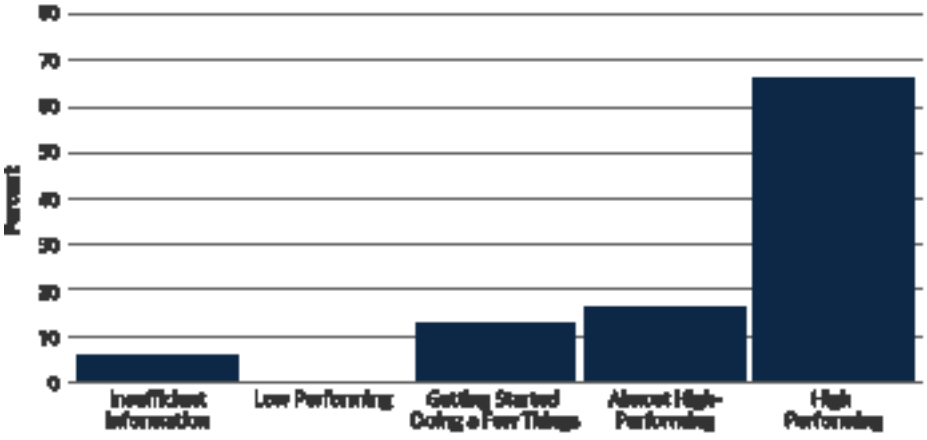
1. Knowing Your Attack Surface
2. Understanding the Difference Between Cyber Intelligence and Cybersecurity
3. Aligning cyber intelligence roles with your organization's needs
4. Having Enough People, Having the Right People
5. Placement of Your Cyber Intel Effort in Your Organization
6. Cyber Intelligence Workflow
7. Threat Prioritization Process
8. Using Past, Present, and Future Data
9. Relationship Between Cyber Intelligence and Insider Threat Teams

ENVIRONMENTAL CONTEXT FACTOR 1: KNOWING YOUR ATTACK SURFACE

WHAT THIS ASSESSMENT FACTOR MEANS

The organization holistically understands its people (including relevance and access) and cyber footprint (including infrastructure, internet presence, physical assets and access, and technology). This understanding informs the tactics, techniques and procedures (TTPs) the organization implements to support cybersecurity and cyber intelligence.

PERFORMANCE SNAPSHOT



Environmental Factor 1: Knowing Your Attack Surface Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Silos blind

A major challenge we observed across organizations was silos. In some organizations, internal business units have separate, distinct IT systems. These business units may not communicate or share data efficiently because IT systems and technology stacks are completely different. Cultural differences and network fragmentation among internal business units exacerbate the effects of silos.

A related challenge is the inability to actively and continuously monitor third parties due to policy and IT architecture and technology stack differentiations. Without visibility into the activities and services of partners, suppliers, and sub-contractors, cyber intelligence teams cannot know how threat actors--and which threat actors--could exploit vulnerabilities within their attack surface.

Inability to identify and track important organizational data presents dangers

Many organizations have trouble identifying the location of confidential and intellectual property data, how data moves across the organization, and when and how individuals interact with it. Many study participants expressed frustration over not having a Data Loss Prevention (DLP) tool. These organizations tended to also lack formalized insider threat programs. Although access control lists help to prevent unauthorized access, they cannot, for example, easily detect an insider stealing forty pages of sensitive information at a slow rate.

GETTING TO HIGH PERFORMANCE

Know your critical assets

High-performing cyber intelligence teams demonstrate a keen understanding of their organization's critical assets, from network endpoints to patent pending technologies. These teams understand Information Technology (IT) and Operational Technology (OT) (industrial control and supervisory control and data acquisition systems (ICS/SCADA) assets, infrastructure, the convergence and associated vulnerabilities between the two. These organizations understand their internet-facing systems, data centers, cloud, network infrastructure, servers, hosts, portals, mobile , IoT and other embedded technologies, and keep track of all hardware and software inventory via a number of commercially available IT Asset Management and Operational Technology monitoring solutions.

IMPROVE YOUR PERFORMANCE

- Conduct a crown-jewel exercise to identify critical assets.
- Work with cybersecurity teams to know and monitor the users accessing your network, the data they use, and their computing equipment.
- Promote regular sharing among your Information Technology, Technology Development and Integration, Cyber Intelligence, Program Management, Security Operations Center, and Security Engineering and Asset Security teams. See Environmental Context Factor 5 for more information.
  - Hold daily standup meetings, calls, or video conferences.
  - Create a physical or virtual fusion center.

Conducting a crown-jewel exercise or analysis can help you understand your critical assets, which range from sensitive technologies to data types moving and resting within your organization. During the course of the exercise, you'll identify the assets themselves, their owners, the risk to your organization if they are compromised, and how they interact with other assets. High-performing organizations reported using existing models for crown-jewel exercises[3] or developing their own crown-jewel exercises by meeting and building relationships with colleagues working on critical assets or patent-pending technologies. For organizations just starting out, the crown-jewel exercise can provide a foundation for building a cyber intelligence effort.

Don't forget about people. High-performing cyber intelligence teams know their organization's employees, contractors, executives, and business partners –and how these individuals access the organization's network and data. High-performing organizations use DMZs and internal and external firewalls for instances where their own employees access internet-facing systems. These organizations use Data Loss Prevention (DLP), Security Information and Event Management (SIEM) and User and Entity Behavior Analytical (UEBA) tools to identify abnormal behavior across users and services such as SMTP, FTP, Telnet, VPN, webmail, and Remote Desktop, as well as exposures from wi-fi hotspots and rogue access points.

Explore creating a fusion center

High-performing cyber intelligence teams build strong relationships with cybersecurity teams and across organizational business units. Virtual or physical "fusion centers" facilitate interaction between the cyber intelligence team, cybersecurity team, and other teams such as network defense, vulnerability management, forensics, incident response, penetration testing, and insider threat. In a fusion center, these teams are often physically co-located, and report on their current work and observations in daily standup meetings.

Foster Cross-Functional Collaboration

Some high-performing teams meet and collaborate daily with other internal business units such as Human Resources, Governance and Compliance, Information Technology (IT), Software Development, Physical Security, and Business Development and Marketing. Formal and informal relationships give the cyber intelligence team a holistic understanding of the organization's environment and future business direction, such as the release of patented technologies, the roll-out of software, and significant mergers or acquisitions. With an understanding of developments in these areas as well as business unit needs and requirements, the cyber intelligence team can provide relevant cyber intelligence reporting these teams and to managers and executives to aid in decision making

3 NIST IR 8179 Criticality Analysis Process Model: Helping Organizations Decide Which Assets Need to Be Secured First, NIST Special Publication 1800-5 IT Asset Management, and NIST SP. 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and organizations

CREATING A FUSION CENTER

Creating a Fusion Center takes time, dedication, and resources, and there are many ways to create a Fusion Center. The implementation and organizational structure of the Fusion Center should be specific to the organization. In the following pages, we provide some examples of how organizations of various sizes and stages of maturity may structure a fusion center. These examples are based on information from our interviews as well as NIST-NICE Standard Practice 800-181[4]

Physical or Virtual?
Organizations we interviewed described advantages of physical and virtual fusion centers. Physical fusion centers have the obvious advantage of allowing individuals across teams to literally turn their chairs and talk with their coworkers to develop meaningful relationships based on working together in the same space and cultural environment.

High-performing organizations described two key advantages to virtual fusion centers: attracting and retaining talent, and forcing collaboration. In a job market where it is difficult to hire and keep skilled cyber intelligence team members, a virtual fusion center can both expand options for attracting talent and provide flexibility to aid in retention. When employees can work from anywhere, an organization can hire from everywhere. Team members can live where cost of living is lower and can easily relocate based on family needs or interests. In addition, the very nature of virtual fusion centers makes collaboration a given. Virtual fusion centers support proactive communication with a variety of tools (e.g., Slack, Skype, a shared TIP), and team members hold daily and weekly stand-ups.

4 (https://doi.org/10.6028/NIST.SP.800-181) and *Structuring the Chief Information Security Officer Organization* (https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf).

BEGINNING

Security Operations

- **Hunt**
- **Vulnerability**
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- **Host and Network Security Monitoring**
- **Incident Response**
  - *Cyber Defense Incident Responder: PR-CIR-1*

Security Engineering and Asset Security

- **Host and Network Security**
- **Malware and Forensics Analysis**
- **Physical Access Control**
- **Information Asset Security**
- **Identity and Access Management**
- **Applications Security**
- **Security Engineering**

DEVELOPING

Security Operations

- **Hunt**
- **Vulnerability**
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- **Host and Network Security Monitoring**
- **Incident Response**
  - *Cyber Defense Incident Responder: PR-CIR-1*

Security Engineering & Asset Security

- **Host and Network Security**
- **Malware and Forensics Analysis**
- **Physical Access Control**
- **Information Asset Security**
- **Identity and Access Management**
- **Applications Security**
- **Security Engineering**

Cyber Intelligence

- **Operational and Tactical**
  - *Threat/Warning Analysts: AN-TWA-001*
  - *Cyber Defense Forensics Analyst: IN-FOR-001*
  - *Cyber Defense Analysts: PR-CDA-001*

Insider Threat

Physical Security

Program Management

- **Program Management Office**
  - *Mission Assessment Specialist: AN-ASA-002*
- **Governance, Risk and Compliance**
  - *Cyber Legal Advisor: OV-LGA-001*
  - *Privacy Officer / Compliance Manager: OV-LGA-002*
- **Internal and External Relationships**
  - *Partner Integration Planner: CO-OPL-003*
- **Business Development and Marketing**

MATURE

Security Operations

- **Hunt**
- **Vulnerability**
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- **Host and Network Security Monitoring**
- **Incident Response**
  - *Cyber Defense Incident Responder: PR-CIR-1*

Security Engineering & Asset Security

- **Host and Network Security**
- **Malware and Forensics Analysis**
- **Physical Access Control**
- **Information Asset Security**
- **Identity and Access Management**
- **Applications Security**
- **Security Engineering**

Program Management

- **Program Management Office**
  - *Mission Assessment Specialist: AN-ASA-002*
- **Governance, Risk and Compliance**
  - *Cyber Legal Advisor: OV-LGA-001*
  - *Privacy Officer / Compliance Manager: OV-LGA-002*
- **Internal and External Relationships**
  - *Partner Integration Planner: CO-OPL-003*
- **Business Development and Marketing**

Cyber Intelligence

- **Threat Analysis**
  - *Threat/Warning Analyst: AN-TWA-001*
  - *Cyber Defense Forensics Analyst: IN-FOR-001*
  - *Cyber Defense Analyst: PR-CDA-001*
- **Collection Management**
  - *Cyber Intelligence Planner: CO-OPL-001*
  - *All Source Collection Manager: CO-CLO-001*
  - *All Source Collection Requirements Manager: CO-CLO-002*
- **Strategic Analysis**
  - *All Source Analyst: AN-ASA-001*
  - *Strategic Analyst*
  - *Geopolitical Analyst*
  - *Intelligence Analyst*
  - *Data Analysts: OTM-DTA-002*

Insider Threat

Physical Security

Technology Development & Integration

- **Data Science and Machine Learning**
  - *Data Analysts: OTM-DTA-002*
  - *Machine Learning Engineer*
- **Software Application and Development**
  - *Research and Development Specialist: SP-TRD-001*
  - *Software Developer: SP-DEV-001*
- **Knowledge Management**
  - *Knowledge Manager: DM-KMG-001*

Key

Groups

Team

Positions

Consider hiring a dedicated physical security analyst

Study participants told us that physical intelligence is the highest-volume, lowest-yield intelligence available, with countless Internet user comments that could constitute threats to physical assets. The alerting makes an enormous amount of work for analysts, and the subjective nature of potential physical threats makes automated detection difficult. That said, organizations are increasingly concerned about physical threats to their organization and are dedicating resources to provide intelligence about them.

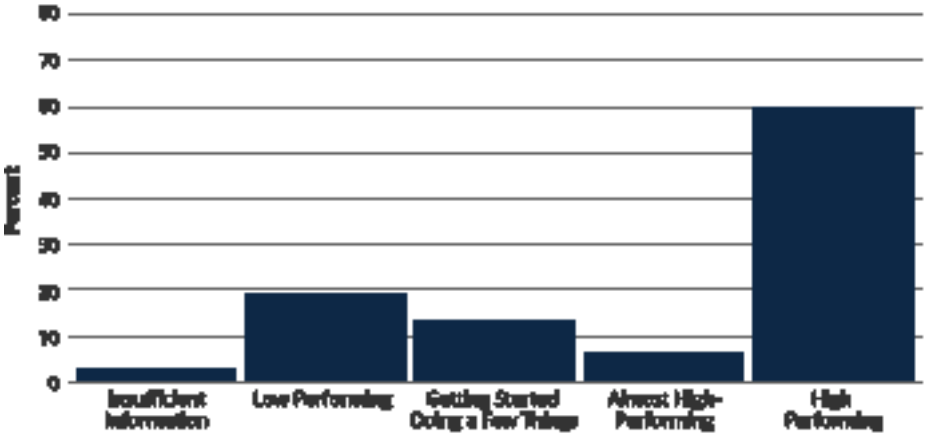
A practice of high-performing organizations is to have a dedicated physical security analyst, sometimes within their fusion center, to provide intelligence on physical threats that could cause harm to the organization's people, operations, and brand. The analyst provides intelligence on threats to the organization's physical locations and partner locations across the globe. Threats can range from malicious cyber actors looking to inflict physical harm, internal foreign country developments (geopolitics), and natural disasters impacting business operations.

ENVIRONMENTAL CONTEXT FACTOR 2: UNDERSTANDING THE DIFFERENCE BETWEEN CYBER INTELLIGENCE AND CYBER SECURITY

WHAT THIS ASSESSMENT FACTOR MEANS

The organization establishes and maintains cyber intelligence and cybersecurity as two work functions distinguished in their mission, purpose, roles, and responsibilities. Entities performing these two work functions interact and collaborate proactively to run the organization's cyber efforts.

PERFORMANCE SNAPSHOT



Environmental Factor 2 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Misunderstanding Cyber Intelligence

While some organizations might receive third-party intelligence daily feed(s); resources constraints enable them to improve their organizations security only through cyber hygiene actions. Failing to create a distinct cyber intelligence team puts your organization at increased risk for harm because you are constantly in a reactive position.

Lack of Communication between Cybersecurity and Cyber Intelligence Teams

Some cyber intelligence teams explained that communication and collaboration with the organization's other cybersecurity functions is inefficient. In the absence of fusion centers or other collaboration mechanisms, communication may be one-way only or may occur through email and chat, hampering collaboration and cyber intelligence performance.

Fusion Centers that Lack Cyber Intelligence Functions

In some organizations, fusion centers resemble operations centers, which consist of cybersecurity teams (vulnerability, incident response, and hunt teams) that typically reside in a security operations center (SOC). These fusion centers do not include cyber intelligence or other teams (physical security, knowledge management, insider threat, technology development teams) as part of the fusion center.

BEST PRACTICES—GETTING TO HIGH-PERFORMANCE

Create a Defined Cyber Intelligence Team

High-performing organizations build cyber intelligence teams that have their own mission, purposes, roles and responsibilities - clearly known and documented within the team and throughout the organization. Mission, purpose, roles and responsibilities are matured and approved by CISO and the board. They are evaluated bi-annually to ensure the team's support to the organization is consistent, meaningful and lasting.

IMPROVE YOUR PERFORMANCE

- Get CISO and Board support to create a cyber intelligence team that has a clear mission. Define and document roles and responsibilities that are approved and understood by the entire organization.
- Build relationships with leadership to help promote your team across the organization.
- Build relationships with business unit leaders to get buy-in on the need for a Fusion Center.
- Exchange ideas with colleagues in cybersecurity, IT, intelligence, technology development, software development, and physical security.

TERM CLARITY

Fusion Center

- Multiple teams of different disciplines
- Located in one physical/virtual location
- Proactively collaborating
- Advances organization-wide decision making for:
  - cybersecurity operations
  - preventive and anticipatory actions based on Threat analysis
  - organizational vital interests based on Strategic analysis
- Engages entire organization and external partners

Operations Center

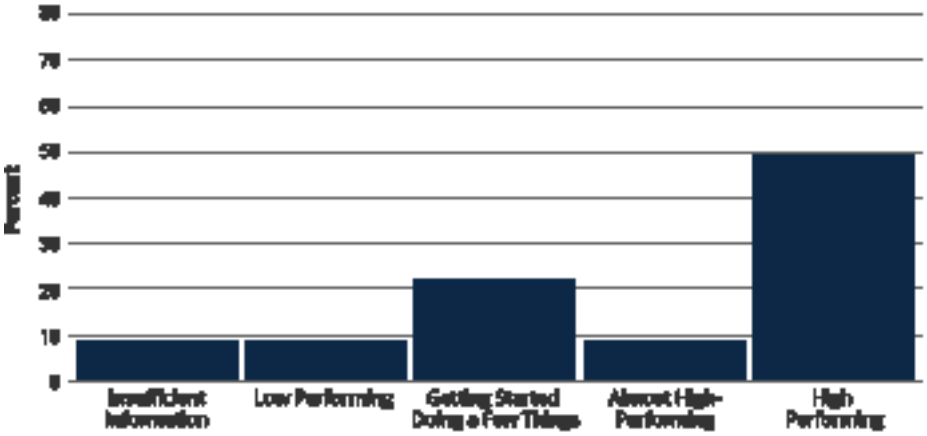
- Multi-disciplined staff
- One or more teams in one physical/virtual locations
- Focused on cybersecurity operations and threat analysis (for example, detecting and responding to incidents, maintaining the current status of operations, and tactical and operational intelligence of possible threats)
- Often a component within a Fusion Center

ENVIRONMENTAL CONTEXT FACTOR 3: ALIGNING CYBER INTELLIGENCE ROLES WITH YOUR ORGANIZATION'S NEEDS

WHAT THIS ASSESSMENT FACTOR MEANS

The organization distinguishes between cybersecurity and cyber intelligence analysts. The organization clearly defines responsibilities for these individuals that support organizational needs in cyber security, cyber intelligence and business mission needs.

PERFORMANCE SNAPSHOT



Environmental Factor 3 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Unclear Roles and Responsibilities

Some organizations lack clearly defined and documented roles and responsibilities for their cybersecurity and cyber intelligence teams. These organizations, (mostly smaller organizations) explained that while roles and responsibilities are conceptually understood, formal documentation and clarity regarding how roles and responsibilities align to support the overall organization mission were unclear or not established. The SEI team also met with organizations that, due to resource constraints, have roles and responsibilities strictly dedicated to cybersecurity efforts. These organizations usually have teams that consist of network monitoring analysts, vulnerability analysts, incident response analysts, hunt analysts, and forensic analysts.

GETTING TO HIGH-PERFORMING

Cross-Functional Teams

High-performing organizations distinguish between and have a mix of cybersecurity and cyber intelligence analysts. These organizations clearly document and articulate each team member's role and responsibilities (defined by skill-set, domain, or even product line) and map them to organizational needs. Team roles and responsibilities are visible and understood across the organization. Visibility streamline processes and helps break down silos.

Regular Evaluation

High-performing cyber intelligence teams regularly evaluate (at least every six months) that they have the right personnel performing the right roles to support the organization.

IMPROVE YOUR PERFORMANCE

- Document team roles and responsibilities and map them to organizational needs.
- Ensure your Cyber Intelligence Team has both strategic analysts--those who are well versed in intelligence, analytical tradecraft, emerging technologies, and geopolitics-- and threat analysts--those who are well versed technical analysis.
- Ensure your Cyber Intelligence team has access to data scientists and machine learning experts.

Balancing technical skills and responsibilities with analytical expertise
Cyber intelligence teams should strike the right balance of having technical staff working alongside those who possess strong intelligence and geopolitical analysis and experience. Consider two types of analysts:

Threat analysts are highly technical; they use technical telemetry (internal/external atomic, behavioral and computed indicators and artifacts[5]) to provide tactical and operational intelligence about threats to the organization or industry to advance cybersecurity operations, and inform Strategic analysis. Roles, responsibilities and skills typically associated with Threat analysts are similar to those in NIST SP 800 181 for Cyber Defense Analysts or Threat Warning Analysts – position titles are sometimes used interchangeably.

Strategic analysts provide holistic intelligence assessments. These analysts produce intelligence rooted in threat analysis considered alongside other information (all-source intelligence) and analytical tradecraft (structured analytical techniques, data science, human-centered design activities). Example assessments relate to strategic threats, threat actors, risks, and opportunities and provide information for decision makers regarding the organization's vital interests. Roles, responsibilities and skills typically associated with Strategic Analysts are similar to all-source intelligence analysts, intelligence analysts, threat actor analysts, risk analysts, or country and geopolitical analysts - position titles are sometimes used interchangeably.

Use of Data Science and Machine Learning
High-performing cyber intelligence teams have access to data scientists and machine learning experts and engineers, as members of their team or as resources they can call on from other parts of the organization. These experts help the team make sense of their data and automate processes and analysis.

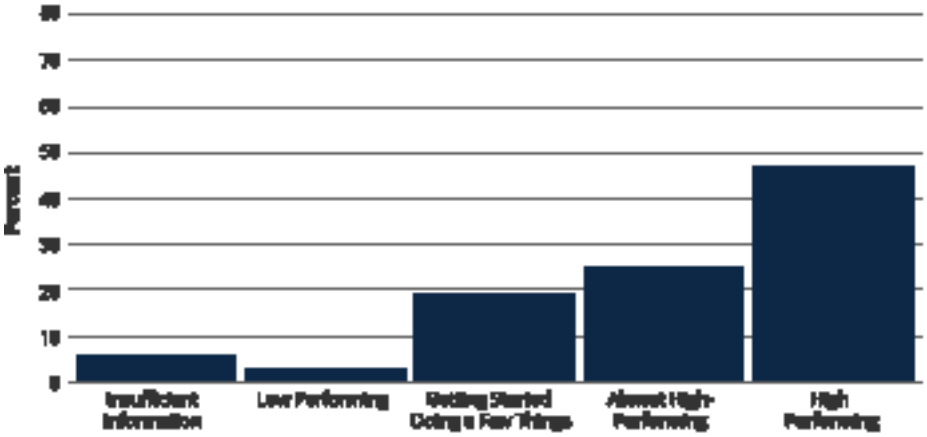
ENVIRONMENTAL CONTEXT FACTOR 4: HAVING ENOUGH PEOPLE, HAVING THE RIGHT PEOPLE

WHAT ASSESSMENT FACTOR MEANS

The organization has the personnel to support its cyber intelligence needs. The cyber intelligence team has sufficient staff to surge and free time to perform self-initiated research. The organization consistently evaluates personnel needs against cyber intelligence needs to ensure that its cyber intelligence team members have expertise to meet those needs.

5 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

PERFORMANCE SNAPSHOT



Environmental Factor 4 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

We need more people!

Well established and nascent cyber intelligence efforts share the challenge of personnel. Some organizations have a one-person cyber intelligence effort, and others are merely staying afloat in complete reactive mode. Without adequate personnel, teams lack the time and resources to do long-term holistic assessments or self-initiated research, and may not be able to surge to support cybersecurity efforts.

In many organizations that struggle with a lack of personnel, budget is a factor. Other organizations report that leadership does not recognize cyber intelligence as a worthy investment or does not understand the difference between cybersecurity and cyber intelligence.

Difficulties Recruiting and Retaining Cyber Intelligence Professionals

Organizations find it difficult to pay enough money to attract the right talent and increase salaries annually at a competitive rate to retain talent. Organizations in the finance sector especially noted the acquisition and retention of talent as a recurring challenge. This difficulty seems to arise in the financial sector because of intense competition among organizations that have robust cyber intelligence programs and can continually outbid one another for talent.

IMPROVE YOUR PERFORMANCE

- Consider NIST SP 800-181 as a resource for building your cyber intelligence team
- Give your analysts the freedom to explore and perform self-initiated research

GETTING TO HIGH-PERFORMING

Leaders Invest in Cyber Intelligence

Organizations with a budget to hire cyber intelligence talent tend to be organizations where leadership values the importance of cyber intelligence.

A Variety of Approaches and Resources for Staffing and Surging

High-performing organizations dedicate resources to surging for both cybersecurity and cyber intelligence efforts using in-house teams and third-party retainers. Some organizations cross-train between teams to provide an internal surge capability. One high-performing organization described training a floating surge force of generalists that can pick up slack anytime anywhere. Another organization is adopting a plan that uses interns to augment their cyber intelligence staff. These interns have cyber intelligence, cybersecurity, and intelligence analysis experience and education. Last, a common practice of high-performing cyber intelligence teams is to have veteran cybersecurity and intelligence analysts train less experienced analysts

The Right Personnel

In our 2013 report, we noted that high-performing organizations were pairing traditional intelligence analysts with cybersecurity and other technical analysts to ensure analytical tradecraft and strategic analysis was formulated into the cyber intelligence team's workflow. This approach is still a best practice. Many organizations are now hiring data scientists and machine learning experts as part of a Technology Development and Integration Team. These individuals work with the cyber intelligence team as team members or collaborators; they help derive meaning out of large data lakes and build in-house customizable tools to assist analysts with pattern and prediction analysis.

Mapping Position Requirements to NIST/NICE Cybersecurity Workforce Framework

A practice of high-performing organizations is to map position requirements to NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework[6] categories, an approach we recommended in the 2013 CITP Workforce Development and Management Implementation Guide. Positions and roles highlighted in NIST SP 800-181 are designed to strengthen the cybersecurity posture of an organization.

BUILDING A HIGH-PERFORMING TEAM

Although each organization should tailor a mapping to NIST/NICE to its own needs, the following positions are commonly represented on high-performing teams.

Cyber Intelligence Team

- All Source-Collection Requirements Manager
- All Source-Collection Manager
- All Source Analyst
- Cyber Intelligence Planner
- Multi-Disciplined Language Analyst
- Threat/Warning Analyst
- Threat Analyst
- Strategic Analyst
- Cyber Defense Forensics Analyst

Cybersecurity Team

- Cyber Defense Incident Responder
- Cyber Defense Analyst

Technology Development and Integration Team

- Data Analysts
- Machine Learning Engineer
- Software Developer
- Research and Development Specialist
- Knowledge Manager

Program Management

- Mission Assessment Specialist
- Partner Integration Planner

Create a Culture of Innovation

Organizations that encourage exploration and innovation tend to have high-performing cyber intelligence teams. Proactive self-initiated research, with top-down encouragement and approval, leads cyber intelligence team members to identify new threat actors targeting the organization and to develop new tools and solutions for addressing complex problems. One high-performing cyber intelligence team allows each analyst two research weeks each year to work on a project of their choice. Another high-performing cyber intelligence team requires self-initiated research every day as a scheduled activity.

6 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf

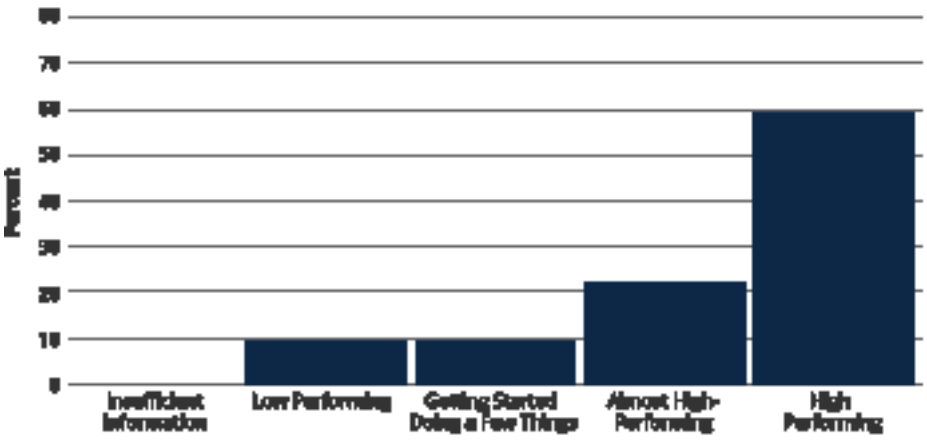
A culture of innovation not only leads to useful tools and solutions, but also gives cyber intelligence team members the chance to be proactive and the freedom to showcase their creative skills and ideas. In this way, retaining great people becomes less of a challenge.

ENVIRONMENTAL CONTEXT FACTOR 5: PLACEMENT OF YOUR CYBER INTEL EFFORT IN YOUR ORGANIZATION

WHAT THIS ASSESSMENT FACTOR MEANS

The cyber intelligence team has consistent access to teams and decision makers throughout the organization as well as associated data.

PERFORMANCE SNAPSHOT



Environmental Factor 5 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Aligning Cyber Intelligence too Closely with Cybersecurity

In 2013, we found that the cyber intelligence team's organizational location affected its focus and performance; this finding holds true for organizations today. Cyber intelligence teams should be closely aligned with functions where they can influence strategic decision making (for example, risk management). However, organizations often align cyber intelligence with security operations and network management, relegating their analysts to reactive, technical tasks supporting cybersecurity.

Organizations that struggle in this area commonly take a "cybersecurity plus" approach to cyber intelligence: they may add a cyber intelligence analyst or a budding intelligence effort within or below a cybersecurity team. As a result, the cyber intelligence analyst may end up reporting to a SOC team lead or other manager focused on cybersecurity, which may limit the analyst to a reactive approach.

Unnecessary Bureaucracy

Organizations we interviewed reported widespread difficulties with layers of management that prevent them from getting intelligence to the right people in a reasonable timeframe, and from getting approvals for new tools or research ideas. For example, one organization reported that their cyber intelligence team analysts report to the team manager, who reports to the Lead for Physical Security, who then reports

to the Chief Information Security Officer (CISO). The CISO for this organization often tasks the cyber intelligence team directly to circumvent the bureaucracy and get quick answers.

GETTING TO HIGH-PERFORMING

Elevate the CISO Position

A common organizational structure is for the cyber intelligence team to report to the CSO or CISO,[7] who then reports to the Chief Information Officer (CIO), who then reports to the Chief Executive Officer (CEO) who sits on the Board of Directors. This structure can perpetuate challenges related to locating cyber intelligence too closely to IT or cybersecurity efforts. High-performing organizations elevate their CISOs, giving them the ability to report directly and frequently to the CEO and board of directors. A growing body of research and reporting describes the advantages of this approach.[8]

Different organizations elevate their CISOs in different ways. For some high-performing organizations, the cyber intelligence team lead (Chief of Cyber Intelligence) has direct, easy, and ongoing formal and informal access to the CSO/CISO. The CSO/CISO has this same level of direct and easy access to the CEO. In other high-performing organizations, the CSO/CISO also sits on the Board of Directors. In this structure, leadership is very much engaged, and the cyber intelligence team can provide intelligence in a timely and efficient manner to advance organization-wide business decisions.

Augment Your Fusion Center with an Enterprising Capability

Fusion centers, described in Environment Factor 1: Knowing Your Attack Surface, help information flow to the right people at the right time; they increase information sharing efficiency, speed the leadership approval process, and ensure everyone is collaborating and on the same page. Some high-performing organizations with fusion centers also embed cyber intelligence analysts in organizational lines of business like HR, Legal, Business Development, Public Relations, Finance, and Contracts. These individuals sit with the business units and explain cyber threats to the organization, take specific requests for information, and provide tailored cyber intelligence products to the business unit.

---

7 Although the CSO and CISO are distinct positions with distinct roles, many organizations use the terms interchangeably in practice. Broadly speaking, the CSO/CISO is responsible for strategically managing and providing risk guidance associated with physical, people, and asset security as well as cybersecurity.

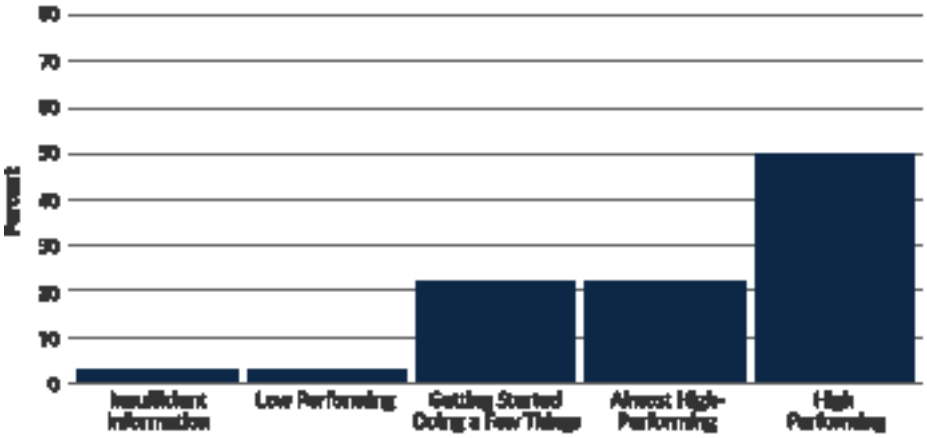
8 https://www.isc2.org/-/media/FAA17021673C4D0387CE9EFD45009EBC.ashx
https://www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos
https://er.educause.edu/articles/2018/6/its-time-to-set-cisos-free
https://www.linkedin.com/pulse/cio-report-ciso-why-j-j-guy
http://www.bankinfosecurity.com/blogs/role-reversal-cio-reports-to-ciso-p-1648
https://www.cio.com/article/3247251/cio-role/goals-for-cios-in-2018.html
https://www.forbes.com/sites/forbestechcouncil/2018/01/09/the-evolving-role-of-the-cio-in-2018/#48b459a21c8e

ENVIRONMENTAL CONTEXT FACTOR 6: CYBER INTELLIGENCE WORKFLOW

THIS ASSESSMENT FACTOR MEANS

The organization has an established and repeatable process that accounts for environment, data gathering, threat analysis, strategic analysis, and reporting and feedback components. This process is reviewed and updated regularly.

PERFORMANCE SNAPSHOT



Environmental Factor 6 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Conceptual or Incomplete Cyber Intelligence Workflows
Many organizations lack a formalized, documented, and repeatable cyber intelligence workflow. Some of these organizations explained that their workflow is largely conceptual and exists in the minds of team members.

A related challenge is incomplete cyber intelligence workflows that most commonly omit strategic analysis. Teams in organizations with incomplete workflows often conduct strategic analysis only if time is permitted, or if the organization has a distinct separate team of analysts capable of performing that level of analysis. Other organizations have separate workflows for each specific team (incident response team, SOC team, vulnerability management team, forensics team), and these distinct workflows do not join into a single comprehensive cyber intelligence workflow. Still other organizations had reactive workflows that were documented and formalized, yet only for cybersecurity and incident response.

IMPROVE YOUR PERFORMANCE

- Incorporate the Cyber Intelligence Framework as a guide to perform cyber intelligence
- Define and document your workflow to ensure that it is repeatable

GETTING TO HIGH-PERFORMING

Use the Cyber Intelligence Framework to perform Cyber Intelligence
High-performing organizations account for all Cyber Intelligence Framework components in workflows that are written down, easy to find, and clearly show how each team contributes. The following list shows practices described by high-performing organizations at every step of the Cyber Intelligence Framework.

BEST PRACTICES FOR WORKFLOWS THROUGHOUT THE CYBER INTELLIGENCE FRAMEWORK

Environmental Context—Planning and Direction

- Understand current organizational exposure to the threat because of vulnerabilities (Risk): People + Cyber Footprint + Physical + Technology
- Conduct crown jewel exercise for critical asset and sensitive technology identification
- Understand organization's entire internal and external networking infrastructure—to include associations with partners and suppliers
- Understand organization's mission, its industry and role within industry
- Understand Leadership Manifested Concerns to generate Strategic Intelligence Requirements
- Identify Gaps and Requirements: Intelligence Requirements, Priority Intelligence Requirements, and Specific Intelligence Requirements and aligned them to each other
- Cyber Intelligence Team creates and manages Requests for Information (RFI) process
- Cyber Intelligence Team **owns** the intelligence requirement process for the **entire** organization

Data Gathering—Collection, Processing and Exploitation

- Threat Analysis: Collect technical telemetry from internal sources (SIEM, EDR, NIDs, NIPs, HIDs, DLPs, SOAR, packet captures, vulnerability scans, all logs) and external telemetry sources via paid third party intelligence providers, open source information and intelligence sources - (HUMINT, SIGINT, MASINT, GEOINT, OSINT, IMINT) to answer SIRs, PIRs, and INs.
- Strategic Analysis: Incorporate Threat Analysis and collect other non-technical information to include: (Geopolitics, Business Intelligence, Human Resources Data, Research and Development Data, Physical Security data and Social Media as examples)
- Data normalization construct / framework built – create a record in a database for each source that includes, but is not limited to fields such as UID – Unique Data Record (line) identifier, or article reference number and TYPE – Common object category (i.e. Malware, Actor) See more on data normalization best practices on page XX in the Data Gathering and Management Section.

Threat analysis—Analysis and Production

- High-performing organizations have threat analysis workflows (or playbooks) to support time-sensitive and action oriented decisions for network and host monitoring, vulnerability management and incident response.
- Workflows are defined, documented, repeatable, and scalable
- IOC's (atomic, behavioral, and computed) are automatically correlated and matched against internal network and endpoint telemetry activity; automated data enrichment through integrated internal platforms and external integrations
- Machine or analyst alerts senior analyst or another machine for decision on elevating – Yes decision leads to triggering an automated workflow within SIEM/TIP playbook integrations or SOAR solution, JIRA
- Lead Analyst(s) assigned adds context (additional current and historical data) creating cyber tactical intelligence to answer what/where/when/how questions regarding threats, attacks, incidents, vulnerabilities, or other unusual network activity for the purpose of generating human and machine mitigating actions.
- Pending event and time constraints, Fusion Center analysts perform cyber operational intelligence adding context to existing tactical intelligence (threat actors, campaigns);start to answer the who and why behind threats
- Enhance mid-to senior level leadership decisions regarding non-immediate but near-term (weekly – quarterly) business process and operational decisions.

Cyber Strategic Intelligence Analysis

- Fuse threat analysis with other external and non-traditional data sources
- Depending on data collected, work with Data Science team to identify any larger trends or anomalies in data collected
- Provide analytical assessments based on threat actor potential, organizational exposure, and organizational impact of threat
- Analyze current and future technologies and geopolitics that may positively/negatively impact the organization and industry
- Perform structured analytical techniques as needed
- Enhance executive leader decision making pertaining to organizational wide financial health, brand, stature, and reputation

Reporting and Feedback—Dissemination and Integration, Reporting and Feeback/Evaluation

- Produce written and verbal reports and briefings (weekly, monthly, quarterly, semi-annually, annually) per leadership and organizational wide requests on topics (Push intelligence as needed to ensure leadership engagement. The cyber intelligence team should not

wait for intelligence to be demanded by leadership. Saying that leadership has not requested it, is not sufficient.) Explain threats to organization in **risk to business** based scenarios:
Ex: With an annual budget of X dollars, the cyber intelligence team over the next year, will protect the organization's critical infrastructure and technologies valued at X dollars. The cyber intelligence will aim to generate X dollars in revenue this year. Revenue generation will be accomplished by establishing new internal and external partner agreements, and informing leadership about threats, risks and opportunities pertaining to organizations vital interests.

- Evaluate workflow processes quarterly – what can be streamlined, what can be updated, what can be automated?
- Create quarterly metrics of intelligence products produced and activity disrupted
- Create informal and formal mechanism for feedback (web portal, email address to team, surveys)
- Create quarterly metrics of feedback received on intelligence products through portal – specific comments, likes, views, downloads of reports
- Identify new requirements based on feedback, analyst requirements and leadership concerns

Human

- Apply critical thinking, creativity and imagination to complex problems
- Understand the allure of "sexy" intelligence, cognitive biases, and logical fallacies
- Perform structured analytical techniques / human-centered design techniques
- Bring context to information (risk to business / industry, trends, threat actor TTP insights)
- Manage, advance, and evaluate relations with internal and external partners (third-party intelligence providers, subsidiaries
- Evaluate processes, policies and tradecraft to ensure feedback is incorporated to ensure effective and efficient intelligence analysis

Human/Machine

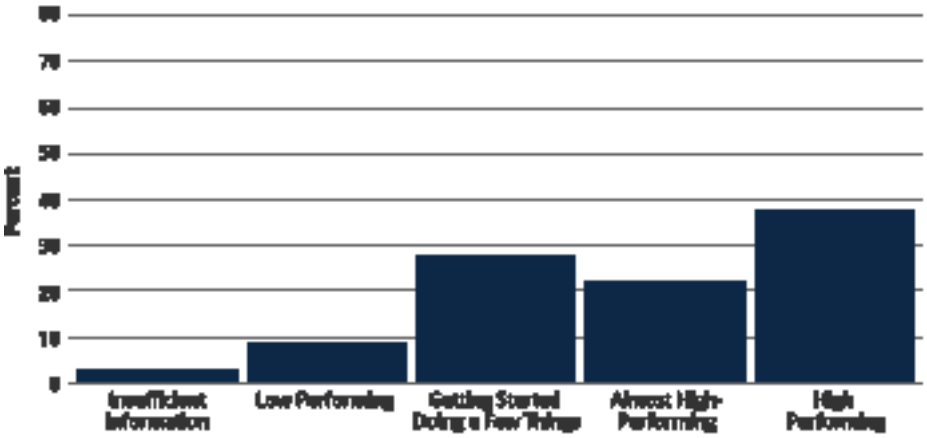
- Real-time status on cyber threats, organizational and international polices, new technologies, organizational developments, business offerings, new patents, new industry developments
- Detect anomalies
- Predict user behavior trends
- Real-time status on network architecture and attack surface
- Automation of manual tasks (parsing emails, attachments, URLs, file detonation, creating incidents, performing historical searches, notifying team members, and sending attachments or indicators through tools like Virus Total or WHOIS.
- Evaluate and score data and **data sources** on top of automation scoring process
- Generate concise tailored reports and presentations to specific audiences and leadership internal and external of organization

ENVIRONMENTAL CONTEXT FACTOR 7: PRIORITIZING THREATS

THIS ASSESSMENT FACTOR MEANS

The organization uses a repeatable threat prioritization process (such as a matrix or scoring system) that incorporates components of the cyber intelligence workflow to identify and prioritize cyber threats based on threat actor potential, target exposure, and organizational impact. This process is reviewed and updated regularly.

PERFORMANCE SNAPSHOT



Environmental Factor 7 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Threat Prioritization Is Ad-Hoc or Narrowly Focused

Teams in organizations across sectors often take an ad hoc approach to prioritizing threats, basing their judgments on current relevant news or gut feelings. In some organizations, executive leadership sets the organization's highest level Intelligence Requirements (sometimes going several years without updating them), and cyber intelligence analysts are left to identify organization gaps and establish appropriate Priority Intelligence Requirements (PIRs) and Specific Intelligence Requirements (SIRs) to collect against executive level Intelligence Requirements—with no established process for doing so.

Some organizations also struggle to create a holistic threat prioritization process, meaning that their process fails to consider threat actor potential to target the organization, organizational exposure to the threat, and the impact of the threat on the organization. Additionally, a number of organizations rely solely on paid Threat Intelligence Platforms to automate threat prioritizations, without conducting additional analysis and evaluation to determine if the automated prioritization is actually organizationally relevant. Some organizations do evaluate and review their own threat prioritization process, however such evaluations occur annually at best. When considering the dynamic and emerging threat landscape, along with rapid industry and technological developments, organizations should holistically evaluate their threat prioritization process and corresponding IRs and PIRs quarterly. SIRs should be evaluated every 60 days.

IMPROVE YOUR PERFORMANCE

- Use public threat frameworks to assist with answering intelligence requirements and for tactical and operational threat prioritization.
- Consider threat actor potential to target the organization, organizational exposure to the threat, and the impact of the threat on the organization to strategically prioritize threats.
- Evaluate strategic threat prioritizations on a quarterly basis

Threat prioritization requires organizations to understand their environment. This means having a holistic understanding of the attack surface in relation to cyber threats: physical and logical attack surface, critical assets, patent pending technologies, executive level Intelligence Requirements (IRs), industry developments, geopolitics and knowledge gaps. Using that information, organizations establish Priority Intelligence Requirements (PIRs) and then lower-level, technical Specific Intelligence Requirements (SIRs). The next step is to collect information to answer the IRs, PIRs, and SIRs. With the information collected as part of the Data Gathering component of the cyber intelligence analysis framework, organizations use human-machine teams to perform Threat analysis or Strategic analysis to create actionable intelligence for leadership. See Data Gathering Factor 1 for more information about the Intelligence Requirement Process.

GETTING TO HIGH-PERFORMING

Use Public Threat Frameworks
High-performing organizations use public cyber threat frameworks to support intelligence analysis and communicate threat prioritizations. Our Public Threat Framework Implementation Guide describes how to use these frameworks and incorporate them into your cyber intelligence effort. Specifically, some teams have their threat analysis, Threat/Warning, and Cyber Defense Analysts map technical internal and external telemetry (atomic, behavioral, and computed indicators) to the MITRE ATT$CK Framework to track changes in threat actor behavior (TTPs) over time. This process assists with answering tactical and technical SIRs and for informing threat prioritizations. When it comes to briefing and writing for senior leadership and the board of directors, some organizations switch to the Lockheed Martin Cyber Kill Chain to communicate attack stages. We also met with organizations that use the Diamond Model to conduct analysis when leadership is primarily interested in attribution.

Prioritize Threats based on Threat Actor Potential, Target Exposure, and Organizational Impact
High-performing organizations tend to consider a variety of factors when prioritizing threats. These considerations commonly fall into the three categories we described in our 2013 Cyber Threat Prioritization Implementation Guide:

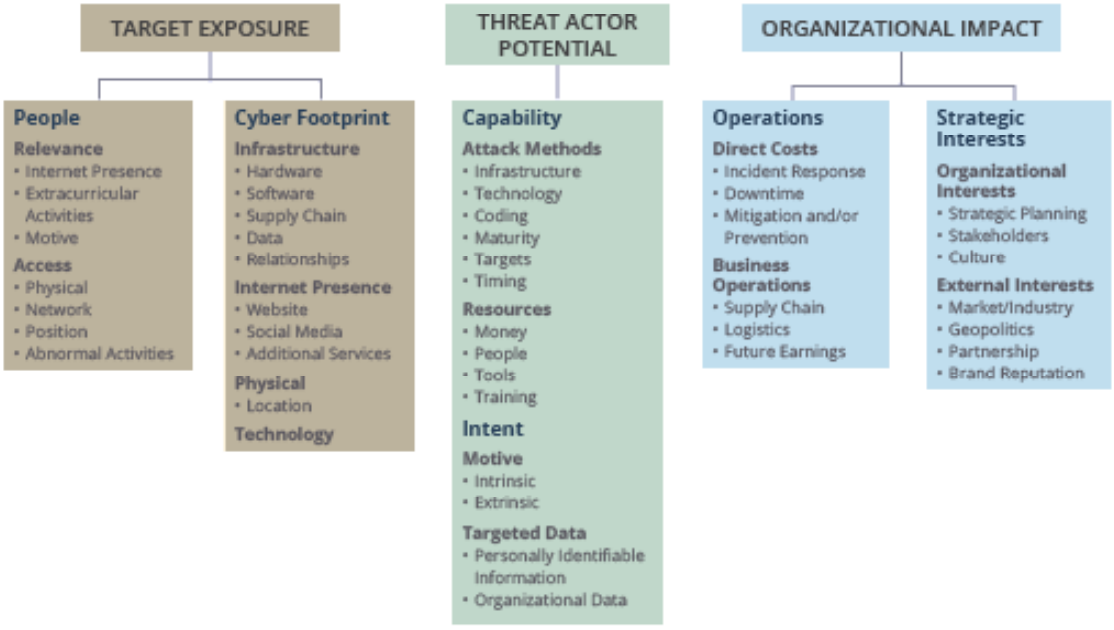
- Threat Actor Potential to Execute the Threat (Capability + Intent)
- Organizational Exposure to the Threat because of Potential Vulnerabilities (People + Cyber Footprint + Physical + Technology)
- Organizational Impact of the Threat (Operational Costs+ Strategic Interests Impact)

KEY TERMS AS DEFINED BY US DHS*

Likelihood: Chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities.
Intent: Determination to achieve an objective
Capability: Means to accomplish a mission, function or objective
Risk: Potential for an unwanted outcome as determined by its likelihood and the consequences -extended definition potential for an adverse outcome assessed as a function of hazard/threats, assets and their vulnerabilities, and consequences
Impact: Measure of effect or influence of an action, person, or thing on another – extended definition: may occur as either direct or indirect results of an action

* DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

PRIORITIZING THREATS FOR MANAGEMENT



Prioritizing Threats for Management High-performing organizations tend to consider a variety of factors when prioritizing threats. These considerations commonly fall into the three categories:

- Threat Actor Potential to Execute the Threat
- Organizational Exposure to the Threat because of Potential Vulnerabilities
- Organizational Impact of the Threat

Use a Tiered Model to Prioritize Threats

Since 2013, high-performing cyber intelligence teams have reported using tiered models to prioritize threats. These models can be homegrown or based on existing tools. Tiered models enable teams to be more agile, focusing on the most important threats; such models also provide a framework for communicating strategic threat prioritizations to leadership. The simple scenario and matrix below provide one example of an approach to tiering threats.

EXAMPLE SCENARIO: THREAT PRIORITIZATION

Threat Actor VenomSYN Using B00MAI Malware

Threat Prioritization Score: Medium

Bottom Line Up Front: A medium risk exists that VenomSYN will target our organization using B00MAI malware. Threat Actor Potential: VenomSYN sends spear-phishing emails wrapping B00MAI malware in a PDF document. VenomSYN targets organizations in Defense and Academic sectors, not organizations in our Health Sector. Target Exposure: VenomSYN may target our employees, however overall exposure to B00MAI malware is low due to our cyber hygiene policies, two-factor Identify and Access Management practices and algorithmic detection capability based on sandbox testing. Organizational Impact: Organizational impact of this threat is assessed as medium. Should VenomSYN breach our systems, containment would be almost immediate. That said, public awareness of the breach could harm our organization's reputation.

Likelihood (Threat Actor Potential)

	High Intent	Medium Intent	Low
High Capabilities	High Threat Actor Potential to execute threat (OIS)	High Threat Actor Potential to execute threat	Medium Threat Actor Potential to execute threat
Medium Capabilities	High Threat Actor Potential to execute threat	Medium Threat Actor Potential to execute threat (OI,OP, OO)	Low Threat Actor Potential to execute threat
Low Capabilities	Medium Threat Actor Potential to execute threat	Low Threat Actor Potential to execute threat	Low Threat Actor Potential to execute threat

Risk (Target Exposure to the threat because of potential vulnerabilities: People, Cyber, Physical, Technological (CPT)

	High CPT Vulnerabilities	Medium CPT Vulnerabilities	Low CPT Vulnerabilities
High People Vulnerabilities	High Target Exposure to the threat because of vulnerabilities (OIS)	High Target Exposure to the threat because of vulnerabilities	Medium Target Exposure to the threat because of vulnerabilities
Medium People Vulnerabilities	High Target Exposure to the threat because of vulnerabilities	Medium Target Exposure to the threat because of vulnerabilities (OI,OP)	Low Target Exposure to the threat because of vulnerabilities
Low People Vulnerabilities	Medium Target Exposure to the threat because of vulnerabilities	Low Target Exposure to the threat because of vulnerabilities	Low Target Exposure to the threat because of vulnerabilities (OO)

Impact (Organizational Impact of the cyber threat on the Target) = Operational Costs + Strategic Interest Impact

	High Strategic Interest Impact	Medium Strategic Interest Impact	Low Strategic Interest Impact
High Operational Costs	High Organizational Impact	High Organizational Impact (OIS)	Medium Organizational Impact
Medium Operational Costs	High Organizational Impact	Medium Organizational Impact (OI,OP)	Low Organizational Impact
Low Operational Costs	Medium Organizational Impact (OO)	Low Organizational Impact	Low Organizational Impact

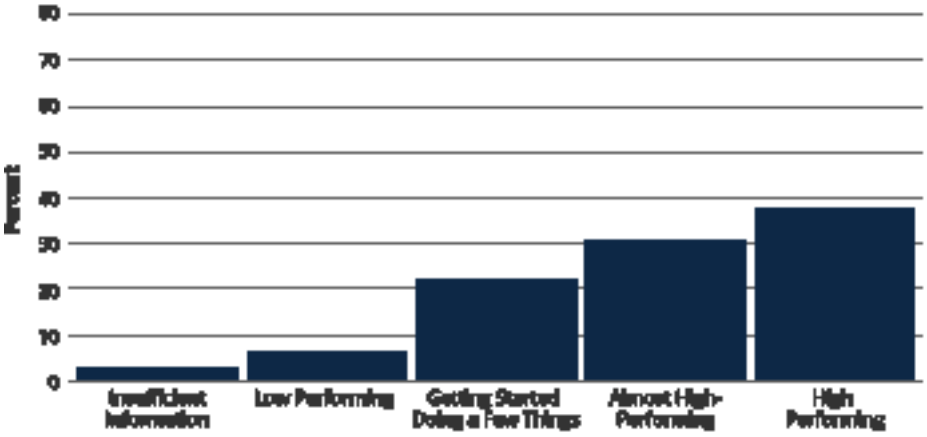
Scenario Matrix OI: Our Industry, OO: Our Organization, OP: Our Partners, OIS: Other Industry Sectors

ENVIRONMENTAL CONTEXT FACTOR 8: USING PAST, PRESENT, AND FUTURE DATA

THIS ASSESSMENT FACTOR MEANS

The organization consistently uses past, present, and future data regarding cyber threats to the organization itself, within its industry, and across industries. The organization reviews lessons learned from prior incidents as part of its cyber intelligence efforts. Data includes significant historical data, current data and both self-developed and vendor-based predictions on future threats.

PERFORMANCE SNAPSHOT



Environmental Factor 8 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

The Focus is only on Today

Although organizations widely acknowledge the importance of past data for informing present and future analysis, many struggle to effectively use past data. Besides the common challenge of resource constraints, organizations struggle with the lack of technology to query and manage past data. Some organizations use email to collect and manage all of their data. Other organizations described limitations with portal search functions and difficulties accessing logs. Even when organizations are able to manage and access old data, many lack a formal structure, method, or documented workflow to incorporate this data.

Organizations also struggle with looking toward the future. Many are not using past and present data, along with data about future threats, geopolitics, and technologies to predict future threats, risks or opportunities to the organization and industry. Resource constraints, along with lack of demand—likely due to the reactive approach we observed at many organizations—make predictive analysis difficult.

IMPROVE YOUR PERFORMANCE

Create capabilities and resources to leverage past data and intelligence on threat actors, IoCs and adversary behavioral trends to derive present and future adversary intent and capabilities.

GETTING TO HIGH-PERFORMING

Make use of tools and veteran team members

High-performing organizations use historical reporting on threat actors, IoCs, and adversary behavioral trends to derive present and future adversary intent and capabilities. A practice of high-performing organizations is using past data and trends to support link analysis, perform IoC reconstruction, inform leadership of current events, or show organizational defense capability improvement overtime. For past

data, some organizations leverage the cloud to query logs, incidents, and post mortems going as far back as ten years. Other organizations have built custom graph databases that enable quick and easy searches to help analysts understand past, present, and future data relationships.

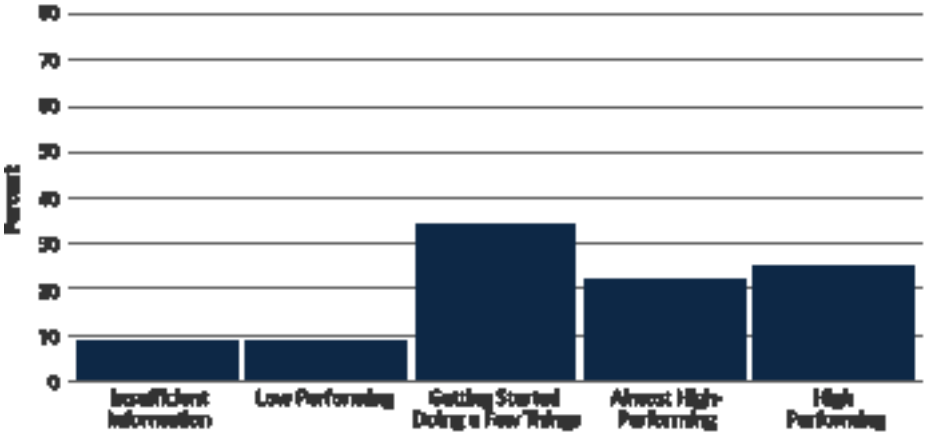
High-performing organizations that have longtime employees do a good job of drawing from those team members' knowledge of past threats and events and the organization itself. Although relying solely on knowledge contained in team members' minds is a bad practice, leveraging team member experiences and perspective along with the appropriate tools and processes can increase the effectiveness of your cyber intelligence effort.

ENVIRONMENTAL CONTEXT FACTOR 9: RELATIONSHIP BETWEEN CYBER INTELLIGENCE AND INSIDER THREAT DETECTION, PREVENTION, AND RESPONSE

THIS ASSESSMENT FACTOR MEANS

The organization's cyber intelligence effort has a relationship with its insider threat effort that supports mutual, proactive information sharing; the teams can access one another's databases and people when needed.

PERFORMANCE SNAPSHOT



Environmental Factor 9 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Absense of a True Insider Threat Effort

Some organizations we interviewed do not have dedicated Insider Threat Programs or teams. For some of these organizations, insider threat detection, prevention, and analysis fall to one person who has other full-time responsibilities within the information technology division or cybersecurity team. Some organizations rely exclusively on technical measures such as standard activity monitoring of databases, access management policies, and Data Loss Prevention (DLP) tools that make up their insider threat program. Other organizations have leadership who view insider threat only as a human error (for example, employees who fall victim to phishing emails); those organizations have not invested in tools like a DLP and instead simply provide training to employees. Still other organizations have not yet built an Insider Threat Team because they are still coming to consensus on what an insider threat actually

IMPROVE YOUR PERFORMANCE

- Create a formal insider threat function that uses a combination of policies, procedures, and technical controls across the organization to protect against malicious insiders.
- Create formal mechanisms to ensure bi-directional and proactive information sharing between the insider threat and cyber intelligence teams.

means to the organization or because they have not yet had a problem related to insider threat.

Lack of Information Sharing Between Insider Threat and Cyber Intelligence Teams
Information Sharing Lacking or Unidirectional
A prevailing challenge for organizations that have insider threat programs is the lack of information sharing between the Insider Threat Team and the Cyber Intelligence Team. Some organizations have no information sharing at all—no passing of indicators, intelligence reports, or shared databases. Some cyber intelligence teams only know if there is an insider threat issue at the organization if the insider threat team reaches out for additional information. Other organizations' cyber intelligence teams pass indicators and intelligence reports to the insider threat team without any reciprocity. Lack of information sharing is sometimes due to data sensitivity, law enforcement/company investigations, and privacy concerns; even so, information sharing should not be one-sided.

GETTING TO HIGH-PERFORMING

Use a DLP
When it comes to technical controls, most high-performing organizations use a DLP and conduct topical DLP analysis in combination with activity monitoring and other access control monitoring to support behavioral analytics.

Create an Insider Threat Efforrt
High-performing organizations have formal insider threat teams, resources, and authorities with policies, procedures and technical controls. High-performing organizations often locate the insider threat program under the CISO/CSO to ensure appropriate information sharing with all cyber and non-cyber teams (including Human Resources) across the organization. Although some organizations embed an insider threat analyst in their fusion center to advance collaboration and communication, most organizations house their insider threat team outside the fusion center.

Build Relationships between Insider Threat and Cyber Intelligence Teams
Cyber intelligence teams and insider threat teams in high-performing organizations recognize that working together is better for the overall protection of the organization's mission. The teams communicate not only through informal personal relationships, but in regular weekly calls and monthly formal meetings. Furthermore, these teams acknowledge that they are each consumers of the other's intelligence products. For example, the cyber intelligence team can send information to the Insider Threat Team: keywords about organizational critical assets and technologies, TTPs for threat actors, organizational references in third-party intelligence reporting, and algorithms to support DLP and behavioral analytics. The insider threat team uses this information to make DLP and other adjustments to its monitoring and training capabilities. In return, the insider threat team can share case results, feedback on keywords, and RFIs to the cyber intelligence team. For additional information about how to create high-performing Insider Threat Programs, refer to the SEI's Common Sense Guide to Mitigating Insider Threats, Fifth Edition.[9]

BEST PRACTICES

APPLYING MACHINE LEARNING TO ASPECTS OF THE INSIDER THREAT PROBLEM

A high-performing organization has created a neural network that learns on unstructured data from sensors surrounding the organization's web browsers and proxy sensors (including partners and affiliates). The organization has applied random forest decision trees to predict a probability that a user will head toward a website or category focused on weapons, criminal networks, and other nefarious sites

9 https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

“…information consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention.”

—Herbert A. Simon

Data Gathering

Collecting the Right Information

INTRODUCTION

When organizations know their environment, they can create the right intelligence requirements for data gathering. Data gathering is the process of using multiple sources (internal and external to the organization) to answer organizational intelligence requirements.

DATA GATHERING ASSESSMENT FACTORS

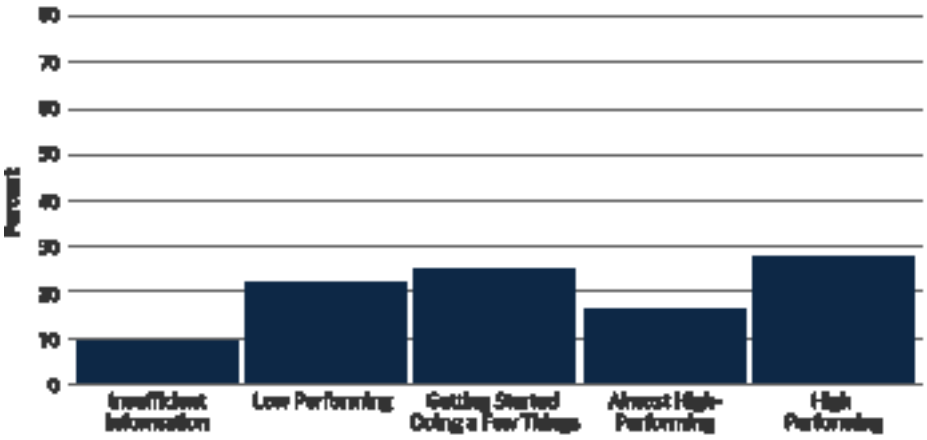
1. Intelligence Requirement Process
2. Organization Information Sharing Process
3. Intelligence Requirement and Data Source Alignment
4. Technology for Data Gathering
5. Data Source Validation

DATA GATHERING FACTOR 1: INTELLIGENCE REQUIREMENT PROCESS

THIS ASSESSMENT FACTOR MEANS

The organization collects data that addresses threat analysis and strategic analysis needs according to intelligence requirements. The organization has a process to ensure analytical needs are met.

PERFORMANCE SNAPSHOT



Data Gathering Factor 1 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of Organization-Wide Intelligence Requirement Process

Without an intelligence requirement process where all leadership, analyst, and business unit intelligence requirements are understood and approved, the collection management team may have trouble identifying gaps, overlaps, or duplication of efforts. Some organizations have no mechanism to create, track, and satisfy intelligence requirements. Other organizations are building their cyber intelligence programs and are just beginning to engage leadership and analysts for intelligence requirements. Some organizations have intelligence requirements that address only cybersecurity concerns such as compliance, patch, and vulnerability management issues. Still others have different intelligence requirement processes for different teams across the organization.

Stale Intelligence Requirements

Organizations struggle with outdated requirements that lead to irrelevant data collection or data collection with diminishing analytical returns. Some organizations have high-level intelligence requirements that were established years ago by senior leadership, some of whom are no longer at the organization.

Difficulties with Third-Party Intelligence Providers

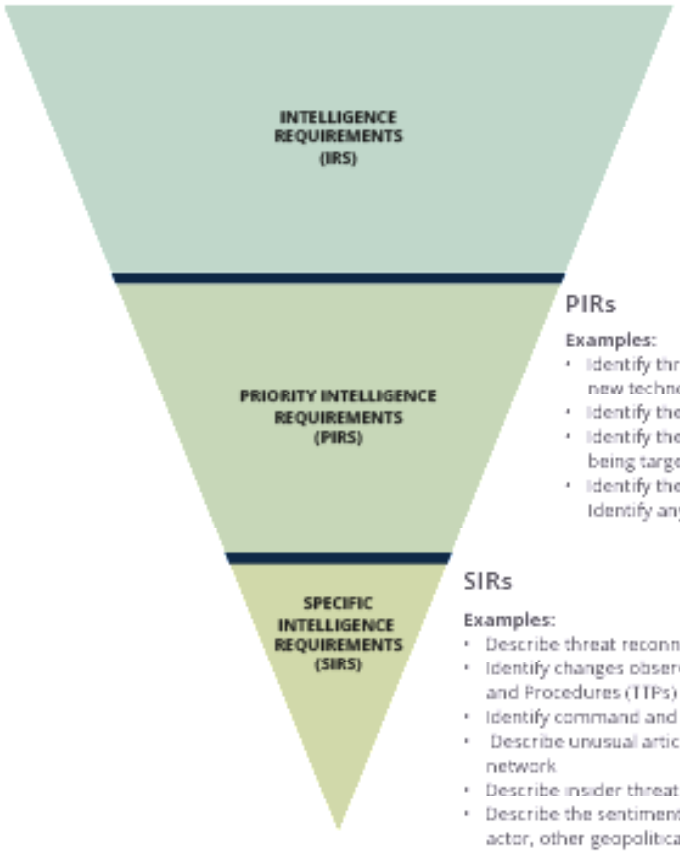
Organizations described a variety of challenges with third-party intelligence providers not meeting the organization's intelligence requirements. One organization explained that intelligence provider feeds do not contain raw data its cyber intelligence team needs for threat analysis. Some third-party intelligence providers produce only finished intelligence products and provide access to sales people, when organizations prefer raw data and access to vendor-specific analysts. Similarly, some third-party intelligence providers require an organization to buy an entire intelligence portfolio when they only need one small aspect of the intelligence provider's service. In a few cases, organizations admitted that they themselves had failed to alert vendors of intelligence requirement changes.

IMPROVE YOUR PERFORMANCE

- Create a collection management team to manage the intelligence requirements process.
- Use intelligence requirements, priority intelligence requirements and specific intelligence requirements.
- Tag organizational specific intelligence requirements to DHS Homeland Security (HSEC) Standing Information Needs (SIN) as appropriate.

INTELLIGENCE REQUIREMENTS

Cyber Intelligence teams consider intelligence requirements (IRs) alongside environmental context information about their attack surface, critical assets, patent pending technologies, business unit needs, industry developments, geopolitics, and knowledge gaps to develop priority intelligence requirements (PIRs) and then more granular and technical specific intelligence requirements (SIRs).



IRs

Examples:

- Identify notable threats to the organization
- Identify internal and external cyber threats targeting the organization
- Identify cyber threats targeting related industries
- Identify cyber threats to our partners

PIRs

Examples:

- Identify threat actors targeting our organization's critical assets or new technologies.
- Identify the threat actors' motives.
- Identify the person, group, entity or asset in the organization that is being targeted.
- Identify the impact of the threat (reputation, revenue, operations). Identify any mitigating controls in place.

SIRs

Examples:

- Describe threat reconnaissance activity that occurred today
- Identify changes observed in a specific threat actor Tactics, Techniques, and Procedures (TTPs) today
- Identify command and control infrastructure a specific threat actor is using
- Describe unusual articles, indicators, or behavior changes across our network
- Describe insider threat attempts observed today
- Describe the sentiment of a country government towards a specific threat actor, other geopolitical information regarding a specific threat actor.

IRs reflect senior leadership and board concerns about threats and risks to the organization's environment, mission, operations, revenue, bottom line, and reputation. They are general in nature and are approved at the highest level of the organization (CEO, President). IRs serve as a baseline and starting point for the organization's collection plan.

PIRs are more detailed and operationally focused and align to IRs. PIRs should be approved by the CEO, Vice President, and CSO/CISO, and should be updated at least every 6 months.

SIRs are operational, tactical, and technical in nature and focus on particular facts, entities, or activities. They also tend to be greater in number than IRs and PIRs and change more frequently based on both the dynamic nature of an organization's environment and the cyber threat landscape. SIRs are created by the cyber intelligence team in collaboration with others in the fusion center and should be approved at the CSO/CISO level. SIRs should be evaluated and audited at least every 60 days.

GETTING TO HIGH-PERFORMING

Create a Collection Management Team to Manage Intelligence Requirements
A practice of high-performing organizations is having a collection management team responsible for capturing, managing, and evaluating senior-executive-level intelligence requirements, priority intelligence requirements, and specific intelligence requirements. The collection management process has three core aspects: a requirement, the actual data gathering, and analysis of the data to answer the requirement. These responsibilities fall to the collection management team. In other words, the collection management team owns, manages, produces, and evaluates the cyber intelligence requirement process, as well as the data gathering and vetting processes. The collection management team establishes collection requirements to ensure the data collected comes from a variety of sources and is aligned to answer IRs, PIRs, SIRs and RFIs. The collection management team also ensures that data collected meets present needs and is aligned to support organizational strategic plans and vision. Last, the Collection Management team develops and tracks the rationale for each data source used and continuously looks for new data sources and technologies to help automate some of these processes.

Based on this best practice and drawing from *Intelligence Community Directive 204, National Intelligence Priorities Framework*,[10] the SEI recommends creating an organizational intelligence priorities framework (OIPF). The OIPF informs future planning, budgeting, programming, and allocation of resources to data collection and analysis. The OIPF should be actively managed so that it reflects organization-wide stakeholder priorities, and the entire OIPF should be reviewed quarterly. Organizations should consider imposing expiration dates on intelligence requirements to force reevaluation. To increase visibility, organizations should consider providing access to the OIPF to all departments that may be able to use it. The OIPF should also show how specific collection sources and their source validation status align to intelligence requirements. Advanced organizations could incorporate an OIPF into existing dashboard capabilities, permitting users to drill down through the IRs, PIRs, and SIRs.

INTELLIGENCE REQUIREMENTS VS. COLLECTION REQUIREMENTS

Intelligence Requirement: Request for information about threats, risks, and opportunities for the purpose of protecting and advancing the organization's mission. Answering Intelligence Requirements requires data collection, analysis and reporting and feedback.

Collection Requirement: Request for using specific types of internal and external data sources and/or variety of sources that provide data to help answer IRs, PIRs, and IRs.

10 Intelligence Community Directive 204. National Intelligence Priorities Framework. 2 January 2015 https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf

Track Customer Needs Using Standing Information Needs

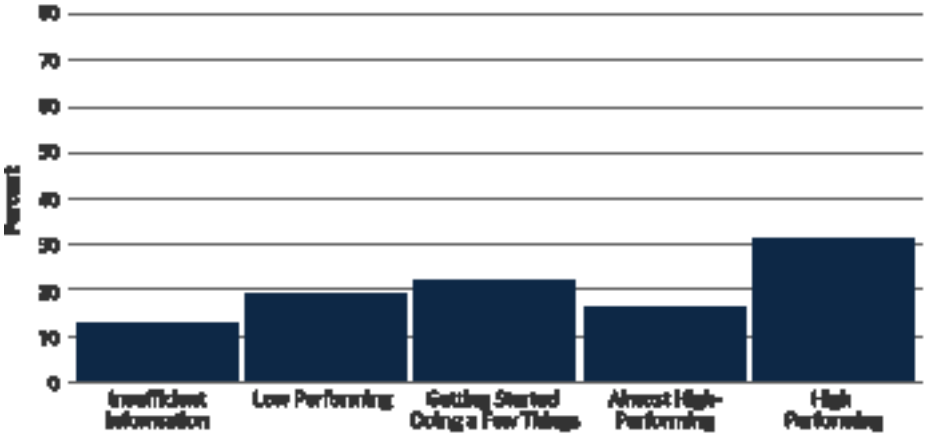
The Department of Homeland Security (DHS) uses Homeland Security (HSEC) Standing Information Needs (SIN) to identify and track customer needs across the department. DHS National Fusion centers also establish their own specific SINs to identify, track, and satisfy customer needs within their area of responsibility. National Fusion Centers and ISACs provide information and intelligence analysis in response to these needs.[11] Some high-performing organizations have practices that relate to standing information needs; specific steps include creating a standing information needs special interest group to determine customers' standing information needs and intelligence requirements and aligning and tag their own IRs, PIRs, and SIRs to HSEC SINs and Fusion Center and ISAC specific Intelligence Requirements. Aligning organizational requirements to national requirements helps guarantee operational relevance and enhances public and private information sharing and trust.

DATA GATHERING FACTOR 2: INTELLIGENCE REQUIREMENT AND DATA SOURCE ALIGNMENT

THIS ASSESSMENT FACTOR MEANS

The organization has a formal repeatable process for aligning data sources to meet intelligence requirements. This process is reviewed and updated regularly.

PERFORMANCE SNAPSHOT



Data Gathering Factor 2 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of people leads to lack of process

For some organizations, no formal, repeatable process exists to align data sources to intelligence requirements, often due to resource constraints. Most of these organizations do not have the people and time to align data sources to particular intelligence requirements and end up following an ad-hoc or trial-by-error process.

Fragmentation and Decentralization

Several organizations explained that no central holistic view exists of all sources used

IMPROVE YOUR PERFORMANCE

- Create a system or mechanism to align data sources to intelligence requirements.
- Use both internal and external data sources to support your cyber intelligence effort.
- Continuously evaluate third-party intelligence providers via scoring criteria.

11 https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/national-network-of-fusion-centers-2015.pdf https://www.hsdl.org/?view&did=817528

by every analyst across the organization; instead, each cyber intelligence analyst has their own set of data sources. One organization noted that its SOC has a collection of sources and procedures for aligning sources, while the cyber intelligence team has different sources and procedures. A lack of a central location for sources may result in duplicative efforts or may lead to a collection gap against an IR, PIR, or SIR. Organizations should have a location the entire Fusion Center can access showing the source, the source's validation, and what is being collected from that source to answer IRs, PIRs, and SIRs. Incorporating this location into any capabilities associated with an OIPF would be beneficial.

GETTING TO HIGH-PERFORMING

Map Data Sources to Intelligence Requirements
High-performing organizations map their data sources to their intelligence requirements. One high-performing organization is currently building an automated capability that aligns existing and new data sources to existing organizational IRs, PIRs, and SIRs.

Evaluate and communicate with intelligence vendors
High-performing organizations often use their collection management teams to manage the organization's relationship with its third-party intelligence providers. The collection management team communicates new requirements, explains the justification and priority behind them, and provides feedback to the third party. For some high-performing organizations, the collection management team collaborates with other members of the cyber intelligence team, (specifically the cyber intelligence analysts) to continuously evaluate third-party intelligence providers via scoring criteria like letter grades. Other high-performing organizations track the third party provider's performance using month-to-month graphs to show how intelligence provided by the vendor answered intelligence requirements and helped the organization; organizations send that feedback to the vendor to let them know how they are doing.

Differentiate between third-party intelligence aggregators and intelligence originators
In evaluating third-party intelligence providers, high-performing organizations identify whether the provider is an intelligence aggregator or an intelligence originator. An intelligence aggregator simply collects and passes intelligence to its customers, while an intelligence originator provides new context to the information, making it actionable and relevant to the customer.

Use a wide variety of Sources
High-performing organizations emphasized two key ideas regarding data source collection: "any data all the time" and "data finds data." High-performing organizations use a variety of internal and external data sources to support intelligence analysis.

First, internal data sources are typically generated messages (logs) or machine data from organizational hardware and software regarding device usage. There are many types of internal logs: traffic logs, operating system logs, firewall logs, IDS and HIDS logs, IoT logs, cloud logs, and vulnerability management logs, just to name a few. These internal data sources are typically ingested, viewed, and analyzed in a SIEM, DLP, Intrusion Detection / Intrusion Prevention (IDS/IPS), Endpoint Detection and Response (EDR) Platform, or Security Orchestration Automation and Response

(SOAR)—or a Third-Party Threat Intelligence Platform (TIP) that integrates many tools. Internal data sources, however, should not be limited to just machine data and logs. Internal data sources should include logs, tips, and other information from data sharing relationships, service level agreements, and collaboration with other internal business units such as Human Resources, Marketing/Sales, Research and Development, Finance, and Supply Chain Management.

External sources are both paid and free third-party intelligence providers or platforms that provide aggregated intelligence and/or additional originated context (actionable and organizationally relevant) about atomic, behavioral, and computed indicators of comprise and associated meta-data analysis (email addresses, IP Addresses, User Agent Strings, etc.) related to vulnerabilities, threat actor groups, threat actor TTPs, threat actor capabilities and motivations, and threat campaigns.

TIP

See Appendix ABC for a complete list of free and paid intelligence vendors and sources that organizations told us they are currently using.

External intelligence vendors may provide information from a collection of sensitive sources, which could include adversary communications in dark / deep / surface web forums, C2 servers, forensic analysis, Virus Total, Shodan, endpoint, and network security data that they have access to from their organizational customers. The Intelligence Community, defense and other government agencies, may also receive indicators and information about threat actors, capabilities and motivations via unclassified and classified sources and means such as Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Human Intelligence (HUMINT), Measurement and Signatures Intelligence (MASINT), Open Source Intelligence (OSINT), and Geospatial Intelligence (GEOINT).

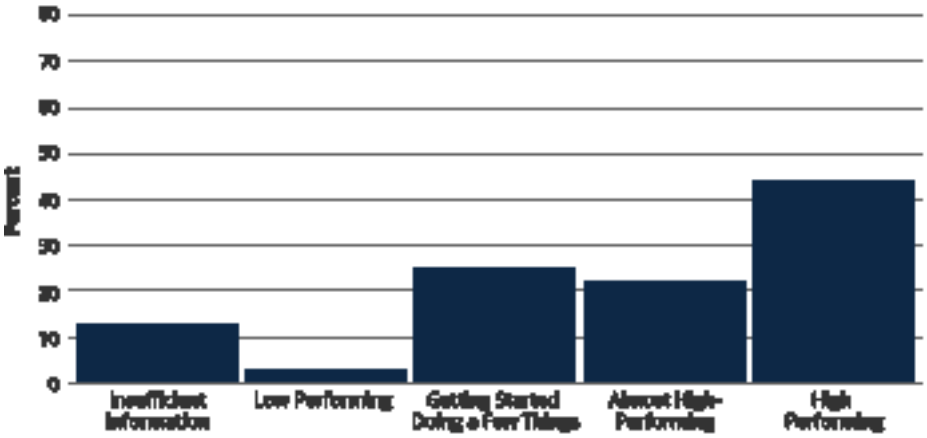
High-performing and larger organizations also create their own global/external business information security officer (BISO) collection capability. These organizations train BISOs in intelligence collection and reporting, and the BISOs provide country-specific intelligence by gathering data from local sources of information and conducting analysis on that data. Adding a BISO collection capability increased one organization's overall monthly production by 30 intelligence reports.

DATA GATHERING FACTOR 3: ORGANIZATION INFORMATION SHARING PROCESS

THIS ASSESSMENT FACTOR MEANS

The organization has formal and informal, bi-directional, and proactive sharing of relevant functional and strategic information and analysis with appropriate internal organizational business units and external partners. The organization assigns staff members to lead information sharing relationships when appropriate. There is a process to review and update the value of information sharing relationships.

PERFORMANCE SNAPSHOT



Data Gathering Factor 3 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Balkanization Impedes an Organization's Internal Information Sharing

We described the challenge of organizational silos in Environmental Context Factor 1. Although logical purposes exist for separation between certain business units (for example, data privacy, proprietary and classified information), silos stymie formal and informal information sharing between internal business units. Information that could be used to protect the organization and support its overall mission is not being shared proactively and across the organization.

Organizational policies, organizational structure, and business-specific technology stacks impede bi-directional and proactive sharing of relevant functional and strategic information and analysis. Organizations described a variety of challenges related to silos, including the absence of formal sharing mechanisms and service level agreements with other key business units, communicating cyber intelligence and important threat data with an organization's own overseas business subsidiaries that are unable to provide headquarters with relevant intelligence and threat data, and lack of involvement by legal and HR departments until those departments have a critical need.

Shortcomings in External Information Sharing

External information sharing—that is, sharing by government, law enforcement, and leading organizations—has improved since our 2013 cyber intelligence study, but challenges remain. Many organizations described benefits from the Department of Homeland Security's (DHS) free Automated Indicator Sharing AIS capability, which allows organizations to receive and share anonymized cyber threat indicators. The

IMPROVE YOUR PERFORMANCE

- Develop joint publications, create CTFs, and host brown bags between Government, Industry on cyber issues
- Use the collection management team and BISOs to build internal and external relationships

Cyber Information Sharing and Collaboration Program (CISCP) provides Indicator Bulletins and Threat Actor and Malware Analysis reports that organizations can use to support their own analysis. The partnership among private industry, academia, government and law enforcement appears to be growing. Some of the organizations we interviewed are deepening their relationships with other government and non-profit organizations such as local FBI Field Offices, the Intelligence Community, and the National Cyber Forensics Training Alliance (NCFTA).

Serious shortcomings remain in the quantity, type, and level of information shared. Government organizations conveyed that private industry organizations do not share enough cyber intelligence with the government, and companies conveyed that government organizations do not share enough cyber intelligence with private industry. Several organizations described challenges with law enforcement in particular: information sharing appears to be a one-way street, with private industry and academic organizations receiving little or no feedback from law enforcement about how information is ultimately used; lack of sharing makes these organizations less inclined to share data and intelligence in the future. Other specific challenges relate to the DHS AIS and CISCP and FBI Private Industry Notifications (PINs). Some organizations described the DHS AIS and CISCP indicators and intelligence as negligible and not useful. Other organizations reported that FBI PINs are not helpful or timely because the organization already knows about the data before the PINs[12] are released.

Separately, organizations voiced their desire for increased cyber intelligence collaboration and partnership with and between financial organizations and Silicon Valley (specifically the "big five" technology companies – Google, Amazon, Facebook, Apple, and Microsoft).

Meaningful Participation in ISACs

Information Sharing and Analysis Centers (ISACs) face challenges when members do not participate in meaningful ways. Organizations explained that because of privacy and proprietary information sharing concerns, they can often only receive information from ISACs; ISACs then struggle to get insight about the members' missions, environments, vulnerabilities, requirements, threat prioritizations, and internal cyber intelligence products.

GETTING TO HIGH-PERFORMING

Share the right information

High-performing organizations share indicators and intelligence analysis with other external organizations, to include National Fusion Centers[13] and ISACs.[14] Such sharing is important and relevant, given that in the 2017 National Network of Fusion Centers Final report, 39 (51%) National Fusion Centers selected cybersecurity as a top five priority in 2017, an increase from 11%. Of those fusion centers, 59% indicated they have the ability to perform strategic cyber analysis, tactical cyber analysis, and technical cyber analysis.[15]

---

12 PINS typically have feedback links https://www.ic3.gov/PIFsurvey/, so organizations should provide constructive feedback to the FBI to advance timely and supportive information sharing.

13 https://nfcausa.org/default.aspx/MenuItemID/242/MenuGroup/Public+Home.htm

14 https://www.nationalisacs.org/member-isacs

15 https://www.hsdl.org/?view&did=817528

High-performing organizations recognize the difference between meaningful information sharing and just information sharing. One high-performing organization shares intelligence with relevant fusion centers and ISACs only when the intelligence is actionable and has received a 51% confidence rating from analysts.

An interesting practice of some high-performing organizations is to share draft cyber intelligence reports and initial analytical judgments with trusted cyber intelligence teams that work for external entities or organizations. Trusted external teams provide comments, analytical recommendations, and other feedback to improve the report. For industry, this practice has the potential to grow into something bigger, such as Intelligence Community collaboration involved with creating National Intelligence Estimates or Intelligence Community Assessments, reports that serve as an example of the entire Intelligence Community's authoritative statement regarding a particular issue.

BUILDING A COLLECTIVE DEFENSE THROUGH INFORMATION SHARING

Cyber touches everything, and a threat to one is a threat to us all. To build a collective defense, organizations across government, industry, and academia should

Do things together
Contact other organizations and companies to create formalized brown bags, town halls, cyber threat frameworks, joint cyber assessments, cross-sector virtual blogs, and chat rooms.

Publish joint reports
The joint creation of cyber intelligence reports by private sector companies, ISAC members and third-party intelligence providers can increase teaming, collaboration, and transparency, which leads to trust. Moreover, jointly produced reports (with appropriate legal guidance to protect privacy / proprietary information and within Traffic Light Protocol guidelines) could bring greater authority and credibility to assessments on cyber issues. Joint publication conveys the reality that a threat to one is a threat to all. Organizations could also reserve the option to publicly disclose their contribution to the report and include supporting and dissenting views on analytical judgments.

Be transparent
Share data (indicators) and knowledge. Government, private sector, and academic organizations as well as ISACs, Fusion Centers, and third-party intelligence providers, can share knowledge about

- Prior attacks and how your organization handled them (lessons learned)
- New attack surfaces
- Using common tools and technology more efficiently
- Internal best practices and challenges
- Team compositions (roles, talent, responsibilities)
- Current strategic threats, campaigns, attribution

Task Collection Management Team with Managing Information Sharing
High-performing organizations usually have a collection management team squarely focused on ensuring successful formal and informal sharing of cyber information and intelligence with internal and external partners, including vendors. The collection management team regularly evaluates its relationships, thinking about new and more

TIP

The collection management team is not responsible for managing overall information security and compliance relationships with other organizational internal business units, suppliers, partners, contractors, and stakeholders. The program management office (PMO), a component of the Fusion Center, should have an Internal/External Relationship Team managing internal and external relationships. This team should also speak to internal business units and other partners and contractors about the value of cyber intelligence. This team should coordinate and work very closely with the cyber intelligence collection management team.

efficient ways to share and receive information. The collection management team also helps to build, in coordination with the PMO's internal and external relationship team, successful information sharing relationships with other internal organizational business units that fall traditionally outside of a fusion center, such as HR, business intelligence, physical security, legal, marketing, finance, technology development, and corporate leadership.

Formalize and document information sharing practices
High-performing organizations often develop cyber intelligence guides and best practices for sharing intelligence with internal business units--and their people understand those guides. Organizations that had fusion centers but were still building a Collection Management Team relied on Business Information Security Officers (BISOs) embedded in each organizational business unit to manage the relationship with the greater fusion center. BISOs act as both a liaison and officer for the fusion center by ensuring CISO polices are formulated into the business unit and enhancing intelligence sharing (intelligence requirements, cyber intelligence reports) with the fusion center.

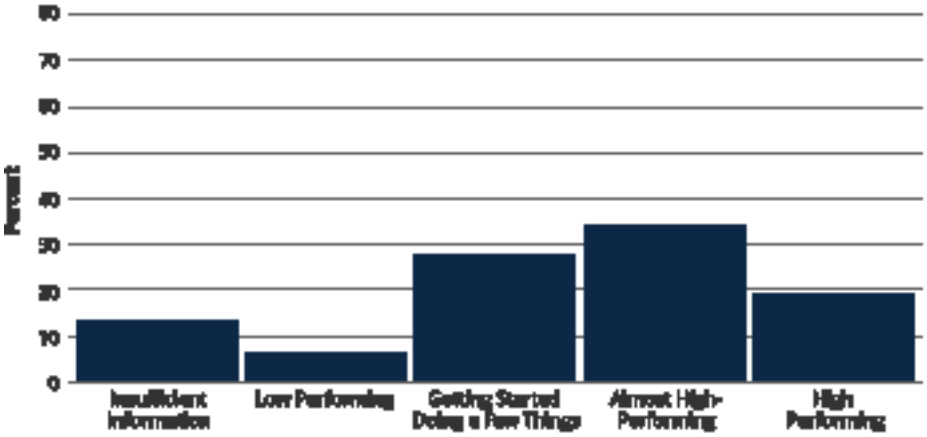
Foster Fusion Center Culture Through Engaged Leadership
Fusion centers must be actively managed by leadership. Leaders of high-performing organizations ensure their fusion centers have a culture that inspires innovation, teamwork, hard work, and a sense of mission. Additionally, the leaders of the fusion centers themselves are engaged, providing guidance and decisions in a timely manner. We discuss more on Leadership Engagement in the Reporting and Feedback section of the report.

DATA GATHERING FACTOR 4: TECHNOLOGY FOR DATA GATHERING

THIS ASSESSMENT FACTOR MEANS

The organization aligns homegrown and off-the-shelf technology with specific environmental context factors and data gathering requirements to tailor tools that consistently satisfy analytical needs. The organization has a technology review process. The organization uses current and emerging technology such as machine learning and automation as appropriate. performance snapshot.

PERFORMANCE SNAPSHOT



Data Gathering Factor 4 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Outdated Technologies, Resource Challenges, and Lack of a Technological Review
Since our 2013 study, more organizations have turned to technologies like SIEMs, SOAR platforms, and threat detection platforms that apply automation, data science, and behavioral analytics to log threat data to support data gathering, incident response, and threat analysis. However, some organizations rely on outdated tools and technologies to support data gathering and data management. These organizations discussed struggles normalizing data and find themselves continuously weeding through false positives. One organization has dedicated a full-time analyst to manually identify and work through daily false positives. Even some large organizations use email as their primary method to collect and manage data, and in other organizations, strategic analysts rely on spreadsheets to track threats and threat actors.

Organizations commonly lack resources (a recurring challenge related to people, capability, and funding) to build customized tools to meet specific analytical and data gathering needs that cannot be met by off-the-shelf technology. Some organizations also expressed challenges acquiring funding approval for new technology; and others discussed how technology fragmentation within their organization hampers mission and collaboration.

Still other organizations lack a technological review process. These organizations struggle to know if their existing technology is outdated, if it is capable of answering new needs, if new technology is available that could help the organization, or if other divisions across the organization are using same or better technology.

Data Normalization and Ingestion Still A Challenge
In our 2013 cyber intelligence study, we found that organizations were inundated with data feeds that came in different formats, making data consumption and integration for analysis extremely challenging. Although significant progress has been made with data language and serialization formats and exchange standards such as MITRE's Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII) 2.0, and OpenIOC, challenges remain. Data normalization is a never-ending hurdle for both organizations and vendors. The problem is compounded by the 2.5 quintillion bytes of data generated every day[16] from existing machines and the increasing number of connected devices and learning systems.

Multiple permutations exist for how organizations receive, document and capture (tag and index), and extract structured and unstructured relevant data and metadata resources (ports, domains, IPs and hashes, timestamps) in XML, JSON, free text, CSV coming from these devices. A data resource from one organization or from one threat intelligence vendor might actually be the same data resource from a different organization or different vendor, even though it is represented by different strings and formats. Today's machines are generally not yet smart enough to recognize the same information formatted in different ways.

IMPROVE YOUR PERFORMANCE

- Write scripts to assist with data ingestion, product dissemination, and phishing responses
- Adopt SOAR platforms to assist with Threat analysis
- Create a technology development and integration team to build customized tools that leverage automation and machine learning for cyber intelligence needs

16 https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#6c197fa060ba

CASE STUDY: DATA NORMALIZATION

A high-performing organization dedicated resources to establishing an organic internal cyber intelligence system using big data frameworks and natural language processing to automate the ingest and normalization of data received from internal and external sources. The system generates a record from each data source that populates field constructs in the following context:

- **UID**: Unique data record (line) identifier, or article reference number
- **TYPE**: Common object category (ie. Actor, Malware)
- **NAME**: Common object designation or name (ie. fuzzy-bear, almawt-hackers, backorifice, bifrost)
- **ALIAS**: Familiar name(s) associated with object from all sources
- **LOCATION**: Geopolitical boundary of actor/group activity (not necessarily physical location of article or indicator) (ie. World, Continent, Country, Region, State, City, Local/Tribe)
- **MOTIVE**: Explicit (Criminal, Political, Espionage, or Other) actor/group estimated motive(s)
- **RISK**: Request or requirement reference, addressing strategic risk ("above C-level") first, then tactical threats ("at C-level or below")
- **COMPENSATING CONTROL**: Freeform (from a defined list) security-led operations existing, emergent, or recommended physical or logical risk/threat compensating control(s)
- **CONFIDENCE**: Source confidence rating (see above "Source Reliability (A-F rating) and Information Content (1-6 rating)")
- **FSEEN**: Date/Time of first seen activity (GMT)
- **LSEEN**: Date/Time of last seen activity (GMT)
- **TAG**: Standardized tagging for sorting, searching, and data distribution
- **NOTE**: Freeform (no format) text field
- **ATTACHMENT**: Object or link extension (actual article/object or referrer)

GETTING TO HIGH-PERFORMING

Form a Team to Investigate Emerging Technology

High-performing organizations have technology development and integration teams comprised of security engineers, developers, data scientists, statisticians, and machine learning experts. The technology development and integration team meets frequently with analysts and leadership and incorporates their input and needs into future technology builds and procurements. The team then builds customized tools for cybersecurity and cyber intelligence purposes and applies automation and machine learning as appropriate.

We met organizations that have created in-house analytical tools that perform like Maltego but are specific to the organization's needs. Another high-performing organization has a team that built a large graph database of all internal and external data it has collected. The graph database is curated and highly-structured and is used for discovery, analysis, and knowledge sharing. The organization's technology development team is currently working on automating tasks within the graph database to hunt for interesting data, connections, and correlations. We also met with an organization that created an in-house, automated collection management system. One participant shared a piece of wisdom with our team: "anything you have to do more than once, you can script," which frees up time, money, and people to focus on more complicated analytics.

Use Diverse Technology to Support Cyber Intelligence

Most high-performing organizations do not rely exclusively on a single tool or an all-in-one" solution via integrations into a Threat Intelligence Platform (TIP) or SIEM. Rather, they incorporate homegrown and a variety of free and paid off-the-shelf tools and technologies to support current data gathering and analysis. For instance, a number of high-performing organizations have incorporated the free open-source ELK stack (Elasticsearch, Logstash, and Kibana) for data processing / aggregation, search, analysis, and visualization. Other organizations use Hadoop, MongoDB, or cloud-based solutions for data storage and management. For intelligence analysis and visualization, a number of high-preforming organizations use free and paid for tools such as BRO, Kali Linux, Process Monitor, Maltego, Analyst Notebook, Malware Information Sharing Platform (MISP), Tableau, and Adobe InDesign/Photoshop. Naturally, SIEMs, DLPs, SOAR, and TIPS provide analysis and visualization features in addition to product integrations with some of these same tools.

Technology also enables organizations to share information quickly and efficiently. We met organizations using Slack, SharePoint and their internal SIEM, TIP, or SOAR platform ticketing systems to share event and incident information. Organizations use Microsoft's Yammer tool as both an organizational social networking tool and incident tracker. Information and reports can be shared, posted, and edited in Yammer, and analysts and leadership can provide feedback and "like" reports and comments. In many high-performing organizations, the fusion center—and specifically the cyber intelligence team—maintains a website for sharing and receiving information such as cyber intelligence reports, current working drafts, best practices, new developments, opportunities for feedback, future reports, and RFIs. On the RFI page, the option exists to explain priority of the information need and track the status once it is submitted

Automation, Artificial Intelligence, and Applied Machine Learning

High-performing organizations recognize that automation is no longer simply nice to have; it is a necessity. Since our 2013 study, organizations have built more scripts to assist with data ingestion, product dissemination, and phishing response. Additionally, a number of organizations are using or incorporating SOAR platforms to help automate incident response and data enrichment tasks. SOAR platforms are designed to automatically integrate data from a variety of internal security tools and gather incident data and context into one single location. SOAR platforms can produce both standard and customizable step-by-step playbooks or workflows that automate manual repeatable tasks such as parsing emails, file detonation, creating incidents, notifying team members, and sending attachments or indicators through Virus Total or WHOIS. Our research also shows that high-performing organizations with resources and funding to purchase or apply machine learning will see direct savings in labor, giving analysts time to work on more pressing issues.

BEST PRACTICES

During our 2013 study, we found that many cyber intelligence tools were single-feature technologies. Although the increased features and capabilities of today's tools make it challenging to categorize them by function, we present an expanded list of tools organizations are using for data management, analysis, and visualization on page ___.

IMPLEMENTING MACHINE LEARNING

The following examples from the *Machine Learning and Cyber Intelligence* implementation guide describe ways organizations can implement machine learning:

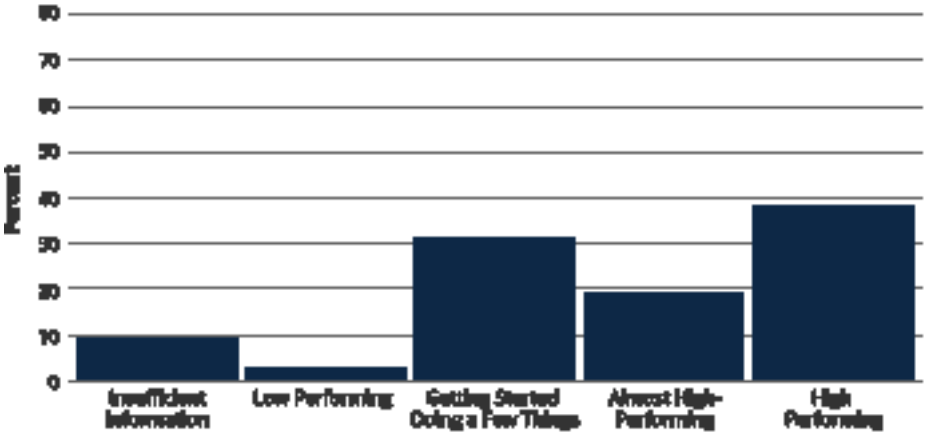
- **Feeding a neural network normalized data using natural language processing.** Physical, logical, and sociocultural data dimensions are systematically categorized by machines. Data artifact, indicator, and behavior characteristics are equalized and weighted against organization risk and decision-making models. The system ranks risk to prioritize threat matching and initiate predictive pattern recognition beyond human analyst capacity. The system qualifies matches of 100% malicious activity and has the option to monitor, act, or maneuver the threat through artificial intelligence and series of mitigating controls. The system generates summary risk and threat judgement for appropriate consumers (C-Suite to Analyst). The system is currently able to process 1.25 petabytes every day and can search back through data on demand.
- **Using supervised learning to train a model on a dataset of 5,000 articles.** The model generates articles twice a day for the entire team. One analyst is responsible for triaging and drilling down on the most serious and pressing items. The model also gets better every day because the analysts provide new training and feedback data to the model as they work. For example, any report written by the cyber intelligence team is tagged with the same tags they used to label and ingest articles originally. This organization claims that the process has reduced the time required for a particular task from eight hours to one hour.
- **Applying dynamic topic modeling to enhance intelligence analysis.** Dynamic topic modeling is a way to analyze the evolution of (unobserved) topics of a collection of documents over time. The ML application helps them answer the questions: What do we believe will happen in the next year? What topics are we seeing or did not look at in our analysis.
- **Using machine learning to help tackle the inside threat problem.** Specifically, training model(s) to learn how web browsers are susceptible to vulnerabilities and also internal user behavior (all logs, files and artifacts the users interacts with). Using a random forest decision tree algorithm, the model predicts the probability that a user's experience is heading toward a threat vector.

DATA GATHERING FACTOR 5: DATA SOURCE VALIDATION

THIS ASSESSMENT FACTOR MEANS

The organization has a repeatable process of validating data through tagging, using multiple sources and assessing the credibility of data sources. This process is reviewed and updated regularly.

PERFORMANCE SNAPSHOT



Data Gathering Factor 5 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of a process for data source validation

Some organizations don't have a process for data source validation at all, others have process that lack consistency, formalization, or transparency across the organization. These difficulties are compounded when analysts have their own data sources outside the central location where an organization's data sources are managed and evaluated. Organizations that have instituted a process for validating data sources explained that they might not review all of their sources regularly (at best annually) to determine if the data sources are still credible and reliable and provide relevant data to support the organization's mission. Last, some organizations only validate the data itself and not the data source.

Lack of a Common Lexicon

Organizations use different terminology to describe a source's validation, such as a credibility ranking, confidence ranking, uniqueness ranking, or reliability ranking. Criteria used to justify validation rankings also vary across organizations and industries, with some organizations using only corroboration by other data sources as the justification for validation.

Reliance on Vendors to Validate Data Sources

Some organizations rely completely on third-party intelligence providers to perform data source validation, often due to lack of resources (people and time) to perform their own validation of sources. In these cases, the notion of "trust but verify" becomes simply "trust." Organizations also explained that some third-party intelligence providers apply different types of ratings and scores that pertain only to the credibility of the data, yet there is no rating or scoring regarding the data source itself. Additionally, because some third-party intelligence providers generate scores using their own proprietary algorithms, organizations often have no clear understanding for the reasoning behind a given score.

IMPROVE YOUR PERFORMANCE

- Use the Admiralty Code as a starting point for data source validation.
- Set a 30-day time limit for vetting data sources and ensuring the data they provide aligns with intelligence requirements.

GETTING TO HIGH-PERFORMING

Evaluate Data Sources In a Repeatable and Transparent Way that Incorporates Multiple Sources

High-performing organizations have formal, holistic, transparent, and repeatable processes for evaluating data sources. These organizations receive third-party intelligence from vendors, yet perform additional separate validation. One organization explained that all internal and external data sources are currently manually reviewed, assessed, and classified every 30 days by a qualified analyst and to ensure they are correctly aligned to intelligence requirements. Another organization looks for a minimum of three data sources to corroborate each source's reporting. Some organizations, especially those in government and law enforcement, validate the data and data sources to the point that there is no uncertainty. There are no confidence levels because "evidence" they gathered must be able to stand up in a court of law.

Building off the Admiralty Code For Source Validation

A number of high-performing organizations and third-party intelligence providers that generate original context use the NATO or Admiralty Code Grading System[17] for conveying source reliability and credibility of information. The Admiralty Code, which provides a binary rating system that considers the reliability of both sources and the information they provide, is a positive step toward a common lexicon or ontology for data source validation.

EVALUATION OF SOURCE RELIABILITY

A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot Be Judged	No bias exists for evaluating the reliability of the source

NATO or Admiralty Code Grading System https://fas.org/irp/doddir/army/fm2-22-3.pdf

17 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf , https://en.wikipedia.org/wiki/Admiralty_code, https://fas.org/irp/doddir/army/fm2-22-3.pdf

EVALUATION OF INFORMATION CONTENT

1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Cannot Be Judged	No bias exists for evaluating the validity of the information

Toward a Common, Robust Lexicon for Validating Data Sources

Trusting data and data sources—identifying what is true and not true and having confidence that data is accurate, is reliable, and hasn't been tampered with—will become a more important challenge in coming years. As more organizations turn to machine learning to assist with decision making and prediction analysis, data quality is increasingly important; organizations must be able to validate the data and models used, and explain the process. Additionally, learning models can be vulnerable to poisoning, model inversion, and extraction attacks that could bias or trick a model's output. The potential for attacks like these means that demonstrating and explaining data source validation will require a greater level of detail, vetting capability, and transparency.

We see room for research to build upon the Admiralty Code to explain a source's authenticity, reliability, and freedom from adversarial tampering. We think it is important to move from a binary system to one that is more 3-dimensional. For instance, the Admiralty Code within Evaluation of Source Reliability does not separate "trustworthiness" (for example, freedom from adversarial control) from authenticity. As a result, it may be possible to reach a number of different scenarios about data source validation not explicitly conveyed in the Admiralty Code. One such scenario would involve a reliable source that provides valid information but has lost access and is getting that valid information from another unknown source; another scenario would involve a source that has access and provides information confirmed by other sources, yet is under adversarial control.

For additional fidelity regarding data source validation, we can look to the US Army FM 2-22.2 where source vetting is described as reliability, accuracy, and response to control.[1] Additionally, the US ODNI's Terms & Definitions of Interest for DoD Counterintelligence Professionals defines vetting as a "generic term to describe the full spectrum of asset evaluation for authenticity, reliability and hostile control."[2] Our team began to explore the idea of incorporating hostile or adversarial control into a more holistic source validation framework. Appendix ABC shows our original exploration into breaking out authenticity, reliability, and adversarial control into data source validation categories. Cyber intelligence teams can add the number and quality of data indicators and articles to provide a ranking for a source. The source ranking can be used to create a source description included in analytical products. Ultimately, we see this as an area for additional research.

---

1 Department of the Army. Counterintelligence. October 2009. FM 2-22.2 (FM 34-60) https://info.publicintelligence.net/USArmy-Counterintelligence.pdf

2 https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf

“When everything is intelligence—
nothing is intelligence.”

—Wilhelm Agrell
University of Lund, Sweden

Threat Analysis

Technical Approach to Inform Cyber Intelligence

INTRODUCTION

Threat analysis is the assessment of technical telemetry and non-technical data about specific threats, threat actors, and their campaigns in relation to your organization and industry. It informs cybersecurity operations and actions (incident response, network defense) and strategic analysis, and it is built on operational threat intelligence and tactical threat intelligence analysis. Threat analysis enables mid- to senior-level decision makers to make near-term decisions pertaining to cyber hygiene, cybersecurity, and incident response. Threat analysis relies heavily on technical skills.

THREAT ANALYSIS ASSESSMENT FACTORS

The Threat analysis component of the Cyber Intelligence Framework has five assessment factors:

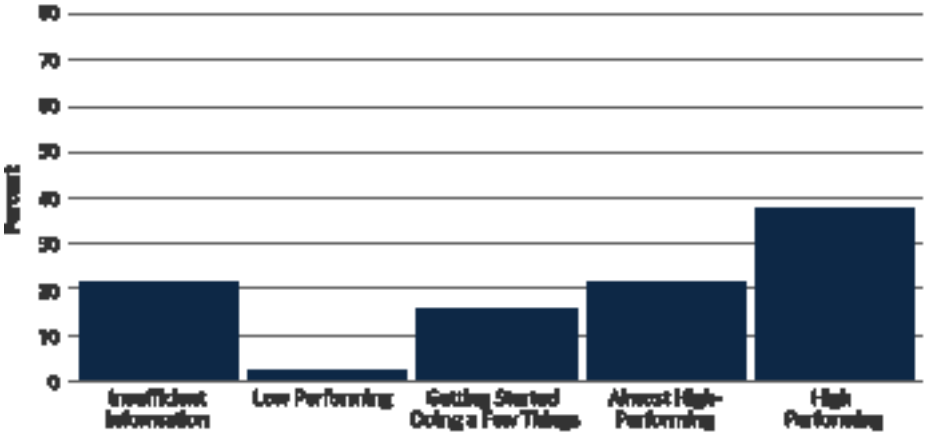
1. Threat analysis Workflow
2. Timeliness and Accuracy of Threat analysis
3. Diversity in Technical Disciplines
4. Traits, Core Competencies, and Skills
5. Threat analysis Tools

THREAT ANALYSIS FACTOR 1: THREAT ANALYSIS WORKFLOW

WHAT THIS ASSESSMENT FACTOR MEANS

The organization has a defined and repeatable threat analysis workflow with clear timelines, roles, and responsibilities. The workflow incorporates other Cyber Intelligence Framework components to provide analysis on specific threats to your organization and industry for the purposes of informing cybersecurity operations/actions and cyber strategic intelligence analysis. The Threat analysis workflow may be thought of as a smaller workflow within the larger overall cyber intelligence workflow.

PERFORMANCE SNAPSHOT



Threat Analysis Factor 1 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

No Formal Threat analysis Workflow

Organizations struggle with workflows that are largely conceptual and abstract; for these organizations, no documentation exists for workflow triggers, roles, responsibilities, or timelines to produce Threat analysis. Although this challenge was more common in smaller organizations, even some larger organizations lacked formally documented and accessible processes and procedures.

We also interviewed organizations that described specific challenges: some lack a ticketing/tracking system to show the status and workflow steps pertaining to an incident. Some organizations that have a Threat analysis workflow are struggling to integrate their organization's threat prioritizations into the workflow or to get their vendor to understand the organization's threat prioritizations.

Threat analysis Workflow Is the Only Workflow

We did meet organizations with defined and documented Threat analysis workflows supporting cybersecurity and incident response missions. Some organizations, often due to the recurring challenge of resource constraints, only focus on internal technical telemetry and do not receive or conduct analysis on other technical and non-technical data feeds from internal business units, industry data, or third-party strategic intelligence. Without this information, the cyber intelligence team lacks the insight to produce strategic reporting.

IMPROVE YOUR PERFORMANCE

- Create a defined and repeatable threat analysis workflow
- Use MITRE ATT&CK and SOAR technologies to assist with threat analysis

THREAT ANALYSIS GENERAL WORKFLOW:

1. Know your environment
2. Identify and understand gaps and intelligence requirements (IRs, and especially PIRs, SIRs)
3. Collect / normalize internal and external telemetry from data sources
4. Conduct Cyber Tactical Intelligence Analysis to answer what/where/when/how questions regarding threats, attacks, incidents, vulnerabilities, or other unusual network activity for the purpose of generating human and machine mitigating actions
5. Conduct Cyber Operational Intelligence, adding context (threat actors, campaigns) to existing tactical intelligence; starting to answer the who and why behind threats
6. Enhance mid-to senior level leadership decisions regarding non-immediate but near-term (weekly – quarterly) business process and operational decisions.
7. Leadership provides feedback

GETTING TO HIGH-PERFORMING

Create a Threat analysis Playbook
High-performing organizations have Threat analysis playbooks that ensure their workflows are defined, documented, repeatable, and scalable. Roles, responsibilities, and timelines are clearly understood. These organizations use SOAR and other customized platforms to manage the process.

Threat analysis workflows for some high-performing organizations start when indicators are automatically correlated and matched against internal network and endpoint telemetry activity in a SIEM. Pre-built alerts notify a junior Cyber Defense Analyst to decide if the alert requires additional analysis. For alerts that require additional analysis, the Cyber Defense Analyst creates a new case within the SIEM, TIP, SOAR Platform, JIRA, or other customized platform with read/write/edit privileges for the entire fusion center.

Threat analysis workflows in other high-performing organizations operate like a tree diagram, and analysis proceeds when certain thresholds are met or workflow milestones are completed. If a threshold for additional analysis is met, a senior cyber defense analyst or cyber defense incident responder becomes the lead analyst. The lead analyst gathers additional current and historical data with assistance from a team of analysts in the fusion center. These analysts have the option to simultaneously add input to the case at any time.

Use Common Frameworks and Tools
Many high-performing organizations are using the MITRE ATT&CK Framework to identify and understand adversarial tactics and techniques that interact with their systems. They also rely on Zeek (formerly BRO) in addition to a SIEM, EDR, or IDS/IPS utility. Zeek assists with searching historical data, malware, and network traffic analysis, and other interesting and important technical data such as user agent strings, protocols, headers, mac addresses, IPs, and certificates. High-performing teams then evaluate collected data, validate the data and data source, and make analytical judgements about the threat potential to the organization with recommendations for mitigation. Depending on the severity of the threat, the fusion center may immediately take action to stop and remediate the threat and will later report to leadership and other internal business units about the threat and actions taken. Again, Threat analysis

is threat specific and enables mid- to senior-level leaders to make immediate to near-term decisions about cyber hygiene, cybersecurity, and incident response to ensure sustained success of business processes and operations.

Save Time and Resources by Using Security Orchestration, Automation and Reponses Technologies

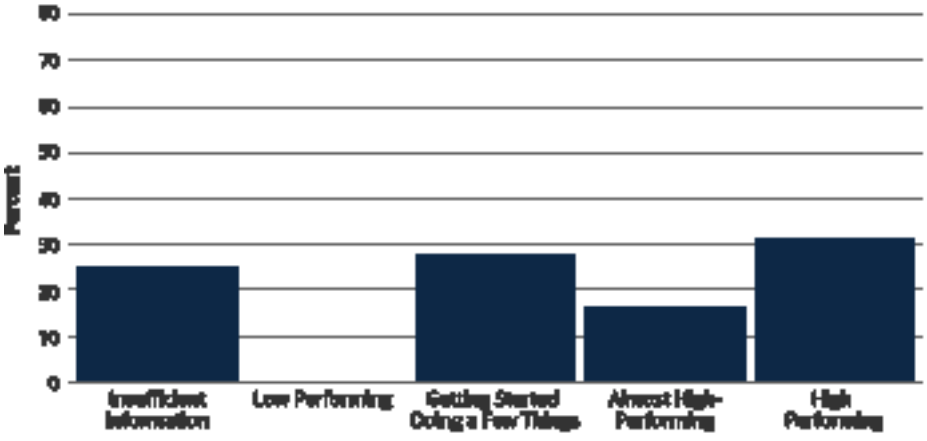
Some high-performing organizations use SOAR solutions to support Threat analysis. When configured appropriately, SOAR technologies can be a force multiplier for organizations with limited staff and time—especially when analysts are drowning in repetitive manual tasks. SOAR technologies automatically connect and coordinate disparate cybersecurity tools, threat intelligence platforms, and other non-security tools and products into a single dashboard. By connecting these tools—as well as people—a SOAR solution automates data enrichment and the execution of tasks like parsing URLs, file detonation, performing historical searches, and sending attachments or indicators through tools like Virus Total or WHOIS). This automation saves response time and reduces analyst workload and human error. The SOAR tool also works with an organization's playbook, allowing organizations to create playbooks from templates or to customize a playbook. The playbooks mimic a tree diagram process with scheduled timelines for sequential or multiple tasks.

THREAT ANALYSIS FACTOR 2: TIMELINESS AND ACCURACY OF THREAT ANALYSIS

THIS ASSESSMENT FACTOR MEANS

The organization's cyber intelligence team is capable of producing time-sensitive and multi-source validated functional analysis. The cyber intelligence team provides analytical updates as needed for information sharing and decision making purposes.

PERFORMANCE SNAPSHOT



Threat Analysis Factor 2 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Inadequate Reporting

Many organizations do not produce threat analysis reporting due to common challenges like lack of resources or lack of process. Others struggle to produce reporting in a timely manner: one organization explained that four days is considered a quick turnaround given their entire Threat analysis workflow, from environmental context to report generation and feedback. Still others produce reports that do not include data source validation language, estimative language, or acknowledgement of intelligence gaps.

IMPROVE YOUR PERFORMANCE

- Use a "shot clock" for Threat analysis reports on particular issues.
- Include data source validation scores, estimative language, and acknowledgment of intelligence gaps in Threat analysis Reports as appropriate.

GETTING TO HIGH-PERFORMING

Create processes to support speed and efficiency

High-performing organizations place a premium on speed and efficiency with formalized processes, plans, and timelines for report generation based on event/incident severity. A high-performing organization described their formalized "shot-clock" process for producing Threat analysis reports: depending the severity of a case, the team must answer immediate leadership requirements within one hour. Within 24 hours, the team must complete an incident analysis or notification report with added original context/analysis and actionable recommendations for decision makers.

To meet leadership-approved timelines, many high-performing organizations incorporate milestones and timelines into SOAR playbooks to assist with Threat analysis and Incident Notification reports. Some organizations also have Service Level Agreements (SLAs) with other internal business units and external partners that dictate timelines for delivery of functional reports.

Provide Specific and Actionable Reporting

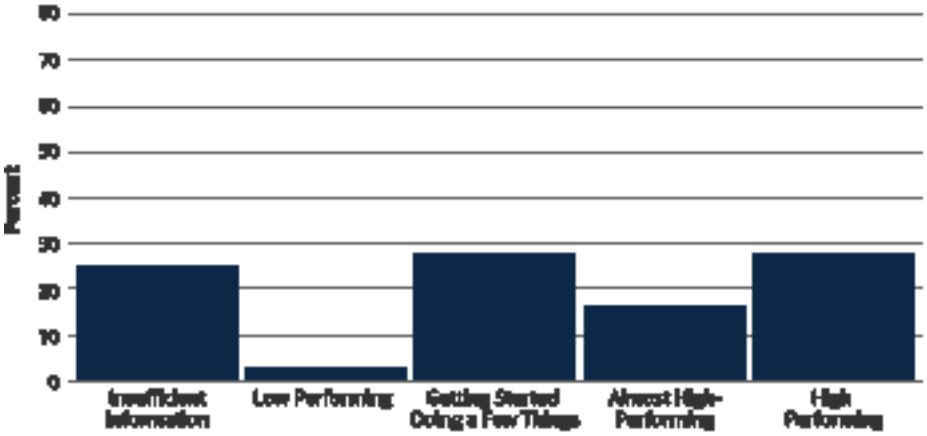
A number of high-performing organizations we met, specifically in the Finance, Health and Public Health and Government Facilities Sectors, produce a variety of Threat analysis reports such as daily reports, weekly situational reports, vulnerability notification reports, after-action reports, and monthly and bi-monthly technical reports on malware behavior, and network and user-behavior telemetry trends. These reports tend to be actionable/operational in nature and are targeted to Fusion Center Leadership and the CISO.

THREAT ANALYSIS FACTOR 3: INCORPORATING DIVERSE DISCIPLINES TO CONDUCT THREAT ANALYSIS

THIS ASSESSMENT FACTOR MEANS

The organization has a repeatable process and structure to incorporate diverse technical knowledge for threat analysis. The organization regularly evaluates that process to ensure it incorporates the technical knowledge and skills to conduct effective and comprehensive threat analysis.

PERFORMANCE SNAPSHOT



Threat Analysis Factor 3 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of Technical Diversity

Some organizations simply do not have a diversity of skills represented on their teams. Even large organizations may have small teams made up of members with similar technical backgrounds. Other cyber intelligence teams explained that they are unable to get management approval to hire new team members, or that they have no evaluation methodology to ensure the team has the right number of people with the right skill sets.

IMPROVE YOUR PERFORMANCE

Identify, document, and publish a listing of all team members with technical skills to support threat analysis

Lack of Visibility into Technical Skills

Many organizations explained that no information about skills is documented. The team simply knows who to go to for any particular technical situation. In small organizations with Cyber Intelligence Teams of 1-3 people, a conceptual process makes sense. For larger teams, the lack of a formal process to incorporate diverse technical skills raises challenges. For example, one team explained that at times they actually do not know who is working on a ticket or issue. For other organizations, the CISO or management simply selects the analyst(s) they think should work on a particular technical issue. This approach leads to single points of failure when the manager or analyst is not available; or if the manager is not aware of all technical skills and experiences existing within the organization.

GETTING TO HIGH-PERFORMING

Know and Document Your Team's Skills

High-performing organizations have teams that have an informal understanding of team member skills as well as formal documentation of team member technical skills and expertise. These organizations have the types of organic relationships we saw in fusion centers, where analysts often know who has what skills based on working closely together. But these organizations also document team member skills and ensure they are visible across the entire team. One high-performing organization has created a matrix listing subject matter experts and their skills sets. This helps the entire organization quickly triage events and assign the right technical analyst as well as identify appropriate peer-review analysts.

Open Lines of Communication with Support from Management

Many high-performing organizations recognize that creating a process to pull in the

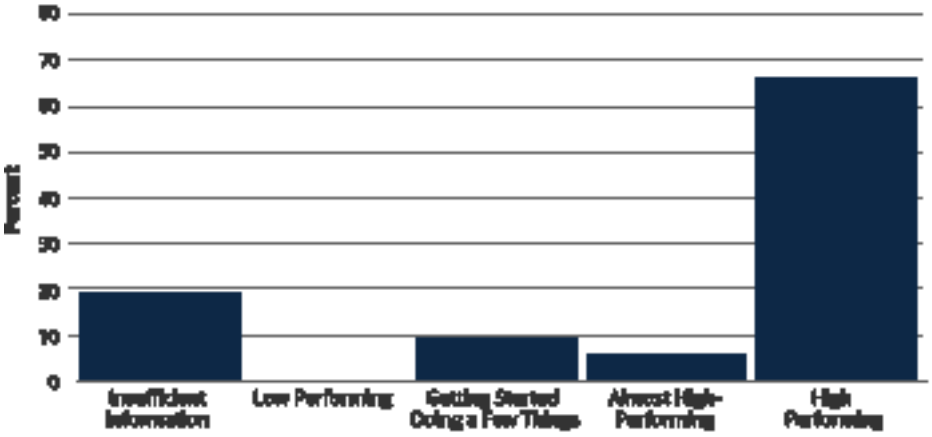
right analysts at the right time is largely a management responsibility. This doesn't mean that managers always pick the analyst(s) they want working on a particular issue. Rather, management creates open lines of communication (across the Fusion Center and the entire organization) that are effectively aligned to ensure that team members with the right skills are pulled in at the right time. While management ensures lines of communication are open, the whole team must participate in proactive communication necessary to incorporate the right people. For example, high-performing organizations often hold weekly sync meetings to educate everyone on current issues and work status. These sync meetings also help everyone know where expertise and transactional memory exists across the team.

THREAT ANALYSIS FACTOR 4: TRAITS, CORE COMPETENCIES, AND SKILLS

THIS ASSESSMENT FACTOR MEANS

Threat Analysts are deeply skilled in computing fundamentals, cybersecurity, technical exploitation, cyber forensics, data collection and examination, networking, and applied artificial intelligence. They are generally inquisitive, persistent, open minded critical thinkers and problem solvers. Threat Analysts are familiar with intelligence analysis, computer science, and data science. Opportunities for formal and informal training are available and encouraged for team members to keep core competencies and skills fresh.[18]

PERFORMANCE SNAPSHOT



Threat Analysis Factor 4 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Small Cyber Intelligence Teams and Limited Opportunities for Training

Some organizations we met have small Cyber Intelligence Teams and rely heavily on third-party intelligence providers. Even when some of these teams collaborate on particular issues, they are unable to cover necessary skills, core competencies and traits to perform effective Threat analysis. Such organizations also explained that they struggle with identifying people to hire that are technically proficient in more than one technical discipline. In other words, a candidate maybe have excellent experience in networks and networking, yet have little experience with malware or programming.

18 For a list of more specific traits, core competencies and skills, see CITP1 Training and Education White Paper and NIST NICE SP 800-181

Technical Teams that Lack Non-Technical Skills
An organization may have Cyber Intelligence Teams with highly technical people, yet they lack communication, collaboration and self-awareness skills. One organization expressed that it would be beneficial for the team to learn about emotional intelligence.

No Management Buy-In for Training
Some cyber intelligence teams explained that there isn't much encouragement, funding, and opportunity to attend technical training or conferences.

Seventy-seven percent of organizations were assessed as High-performing for having the traits, core competencies and skills to perform threat analysis. As part of the 77%, organizations in the Energy, Food and Agriculture, Health and Public Health, Transportation and Information Technology sectors were 100% high-performing.

In 2013, only 22% of organizations were high-performing in having the traits, core competencies, and skills to perform threat analysis. That number has increased to 77%.

Small Cyber Intelligence Teams and Limited Opportunities for Training Hampers Effective Threat analysis
Some organizations have very small cyber intelligence teams and rely heavily on third-party intelligence providers. Even when combined, team members cannot cover necessary skills, core competencies and traits to perform effective threat analysis. Many organizations explained that they struggle with identifying people to hire that are technically proficient in more than one technical discipline. In other words, a candidate maybe have excellent experience in networks and networking, yet have little experience with malware or programming. Alternatively, organization may have cyber intelligence teams comprised of highly technical people, yet they lack communication, collaboration skills and self-awareness skills. Indeed, one organization expressed that it would be beneficial for the team to learn about emotional intelligence. Some cyber intelligence teams in the Food and Agriculture, Health and Public Health and Government Facilities sectors explained that there isn't much encouragement, funding, and opportunity to attend technical training or conferences.

GETTING TO HIGH-PERFORMING

Build teams with depth and breadth in technical disciplines
High-performing organizations have deep and wide benches across many technical disciplines. From a strictly technical standpoint, high-performing organizations have team members with backgrounds that broadly fit into computing fundamentals, cybersecurity, technical exploitation, data collection and examination, communication and collaboration, and applied artificial intelligence. More specifically, we met people skilled in forensics and malware analysis, reverse engineering, intrusion analysis, incident response, network forensics, network and information architecture engineering, operating systems, networking, mobile devices, mobile and web applications, social engineering, operational technologies, vulnerability analysis, cryptography, pen testing, programming and software development, data science and machine learning.

High-performing organizations expressed that many team members have deep knowledge and experience with a variety of tools or that they are fast learners. Individuals need to rapidly manipulate tools to generate additional context and provide options and solutions quickly for decision makers.

IMPROVE YOUR PERFORMANCE

- Use NIST SP 800 -181 as a hiring guide; look for individuals with subject matter knowledge across many technical disciplines and deep technical expertise in a least one discipline.
- Ensure technical applicants have non-technical skills: Critical Thinking, Self-Awareness, Communication Skills
- Test applicants by having them provide a work sample on addressing a relevant cyber issue.
- Put new employees through mandatory introductory training on a particular technical specialization.
- Run less experienced analysts through internal mock threat scenarios where they draft and brief threat assessments.
- Match new employees with senior technical analysts for ongoing mentoring.

Test Candidates for Technical Skills and Look for Non-Technical Skills
High-performing organizations commonly assess skill gaps across their teams. Then, using NIST NICE 800-181 as a guide, they look to hire individuals with a proven record of expertise, aptitude, hands-on tool familiarity and a deep desire to learn and improve. Many organizations explained that experience carries greater weight than education. They also test applicants with some type of work sample. For example, one organization evaluates applicants based on whether they can choose an important Cyber Intelligence question and answer it effectively.

Many organizations expressed that while a basic understanding of IT and cybersecurity is important, technical skills can be taught. A major theme throughout our interviews with study participants was the importance of non-technical skills. Organizations across Finance, Health and Public Health, Government, and the Defense Industrial Base sectors emphasized the importance of a passion to learn, curiosity, open-mindedness, adaptability, critical thinking -specifically problem solving, and the ability to communicate effectively without ego (writing, briefing) technical concepts to different audiences. Additionally, individuals performing Threat analysis should have familiarity with and understanding of intelligence analysis and structured analytical techniques.

Create a Culture that Encourages Everyday Learning and Training
High-performing organizations recognize that experts want to work for winning and highly capable companies—training their people is good for morale and their bottom line. Organizations we interviewed, specifically in the Finance, Energy, and Government Facilities continuously provide a variety of internal and external learning and training opportunities. Examples include mandatory introductory training for new employees in particular technical areas, conducting internal mock threat scenarios where newer analysts draft and brief threat assessments, and matching new employees with senior technical analysts for ongoing mentoring.

Many high-performing organizations encourage employees to take online technical training and attend conferences, technical exchanges, and free webinars. These organizations typically also have large budgets for training, in some cases, more than $8,000 per year per employee. Employees are sent to well-known industry training venues and conferences to build technical skills on topics such as malware and network analysis, forensics, and incident response—and to make professional connections with other cyber intelligence professionals. Employees receiving technical training or attending conference brief or teach their team about what they learned when they return. Some organizations additionally set funding aside for outside vendors to visit onsite and train the team on a particular skill or new tool.

TIP: HIRING

A common theme when hiring is to shoot for the letter "T" model for technical positions, meaning that employees should have broad subject matter knowledge and experience across many different threat analysis disciplines and one area in which they have tremendous technical depth and experience. Better than the "T" model, is Π, where an employee has broad knowledge and experience across many different cyber intelligence disciplines and two areas of technical depth and experience.

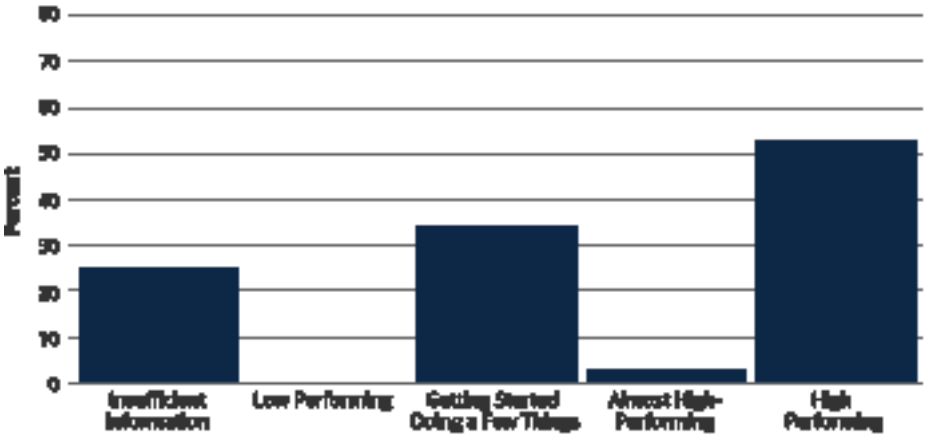
THREAT ANALYSIS FACTOR 5: THREAT ANALYSIS TOOLS

WHAT THIS ASSESSMENT FACTOR MEANS

The organization has an appropriate combination of homegrown and off-the-shelf technical analysis tools to support Threat analysis. Tools are appropriately configured to support the organization, are readily available, and are evaluated routinely to ensure they meet organizational needs.

High-Performing Organizations
The organization has an appropriate combination of homegrown and off-the-shelf technical analysis tools to support threat analysis; tools are appropriately configured to support the organization; tools are readily available; and tools are evaluated routinely to ensure they meet organizational needs.

PERFORMANCE SNAPSHOT



Threat Analysis Factor 5 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Getting the right tools and technology
Some organizations expressed challenges with creating or acquiring technology to support Threat analysis. For instance, we met with an organization relying primarily on email as its mechanism for data collection, management and analysis. Additionally, we interviewed organizations expressing the need, yet lack purchasing authority to acquire new and better technology. Some organization are specifically seeking DLPs, better event correlation and analysis tools, and integration technologies like a SIEM, EDR, DLP, or TIP.

We also met organizations that don't have people with the skills/expertise to build customized programs and tools, or write scripts to make internal and external information more useful to their organization's needs. Last, we interviewed organizations that explained they do not have a process/strategy for evaluating their current tools and technologies against future needs to perform Threat analysis.

IMPROVE YOUR PERFORMANCE

- Create a strategy to analyze your current tool and technologies needs to identify current gaps and future needs.
- Use open source tools like Virus Total and Zeek to support Threat analysis

GETTING TO HIGH-PERFORMING

Create a strategy for using Open-Source, Paid and Customized Tools and Technologies to support Threat analysis
A practice of high-performing organizations is creating a Threat analysis tools and technologies strategy. Such a strategy usually involves regular evaluation of current organizational tools and technologies vs. current needs, identification of tools and technologies that will be built in-house vs. purchased, and identification of tools and technologies needed in the next few years. Routine evaluation of tools and technologies ensures they assist the Cyber Intelligence Team in performing effective Threat analysis to answer changing SIRs, PIRs, IRs. A method for evaluation may involve leadership issuing an annual or bi-annual solicitation for tool and technology requirements from the Fusion Center and other parts of the organization to understand organizational needs before exploring COTS or in-house solutions.

High-performing organizations also take the necessary time to configure and test new tools and technology before launching them on their network.

Use Tools to Their Full Potential

High-performing organizations use paid tools like IDA PRO, Joe Sandbox, Virus Total Premium, Splunk, RSA Netwitness, and the ELK Stack (Elastic Search, Logstash, and Kibana). Open-source tools include Kali Linux, MISP, WHOIS, Cuckoo Sandbox, Virus Total, Olydbg, Shodan, Wireshark, Snort, and Zeek.

The following are just a few interesting examples of how organizations we interviewed use tools and technologies to support Threat analysis:

- As a premium customer of Virus Total Intelligence, the Cyber Intelligence Team creates specific YARA rules looking for indicators important to their organization. When team member uploads a file to Virus Total and it meets the team's established criteria, the team is immediately alerted. The team then retrieves the document for additional investigation.
- The cyber intelligence team uses Splunk and Zeek concurrently for analysis and validation. The organization's Zeek clusters provide analytics on network traffic such top protocols, top talkers, and top ports, acting as an audit on top of Splunk.
- The cyber intelligence team writes scripts to facilitate IOC extraction from .pdf and .doc files, and creates tools to perform secure remote file retrieval. The team is working on creating ML algorithms for use in Splunk to identify anomalous user activity, malware beaconing, and data exfiltration.
- The cyber intelligence team is building in-house malware labs for testing and analysis using open-source tools such as VMware, pestudio, process monitor, process explorer, Wireshark, and Zeek.
- The organization has created a system where a neural network is fed normalized data (indicators and artifacts) using Natural Language Processing (NLP). The system then searches for matches with 100% malicious activity and has the option of generating risk and threat judgments reports to the appropriate human analysts for additional analysis.

TIP

WHAT TOOLS ARE ORGANIZATIONS USING?

Diversity in tools and technologies is important. We interviewed high-performing organizations that have a good balance of open-source, COTS, and homegrown tools and technologies. As part of our research, we captured a list of the tools participants are using for threat analysis. We present an expanded list on page ___.

TIP

See the Machine Learning and Cyber Intelligence Implementation Guide to learn more about using machine learning to support Threat analysis on challenges such as malware attribution, insider threat analysis, and identifying, sorting, and prioritizing information.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

—Sun Tzu
The Art of War.

Strategic Analysis

Understanding the Big Picture

INTRODUCTION

Strategic analysis is the process of conducting holistic analysis on threats and opportunities. Holistically assessing threats is based on analysis of threat actor potential, organizational exposure, and organizational impact of the threat. Strategic analysis answers "who" and "why" questions related to threats and threat actors.

Strategic analysis is not only comprehensive, but anticipatory. Strategic analysis goes beyond threat analysis to incorporate analysis regarding emerging technologies and geopolitics that may impact or provide opportunities for the organization now and in the future. It can be actionable, enabling executive leaders to make risk-based decisions pertaining to the organization's financial health, brand, stature, and reputation.

STRATEGIC ANALYSIS FACTORS

In evaluating the state of the practice of cyber intelligence in terms of Environmental Context, we considered the following factors:

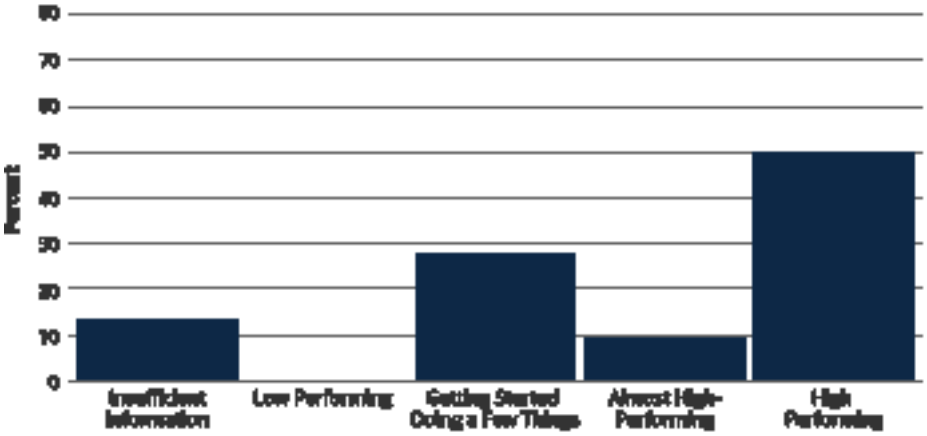
1. Understanding the difference between Strategic analysis and Threat analysis
2. Strategic analysis Workflow
3. Diversity Among Strategic Disciplines
4. Traits, Core Competencies and Skills
5. Strategic analysis Tools
6. Analytical Tradecraft Applied to Cyber Intelligence Analysis

STRATEGIC ANALYSIS FACTOR 1: UNDERSTANDING THE DIFFERENCE BETWEEN STRATEGIC AND THREAT ANALYSIS

What This Assessment Factor Means

The organization distinguishes between threat analysis and strategcis analysis. Collaboration between threat analysts and strategic analysts is proactive and efficient.

PERFORMANCE SNAPSHOT



Environmental Factor 2 Performance Snapshot The graph on the left shows how participants in the study are performing in this assessment factor.

COMMON CHALLENGES

Inability to Implement Strategic analysis

Most Cyber Intelligence Teams we interviewed recognize the importance performing Strategic analysis, but many simply aren't doing it. Lack of resources and leadership commitment and understanding lead to cyber intelligence teams that are geared more towards Threat analysis to inform cybersecurity efforts such as network defense, cyber hygiene, compliance, and incident response.

IMPROVE YOUR PERFORMANCE

Create a separate and distinct Strategic analysis Team

We met organizations without any strategic analysts and no requisitions to perform that type of work. We also met organizations that have only one person on the entire team creating strategic analysis reports – a task too large for any one person, especially in larger organizations. One team explained that all of its leadership has backgrounds in cybersecurity, patching and vulnerabilities and as a result they do not understand the importance of Strategic analysis. Most organizations lacking a strategic analysis capability tend to rely solely on third-party intelligence providers to provide that type of analysis.

Data Silos

Additionally we encountered some Strategic Analysts discussing challenges accessing cybersecurity data and intelligence from cybersecurity or threat teams. Most of these data silos stem from differentiations in technology stacks, culture, sharing policies or SLAs, and teams being physically separated from one another. One organization explained that while their TIP supports threat actor profiling (good for strategic analysis) they face challenges mapping / tagging data in the TIP to the MITRE ATT&CK framework, which could later be used to support Strategic analysis.

GETTING TO HIGH-PERFORMING

Create a separate team focused on Strategic analysis

High-performing organizations have Strategic analysis teams with formalized responsibilities, policies, and procedures—and those teams proactively collaborate with cybersecurity and threat teams. A large organization we met dedicated resources and commitment by standing up a ten-person team focused on Strategic analysis.

THE VALUE OF STRATEGIC ANALYSIS

In analyzing threat intelligence alongside non-traditional data from departments such as HR, Physical Security, and Legal, Strategic Analysts develop depth, context, and perspective on particular issues. These analysts understand the circumstances that form the setting for a past, current or future event, incident, or issue. They use this understanding to create reports and briefings to executive leadership that contain judgments and actionable recommendations, going from technical to non-technical with a risk-based perspective.

Strategic Analysis not only informs leadership about organizational risks. It also informs Threat and Cybersecurity Teams about holistic current and future threats, risks and opportunities. Analysis detailing threat actor behavior over time, or specific threat actor capabilities and intent, or even how emerging technologies enable new threats and opportunities gives these teams insight into how to better prepare and respond to events and incidents. Lastly, Strategic Cyber Intelligence Analysis provides the Collection Management Team with ideas and guidance on new areas for tasking data sources.

Answer IRs and PIRs

In high-performing organizations, Strategic Analysts aim to answer (usually in quarterly / annual reports and briefings) executive leadership level Intelligence Requirements and Priority Intelligence Requirements. This level of analysis is typically geared towards assisting executive leadership in making risk-based decisions pertaining to organization's financial health, brand, stature, and reputation. Analysis can be extremely deep and detailed on a particular topic, and it can also be more broad-based focused on trends.

Foster Collaboration

Strategic analysis provides strategic analysts and threat analysts with insight on threat actors' motivations and capabilities, threat and risk trends impacting the organization and industry. Because of the complimentary nature between threat analysis and strategic analysis, strong collaboration must exist. Most high-performing organizations have Fusion Centers or one location where all analysts physically sit together to foster that collaboration. However, we interviewed one high-performing organization that purposely locates its strategic Analysts outside of the Fusion Center to prevent these analysts from becoming to mired in the tactical and operational intelligence.

Produce the Right Reports for Your Organization

We interviewed Strategic Analysts that produce or contribute a variety of reports. A number of these reports focus on future threats and opportunities to the organization, which may help identify new Intelligence requirements and research and development areas. Typical reports include

- Ranking and tracking threat actor motivations, capabilities and lifecycles against the organization's critical assets and technologies at risk
- Targeting packages for the pen-testing team
- Tracking APTs as a mission and identifying threat actors (down to individual people) and why they are motivated to target the organization, its third parties and industry
- Identifying and mapping threat actors to geographic locations
- Impact/opportunity presented quantum computing, machine learning, 5G, and crypto-currencies

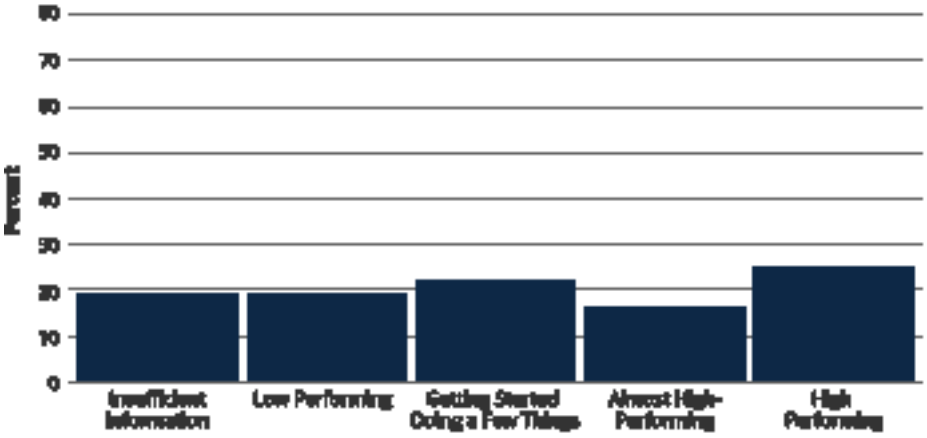
- Foreign travel concerns
- Opening a business in a foreign country
- Where/what the organization should be investing in (technology, other companies)
- Company mergers and acquisitions
- Supply Chain analysis
- How a particular technology may impact a line of business
- Potential geopolitical, technological and economic disruptions to business
- Future foreign country forecasts
- Assessing organizational emerging technology and how that lines up with company five year plans and threat actor capabilities
- Assessing what specific threat incidents mean for the company moving forward

STRATEGIC ANALYSIS FACTOR 2: STRATEGIC ANALYSIS WORKFLOW

WHAT THIS ASSESSMENT FACTOR MEANS

The organization has a defined and repeatable Strategic Intelligence Analysis workflow with clear timelines, roles, and responsibilities. The workflow incorporates other Cyber Intelligence Framework components to create analytical products holistically assessing threats, risks, and opportunities for the organization and industry.

PERFORMANCE SNAPSHOT



Strategic Analysis Factor 2 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Non-existent, ad-hoc, or multiple workflows

Nearly 20% of the organizations we met told us they did not produce strategic analysis reports; these organizations do not have a strategic analysis workflow. Other organizations incorporate aspects of a Strategic analysis workflow; however the workflow is ad-hoc, not formalized, and not repeatable. For instance, we met some organizations that produce Strategic Intelligence Analysis reports however they have no established timelines for report production. Methodologies, processes, technologies and templates used vary across analysts.

IMPROVE YOUR PERFORMANCE

- Create a defined and repeatable Strategic analysis Workflow to answers IRs and PIRs. The workflow should leverage all components of the Cyber Intelligence Framework to support strategic analysis on threats, risks, and opportunities.
- Focus on attribution to open new collection tasking against a particular threat actor, to reveal greater insight into threat actor modus operandi, and to assist with target package generation to mimic the specific threat actor for the pen testing team

SEPARATING WORKFLOWS: THREAT ANALYSIS AND STRATEGIC ANALYSIS

A recurring theme we noticed during our interviews was that participating organizations had difficulty distinguishing between strategic and non-strategic components and activities—and workflow is one area where we saw this difficulty. The workflows begin and end with the same components. However, unique components within the Threat analysis workflow are designed to inform cybersecurity operations/actions, while components within the Strategic analysis workflow involve holistically assessing threats, risks, and opportunities.

Threat analysis

Performed to make immediate to near-term decisions pertaining to cyber hygiene, cybersecurity, and incident response (deny, disrupt, neutralize, deceive, exploit, defeat) to ensure sustained success of business processes and operations. It relies heavily on technical skills and is threat specific.

General Workflow

1. Know your environment
2. Identify and understand gaps and intelligence requirements (IRs, and especially PIRs, SIRs)
3. Collect / normalize internal and external telemetry from data sources
4. Conduct Cyber Tactical Intelligence Analysis to answer what/where/when/how questions regarding threats, attacks, incidents, vulnerabilities, or other unusual network activity for the purpose of generating human and machine mitigating actions
5. Conduct Cyber Operational Intelligence, adding context (threat actors, campaigns) to existing tactical intelligence; starting to answer the who and why behind threats
6. Enhance mid-to senior level leadership decisions regarding non-immediate but near-term (weekly – quarterly) business process and operational decisions.
7. Leadership provides feedback

Strategic analysis

Performed to holistically assess threats, risks, and emerging technologies and geopolitics that may impact/provide opportunities for the organization now and in the future. Informs Threat Analysts, the Collection Management Team and enhances executive decision-making about organizational strategic issues and opportunities.

General Workflow

1. Know your environment
2. Identify and understand gaps and intelligence requirements
3. Fuse Threat analysis with other external and non-traditional data sources
4. Depending on data collected, work with Data Science team to identify larger trends or anomalies in data collected
5. Perform structured analytical techniques and human-centered design activities as needed
6. Provide analytical assessments based on threat actor potential, organizational exposure, and organizational impact of threat
7. Analyze current and future technologies and geopolitics that may positively/negatively impact the organization and industry
8. Enhance executive leader decision making by answering IRs and providing intelligence pertaining to organizational strategic risks regarding financial health, brand, stature, and reputation
9. Leadership provides feedback

GETTING TO HIGH-PERFORMING

Attribution Matters

Attribution can be extremely challenging, but it is an important practice that helps organizations know their enemies. Government and Law Enforcement organizations typically perform attribution for arrest and evidence purposes, and other organizations commonly use it for understanding fraud. A practice of high-performing organizations is to provide attribution information to law enforcement to hold perpetrators accountable for their actions. When organizations know the threat actor(s) intent on targeting them, they can protect their organization from those threat actors and the TTPs those threat actors may use to target a new technology the organization plans to be first to market.

ATTRIBUTION: RECOMMENDED RESOURCES

The ODNI Guide to Cyber Attribution describes how analysts can assess responsibility for a cyber attack. The guide suggests three ways:

1. Point of origin (neighborhood, city, state, country, region)
2. Specific digital device or online persona
3. Or the individual or organization that directed the activity

The *Cyber Intelligence Tradecraft Project Threat Prioritization Guid*e provides categories for collecting and analyzing information on Threat Actor Potential, which could assist with cyber attribution:

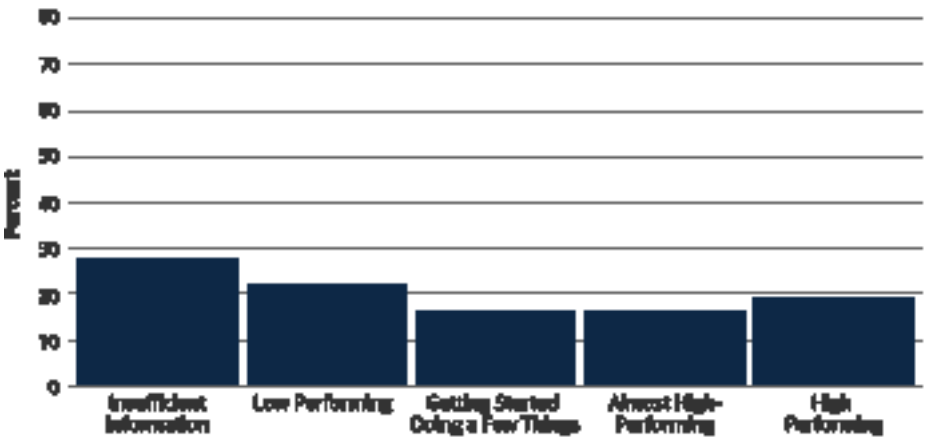
- Infrastructure
- Technology
- Coding
- Maturity
- Targets of interest
- Timing ability
- Funding
- People
- Tools and Training
- Intrinsic and Extrinsic motivations
- Targeted data and organizational systems

STRATEGIC ANALYSIS FACTOR 3: INCORPORATING DIVERSE DISCIPLINES TO CONDUCT STRATEGIC ANALYSIS

WHAT THIS ASSESSMENT FACTOR MEANS

The organization has a process and structure to incorporate diverse disciplines to conduct Strategic analysis. The organization regularly evaluates the Strategic analysis process to ensure it incorporates the right knowledge and skills to enhance executive leadership decision making pertaining to organizational vital interests (financial health, brand, stature, and reputation).

PERFORMANCE SNAPSHOT



Strategic Analysis Factor 3 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Resource Constraints

Organizations in all sectors have resource limitations preventing the production of Strategic Assessments. Organizations simply lack personnel to build a Strategic Team and as a result are unable to commit time and energy to produce these assessments. On some occasions we met with teams of one to three people responsible for both cybersecurity and cyber intelligence for large -even global organizations.

Hiring Team Members with the Same Skills

Additionally, we met with organizations that do not diversify skills when hiring. They seem to hire individuals with the same skills and experience, typically those technically competent in cybersecurity, forensics, reverse engineering, intrusion analysis, operating systems and network and information architecture engineering.

Lack of Process

Only about 20% of organizations were high-performing for having a process to incorporate diverse disciplines to conduct Strategic analysis. Some organizations maintain a process, yet explained it is more ad-hoc in nature - nothing is written down explaining whose expertise is needed or good to leverage for particular issues. Analysts that do contribute to these products are typically analysts with the same experience or background.

GETTING TO HIGH PERFORMING

Build Collaboration In

We met organizations that have entire teams performing Strategic analysis. These analysts are typically intelligence analysts and geopolitical analysts. Analysts tend to be organized or assigned to threats, threat types, or by regions or countries. A practice of high-performing organizations is to ensure there is proactive collaboration between Strategic analysts and data scientists. The data scientists build tools for both strategic analysts and threat analysts. They also help with identifying trends and correlations. Indeed, one high-performing organization explained that "you need data scientists to win wars."

Another practice of high-performing organizations is to have a codified process to incorporate diverse disciplines to conduct strategic analysis. As noted in section CTI3, Management investment and oversight ensures the right analysts are pulled in at the right time. This doesn't mean management always picks the person it wants working on a particular issue. Rather, management creates open lines of communication (across the Fusion Center and the entire organization) that are effectively aligned to ensure the right group of diverse people are pulled in at the right time. An attribute of high-performing organizations is to also regularly evaluate that process to ensure the right knowledge and skills across the entire organization are brought to bear.

To assist with Strategic analysis, high-performing Cyber Intelligence Teams bring in people with diverse backgrounds to participate in brainstorming sessions, weekly sync and collaboration meetings, and peer reviews of strategic products. An area of interest for future research might be exploring "SOAR-like" technology for automated data enrichment of data sets within and outside the organization and playbook generation that connects diverse analysts across the organization to contribute to Strategic analytical products on holistic threats, risks, and opportunities.

IMPROVE YOUR PERFORMANCE

- Create open lines of communication (across the Fusion Center and the entire organization) to ensure the right group of diverse people are pulled in at the right.
- Hire data scientists to work with cyber intelligence analysts for purpose of identifying trends, patterns, anomalies
- Regularly evaluate that process to ensure the right knowledge and skills across the entire organization are brought to bear.

STRATEGIC ANALYSIS FACTOR 4: TRAITS, CORE COMPETENCIES, AND SKILLS

What This Assessment Factor Means

Analysts have the traits, core competencies and skills to perform Strategic analysis. Many opportunities for formal and informal training are available and encouraged for team members to keep core competencies and skills fresh.

Traits:

- Inquisitive
- Persistent
- self-motivated
- intellectually independent
- able to learn quickly
- open minded
- adaptable

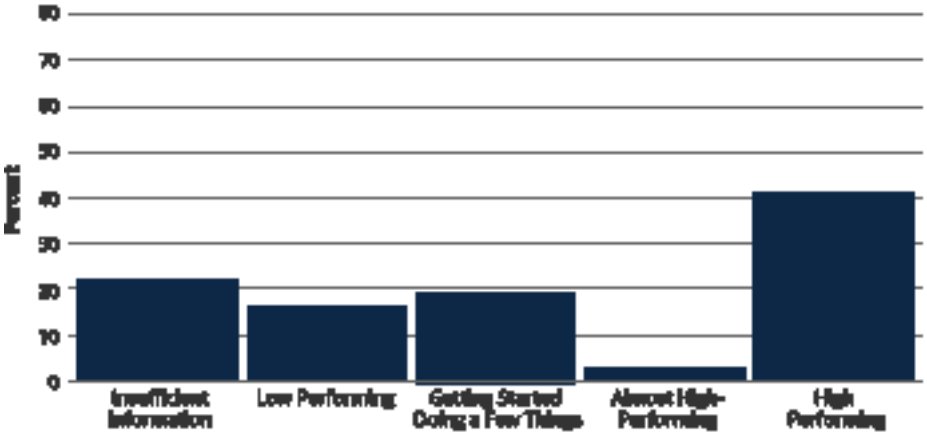
Core Competencies:

- critical thinking
- problem solving
- intelligence analysis
- data collection
- communication and collaboration
- knowledge about industry and geopolitics

Basic skills in

- computing and cybersecurity fundamentals
- technical exploitation
- computer science and data science

PERFORMANCE SNAPSHOT



Strategic Analysis Factor 4 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Organizations lack personnel and leadership commitment to perform Strategic analysis

Some organizations interviewed performing Strategic analysis face talent and acquisition challenges, tending to lack a bench of analysts to support this level of analysis. Two other organizations in the Finance sector with Strategic analysis teams explained that some team members have no intelligence analysis experience or background in analytical techniques or geopolitics. When it came to formal and informal training for Strategic analysis, organizations we interviewed primarily in the Finance and Government Facilities sectors indicated that they do not offer formal training in intelligence analysis, data collection, or human-centered design techniques. Training for these organizations is very much on the job.

Difference in styles between military and other government agency trained Intelligence Analysts

Based on their experience, a few industry organizations explained that hiring former military officers with training in intelligence may not be the best fit for Strategic analysis. For instance, a team commented that military officers are usually more

IMPROVE YOUR PERFORMANCE

- Refer to NIST SP 800-181 as a guide for hiring to perform Strategic analysis.
- Hire individuals that have experience and can demonstrate strong critical thinking skills. You can always teach and provide on-the job-training for technical skills.

skilled and interested in operations and not strategic analysis and writing. Another team from a large industry organization remarked that officers with straight military intelligence background (and NO technical experience) tend to see things in pure military terms and perspectives. For Strategic analysis, these high-performing industry organizations recommend hiring Intelligence Analysts that have had experience from a "three letter" Intelligence Agency.

GETTING TO HIGH-PERFORMING

Prioritize Critical Thinking and Other Non-Technical Skills When Building Your Team

Critical thinking—specifically problem solving—is the skill high-performing organizations cited most frequently when describing their Strategic Team. Organizations explained that critical thinking skills are needed for identifying patterns, relationships, sources and for corroborate information. One high-performing organization noted that their Strategic Analysts need to have the ability to think about problems in non-rigid ways, have a healthy skepticism, be imaginative, see the big picture, and have the foresight to ask broad questions, such as "Do we still need to be doing things this way?" Indeed, other organizations explained to us that they will always hire a candidate with a great analytical mind and a mediocre cyber background, over a candidate who has an extensive cyber background but is not a critical thinker. These organizations emphasized that while it is possible to provide technical training, it is more difficult to teach critical thinking.

A practice of high-performing organizations is to refer to NIST SP 800-181 as a guide for hiring individuals with the right Knowledge, Skills and Abilities KSA to perform Strategic analysis. The following NIST NICE SP 800-181 KSA's map to critical thinking and problem solving: S0359, A0035, A0080, A0081, A0070, A0106, A0118, A0122.

Other traits high-performing organizations either hire for or already have on their Strategic team include: intellectual independence, curiosity, tenacity, strong work ethic, inquisitiveness, the ability to let others poke holes in their analysis, recognize when they don't know something, a sense of humor, confidence to arrive at judgments without complete information, and strong interpersonal skills and emotional intelligence. Many high-performing organizations also explained that their Strategic Analysts have a desire and passion to stay current on cyber threats, geopolitics, industry developments (always reading news and blogs) and developments within their own organization.

Provide Professional Development to Learn Technical Skills and Make Connections

A practice of high-performing organizations is to send their intelligence analysts and other non-technical analysts to industry training venues and conferences to build and in some cases take introductory technical skills courses on topics such as network analysis, forensics, incident response and to make professional connections with other professionals. Employees receiving technical training or attending conference return and brief / teach their team about what they learned.

Communicate Clearly with Technical and Non-Technical Audiences

Strategic Analysts need sufficient technical acumen to communicate effectively with other technical analysts across the organization. They also need skills to communicate clearly and efficiently with non-technical audiences, specifically executive leadership. Many high-performing organizations, mostly in the Finance, Communications,

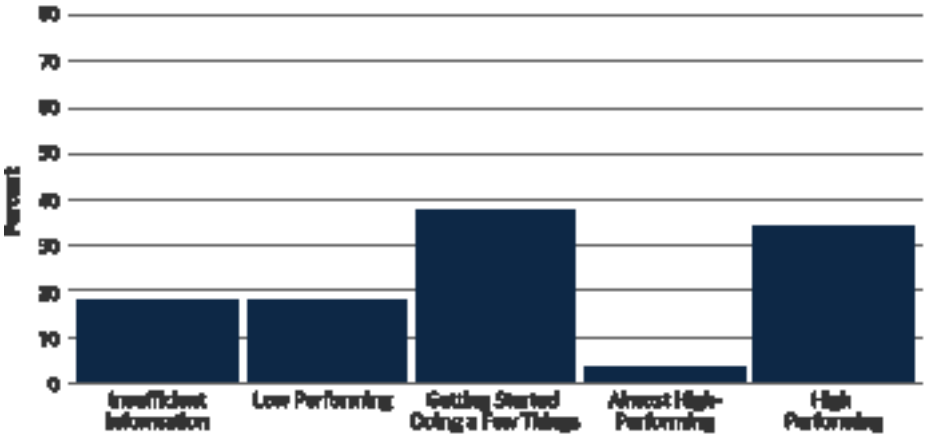
Food and Agriculture, and Government Facilities sectors stressed how their analysts are strong at presenting at different altitudes depending on the audience. They are really strong at communicating (writing and briefing) the strategic context and risk perspective to executive leadership.

STRATEGIC ANALYSIS FACTOR 5: STRATEGIC ANALYSIS TOOLS

WHAT THIS ASSESSMENT FACTOR MEANS

The organization has a combination of homegrown and off-the-shelf (as appropriate) tools to support Strategic analysis. Tools are appropriately configured, readily available, and evaluated routinely to ensure they meet organizational needs.

PERFORMANCE SNAPSHOT



Strategic Analysis Factor 5 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Over reliance on Third-Party Intelligence Provider assessments

We met organizations that rely solely on third-party intelligence providers to provide strategic analytical assessments on threat actors, industry developments and geopolitics. These organizations do not have tools and resources to conduct additional analysis incorporating third-party assessments and making them relevant to their specific organization's mission and interests. As noted earlier, we met with organizations where Strategic Analysts rely on Excel to track threats and threat actors.

Fragmentation of Tools and Knowledge

Some organizations we interviewed expressed the need for a single "pane of glass" across their systems that enables analysts to search and conduct analysis at all levels. Other organizations are hoping to purchase or create a knowledge management system that allows Strategic Analysts to access data and conduct analysis using a system like Palantir. That said, some organizations expressed that tools should not dictate or put Strategic analysts in a box in terms of how they perform his/her job. A tool is one instrument assisting in the entire Strategic analysis process.

TIP

THE PROMISE OF MACHINE LEARNING

Incorporating machine learning into Strategic analysis will become prevalent in the future as organizations find more efficient ways to complement threat analysis by gathering data from Human Resources, Business Intelligence, Physical Security, Legal, Marketing, Finance, Technology Development, Corporate Leadership and external technical and non-technical data about Geopolitics, Industry Developments, and Technology and Innovation. Our Machine Learning and Cyber Intelligence Implementation Guide discusses, among other thing, how machine learning can enhance Strategic analysis on challenges such identifying attack commonalities, associations between threat actors and events, or predicting possible insider threats, or geopolitical events in a country.

GETTING TO HIGH-PERFORMING

Regularly Evaluate Strategic analysis tools

A practice of high-performing organizations is to regularly evaluate Strategic analysis tools to ensure they meet current and future organizational needs. Evaluation leads to purchasing or building homegrown customized tools to make data and subsequent analysis relevant to the organization's mission. Before incorporating new tools on their network, these organizations ensure the tools are appropriately configured to integrate well with other tools.

Use a Mix of Tools

Since strategic analysis is grounded in threat analysis and other non-traditional data sources, technical tools used for Threat analysis are certainly useful for Strategic analysis.

Most high-performing organizations additionally employ a good mix of analytical and visualization tools. Common Strategic analysis tools utilized by high-performing organizations we met include: ELK Stack, Maltego, MISP, I2 Analyst Notebook, Palantir, Tableau, Adobe InDesign and Photoshop for graphics. As noted in section Threat Analysis Factor 5, we captured lists of open-source and paid for tools organizations are using. A chart showing these tools can be found in appendix ABC.

IMPROVE YOUR PERFORMANCE

- Regularly evaluate Strategic analysis tools to ensure they meet current and future organizational needs.
- Before incorporating new tools on your network, ensure they are appropriately configured to integrate well with other tools.
- Use a mix of analytical and visualization tools, such as ELK Stack, Maltego, MISP, I2 Analyst Notebook, Palantir, and Tableau.

STRATEGIC ANALYSIS FACTOR 6: ANALYTICAL TRADECRAFT APPLIED TO CYBER INTELLIGENCE ANALYSIS

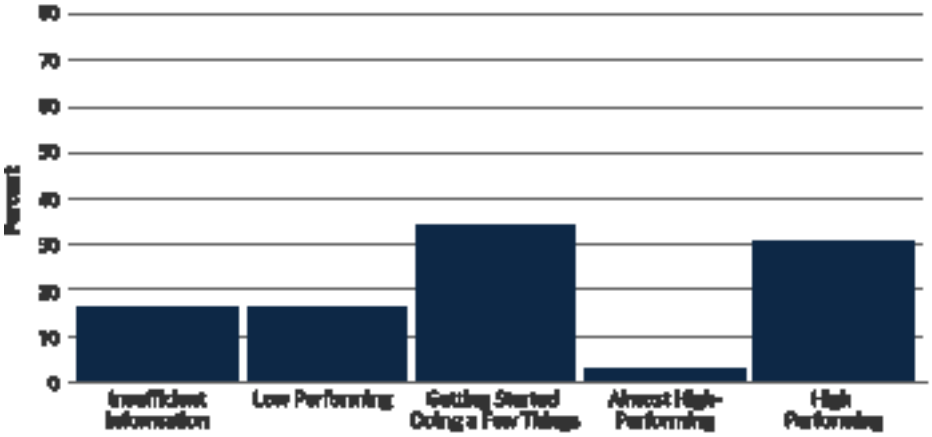
WHAT THIS ASSESSMENT FACTOR MEANS

The organization has a repeatable process for incorporating structured analytical techniques into its cyber intelligence analysis. The organizations writes cyber intelligence reports that describe the quality of and credibility of sources and data methodologies, use estimative language (expressions of likelihood and confidence) are customer relevant, and incorporate visual information where appropriate. This process is reviewed and updated regularly.

HIGH-PERFORMING ORGANIZATION

The organization has a repeatable process for incorporating structured analytical techniques into its cyber intelligence analysis. The organizations writes cyber intelligence reports that describe the quality of and credibility of sources and data methodologies, use estimative language (expressions of likelihood and confidence) are customer relevant, and incorporate visual information where appropriate. This process is reviewed and updated regularly.

PERFORMANCE SNAPSHOT



Strategic Analysis Factor 6 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of Formalized Process for Incorporating Analytical Tradecraft

At least five organizations we interviewed do not apply any analytical tradecraft into their analysis process. We met organizations not incorporating analysis of alternatives via structured analytical techniques or using estimative language (expressions of likelihood and confidence) in intelligence assessment reports to leadership. Organizations also do not include source descriptors and/or source validation, intelligence gaps and uncertainties, and the impact of intelligence gaps and uncertainties on assessments and judgments.

Other organizations explained they lack resources (people and time) to incorporate analytical techniques, yet recognize the importance of analytical tradecraft. Indeed, some organizations explained that their team could have benefited from learning about intelligence analytical standards earlier, as they have worked with others that have written assessments that jumped to conclusions, lacked analytical thought, and were personality driven.

Most organizations we met attempt to incorporate, albeit on an ad-hoc basis, analytical tradecraft into workflows, specifically for performing Strategic analysis. For these organizations, there is no agreed upon policy/procedure for how to incorporate analytical tradecraft into assessments. In other words, there is no formalized process in terms of when and how to include source descriptions and validation, expressions of likelihood and confidence levels. Additionally, one organization explained that they will only occasionally perform Red Teaming, Analysis of Competing Hypotheses (ACH), or Devil's Advocacy for Strategic analysis. Another organization talked about how only some analysts (not all) use estimative language and include intelligence gaps and source validation.

IMPROVE YOUR PERFORMANCE

- Apply as appropriate, structured analytical techniques on top of and in addition to cyber threat frameworks, such as the Lockheed Martin Kill Chain and Diamond Model when performing Strategic analysis
- Avoid combining confidence in judgements (Confidence Level) with a degree of probability of an event or development (Very Likely) in the same sentence. Make them two sentences.

TIP

ANALYSIS OF ALTERNATIVES DEFINED

"The systematic evaluation of different hypotheses to explain events or phenomena, explore near-term outcomes, and imagine possible futures to mitigate surprises and risks." (ICD 203)

MAKE INFORMED DECISIONS ABOUT HOW TO APPLY ANALYTICAL TRADECRAFT

It is generally not realistic to apply structured analytical techniques and analytical standards to every threat report. That is simply not feasible or logical when it comes to the speed and demands of mission (such network defense, cyber hygiene and incident response) and other fast-paced (machine and human) generated analysis that leads to immediate and near-term actionable cybersecurity focused recommendations. For example, it doesn't make sense to perform a structured analytical technique or write a report with source validations that suggest patch management or block an IP address. Just do the patch and block the IP address first, and then draft a weekly report or perform analysis later addressing the particular event, anomalous behavior and mitigation actions taken. Organizations should make informed decisions, pending resources and timing based on threat/event criticality if incorporating analytical tradecraft into Threat analysis is feasible either before or after mitigation actions are taken. Most reports, at least at the operational and strategic analysis level, should include estimative language, source descriptors or source validation, confidence level and intelligence gaps.

GETTING TO HIGH-PERFORMING

Adopt ICD 203, 206 and Structured Analytical Techniques into your Cyber Intelligence Practices

A practice of high-performing organizations is to use Intelligence Community Directive (ICD 203) as the foundation and guideline for applying analytic standards to their cyber intelligence analysis workflows. At least 20 organizations we interviewed across Finance, Energy, Government Facilities, and Commercial Facilities sectors incorporate analytical standards into cyber intelligence analysis workflows, specifically when performing Strategic analysis. While some processes are not truly formulized in these organizations, they do apply structured analytical techniques on top of and in addition to, cyber threat frameworks such as the Lockheed Martin Kill Chain and Diamond Model. Structured analytical techniques are used to help the analyst be mindful of cognitive biases, logical fallacies and not "run on automatic".

Some organizations we met explained that they use these structured analytical techniques: Brainstorming/Ideation sessions, Key Assumptions Checks, ACH, Future's Analysis, Devil's Advocacy, Red Teaming, Decision Trees and What If Analysis. We met with Cyber Intelligence Teams that conduct Root Cause Analysis; and one organization brought in specialists to help their team perform Root Cause Analysis on a particular event. Other organizations bolster analytic rigor by purposely pairing intelligence analysts with data scientists on threat actor behavior deep dives, emerging threats and opportunities assessments. Another high-performing organization ensures that each of its Strategic analysts are giving a copy of the *CIA's A Tradecraft Primer: Structured Analytical Techniques for improving Intelligence Analysis*. They also post ICD 203 standards on their internal Wikipage.[19]

BEST PRACTICES

HUMAN-CENTERED DESIGN METHODS

Organizations should explore human-centered design techniques such as Affinity Clustering, Bull's Eye Diagramming, and Importance/Difficulty Matrixes when evaluating threats, risk and opportunities. See the *Luma Institute. Innovating for People. Handbook of Human-Centered Design Methods.*

19 A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. March 2009. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf
Intelligence Community Directive 203. Analytic Standards. 2 January 2015. https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

Some Strategic Analysts incorporate expressions of likelihood and confidence in their intelligence assessments. Strategic Analysts in at least 13 high-performing organizations (Defense Industrial Base, Government Facilities, Information Technology and Communications sectors) are doing this and also include a scale or description describing the meaning of likelihood degrees and confidence levels. A number of high-performing organizations are pulling from the ICD 203 expression of likelihood scale and then use High, Medium/Moderate, Low to describe confidence levels for assessments or judgments in reports. A practice of high-performing organization is to also include intelligence gaps, source descriptors / characterization and source validation in both threat analysis and strategic analysis reports. Of the organizations we met that are doing this, source validation ratings are usually based off of the Admiralty Code.

TIP

Products expressing an analyst's confidence in judgements (Confidence Level) should *not* combine a degree of probability of an event or development (Very Likely) in the same sentence. Make them two sentences. (ICD 203)

For example, don't write this:

- "We assess with moderate confidence that cyber espionage malware ABC is linked to Threat Group XYZ and that its spear-phishing emails targeting machine learning experts will almost certainly continue in the near term."

Write this instead:

- "We assess with moderate confidence that cyber espionage malware ABC is linked to Threat Group XYZ."
- "Their use of spear-phishing to target machine learning experts in our organization and industry will almost certainly continue in the near term."

"If you can't explain it simply, you don't understand it well enough."

—Albert Einstein

Reporting and Feedback

Communicating with Teams and Decision Makers

INTRODUCTION

Reporting and Feedback is the communication of and subsequent feedback to analysts regarding their products and work performance. It identifies intelligence requirements and intelligence gaps.

REPORTING AND FEEDBACK FACTORS

In evaluating the state of the practice of cyber intelligence in terms of Reporting and Feedback, we considered the following factors:

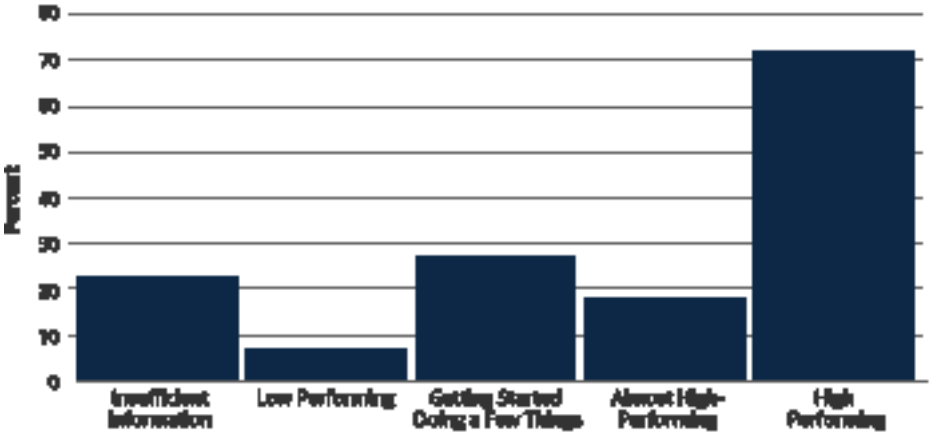
1. Cyber Intelligence Report Types
2. Actionable and Predictive Analysis
3. Leadership Involvement
4. Influence on Decision Making
5. Feedback Mechanisms for Analysts
6. Influence of Feedback on Data Gathering and Analysis
7. Satisfying Intelligence Consumers
8. Capturing Return on Investment

REPORTING AND FEEDBACK FACTOR 1: CYBER INTELLIGENCE REPORT TYPES

WHAT THIS ASSESSMENT FACTOR MEANS

The organization applies a strategy and timeline to generate reports from a varied product line. The product line addresses customer needs, is stored, and can be accessed by internal and external partners as appropriate.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 1 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of Resources and Leadership Strategy to Produce Cyber Intelligence Reports
We met organizations not producing cyber intelligence reports. In other words, there is no report product line addressing internal business units or external customers' requirements or needs. Most organizations not producing threat analysis or strategic analysis reports explained that they do not have enough people and time to generate reports. With such limited resources, these teams can only be focused on cybersecurity issues associated with cyber hygiene and incident response.

At least ten organizations explained that they do produce threat analysis and strategic analysis reports, however it is on an ad-hoc basis. There is no formulized schedule for report production or timeline for creating different report types. For other organizations, reports are simply event-driven emails. Other teams we met discussed how there is no leadership (CISO and up) buy-in, vision or strategy to create Cyber Intelligence Reports. More specifically, these teams discussed how there is no strategy for a Cyber Intelligence product line and that they have received little guidance from leadership on requirements, timelines and layouts for cyber intelligence reports.

Some organizations discussed challenges pertaining to delays in the review and dissemination process of operational and tactical level Cyber Intelligence reports. These organizations talked about workflow issues and the high-number of coordinators. Today's reports are being disseminated about yesterday's issues. Indeed, an organization talked about how 24 hours is ideal for them creating and disseminating tactical and operational reporting, but that is rarely achieved as four days is actually considered quick.

IMPROVE YOUR PERFORMANCE

- Create a strategy for a Cyber Intelligence product line that includes timelines and layouts for cyber intelligence reports.
- Build a varied Cyber Intelligence product line that addresses immediate needs, CISO and Executive Leadership requests, as well as specific internal business units and external customers and partner requests.

TIP

Reasons for why there is no leadership buy-in for report production could vary from budget constraints to a lack of understanding about cyber intelligence.

GETTING TO HIGH-PERFORMING

A practice of high-performing organizations is to have a varied Cyber Intelligence product line. These organizations have threat (operational and tactical) analysis and strategic analysis reports that address immediate needs, CISO and Executive Leadership requests, as well as specific internal business units and external customers and partner requests. SLAs and SOPs hold these organizations to their commitments and ensure that decision makers and other readers know what to expect. We met with organizations that produce reports daily, weekly, monthly, quarterly and annually. Study participants reported producing a variety of reports / briefings, including

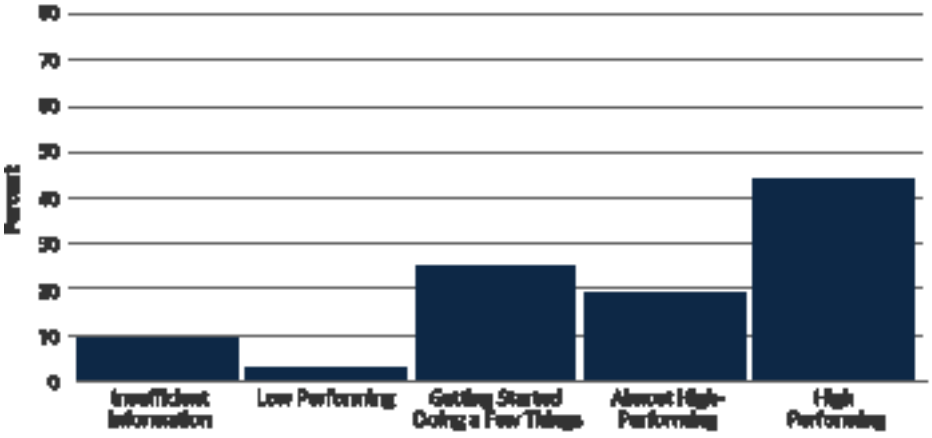
- Vulnerability Reports
- Threat Analysis Reports
  - Threat Actors
  - Threats to Sectors
  - Malware Analysis
- Threat Priority Lists
- Bi-Annual and Annual Threat Assessment
- Targeting Packages for Pen Testing Team
- Vulnerability Reports
- Technology Program Threat Assessments
- Geopolitical Events
- Industry Developments
- Patch Status Reports
- Anti-Virus Reports
- Threat News
- Executive Reports
- Future Threat Analysis Reports
- Daily Sector Reports
- Tactical Reports: Articles, indicators, and behavior summary
- Incident Reponses Reports
- After Action Reports
- Briefings to CISO/CSO twice a week
- Monthly Executive Council Briefings
- Bi-annual Board Briefings

REPORTING AND FEEDBACK FACTOR 2: ACTIONABLE AND PREDICTIVE ANALYSIS

WHAT THIS ASSESSMENT FACTOR MEANS

The organization has a mechanism for reporting actionable and predictive analysis when necessary. Cyber intelligence reports include predictive analysis focusing on near- and long-term threats to the organization. Measures for evaluating prediction accuracy are in place.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 2 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of Predictive Analysis

Predictive analysis is performed and incorporated into longer-term Strategic reports pertaining to threats, risks, and opportunities involving organizational vital interests. At least 15 organizations interviewed do not include predictions in their Cyber Intelligence Reports. These organizations generally have zero to little resources (people and time) to support a Strategic analytical capability. These organizations were represented in the Finance, Health and Public Health, Government, Academic and Energy sectors. Some organizations also explained they probably could perform predictive analysis; however they are not collecting the right data to support that type analysis. Other organizations remarked that they do include predictive analysis in Cyber Intelligence reports, however it is done inconsistently. Many organizations we met stated that they have no measures in place to evaluate for prediction accuracy.

At least four organizations interviewed do not include actionable recommendations in their Cyber Intelligence reports. Additionally, other organizations explained that actionable recommendations are designed to answer only tactical level SIRs and are only for cybersecurity operations, mitigations and cyber hygiene which usually falls to the SOC. One organization explained that they do not put formal recommendations into Strategic reports because the cyber landscape changes so fast and is too dynamic. The organization is concerned about recommending an action that has been overcome by events.

IMPROVE YOUR PERFORMANCE

- Include Actionable Recommendations in Key Judgments or in Bottom-Line-Up-Front sections of Cyber Intelligence reports.
- Incorporate analytical predictions into strategic reports pertaining to threats, risks and opportunities involving organizational vital interests

GETTING TO HIGH-PERFORMING

Include predictions and actionable recommendations in Cyber Intelligence Reports

A practice of high-performing organizations is to incorporate predictions into Strategic reports pertaining to threats, risks and opportunities involving organizational vital interests. We met with Cyber Intelligence teams predicting when their own emerging patent-pending technology will become profitable, and how that aligns with the organization's own future business plans. We also interviewed Cyber Intelligence teams producing future country risk assessments, predicting what and how new technologies will impact the organization' business operations, and how new tools enable the organization to be proactive against threats. A practice of high-performing organizations is to also include predictions into more time-sensitive operationally focused reports about threat actor intentions, capabilities, operations and campaigns. Some organizations produce reports that predict whether a specific threat actor will target the organization, or malware types that could cause the most damage to the organization. To assist with prediction analysis, another practice of high-performing organizations is for their Cyber Intelligence team to work closely with data scientists (data scientists are either part of the cyber intelligence team or are co-located within the Fusion Center). These organizations "apply data science to actions on objectives" to determine a risk score associated with a given or proposed action. Time-permitting, structured analytical techniques such as *Alternative Futures Analysis*[20] or Human-Centered Design Techniques such as *What's on Your Radar* and *Creative Matrix* can assist prediction analysis.[21]

20 https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

21 Luma Institute. Human-Centered Design Thinking.

Many high-performing organizations include actionable recommendations in all their reports, even quarterly reports describing threat actor TTPs. Others described the benefits of including actionable recommendations depends on the situation and audience. For these organizations, actionable recommendations are mostly used to support cybersecurity and cyber hygiene needs based on data and subsequent analysis collected at the tactical/technical SIR level. These are more immediate – near term actions/mitigations/controls such as blocking IP addresses, implementing Network IDS rules, patching vulnerabilities, or searching for specific hashes or strings. Additionally, a practice of high-performing organizations is to not write a report recommending a particular course of action at the SIR level. Rather these organizations take the necessary course of action first to protect the organization, and then later write a daily or weekly after-action report. Another practice of high-performing organizations is to have daily operations briefings or standups in the Fusion Center in front of the CSO/CISO. The briefings include proposed actionable recommendations, or actions that have already been taken to protect the organization over the course of the day. Finally, actionable recommendations should be included in a Cyber Intelligence reports' Key Judgements section or in a Bottom Line Up Front..

TIP

A report without recommendations can still be useful. These reports add value with their insight and context about threat activity.

Describing Actionable Recommendations at the tactical, operational and strategic level.

Threat analysis leads to actionable recommendations at an operational and tactical level in response to threats, threat actors, and campaigns. Possible actionable recommendation examples at the tactical level could be: block this IP, patch these vulnerabilities, or disable a particular feature in an application. Actionable recommendations at the operational level follow from internal and external technical telemetry evaluation regarding a specific threat actor. Possible actionable recommendation examples at the operational level might be: updating organizational-wide password rules, segmenting controls systems with a DMZ from the public facing internet and business networks, incorporating a DLP, creating a honeypot, putting sensitive technology research on separate servers, or engaging the Collection Management Team to task new collection on a specific threat actor.

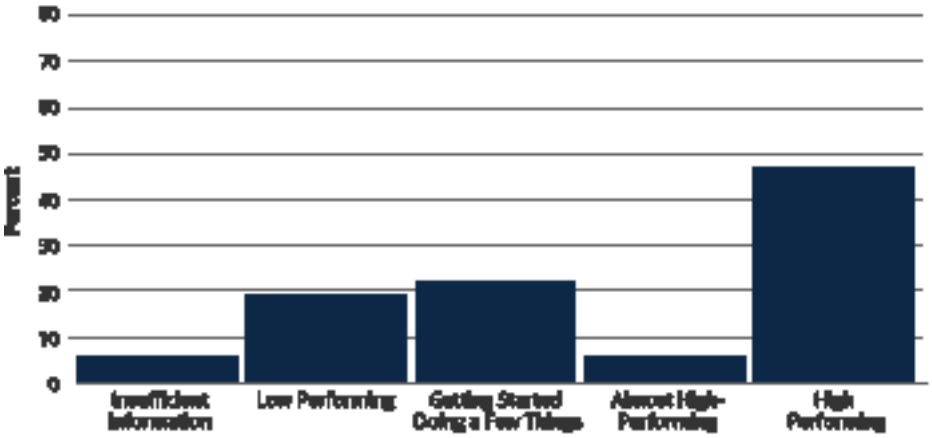
Strategic analysis is the process of conducting holistic analysis on threats AND opportunities. Holistically assessing threats is based on analysis of threat actor potential, organizational exposure and organizational impact of the threat. One might also perform Strategic analysis to provide deep clarity on the who and why behind threats and threat actors. Strategic analysis goes beyond threat analysis to incorporate analysis regarding emerging technologies and geopolitics that may impact/provide opportunities for the organization now and in the future. It can be actionable, yet is based more on analytical judgments, enabling executive leaders to make risk-based decisions pertaining to organizational vital interests. Possible actionable recommendation examples at the strategic level might be: not opening an office in a foreign location, merging with one organization and not the other, using a particular supplier, switching to new a software provider, or investing in new technology.

REPORTING AND FEEDBACK FACTOR 3: LEADERSHIP INVOLVEMENT

WHAT THIS ASSESSMENT FACTOR MEANS

The organization's leadership influences the cyber intelligence effort by consistently providing items of interest, suggestions, praise, and format and production timeline requests for functional and strategic analytical products.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 3 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Reactionary Involvement from Leadership

Organizations commonly struggle with leaders who get involved only when there is a crisis. Leaders at these organizations take a "no news is good news" approach to cyber intelligence; at best, they may request a briefing during a crisis, ask for followup information after an incident, or express appreciation that an incident has not happened. Cyber intelligence teams facing this challenge expressed a desire for leadership to be more active with setting strategy, specifically in risk management and setting PIRs.

IMPROVE YOUR PERFORMANCE

- Send cyber intelligence reports to your organization's board of directors.
- Create and perform a "road show" to showcase your team's capabilities.

GETTING TO HIGH-PERFORMING

Involve Your Organization's Board of Directors

High-performing organizations frequently have a very involved board of directors that understands the importance, if not the details, of cyber intelligence and cybersecurity. For some organizations, the CISO or CTO sits on the board or has close contact with the board and can be an advocate for the cyber intelligence team. In other cases, the cyber intelligence team sends reports to the board. One team mentioned that they instituted this practice after a high-profile breach.

Be Your Own Advocate

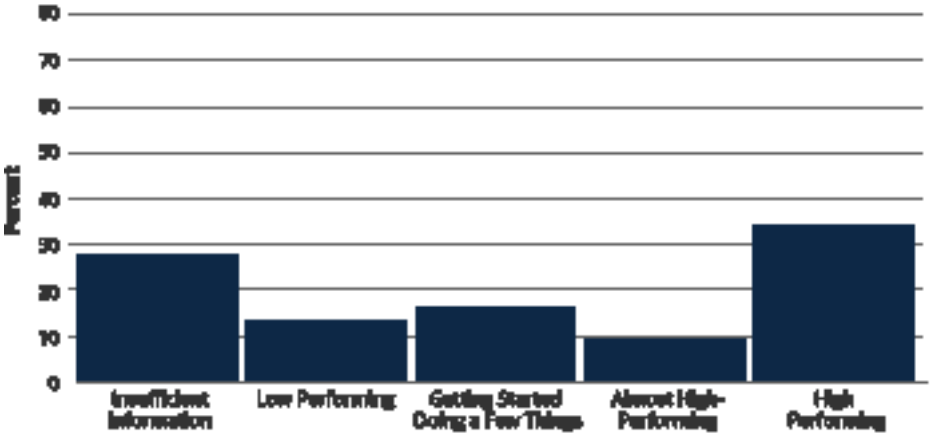
To build relationships with leaders, teams at high-performing organizations take proactive steps to showcase their work. One team developed a road show it performed for departments across the organization to familiarize those groups with their capabilities and successes. The team was initially discouraged and somewhat exhausted by what they described as a huge education process, but in the end, the payoff was worth it. That team has buy-in from senior leadership, who helps them get into hard-to-crack directorates.

REPORTING AND FEEDBACK FACTOR 4: INFLUENCE ON DECISION MAKING

WHAT THIS ASSESSMENT FACTOR MEANS

The organization's leadership incorporates cyber intelligence reporting into its decision making on issues relating to its Environment, Data Gathering, Threat analysis, Strategic analysis, cyber security, and overall risk management and business decisions regarding organizational vital interests.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 4 Performance Snapshot The graph on the left shows how participants in the study are performing in this assessment factor.

COMMON CHALLENGES

Lack of Leadership Knowledge About Cyber Intelligence

Some organizations explained that their leadership (specifically at the board level) does not understand cyber or the return on investment cyber intelligence brings to the organization. Teams on these organizations commented that they are constantly educating leadership about cyber. They do this to enable leadership to ask the right questions and know what to do with cyber intelligence when it is presented to them. Other teams explained that leadership only uses cyber intelligence when it involves technology purchase decisions. One Cyber Intelligence team supporting a large organization commented that their leadership does not seem to be doing anything on a strategic level with cyber intelligence reports the team produces.

Lack of Access to Leadership

As mentioned in earlier sections, some cyber intelligence teams lack consistent access to the CISO and board. For example, one team has briefed its CISO just three times in the last seven years, and another was briefing the board for the first time in ten years. Additionally, some organizations within the Finance, Defense Industrial Base, and Academic Sectors explained that they lack information and/or have zero visibility into how leadership actually uses cyber intelligence to enhance decision making. There is no feedback.

IMPROVE YOUR PERFORMANCE

- Senior leadership should champion the Cyber Intelligence team by referencing the team's reports in speeches and talks across the organization
- Use the Cyber Intelligence team as a testing ground for new tools and technologies that could later be adopted and scaled across the entire organization
- Keep metrics and feedback on leadership, partner and customer usage and implementation of the Cyber Intelligence team's recommendations.

GETTING TO HIGH-PERFORMING

Use cyber intelligence to enhance decision making

Leadership using cyber intelligence to enhance decision making is a practice of high-performing organizations. Some teams we met explained how its leadership - CSO/

CISO and up through C-Suite executives and the board – is constantly refining how the organization conducts business based the Cyber Intelligence team's work. Indeed, one organization explained how senior executives meet every day to discuss, among other things, cyber issues and the cyber intelligence team's analysis. We met with Cyber Intelligence teams that explained how their CEO champions the Cyber Intelligence team by referencing the team's reports in speeches and talks across the organization. Other teams described how leadership of different business units regularly receive cyber intelligence reports.

We also met organizations where the Cyber Intelligence team is considered such a trusted authority that they are constantly being pulled into internal organizational-wide business unit leadership meetings. For instance, one organization is tapping its Cyber Intelligence team's expertise to help build the organization's insider threat program.

Cyber Intelligence teams across the Communications, Commercial Services, Government Facilities and Financial Services Sectors explained how leadership leverages their reporting and recommendations pertaining to tool and technology purchases that will better protect the organization. For example, Cyber Intelligence teams we interviewed have influenced leadership to purchase passive DNS scanning tools and bitcoin wallet analysis tools. Another practice of high-performing organizations is to use the Cyber Intelligence team as a testing ground for new tools and technologies that could later be adopted and scaled across the entire organization.

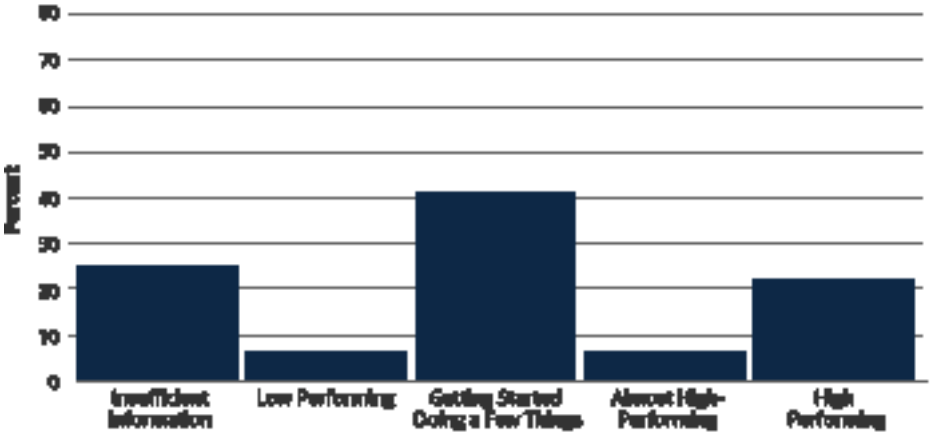
Organizations provided other examples of how Cyber Intelligence is influencing their leadership's decision making: helping executives, the board and lawyers understand who/what is and will be the biggest threats to the organization; leadership requiring the organization to review and enhance existing controls; opening offices in foreign locations; re-prioritizing resources and budgets; increasing support to new or existing projects; providing recommendations on vendor purchase options; and acquisition support. Finally, a practice of high-performing organizations is to track, keep metrics and feedback on leadership, partner and customer usage and implementation of the cyber intelligence team's recommendations.

REPORTING AND FEEDBACK FACTOR 5: FEEDBACK MECHANISMS FOR THE CYBER INTELLIGENCE TEAM

WHAT THIS ASSESSMENT FACTOR MEANS

Formal and informal mechanisms are in place for customers, collaborators, and stakeholders to provide feedback to the Cyber Intelligence Team.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 5 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Lack of Feedback Mechanisms

At least 13 organizations we interviewed have no formal mechanisms in place for analysts to receive feedback from leadership, customers, collaborators and stakeholders before and after a report is published. Most cyber intelligence teams interviewed receive feedback on their intelligence reports informally before and after publication. Informal mechanisms include email, peer-to-peer reviews, conversations and leadership reviews. Formal mechanisms may range from websites, portals, wikis, surveys and annual or biannual performance reviews. These Cyber Intelligence teams explained that they are sometimes unclear if they are meeting leadership, customer, collaborator and stakeholder expectations. For other organizations, specifically in the Finance and Energy sectors, email is the primary and often only mechanism analysts receive feedback. Still other organizations said that external customers and stakeholders as well as internal business units do not regularly provide feedback on their Cyber Intelligence reports. This may be due however to the fact that the published intelligence reports lack a comment or feedback section. Lastly, some Cyber Intelligence teams commented that peer-review and coordination processes are too extensive, preventing and holding up timely report publication and dissemination.

IMPROVE YOUR PERFORMANCE

- Use a combination of portals, wikis, surveys, email, peer-to-peer conversations, annual reviews, and engagement teams for the Cyber Intelligence team to receive feedback.
- Append surveys or feedback links to finished Cyber Intelligence reports.
- Create a system, policy and culture where rapid feedback to draft reports is the norm so originating analysts can quickly course correct and make necessary adjustments.

GETTING TO HIGH-PERFORMING

Create multiple ways analysts receive feedback before and after report publication

A practice of high-performing organizations is using multiple informal and formal mechanisms to receive feedback. Feedback may be in the format of questions or comments about reports, new requirements, ideas for new sources, and suggestions for analytical and workflow improvements. We met Cyber Intelligence teams using a combination of portals, wikis, surveys, email, peer-to-peer conversations, annual reviews, and engagement teams to interact with/receive feedback from organizational leadership and other internal and external customers. Having a distinct Internal and External Relationship Engagement Team (as noted in Environmental Context Factor 5: Program Management Team: Internal and External Relationship) , that is co-located with the Cyber Intelligence Team as part of an organization's Fusion Center is best practice. More specifically, it enables Cyber Intelligence teams to be readily available for contact by leadership, internal and external customers, collaborators and stakeholders at any time. In addition to the ongoing daily engagement with internal and external customer, one organization's Cyber Intelligence team holds bi-annual

meetings/conferences with ALL customers and stakeholders together about cyber issues, where they solicit feedback on their performance.

Another practice of high-performing organizations is to append surveys to finished Cyber Intelligence reports. Surveys inform the Cyber Intelligence team about what's working, not working, and internal and external customers interest in reports. Other organizations have created a feedback link in every published report. A method that one high-performing organization has adopted is the creation of a pop-up window on the Cyber Intelligence team's website where readers can enter feedback or ask questions. As noted in Data Gathering Factor 4: Technology for Data Gathering, Microsoft's Yammer tool is useful as both an organizational social networking tool and as an incident tracker. Yammer enables the Cyber Intelligence team to receive feedback from across the organization in a real-time social network type environment. Employees (to include C-Suite Executives for instance) have the option to like, share, reply, praise, update posts and also create polls.

Commit to Peer Reviews

A practice of high-performing organization is to have a rigorous, yet vigorous peer review process to ensure the timely publication of reports. One organization explained that they have instituted a cultural practice of providing rapid feedback to draft reports so originating analysts can quickly course correct and make necessary adjustments. For another organization, they have two peers review all reports, one peer is on the Cyber Intelligence team and the other works outside of the Cyber Intelligence team. High-performing organizations also ensure draft reports are reviewed by supervisors and direct managers before publication and dissemination.

Don't wait to publish the report

A characteristic of high-performing organizations is following the rule of thumb that the 100% solution is less relevant when only a 70% solution is possible. Waiting to publish a report or disclose until you have the complete picture tends diminish operational relevance. In other words, the law of diminished returns comes into effect and report impact attenuates the longer you wait. It is certainly more than okay, in fact regarded, to publish and openly note your team only has the 70% solution at this point.

REPORTING AND FEEDBACK FACTOR 6: INFLUENCE OF FEEDBACK ON DATA GATHERING AND ANALYSIS

WHAT THIS ASSESSMENT FACTOR MEANS

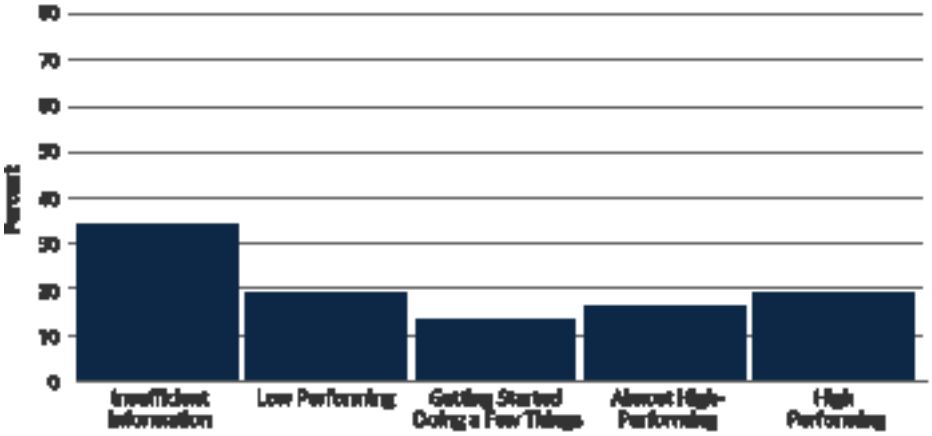
Formal and informal processes ensure that data gathering and analysis efforts are influenced by feedback received from customers, collaborators and stakeholders.

TIP

IMPROVING PEER REVIEW EFFICIENCY

One suggestion to improve peer review-efficiency is a policy where reviewers are allotted a given amount of time to review/edit a draft report before being automatically skipped in the process. Mandatory reviewers are established and cannot be skipped. For example, cyber issues requiring less than 24 hours for a report should naturally and generally have a short list of reviewers. Individuals are automatically alerted about the report, and are only allotted 1 hour (for example) to provide feedback on the report. Feedback options could range from approve, disprove with suggestions, approve with corrections etc. Longer review time-frames are report-type dependent. The entire process should be visible and auditable across the Fusion Center so everyone knows who contributed and provided feedback, and who was automatically skipped. In the future, it is foreseeable that such a system could learn and provide suggestions as to which individuals across an organization should review a draft report based on time sensitivities, peoples' availability and team expertise.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 6 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Cyber Intelligence Teams receive little feedback regarding their analysis and data gathering

If feedback mechanisms are not in place for analysts to receive feedback (Reporting and Feedback Assessment Factor 5), then there is no way for feedback to influence the Cyber Intelligence team's data gathering and analysis efforts. As noted earlier in the Reporting and Feedback Assessment Factor Five section, that was certainly the case with a number of organizations we interviewed, mechanisms were not in place. For this particular assessment factor, at least 11 Cyber Intelligence teams across the Finance, Academic, Health and Public Health, and Information Technology sectors explained they receive zero to very little feedback from leadership, customers, collaborators, and stakeholders that influence the team's data gathering and analysis efforts. When Cyber Intelligence teams do not receive feedback, (either in the Evaluation and Feedback step in the Traditional Intelligence Cycle or via continuous feedback implied/encouraged within all components of Cyber Intelligence Framework) the Cyber Intelligence team's performance suffers. And your organization's ability to better protect itself may also suffers. More specifically, when teams are not receiving new or updated Intelligence Requirements, the data they are collecting and subsequently performing analysis on, may no longer be relevant. New threats and risks emerge every day that could be missed.

That said, at least three organizations interviewed explained that feedback from leadership, customers, collaborators and stakeholders can influence the creation of new requirements, specifically SIRs at the more technical/tactical level. One Cyber Intelligence team discussed how leadership and other stakeholders can influence data collection and analysis, but not necessarily the team's workflow.

GETTING TO HIGH-PERFORMING

Take Action Based on Feedback

Your Cyber Intelligence team's performance depends on feedback from leadership, customers, collaborators and stakeholders. At least 16 organizations we interviewed across the Information Technology, Finance, Food and Agriculture, Communications, Energy, and Government Facilities sectors explained that feedback from leadership, customers, collaborators and stakeholders influences the cyber intelligence team's data gathering and analysis efforts.

IMPROVE YOUR PERFORMANCE

- Create a new position for an analyst to be the central point for all requirements – a starting point for a Collection Management Team.
- Solicit feedback from leadership, customers, collaborators, and stakeholders to improve the Cyber Intelligence Team's performance.
- To build trust, be honest in reports: Explain areas where you lack information, have intelligence gaps, or lack confidence in judgments.

TIP

This Reporting and Feedback Assessment Factor Six is closely related, but is not the same as Reporting and Feedback Assessment Factor Five, *Feedback Mechanisms for Analysts*. The distinction between these two assessment factors is that Report and Feedback Assessment Factor Five assessed if organizations have mechanisms in place for analysts to receive feedback. Reporting and Feedback Assessment Factor is more concerned with whether feedback analysts receive, **actually influences data gathering and analysis efforts.**

Organizations discussed how leadership, internal business unit and external customers feedback enabled the Cyber Intelligence team to identify new intelligence requirements and subsequent intelligence gaps. New requirements lead to changes in internal data collection strategies, the passing of new requirements to third-party intelligence providers, and subsequent analysis of that data. Because one organization received so many requirements, the organization created a new position for an analyst to be the central point for all requirements – a starting point for a collection management team. We also met with organizations that described how feedback from leadership enhanced the cyber intelligence team's strategy and workflow. For instance, one high-performing organization discussed how leadership's feedback led to an extensive review and update of how all tactical alerts were created and disseminated. Other organizations described how feedback identified gaps that could be filled with better data gathering and analysis tools, leading to new budget requests. Some cyber intelligence teams also discussed that feedback influenced not just content, but the format and manner in which the intelligence reports are presented to leadership and customers.

Build trust by being transparent

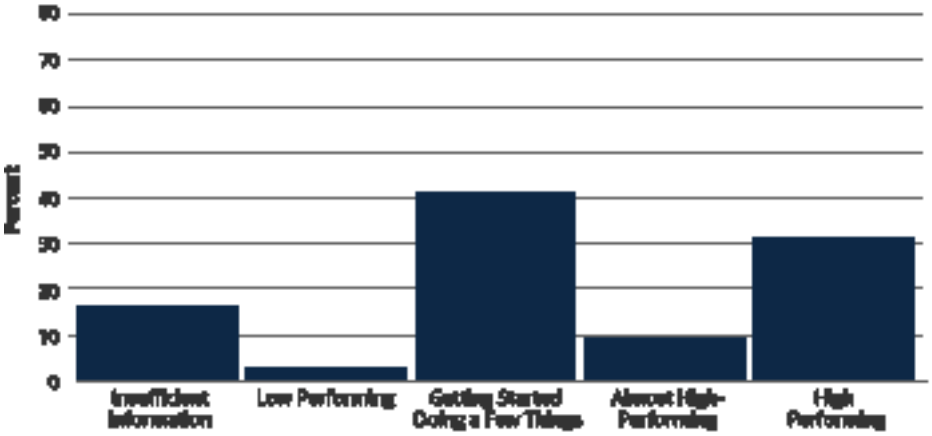
Being transparent is a practice of high-performing organizations. In other words, publishing a Cyber Intelligence report on an important cyber issue that also clearly explains areas where you lack information, have intelligence gaps or are less confident in judgments is a best practice. Again, 100% solutions are less relevant when only 70% solutions are possible. Don't wait to disclose or release your report. Release it and continue to acquire the information you need. Being transparent creates trust with leadership, customers, collaborators and stakeholders. Trust is the bedrock for receiving meaningful feedback that can influence data gathering, analysis and overall strategy. Being transparent builds stronger relationships and understanding. With better understanding, Cyber Intelligence analysts can start predicting questions, and answer them before they are even asked.

REPORTING AND FEEDBACK FACTOR 7: INFLUENCE OF FEEDBACK ON DATA GATHERING AND ANALYSIS

WHAT THIS ASSESSMENT FACTOR MEANS

The organization has formal and informal processes to consistently ascertain whether consumers are satisfied with the Cyber Intelligence team's performance, specifically the quality, quantity, and timeliness of cyber intelligence reports.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 7 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Cyber Intelligence Teams Struggle to know if they are satisfying consumers

As with Cyber Intelligence analysts needing feedback to improve data gathering and analysis, organizations should build mechanisms to know if their consumers are satisfied the Cyber Intelligence team's performance. Consumers can consist of internal and external leadership, collaborators, customers, and stakeholders. Cyber Intelligence teams we met struggled knowing if consumers were satisfied with their performance and the quality, quantity and timeliness of their products. At least ten teams interviewed that they are unable to consistently know if their consumers (internal and external) are satisfied with their Cyber Intelligence reports. These organizations explained that while consumers may occasionally provide feedback, they did not have a formulized and repeatable process established, or tools such as a website, survey, portal or wiki to ascertain consumer feedback. Indeed, one team talked about how they are constantly trying to read the tea leaves to figure out how consumers will interpret reports they produced.

Other Cyber Intelligence teams explained that their organization had yet to create a formal method to track and document that feedback. Some Cyber Intelligence teams keep metrics on the number of reports produced, yet do not track if/how the reports produced meet consumer requirements. Lastly, it was mentioned to again to the SEI team that consumers may not know enough about cyber to know if they are satisfied or not.

GETTING TO HIGH-PERFORMING

Create Multiple Avenues to ascertain consumer satisfaction

Creating avenues for your Cyber Intelligence team to know if consumers are satisfied is a practice of high-performing organizations. They do this because consumer feedback leads to changes (people, process, and technology) that enable your Cyber Intelligence team to perform at a higher level and meet/exceed consumer demands.

Most high-performing organizations adopt multiple methods to determine consumer satisfaction pertaining to their Cyber Intelligence team. First, and as noted earlier, a practice of high-performing organizations is to have an Internal and External Engagement Team to make certain consumers are satisfied. In addition to ensuring Intelligence Requirements are met, the Engagement Team prioritizes consumers,

IMPROVE YOUR PERFORMANCE

Interact with intelligence consumers: build an Engagement Team, hold brown-bags, attend internal business unit meetings, track consumer satisfaction using tools, and host periodic "Cyber Intelligence days."

TIP

There is a distinction between Reporting and Feedback Assessment Factor Seven, *Satisfying Intelligence Consumers* and Reporting and Feedback Assessment Factor Five, *Feedback Mechanisms for Analysts.* Reporting and Feedback Assessment Factor Five assessed if organizations have mechanisms in place for Cyber Intelligence Analysts to receive feedback. Reporting and Feedback Assessment Factor Seven however is more concerned with organizations knowing if their Intelligence Consumers (Internal and External) are satisfied with the cyber intelligence team and its products. There is some overlap however between the two assessment factors. For instance, mechanisms to know if Consumers are satisfied (surveys, wikis, portals, websites, meetings) may be the same, overlap, or are entirely different than mechanisms created for Cyber Intelligence analysts to receive feedback on their reports and performance.

and report publication and distribution cycles for the team. For example, executive leadership is likely the highest priority consumer, perhaps followed by specific internal business units or key partners and subsidiaries.

Most organizations we interviewed though did not have an Engagement Team. Some of these organizations shared how giving feedback was a core value embedded in their organization's culture. Some Cyber Intelligence teams for instance, discussed how they have daily standups with the CSO/CISO and receive direct and immediate feedback. Other teams explained that their manager briefs the C-Suite and Board frequently (several times a week) and returns with feedback. Additional methods to determine internal/external consumer satisfaction includes holding brown-bags, attending other internal business unit meetings, portals, surveys, websites, surveys, blogs, and holding annual or bi-annual "Cyber Intelligence days" where the team showcases its work and provides opportunities for feedback.

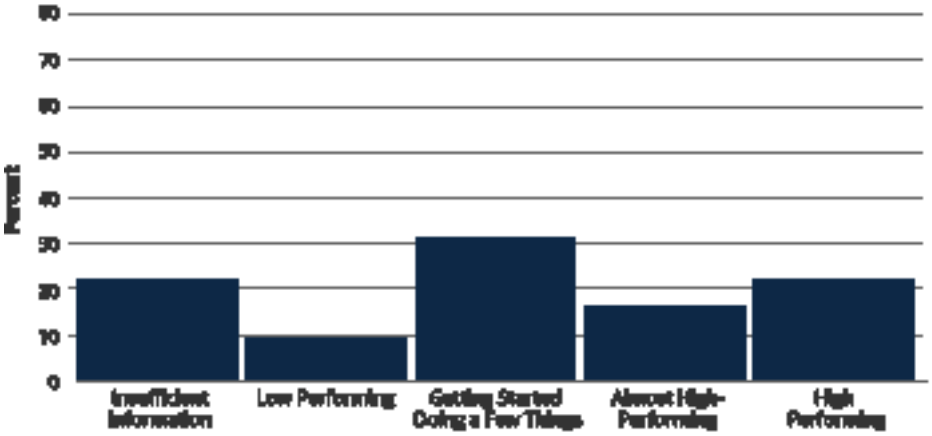
Another practice of high-performing organizations is building metrics to assess/show consumer satisfaction. These metrics are utilized to justify the Cyber Intelligence team's return on investment for the organization (See Reporting and Feedback Section 8 for more information about demonstrating ROI). Example metrics organizations include report production numbers, the number of reports addressing or tagged to Executive Leadership Intelligence Requirements, Priority Intelligence Requirements, tools showing how often reports were opened and by whom, and finally internal and external service level agreements renewed or newly established.

REPORTING AND FEEDBACK FACTOR 8: CAPTURING RETURN ON INVESTMENT

WHAT THIS ASSESSMENT FACTOR MEANS

The organization captures return on investment (ROI) for its cyber intelligence efforts. High-performing organizations have a clear definition for what ROI means to them. The organization regularly tracks, monitors, and reports ROI to leadership for its cyber intelligence efforts, tools, personnel, and data feeds. The organization uses ROI information in a strategic fashion to manage current and future Cyber Intelligence investments.

PERFORMANCE SNAPSHOT



Reporting and Feedback Factor 8 Performance Snapshot The graph on the left shows how study participants are performing in this factor.

COMMON CHALLENGES

Cyber Intelligence Teams struggle to show why they matter

Cyber is ubiquitous. Yet a common challenge expressed to the SEI team was that not everyone, especially executive level leadership, is comfortable with cyber. Some Cyber Intelligence teams discussed difficulties demonstrating their Cyber Intelligence efforts because educating leadership is a constant endeavor. Other organizations expressed concern that leadership "doesn't care" about cyber, yet wonders why security is so expensive; or that leadership only cares about "celebrity vulnerabilities."

Some Cyber Intelligence teams struggle demonstrating ROI because their organization has no clear definition about what ROI means. Teams explained how they have no metrics or ways to track ROI. Other organizations highlighted that their challenge was more of an access issue to leadership. These teams have metrics, yet find it difficult getting in front of leadership. A few teams explained that their leadership doesn't even ask for metrics – at least not on a routine basis. Still some Cyber Intelligence teams were of the belief that demonstrating ROI will always be a challenge, similar to how it is for Intelligence Community as a whole. In other words, you don't typically hear about Intelligence Community successes, usually only mistakes or incidents. One organization explained that as long as they don't make the news, they are demonstrating ROI. Lastly, some teams expressed that leadership views Cyber Intelligence and more specifically cybersecurity only through the prism of cost avoidance, as opposed to an asset that can be both cost avoidance and a return on investment.

IMPROVE YOUR PERFORMANCE

- Create a defined and repeatable Strategic analysis Workflow to answers IRs and PIRs. The workflow should leverage all components of the Cyber Intelligence Framework to support strategic analysis on threats, risks, and opportunities.
- Focus on attribution to open new collection tasking against a particular threat actor, to reveal greater insight into threat actor modus operandi, and to assist with target package generation to mimic the specific threat actor for the pen testing team

GETTING TO HIGH-PERFORMING

Track and showcase metrics for cost avoidance and revenue generation

High-performing organizations demonstrate ROI by protecting the organization and providing actionable insights to enhance leadership decision making about emerging threats, risks and opportunities pertaining to organizational vital interests. This is possible because the Cyber Intelligence team's input is strategically formalized into the organization's overall business decision calculus from a systems perspective (people, process, and technology). Additionally, high-performing organizations grasp the concept that Cyber Intelligence teams demonstrate value beyond just cost avoidance. There can be an income component to Cyber Intelligence. We list below metrics organizations track and provide to leadership; as well as ways to demonstrate cost avoidance and return on investment for cyber intelligence.

High-performing organizations track the following metrics on a daily, weekly, monthly, and annual basis:

- External reports from other sources confirming your own cyber intelligence team's analysis
- New and repeat internal and external consumers for cyber intelligence products and tools
- New cases / incidents initiated and successfully resolved
- Vulnerabilities identified and fixed
- Phishing pages taken down
- People accessing your website or portal
- Threats identified targeting the organization
- Reports types downloaded
- The number of times reports were downloaded from your website or portal
- Important business decisions and meetings where the Cyber Intelligence team provided advice and guidance
- Business decisions across the organization that leveraged Cyber Intelligence products

Teams at high-performing organizations show cost avoidance. For example,

- Develop deep internal and self-generating cyber intelligence expertise, as well as tools and systems. This enables your organization to not be so reliant on hiring outside consultants, typically a cash expense
- Cyber Intelligence influencing leadership to not open a facility in a foreign location saves costs
- Cyber Intelligence passed to cybersecurity teams (SOC, Incident Response, Vulnerability Team, Network Defense) leading to new mitigations and controls that protect the organization
- Expenses saved after updating networks or patching "ABC" policy
- Adopting a Virtual Fusion Center or aspects of a virtual fusion center that may save on location expenses
- Showing organizational impact/costs of specific threats targeting industry partners – and if the threat targeted the organization itself
- Showing organizational impact/costs of specific threats targeting the organization itself were not stopped
- Streamlining manual tasks with automation and machine learning may reduce expenses
- Creating targeting packages for the pen testing team to use against organizational assets or proprietary technology. This may demonstrate how hard / easy it is to target a specific asset or technology.
- Renegotiating deals with vendors based on vendor performance
- Keeping current with security and compliance regulations

Demonstrating ROI tends to be more challenging than demonstrating cost avoidance. Specifically, ROI implies there is a monetary, specifically income value attributed to the Cyber Intelligence team's performance. A practice of high-performing organizations is to first create a financially defined ROI definition that has clear measures and timeframes. A possible and hypothetical example might be:

With an annual budget of X dollars, the cyber intelligence team over the next year will protect the organization's critical infrastructure and technologies valued at X dollars. The cyber

intelligence will aim to generate X dollars in revenue this year. Revenue generation will be accomplished by establishing new internal and external partner agreements, and informing leadership about threats, risks and opportunities pertaining to organizations vital interests.

Examples of ways to demonstrate or achieve ROI:

- You have built such an amazing high-performing Cyber Intelligence team, that as a result, your organization is very appealing to other companies looking to be acquired or merge with a better Cyber Intelligence performing organization
- Cyber Intelligence advancing leadership decision making regarding strategic technology development and procurement
- Embedding BISOs or Cyber Intelligence analysts in internal business units (Business Development, Physical Security, Marketing, Technology Procurement, Legal and HR) to provide tailored cyber intelligence to those units. This may not result in a true cash transaction, yet at a minimum would likely show as an internal business expense for that specific business unit
- Your Cyber Intelligence team becomes an industry leader in providing Cyber Intelligence. Other organizational peers are charged annual fees to receive your organization's cyber intelligence products, briefings, or partnership for joint simulations and other related expertise.

Lastly, the manner in which ROI and cost avoidance is communicated to executive leadership is critical. Cyber Intelligence teams may track all the metrics they want. However, it either won't matter or will fall on deaf ears if the Cyber intelligence team is unable to communicate metrics in business-risk based terms, ascribing monetary values to events, incidents and opportunities as those listed above.

The Future of Cyber and Cyber Intelligence

During our interviews we asked participants questions about the future of cyber and cyber intelligence. The SEI team grouped participants' responses into themes. The most common groupings are shown below.

Five years from now, what skills, knowledge, and experience do you think will be important to have for cyber intelligence analysts?

A diversity of skills, knowledge and experience will be needed to become a high-performing cyber intelligence team. Most, if not all the skills, knowledge and experience listed below are already in need. Organizations we interviewed simply explained however, that they will need more of it.

Technical skills, Knowledge and Experience

- Computing
  - Networking fundamentals
- Programming and Coding: Python, C++, API programming, REST,
  - Databases: Mongo DB
- Artificial Intelligence, specifically Machine Learning
  - How to build models
  - Data Science
    - Big Data Analytics
  - Automation
    - Scripting
- Experience working on a Cyber Intelligence Team
- Cloud Analysis and engineering
- Mobile
- Embedded Devices
- SOC skills
- Malware Analysis
- Staying Fresh on Tools

Non-Technical Skills Knowledge and Experience

- Knowledge about threats actors
- Cross-Domain Intelligence Analysis
  - Critical Thinking
  - Connecting Dots, Link Analysis
- Communication skills but have technical aptitude to learn
  - Integration and communication
  - Interpersonal Skills
  - Emotional Intelligence
- Privacy Analysis
- Criminal Psychology
- Organizational skills
- Research skills
- Social Media Exploitation and Open Source Intelligence Techniques

What technologies will be relevant / impact the future of cyber intelligence performance in the next five years? Why and how? (Cloud, IoT, Mobile, A/I and Machine Learning, AR/VR, Automation, Brain Computer Interfaces)

We asked organizations what technologies they believe will be relevant and impact the future of cyber intelligence performance in the next five years. The most common / frequent technologies that were mentioned are listed below. Maybe not so ironically, some technologies listed are also viewed by organizations as the biggest future threats in the following question.

- Artificial Intelligence
  - Will Impact how we respond to attacks
  - Will change how organizations recruit new talent and allocate monetary investments
  - Machine Learning
    - Help analyze bigger data sets that will require more software development
    - Technology that automatically answers Intelligence Requirements
    - Making risk decisions about other types of telemetry aside from Hashes and IPs
- Automation
- Cloud
  - Presents new challenges and opportunities
  - Cloud becomes operations infrastructure
  - Machine Learning capabilities through the cloud will better alert you to threats
- Unified Digital Landscape
  - Everything Smart (IoT Devices, Phones, Vehicles, Buildings)
- Big Data and Big Data Analytics
  - Changing Data sets and collection sources
  - Ability to process big data, draw connections,
  - Anything that can house big data, manage it, run analytics on it
- Quantum Computing
- Encryption
- Brain–Computer Interfaces

What are you biggest future threats?

- Technology, and its unintended consequences
  - Artificial Intelligence
    - Adversaries using Artificial Intelligence such as machine learning against us, so it will continue to be an arms race
    - Malware that learns
    - Generative Adversarial Networks
  - Cloud
    - How to secure it and get value out of it at same time
  - Botnets
    - Ransomware at scale
- Data
  - Threat of drowning in data
  - Loss of trust in data
    - Disinformation
      - What is true and not true will be an increasing challenge

- Targets
  - Failing to educate people
    - People are weakest link
  - Unified Digital Landscape
    - Everything Smart (IoT Devices, Phones, Vehicles, Buildings)
      - Not enough security built into IoT devices
    - Machine Learning Models
    - Cloud
      - Huge attack surfaces, largely controlled by small number of big companies
  - Industrial Control Systems
  - Mergers and acquisitions creating larger attack surfaces
  - Vertical pivoting from user networks to operational critical infrastructures and ICS
  - Third-party vendors
  - Supply-chain Threats
  - Social Media Targeting of employees
- Policy Stagnation
  - Laws and sharing of data
  - Intersection of technology and rules (Cyber and GDPR)
    - Laws too slow to keep up with pace of technology
  - Block-Chain decentralization, lack of regulation and monitoring
- Cyber Sovereignty and Internet Balkanization
  - Privacy
    - Leveraging GDPR for advantage
- Encryption
  - Quantum Computing
    - Some algorithms today are non- quantum safe.
  - Not have enough diversity and wider adoption of the same algorithms
  - TLS version 1.3 could make deep packet inspection challenging
  - Threat actors are moving more towards encrypted chats like WeChat, WhatsApp and Telegram to conduct business.
    - Some encrypted chats have their own block chain platform and cryptocurrency
- People
  - Staffing and Retention
    - Not enough people that understand security, intelligence, forensics, and technology
- Threat Actors
  - Understanding the threat actor supply chain
    - Not just one person behind a threat (programmer, buyers, seller)
  - Foreign Nation States / Cyber Criminal Organizations
    - China's cyber strategy
    - Nation State Hacking from North Korea, Iran, Russia and China
    - State Sponsored attacks - More state actors and criminal organizations working together
    - Diffusion / Proliferation of Nation-state capabilities to other nation-states and to individuals
    - Nation-State attacks more sophisticated, incorporating levels of deception, operational security awareness
  - Insiders

Conclusion

In this report, we defined cyber intelligence as acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making. Performing Cyber Intelligence is to know which threat actors have intent and capability to target your organization and industry, it is tracking malware campaigns that may disrupt your operations, understanding your supply chain vulnerabilities, assessing potential mergers and acquisitions, geopolitics, and emerging technologies that may impact your organization. In 2018, we interviewed 32 organizations representing a variety of sectors to understand their best practices and biggest challenges in cyber intelligence. Some important best practices included:

Understanding that cyber intelligence is not cybersecurity. Organizations should create a dedicated cyber intelligence team that follows a defined and repeatable cyber intelligence workflow based on these framework components: environmental context, data gathering, threat analysis, strategic analysis, and reporting and feedback. We learned that having a collaborative, diverse Fusion Center with strong leadership engagement is best practice. Fusion Centers help break down silos and enable quick information sharing and analysis. A mature Fusion Center may comprise of: the SOCs, Security Engineering and Asset Security, Cyber Intelligence, Program Management and Technology and Development Teams. Another best practice is building a Collection Management team to identify and track Intelligence Requirements and validate data and data sources. We also saw high-performing organizations bring in machine learning engineers, data scientists and incorporate SOAR technologies to automate manual tasks in the cyber intelligence workflow. Another best practice is ensuring that the cyber intelligence team's analysis is incorporated into leadership decision making processes from tactical to strategic levels. Lastly, Cyber intelligence reports and briefings should be produced on a variety of subjects and according to an agreed upon schedule. A committed and engaged leadership team should provide feedback to the cyber intelligence team.

The report also outlined challenges organizations were confronting. Some important ones included:

Cyber definitions vary across organizations. This is important because how we understand and define words leads to actions. A number of organizations are unclear about the difference between cybersecurity and cyber intelligence. While some organizations do understand that cybersecurity is not cyber intelligence, they lack resources to actually perform cyber intelligence. We interviewed organizations without formal workflows for producing cyber intelligence. Practices were conceptual and ad-hoc. Another challenge was that organizations (big and small) expressed difficulty accessing relevant data across their organization, industry and other sectors. We met organizations seeking more people with diverse skills to perform different types of threat and strategic analysis. Additionally, some organizations lack formal intelligence requirement and data validation processes and rely exclusively on third-party intelligence providers. We interviewed cyber intelligence teams using outdated tools and technology for data gathering and analysis. Lastly, a good number

of cyber intelligence teams expressd the desire for their leadership to have more cyber education; and for leadership to champion the team's efforts and provide feedback on its performance.

This study included three implementation guides. The implementation guides are how-to-steps for leveraging machine learning for cyber intelligence, IoT for cyber intelligence, and different cyber threat frameworks to support cyber intelligence.

An important observation in this study is that humans and machines, especially in large resourced organizations are beginning to team together to acquire, process, analyze and disseminate information about threats, risks, and opportunities in the cyber domain to enhance decision making. In the next few years, humans and machines will team more and team better. That needs to be replicated between humans. In other words, more and better teaming is needed between humans across government, industry and academia. This is something we must work on every day.

Let's get to it!

Glossary & Appendix

Terms Defined

1. **Analytical Acumen**: The framework's center of gravity and represents what a human analyst brings to cyber intelligence. Analytical Acumen is and art and science. As an art, no analyst produces intelligence the same way, and the reason for that is that we all have our own personal instincts, biases, experiences, and a host of other nuances that impact the creativity and imagination that we bring to a cyber issue. As a science, an analyst seek outlets: technology, conceptual frameworks, analytical methodology, information collection methods, to best channel their creativity and imagination (the Art) into intelligence.
2. **Artificial Intelligence**: Systems that understand the world and independently make smart decisions based on that understanding.[22]
3. **Atomic Indicators**: "Pieces of data that are indicators of adversary activity on their own. Examples include IP addresses, email addresses, a static string in a Covert Command-and-control (C2) channel, or fully-qualified domain names (FQDN's). (Michael Cloppert)[23]
4. **Behavioral Indicators**: "Those which combine other indicators—including other behaviors - to form a profile."(Michael Cloppert)[24]
5. **Capability**: Means to accomplish a mission, function or objective[25]
6. **Computed Indicators**: those which are, well, computed. The most common amongst these indicators are hashes of malicious files, but can also include specific data in decoded custom C2 protocols, etc. Your more complicated IDS signatures may fall into this category. (Michael Cloppert)[26]
7. **Cyber Hygiene**: Cybersecurity efforts are sometimes called "cyber hygiene." "Cyber hygiene includes such activities as inventorying hardware and software assets; configuring firewalls and other commercial products; scanning for vulnerabilities; patching systems; and monitoring."[27]
8. **Cyber Intelligence**: Acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making.
9. **Cyber Security**: Actions or measures taken to ensure a state of inviolability of the confidentiality, integrity, and availability of data and computer systems from hostile acts or influences.[28]
10. **Threat analysis**: Threat analysis is literally the discipline of intelligence analysis pertaining to threats in the cyber domain. More specifically, it is the assessment

---

22 https://ai.cs.cmu.edu/about

23 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

24 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

25 DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

26 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

27 https://www.nist.gov/blogs/taking-measure/rethinking-cybersecurity-inside-out Ron Ross. November 15, 2016

28 The definition for cybersecurity created based on analyzing participating organizational responses and from the DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

of technical telemetry and non-technical data pertaining to specific threats, threat actors and their campaigns to your organization and industry for the purpose of informing cybersecurity operations/actions (incident response, network defense) and strategic analysis. Threat analysis is built on operational and tactical analysis. It is threat specific and enables decision-makers (CSO/CISO and other mid-to senior level decision-making) to make immediate to near-term decisions pertaining to cyber hygiene, cybersecurity, and incident response (deny, disrupt, neutralize, deceive, exploit, defeat) to ensure sustained success of business processes and operations. Threat analysis relies heavily on technical skills and is threat related.

11. **Environmental Context**: Everything you need to know about your organization internally and externally. Includes understanding organization's entire attack surface; and threats, risks and opportunities targeting you organization and industry, and the impact of those threats, risks and opportunities to your organization and industry. Includes deeply knowing your internal and external network and operations, to include but not limited to: the organizations servers, operating systems, endpoints, data centers, organization's business, its mission and culture, organizational processes and policies, business partners, geopolitics, emerging technologies, and position in industry relative to competitors. Attaining Environmental Context is a continuous process and influences what data is needed to perform cyber intelligence.
12. **Data Gathering**: Using multiple sources (internal and external to the organization) to gather data for the purpose of answering organizational intelligence requirements.
13. **Diamond Model of Intrusion Analysis**: "model establishing the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim. These features are edge-connected representing their underlying relationships and arranged in the shape of a diamond, giving the model its name: the Diamond Model."[29]
14. **Reporting and Feedback**: Formal and informal communication of and subsequent feedback to cyber intelligence analysts regarding their products and work performance. Reporting and Feedback identifies intelligence requirements, intelligence gaps, concepts needing further explanation and opportunities for collaboration.
15. **Human-Center Design**: Design and management framework that develops solutions to problems by involving the human perspective in all steps of the problem-solving process. Human involvement typically takes place in observing the problem within context, brainstorming, conceptualizing, developing, and implementing the solution.[30]
16. **Intelligence**: "The product resulting from the collection, analysis, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (JP 1-02 and JP 2-0, Joint Intelligence 22 October 2013)"[31]
17. **Impact**: Measure of effect or influence of an action, person, or thing on another—extended definition: may occur as either direct or indirect results of an action.[32]

---

29 https://apps.dtic.mil/docs/citations/ADA586960

30 https://en.wikipedia.org/wiki/Human-centered_design

31 https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf

32 DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

18. **Intent**: Determination to achieve an objective.[33]
19. **Lockheed Martin Kill Chain**: The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.[34]
20. **Machine Learning**: A field at the intersection of Statistics & Computer Science. Fundamentally, it is about learning from data: summarizing patterns, making predictions, and identifying key characteristics of a group of interest, among many other tasks.
21. **MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)**: "MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."[35]
22. **Office of the Director of National Intelligence, Cyber Threat Framework**: "Developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The Cyber Threat Framework is applicable to anyone who works cyber-related activities, its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity. The framework and its associated lexicon provide a means for consistently describing cyber threat activity in a manner that enables efficient information sharing and cyber threat analysis, that is useful to both senior policy/decision makers and detail oriented cyber technicians alike."[36]
23. **Operational Analysis:** Analysis of specific threats, threat actors, their campaigns, intentions and capabilities against an organization and its industry. Operational Analysis answers Priority and Specific Intelligence Requirements (PIR, SIR) to enhance CSO/CISO and other mid-to senior level decision-makers leadership decisions regarding non-immediate but near-term (weekly–quarterly) business process and cybersecurity decisions.
24. **Risk**: Potential for an unwanted outcome as determined by its likelihood and the consequences -extended definition potential for an adverse outcome assessed as a function of hazard/threats, assets and their vulnerabilities, and consequences.[37]
25. **Strategic analysis**: Strategic analysis is the process of conducting holistic analysis on threats AND opportunities. Holistically assessing threats is based on analysis of threat actor potential, organizational exposure and organizational impact of the threat. One might also perform Strategic analysis to provide deep clarity on the who and why behind threats and threat actors. Strategic analysis goes beyond threat analysis to incorporate analysis regarding emerging technologies and geopolitics that may impact/provide opportunities for the organization now and in the future. In this light, Strategic analysis is not only comprehensive, but ANTICIPATORY. It can be actionable, yet is based more on analytical judgments, enabling executive leaders to make risk-based decisions pertaining to organizational wide financial health, brand, stature, and reputation.
26. **Tactical Analysis:** Analysis of specific threats, attacks, incidents, vulnerabilities, or unusual network activity that enhances decision making for network defenders, incident responders, and machines pertaining to cybersecurity and incident response. Information analyzed is usually technical telemetry such as network and endpoint activity, atomic, behavioral, and computed indicators[1] such as: malware samples, hash values, domains, IPs, logs, email header

---

33 DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

34 https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

35 https://attack.mitre.org

36 https://www.dni.gov/index.php/cyber-threat-framework

37 DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

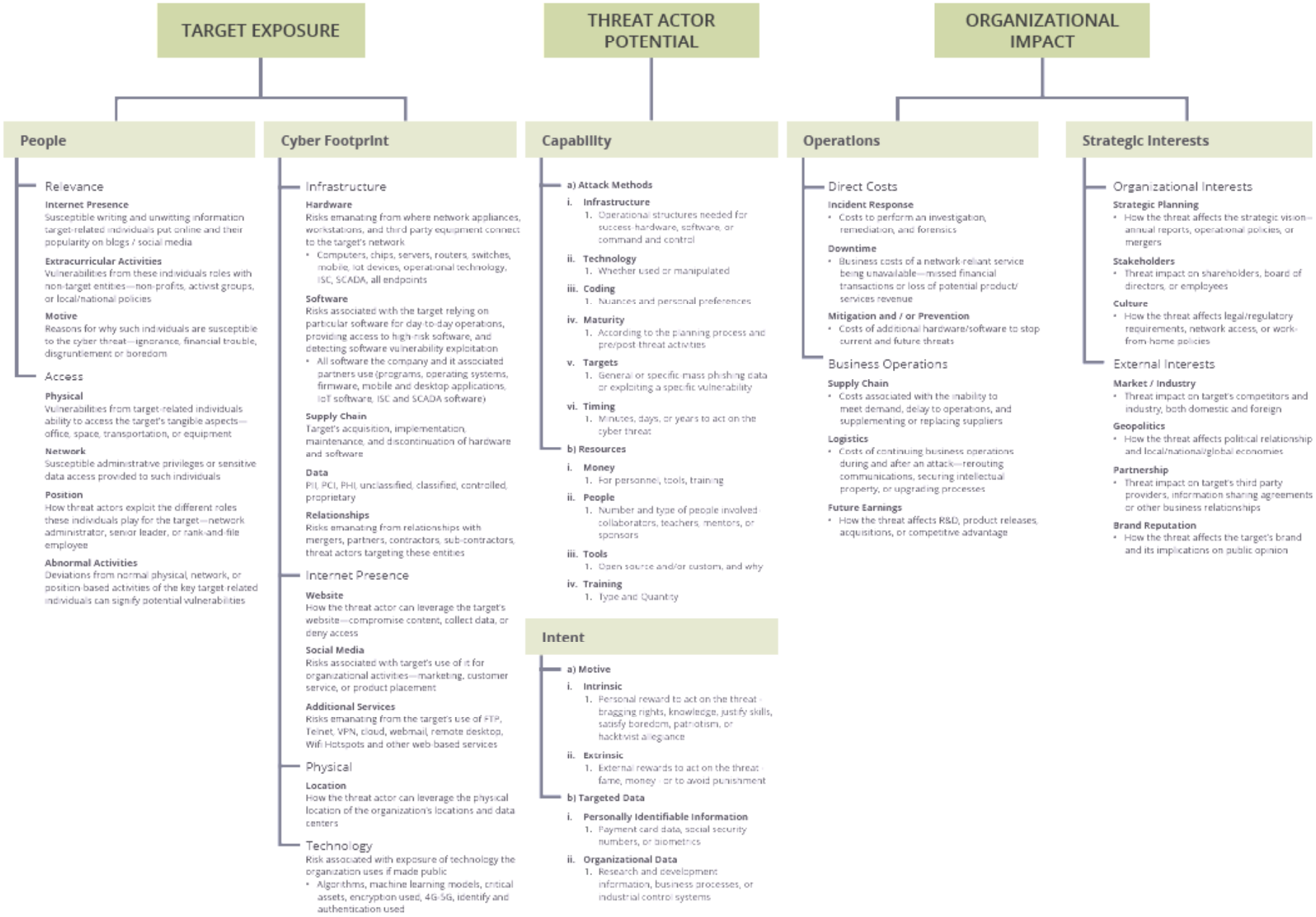
information. Tactical analysis tends to answer Specific Intelligence Requirements (SIRs) and the immediate, daily and weekly what/where/when/how questions about threats.

27. **Threat**: Indication of potential harm to life, information, operations, the environment and/or property—extended definition—may be a natural or human-created occurrence and includes capabilities, intentions, and attack methods of adversaries used to exploit circumstances or occurrences with the intent to cause harm.[38]
28. **Structured Analytical Techniques**: analytic techniques designed to help individual analysts challenge their analytical arguments and mind-sets. Techniques are grouped by diagnostic, contrarian and imaginative thinking.[39]

38 DHS Lexicon Terms and Definitions Instruction Manual 262-12-002-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

39 https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

PRIORITIZING THREATS FOR MANAGEMENT (FULL VIEW)



MOST POPULAR CYBER INTELLIGENCE TOOLS

Participants reported using a wide array of tools in their cyber intelligence practices. The following graph shows the most popular tools among participants and their uses. The list includes a mix of free, open-source, and paid tools and services.

Data Management	Analysis	Visualization	Third-Party Intelligence	Tool Name
			■	Anomali Threat Intelligence
			■	CrowdStrike
			■	DHS - CISCP
■				Elastic Search
			■	FBI
			■	FS-ISAC
			■	FireEye - iSIGHT Intelligence
			■	Flashpoint Intelligence Platform
■				Hadoop
	■	■		I2 analyst notebook
			■	IBM X-Force Threat Intelligence
	■			IDA for Malware Analysis
	■			Joe Sandbox
		■		Kibana
	■			MISP
	■	■		Maltego
		■		Malware Information Sharing Platform
			■	NCFTA
			■	ProofPoint ET ProFeeds
			■	ProofPoint Emerging Threat Intelligence
			■	Recorded Future
	■	■		Splunk
	■			Virus Total VirusTotal

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412.268.5800 | 888.201.4479
Web: sei.cmu.edu
Email: info@sei.cmu.edu