Thinking Like An Analyst

Paul Krystosek, PhD
CERT Security Operations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA, USA

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

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.

DM19-0550

Overview

Introduction

Context

Gathering Data

Microanalysis

Macroanalysis

Reporting

Course objectives

Describe a model of the analysis process, with distinct stages

Identify selected processes and results associated with each stage

Characterize key thinking issues (biases) that can affect analysis results

Apply the analysis process to a body of data

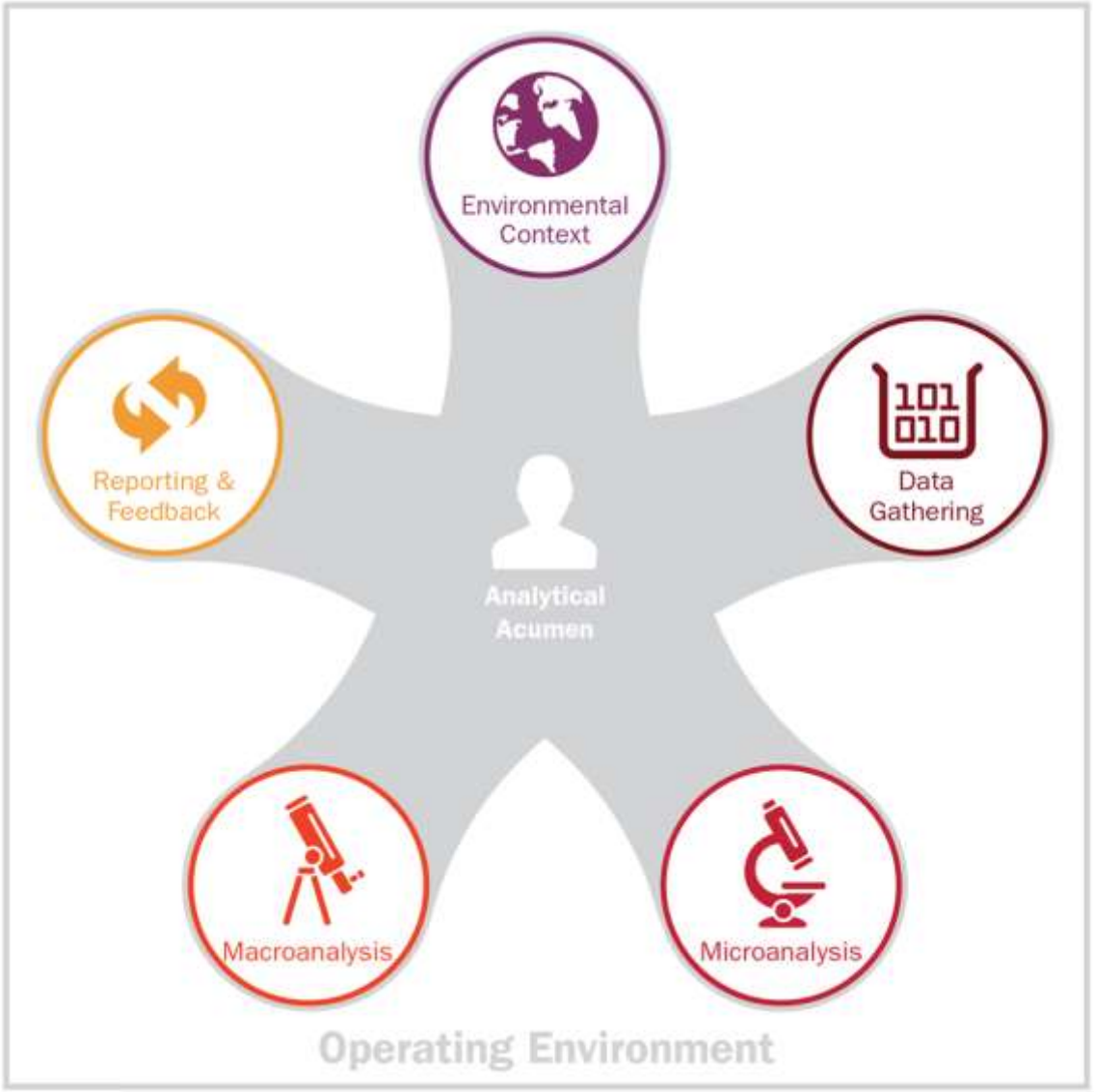
What is analysis?
Intelligence Analysis

Intelligence analysis is the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context. (*CIA, Center for the Study of Intelligence. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm*)

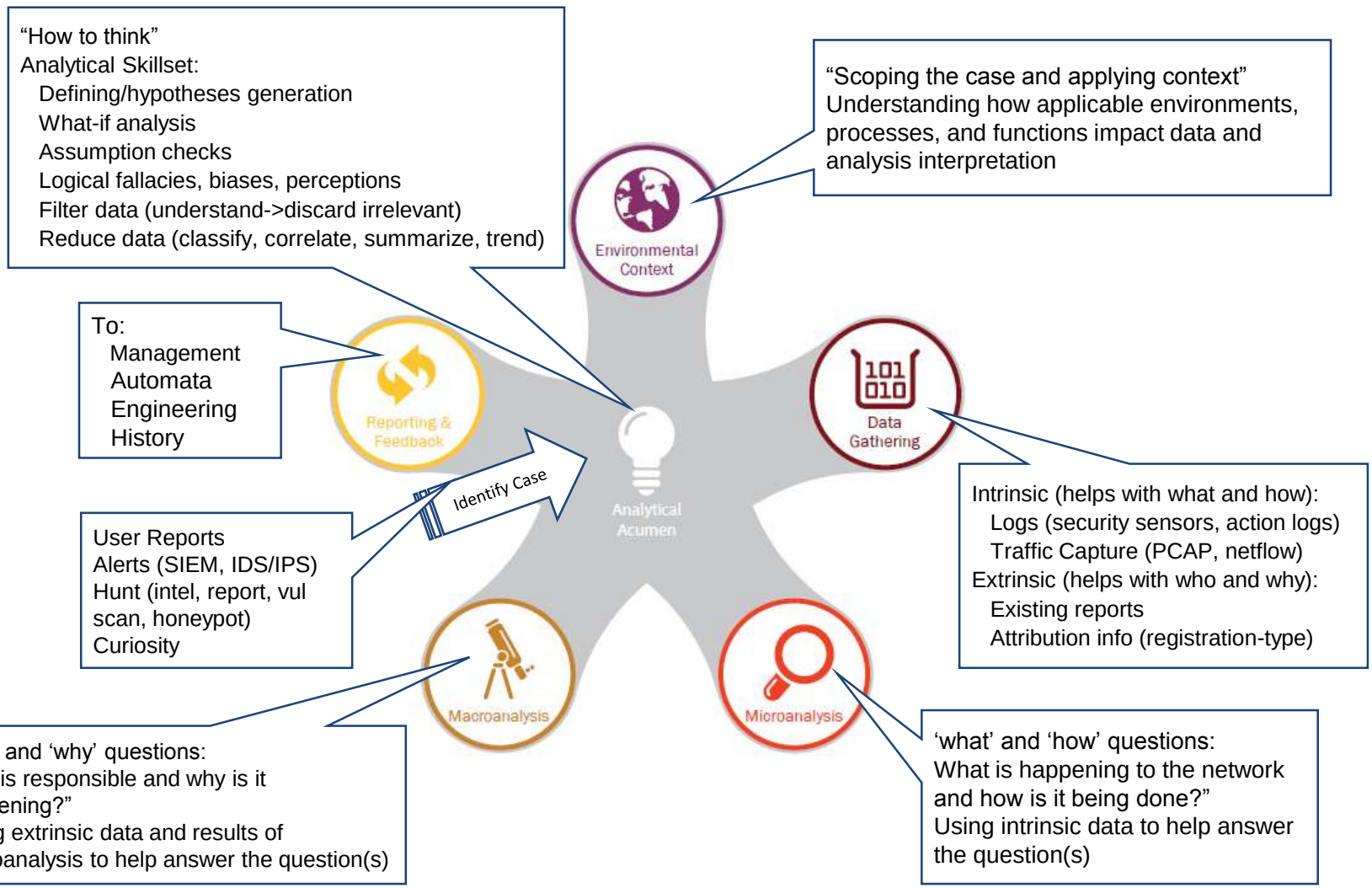
Intelligence analysis is the process by which the information collected about an opponent is used to answer tactical questions about current operations or to predict future behavior. (*RAND Corp. https://www.rand.org/topics/intelligence-analysis.html*)

What is analysis? More Generally

The process of using data, context, analytical techniques and critical thinking skills to answer a question or test a hypothesis and make the results usable.



What are we covering?
Analysis Framework



What are we covering?

Environmental Context

- why context matters
- knowing a cyber environment
- when context is missing

Gathering Data

- What do you need?
- Where do you get it?
- What if you can't find it?

Microanalysis

- finding what and how
  - traffic, logs, and basic statistics

Macroanalysis

- finding who and why
  - intelligence sources and basic fusion

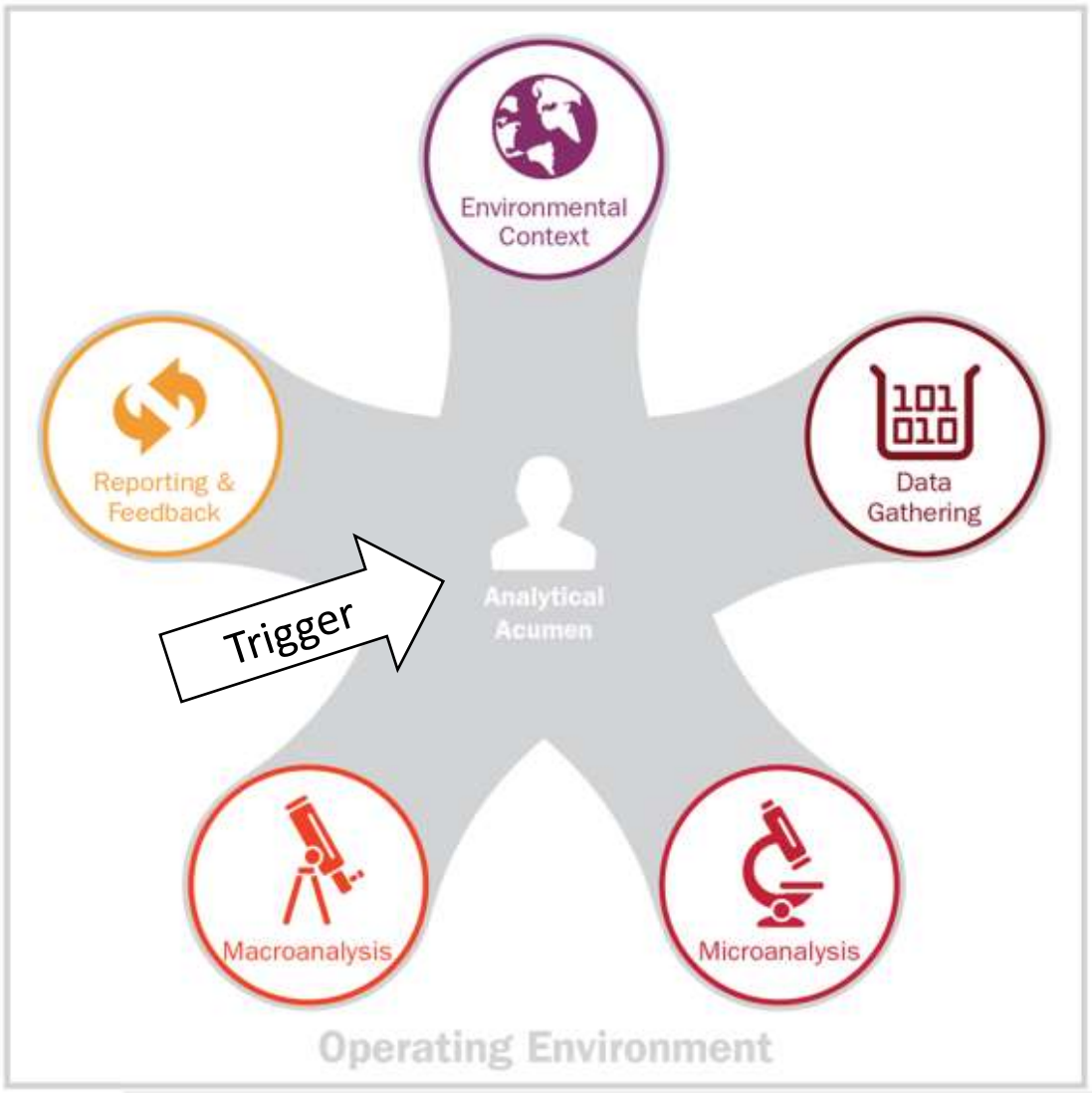
Reporting and Feedback

- sharing is important

Analytic Acumen

- cognitive biases
- hypotheses
- what-if analysis
- Do you really need more data?
- Satisficing is not sufficient.
- Is cyber analysis a puzzle?
- Facts require interpretations; they don't speak for themselves.

Analysis Framework



Where to begin?

At the end!

To start, answer questions like

- What do I want to find out?
- What do I think is happening?

Then use the answers to make hypotheses.

Hypotheses

A clear, specific statement of what you are trying to prove or disprove.

The statement must be testable.

Hypothesis Examples

Bad Example

Hypothesis: This email is bad.

What is “bad”? This is not clear, specific, or objective.

Good Example

Hypothesis: This email is trying to get the recipient to install malware through an executable attachment.

This is not comprehensive as to all we may consider bad, but is testable.

Comprehensiveness

Favor simple statements over complex ones.

It is fine to have multiple sub-hypotheses that you need to choose between or decide if they are all wrong or all right.

Example:

This email is bad because it

- is trying to get the recipient to install software through an executable attachment
- links to a known malicious URL
- requests the user to provide sensitive data to an unauthorized or spoofed entity

Example 1 Introduction

Coordination between governments is difficult.

- Resources
- Who is in charge?
- Varying priorities
- Authorization to act (International Law issues)

Cyber activity frequently crosses national boundaries.

- Routing
- Hosting
- Does this constitute international commerce?

Example 1 explores International cooperation on critical infrastructure protection.

Example 1

Email message

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts from multiple (100+) sources to 10.127.77.135 port TCP/22, for accounts “root”, “admin”, and “fsmithe”. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

Email legitimacy is confirmed (also sent encrypted with a valid public key).

Example 1: Who

Email message

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts **from multiple (100+) sources** to 10.127.77.135 port TCP/22, for accounts “root”, “admin”, and “fsmithe”. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the **Country1** Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

From “multiple sources” to Country1

Example 1: What

Email message

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) **persistent login attempts** from multiple (100+) sources to 10.127.77.135 port TCP/22, for accounts **"root", "admin", and "fsmithe"**. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. **Attempts to block** the attack by restricting port 22 access have **not been successful to this point**. **Assistance in dealing with this activity is requested.**

Targeted attack: "root, admin, and fsmithe"
Evasion of defenses. Request for aid

Example 1: Hypotheses

1. This is a hoax perpetrated on Country1.
2. This is real activity, but no damage is resulting, so it can be ignored.
3. This is real activity, but damage is minor, so it can be ignored.
4. This is real activity and very damaging, escalate it for more action.
5. This is real activity, need further information to assess it for escalation.

With hypotheses, now what?

Make a plan.

Answer questions like

- Can I directly prove my hypotheses?
- What information do I need to prove my hypotheses wrong?
- What information do I need to support my hypotheses?
- How do I get that information?
- What circumstances and environment factors (context) will influence what I see and how I interpret the information I find?
- What assumptions must I make?

Proving vs. Disproving

There are many cases where it is more effective and efficient to try to disprove a hypothesis instead of trying to prove it.

- Find counter-examples.
- Find examples where specific behavior occurs in other contexts.
- Find examples where interpretation of behavior is not reasonable (too frequent, wrong endpoints, too regular).

Example

The number of attacks against infrastructure companies is the same as those on the commercial sector in general.

Proving vs. Disproving (continued)

There are many cases where it is not really possible for an analyst to prove a hypotheses.

- Data not available
- Data too sensitive to include
- Data too uncertain

Example

Attacker ABC is deliberately targeting IoT video cameras.

- Proving **intentions** is very difficult. Without talking to the attacker, it is indistinguishable whether the attacks targeted a specific type of device, the attacks were just the ones caught, or the attacks were only successful on those devices.

Proving vs. Disproving (one more time)

Hypothesis	Prove	Disprove
"*This* will never happen"		
More network traffic from a web client than to it, means exfiltration		
Attacks on ___ are always preceded by a recon scan		

Terminology: Acumen

Acumen: A power to see what is not evident to the average mind.

Suggested synonyms for acumen:
discernment, perception, insight

https://www.merriam-webster.com/dictionary/acumen

Analytical Acumen: Anchoring Bias

People tend to over-rely on a single piece of information, often the first piece of information received. This is a big component of social engineering.

Examples

The financial department gets an email request from an “executive” to wire money to a new vendor for a deal that just closed. The email address appears to be correct for the executive, so the money is wired without verifying the request with the executive by other means.

I was told that this type of attack is always from Country X

Summary: Introduction to Analysis

Collecting information

Determining behavior (network and enemy)

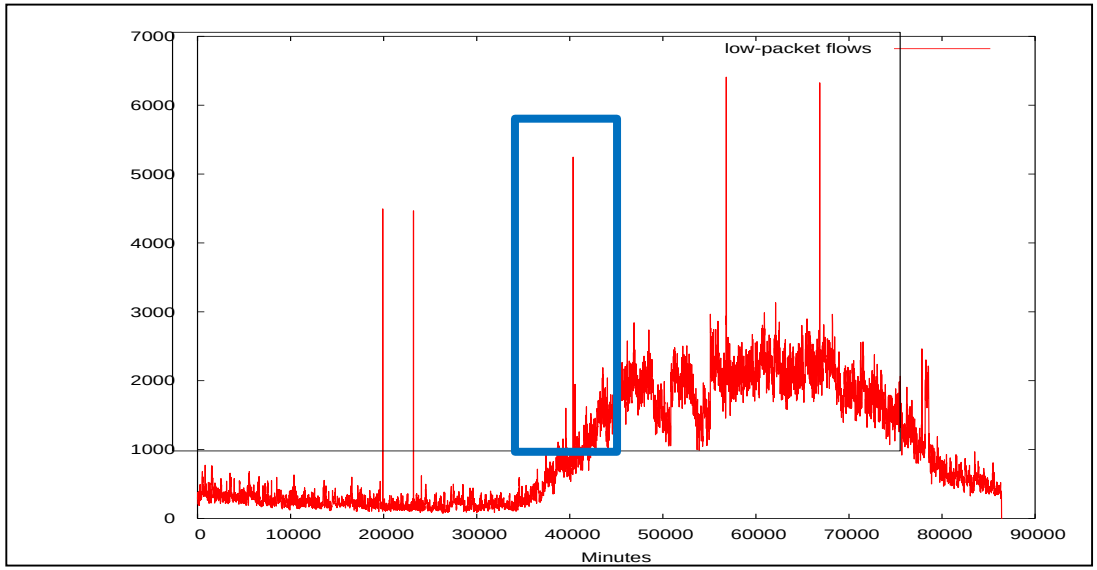
- Hypotheses
- Testing/Proving
- Avoiding bias

Thinking Like An Analyst: Context

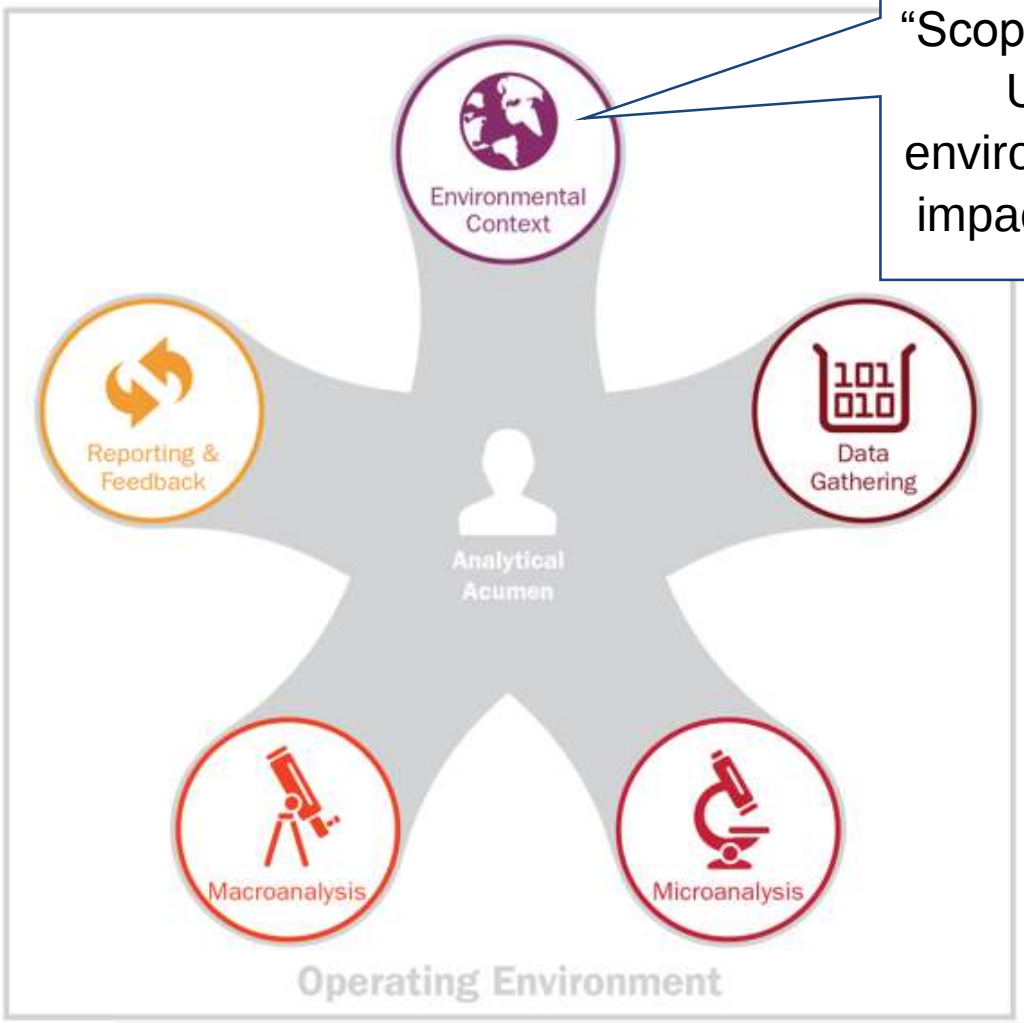
- Evaluating hypotheses
- Environmental context
- What-If analysis
- Selective perception bias

Evaluating Hypotheses: Spike

1. This spike is too brief to worry about.
2. This spike is a DDoS attack.
3. This spike has the characteristics of a DDoS attack and is directed against the webserver.
4. This spike means we made someone mad and they are attacking us.



Analysis Framework



"Scoping the case and applying context"
Understanding how applicable environments, processes, and functions impact data and analysis interpretation

Why Context Matters

Context provides the details

- needed to gauge potential impact and prioritize investigations that let you determine mitigations and recourse
- necessary to identify the scope of an investigation
- necessary to identify the vulnerabilities that allowed an event
- required to understand the types of analyses needed to get insightful results

Knowing a Cyber Environment

Cyber environments consist of

- assets
- people
- policies, protocols, and procedures

Hopefully, these are documented in

- network maps, asset lists
- user lists, user roles
- employee manuals, acceptable use policies
- configuration policies, standard operating procedure documents
- incident response plans

When Context Is Missing

Things to try when context is missing.

- Ask someone who might know the context.
- Infer it from available information.
- Guess at the possibilities and engage in simple “what-if” analysis.

Example information sources

- Network traffic (behavior analysis)
- Host configurations (DHCP information)
- New employee documentation (wiki)

When Context Is Missing – Example

Adapted from an actual incident report

The incident response team receives a report

- User “abc” attempted to login to server “x”.
- The attempt was successful.
- The login was from an Eastern European country.
- The login was escalated to root access.
- Changes were made to a network device configuration

What should be done?

- Undo the changes and lock abc’s account.
- Panic!
- Get more information.
- Examine the changes in detail.

When Context Is Missing – Example Response

What should be done?

- Undo the changes and lock abc's account.
- Panic!
- **Get more information.**
- Examine the changes in detail.

Good choice!

It turns out that "abc" is a senior network security analyst.

User "abc" was asked to help an eastern European CSIRT with a problem.

While there, "abc" received an email from someone (who did not know where "abc" was) asking for changes to be made to a network device configuration.

Which "abc" did, securely through a VPN.

Context Example 1

Email message

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts from multiple (100+) sources to 10.127.77.135 port TCP/22, for accounts “root”, “admin”, and “fsmithe”. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

What elements could be enriched with more information?

Context Example 1 – Added Elements

Email message:

From: **Country1 CSIRT (csirt@country1.c1)**
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts from multiple (100+) sources to **10.127.77.135** port TCP/22, for **accounts "root", "admin", and "fsmithe"**. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. **The host in question** is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

More context needed: IP address, accounts, hosting, contacts

Example 1 Context

`10.127.77.135  resolves to www.country1.cc1`

TCP Port 22 is Secure Shell (SSH) service port

F. Smithe: Director, Office of Emergency Management
Country1 Division of Emergency Management

What else would we need to know?

- List of source IP addresses and resolutions
- Why blocking is not successful
- Activity elsewhere?

Strategies

- Reach back to reporter
- On-line investigation

Further Context in Example 1

`www.country1.cc1` has variety of roles

- Administrative comments to Ministry of Foreign Affairs
- Gambling licensing
- Voter registration & campaign financing
- Durable medical equipment
- Businesses, trademarks, trade names

Smithe is public contact for MFA Department of Cyber Security (This information gathered from: LinkedIn, public reports etc.)

Reasonable hypotheses

- Someone is trying to compromise credentials.
- Someone is trying to deface the web site.

Analytic Acumen: What-if Analysis

What-if analysis involves testing how different values for a variable change the analysis outcome.

This is useful when the actual value for a variable is unknown.

Example

- Internet traffic to a known-bad URL was detected in network flow. It is unknown if the web proxy allowed the traffic out to its destination or not.
  - Possibility A is that the web proxy allowed the traffic, so further investigation is needed.
  - Possibility B is that the web proxy blocked the traffic, so further investigation is not needed.

Analytic Acumen: Selective Perception Bias

Expectations do not always match reality and can lead to overlooked information and misinterpretation.

Be cautious about how your expectations influence what you see.

Example

- Analyst receives an alert from a virus scanner about a file with a detection of EICAR Test File.
- Analyst's expectation is that the virus scanner found malware, so the detection is escalated.
- Reality is that EICAR Test File is a testing mechanism for security appliances. Similarly, PUPs often trigger suspicious alerts.

EICAR: European Institute for Computer Antivirus Research
PUPs: Potentially Unwanted Programs

Summary: Context

Security is a system problem.

System is a context.

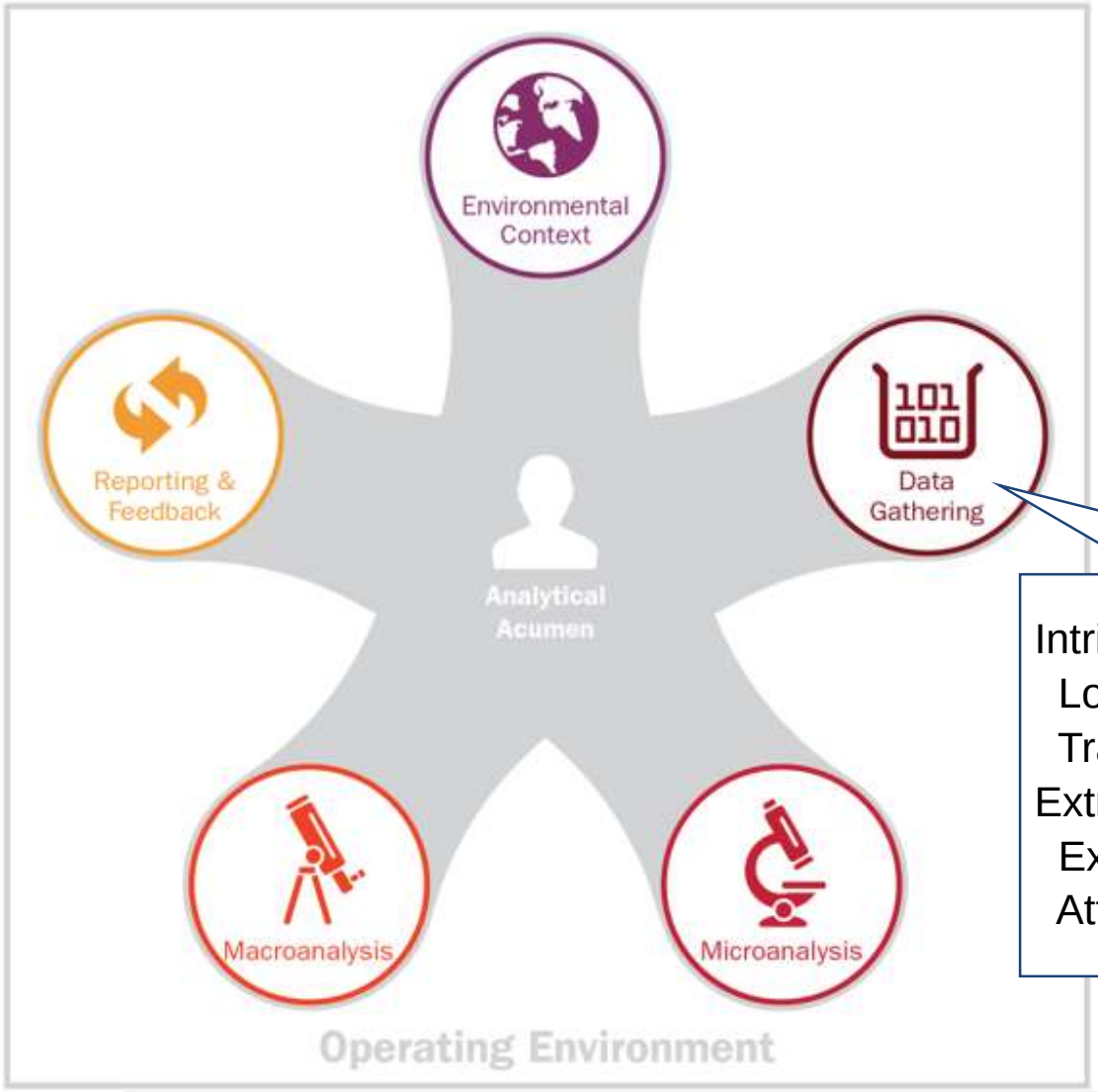
Consider alternative interpretations.

Watch out for your expectations.

Thinking Like An Analyst: Gathering Data

- Data needs
- Getting data
- Do we really need it?
- Information bias

Analysis Framework – Data Gathering



Intrinsic (helps with what and how):
- Logs (security sensors, action logs)
- Traffic Capture (PCAP, netflow)

Extrinsic (helps with who and why):
- Existing reports
- Attribution info (registration-type)

What do you need?

Evidence to support or disprove the hypotheses.

In the cyber realm this may include information on

- how appliances, services, and threats operate.
- a device's (or user's) activities.
- relevant policies, allowed activities, and expected uses.

Where do you get it?

How appliances, services, and threats operate

- domain knowledge, specifications (like RFCs)
- user manuals, white papers, observations
- device and appliance configurations/environment setup
- threat reports (e.g., intelligence reports, malware analysis results)

A device's (or user's) activities

- logs
- eye-witness accounts

Relevant policies, allowed activities, and expected uses

- organizational policies, management expectations

What if you still can’t find it?

Just like for missing context

- Ask someone who might know this information.
- Infer it from available information.
- Guess at the possibilities and engage in simple “what-if” analysis.

Gathering Example 1

Email message

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts from multiple (100+) sources to 10.127.77.135 port TCP/22, for accounts “root”, “admin”, and “fsmithe”. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

Gathering Example 1: Data

Further interaction with reporting team at Country1

- 127 IP addresses as source data, including both foreign and domestic addresses
  - 20 within Country1 Government
  - None within Country2 Government
  - None appear on google search as sources of attacks
- Several packet captures of attempted login show a series of attempts with successive passwords apparently taken from a dictionary.
- Password policy at Country1 specifies passwords not be dictionary words and is enforced by technology.
- Messages log from target computer shows unusual activity by “root”, “get” of files from a remote server not commonly connected to.
- No change to web content, no threats received.

Example 1: Revised Hypotheses

1. Someone has compromised credentials on the server.
2. Someone is trying to deface the web site.
3. Someone is trying to access through the web site to attack something else.

Analytic Acumen: Do you really need more?

The desire for more information is a common theme among analysts, but more is not always better.

Questions to ask

- Do I truly understand the data I already have?
- Is the data I need missing or do I just need to find it in what I have?
- Do I need more data or different data?

Example 1: Analytical Acumen

Possible additional data

- a threat feed?
- more attempted logins in depth?
- logins from other sources?
- interview agency leaders (including Mr. Smithe)?
- logs of agency servers?

What data do we need to evaluate hypotheses, or to develop new ones?

What data will be a distraction?

Analytic Acumen: Information Bias

People tend to seek information even when that information will not change the end results.

Analysts need to focus on the information that will change an interpretation or decision.

Example

An analyst gets an alert about traffic from a specific IP address. He or she starts by looking up the geolocation of the address, even though that is not a criteria for determining maliciousness.

Relevant or Not?

Should a manager reprimand an employee who visited a blocked website?

1. The website was registered in a foreign country.
2. The website's default language was not English.
3. The website is categorized as unknown.
4. The employee was supposed to be taking care of patients.

Do I need to take an umbrella tomorrow?

1. Tonight's sky is red.
2. Leaves are upside down.
3. Farmer's Almanac states this month will be rainier than normal.
4. It is currently raining.
5. It rained on this day last year.
6. I only park in garages.

Should I click the link?

1. Sender is my grandmother.
2. Email appears to be a chain letter.
3. Mouse-over points to a tinyurl.
4. You know everyone else in the recipient group.

Should I buy a lottery ticket?

1. I found a penny heads up.
2. I have a few extra bucks.
3. I could play my lucky numbers.
4. I rigged the system.

Should I ignore this certificate warning?

1. It occurs on a page on our work domain.
2. It is a self-signed certificate warning.
3. It uses RC4.
4. The webpage was not blocked by the web proxy.

Summary: Gathering Data

Look for a variety of available data.

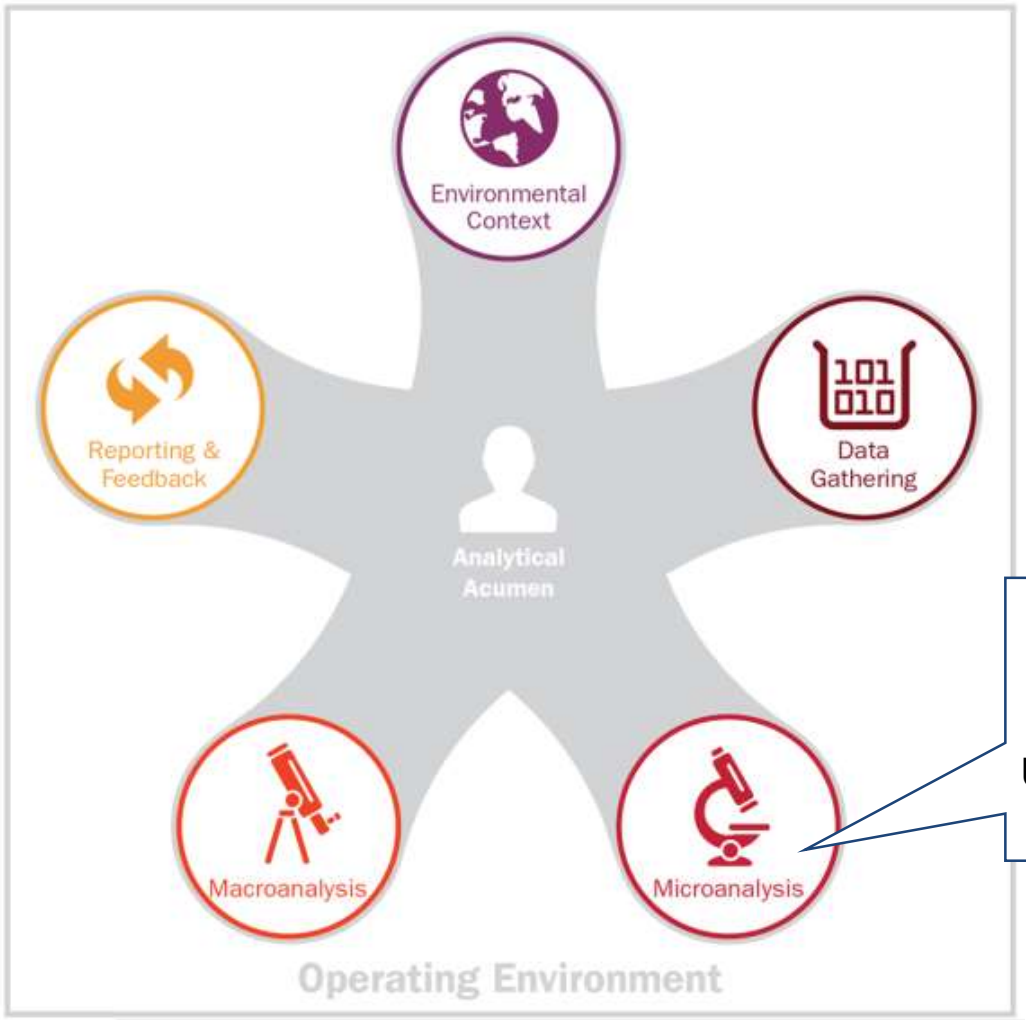
Watch out for collection artifacts.

More is not always better.

Thinking Like An Analyst: Microanalysis

- What is Microanalysis?
- Common methods
- Statistics and Anomaly Detection
- Satisfactory vs. Sufficient
- Confirmation and conservatism biases

Analysis Framework – Microanalysis



'what' and 'how' questions: what is happening to the network and how is it being done?"
Using intrinsic data to help answer the question(s)

What is microanalysis?

The process of trying to figure out what occurred and how it happened

- Or, if something occurred at all

Example scenario	What needs to be determined
Alert about use of privileged account on a sensitive server	Was the use authorized? If not, what did the user do? How did the account get access?
Email submitted to abuse mail box	Did the email result in infection for the submitter or any other recipient?

Common Microanalysis Techniques

Direct investigation

- looking at an asset or various logs to find direct evidence

Computational analysis

- using statistics and other computational methods to find anomalies or patterns as evidence

Direct Investigation

In the cyber realm, direct investigation may involve

- checking device security or application logs
  - web proxy/firewall
  - server/PC
- looking through network traffic capture
  - network flow
  - full packet capture
- examining files
- forensic analysis of a device
- talking to end users or administrators

Computational Methods

Types of computational methods

- statistical
  - using statistics to gain insight from data
- machine learning
  - transforming or analyzing the data to find something you didn't know before
- data mining
  - extracting something you know is there from a large dataset

Methods and concepts have varying levels of complexity

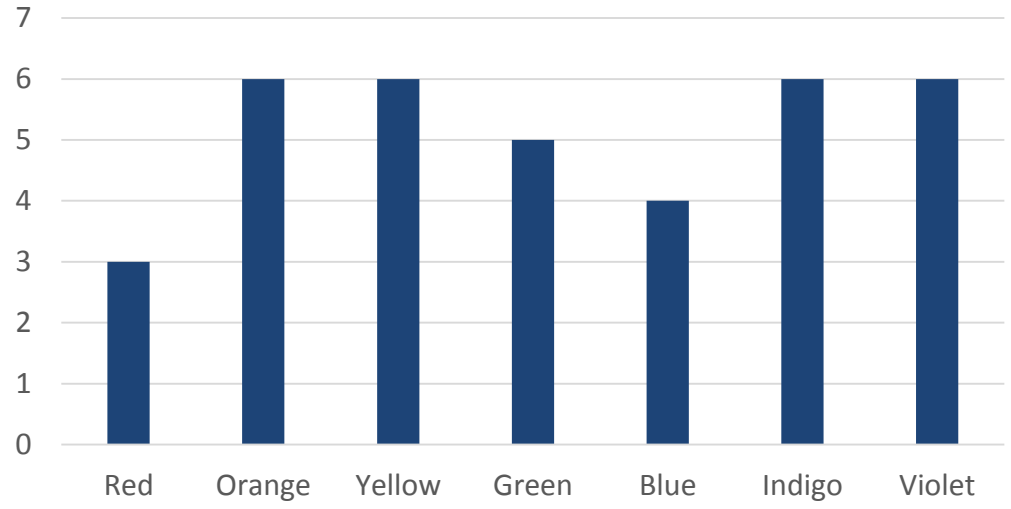
- means, normal distributions, standard deviations
- clustering
- trend analysis

Statistics and Anomaly Detection

Mean

Simple average

1. Add up the items.
2. Divide the result by the number of items.



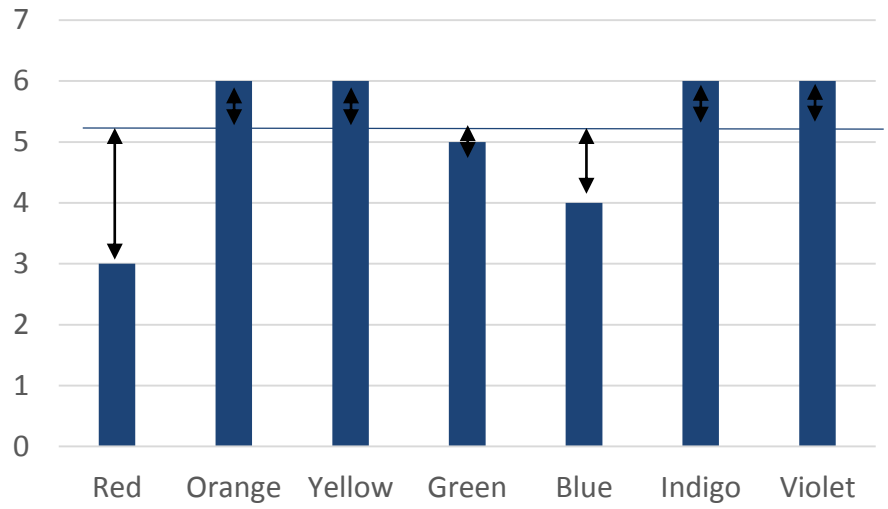
Example: compute the mean number of letters in the colors of the rainbow

(3 + 6 + 6 + 5 + 4 + 6 + 6) ÷ 7 = 5.14…

Variance

Measures how different the values are from the mean, on average.

More technically, variance is the mean of the squared difference from the mean of all items.



Example: variance of number of letters in the colors of the rainbow

$[(3 - 5.14)^2 + (6 - 5.14)^2 + (6 - 5.14)^2 + (5 - 5.14)^2$

$+ (4 - 5.14)^2 + (6 - 5.14)^2 + (6 - 5.14)^2] \div 7 =$

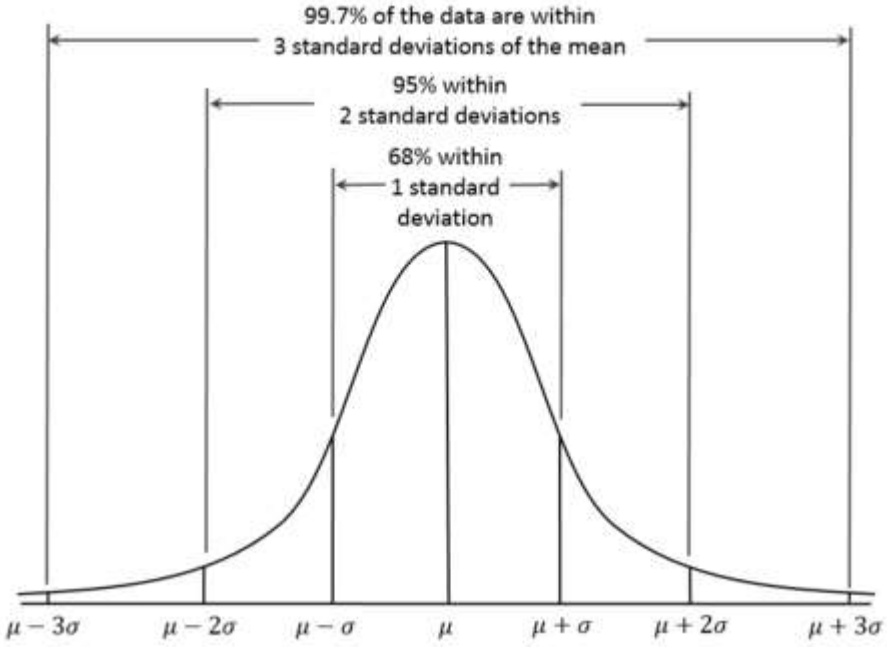
$[-2.14^2 + .86^2 + .86^2 - .14^2 - 1.14^2 + .86^2 + .86^2] \div 7 =$

$[4.5796 + .7396 + .7396 + .0196 + 1.2996 + .7396 + .7396] \div 7 = 8.8572 \div 7 = 1.265\ldots$

Why do we care?

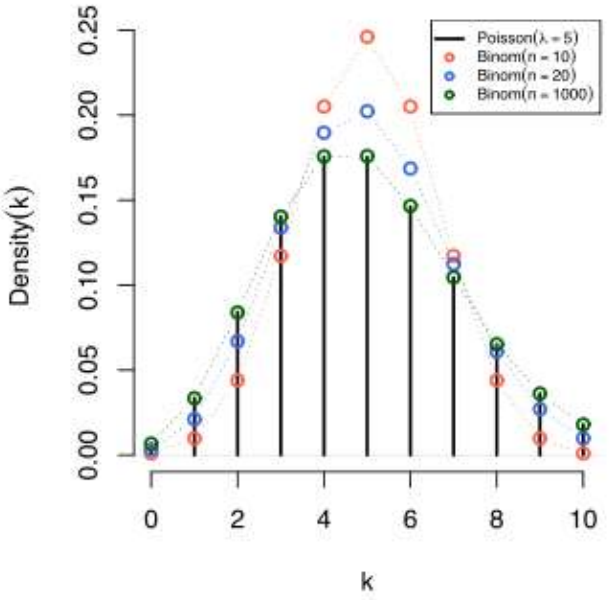
Values occurs in predictable frequencies.

https://en.wikipedia.org/wiki/68%E2%80%9395%E2%80%9399.7_rule



This is true even if your data is not a normal distribution.

https://en.wikipedia.org/wiki/Poisson_distribution



This means we can say how likely a value is to occur.

Microanalysis Example

Microanalysis Example 1

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts from multiple (100+) sources to 10.127.77.135 port TCP/22, for accounts “root”, “admin”, and “fsmithe”. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

Microanalysis of Web Host Logs

Series of GET commands, some successful (200), some not (401)

Some external address re-use

All reference vreg – voter registration function on web site

Human-oriented timeframe

198.51.100.17 - - [07/Sep/2018:16:05:49 -0800] "GET /ct1/www/vreg?topicparent=Main.ConfigurationVariables HTTP/1.1" 401 12846

198.51.100.17 - - [07/Sep/2018:16:06:51 -0800] "GET /ct1/www/vreg?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523

203.0.113.22 - - [07/Sep/2018:16:10:02 -0800] "GET /mailman/listinfo/vreg HTTP/1.1" 200 6291

198.51.100.105 - - [07/Sep/2018:16:11:58 -0800] "GET /ct1/www/vreg/main.html HTTP/1.1" 200 7352

203.0.113.22 - - [07/Sep/2018:16:20:55 -0800] "GET /ct1/www/vreg/update.html HTTP/1.1" 200 5253

172.16.29.5 - - [07/Sep/2018:16:23:12 -0800] "GET /ct1/www/vreg/owa?template=oopsmore&m1=1.12&m2=1.12 HTTP/1.1" 200 11382

Log sample adapted from http://www.monitorware.com/en/logsamples/apache.php

SSH Logs from Web Server

Sep 07 14:22:28 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2

Sep 07 14:22:28 slacker sshd[21487]: Failed password for fsmithe from 192.168.20.185 port 1045 ssh2

Sep 07 18:27:45 slacker sshd[22325]: Illegal user admin from 218.49.183.17

Sep 07 18:27:46 slacker sshd[22325]: Failed password for illegal user admin from 218.49.183.17 port 48849 ssh2

Sep 07 18:27:46 slacker sshd[20325]: error: Could not get shadow information for NOUSER

Sep 07 20:22:28 slacker sshd[8813]: Accepted password for fsmithe from 192.168.20.185 port 1066 ssh2

Sep 07 20:22:28 slacker sshd[23857]: [ID 702911 auth.notice] User fsmithe, coming from 192.168.2.185, - authenticated.

Note: F. Smithe was on known business travel – flight departed at 19:30, landed at 22:30 on Sept. 7.

Mail Log from Web Server

Sep 9 16:50:19 dv qmail: 1223077819.930048 new msg 163786382

Sep 9 16:50:19 dv qmail: 1223077819.930096 info msg 163786382: bytes 1278560 from <> qp 24106 uid 2522

Sep 9 16:50:19 dv qmail: 1223077819.937789 starting delivery 2: msg 163786382 to fsmithe.ct1@gmail.com

Sep 9 16:50:19 dv qmail: 1223077819.937835 status: local 1/10 remote 0/20

Sep 9 16:50:19 dv qmail-local-handlers[24107]: Handlers Filter before-local for qmail started ...

Sep 9 16:50:19 dv qmail-local-handlers[24107]: from=fsmithe@dem.cc1.

Sep 9 16:50:19 dv qmail-local-handlers[24107]: to=fsmithe.ct1@gmail.com

Sep 9 16:50:20 dv qmail: 1223077820.159866 delivery 2: success: did_0+0+2/

Sep 9 16:50:20 dv qmail: 1223077820.160087 status: local 0/10 remote 0/20

Sep 9 16:50:20 dv qmail: 1223077820.160159 end msg 163786382

Note: F. Smithe denies having a gmail account fsmithe.ct1.

Application Data from Web Server

Transaction Count for September

Application	Average for September	September 2018	Notes
Administrative	450	900	Comments
Gaming	210	185	Game Licenses
Voter	350	144,750	Reg and Addrs
Medical	110	95	DME Approval
Trademark	950	1,237	Registration
Licenses	710	680	Business

Analytic Acumen: Satisfactory Is Not [Always] Sufficient

Satisficing is the strategy that looks for the first “satisfactory” solution, answer, or decision—as opposed to the optimal one.

There are many instances where this is a reasonable strategy.

- Choosing what to eat for lunch
- Investigating and handling low-impact threats

But following this strategy can have undesired consequences.

- In hiring, it can lead to poorly-formed teams that lack diversity and have incompatible personalities.
- In malware response, it can lead to reoccurring or spreading infections.

Analytic Acumen: Confirmation and Conservatism Biases

Confirmation: people tend to only consider information that confirms their already-held beliefs.

Conservatism: people prefer evidence that supports their current beliefs, even when new evidence suggests a change is needed.

Actively look for information that question beliefs.

Example

An organization experiences a cyber campaign they believe is by a certain nation-state. They research indicators they see in the attack and find some of them are associated with attacks by that nation-state. They ignore indicators having no association with that nation-state or disregard information that these indicators are also used by many other actors.

Microanalysis

Large events are made up of small actions.

Microanalysis seeks to identify both what happened in actions, and what details each action yields for the larger event.

- Lots of data crawling
- Statistics, contrasting, trending

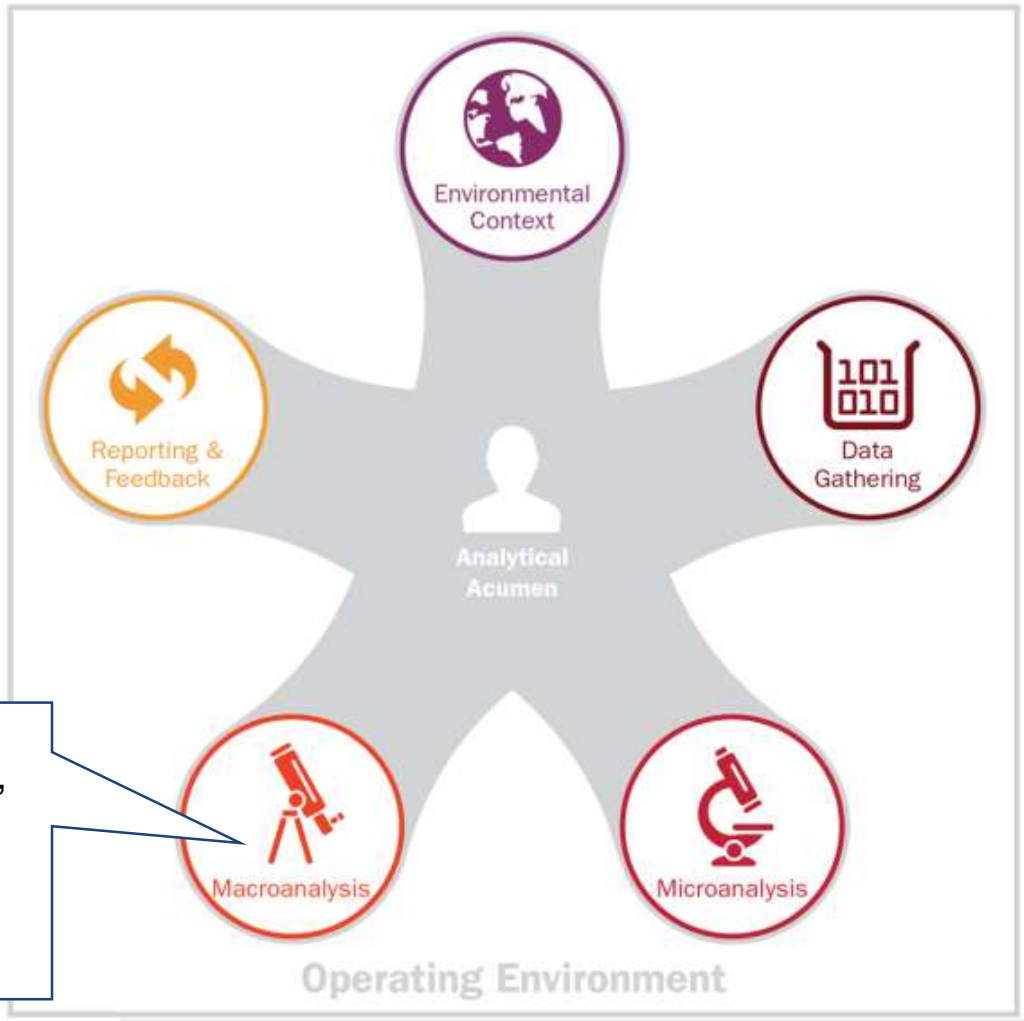
Watch out for “satisfactory” answers that might not account for the data.

Watch out for prior-held beliefs; try to look at the data with fresh eyes.

Thinking Like An Analyst: Macroanalysis

- What is macroanalysis?
- Techniques
- Mosaic theory
- Recency bias

Analysis Framework – Macroanalysis



'who' and 'why' questions: who is responsible and why is it happening?" Using extrinsic data and results of microanalysis to help answer the question(s)

What is macroanalysis?

The process of adding perspective, context, and depth to analysis

- Often, this involves trying to figure out who (or what) did something and why they did it.

Example scenario	What needs to be determined
Unauthorized use of a privileged account on a sensitive server	Who used the account? What was their end goal?
Spear phishing email sent to a researcher	Who sent the email? What did they hope to gain by it?

Common Macroanalysis Techniques

Intelligence research

- using existing reports on similar events to provide insight

Data fusion

- pulling together related information from various sources to provide more complete data

Intelligence Research

In the cyber realm, intelligence research sources include

- blogs (e.g., insights.sei.cmu.edu, isc.sans.edu)
- government information (e.g., www.us-cert.gov, www.enisa.europa.eu)
- vendor reports (Verizon DBIR, Microsoft trends)
- social media sites
- darkweb sites (caution)

Data Fusion

Fusing small pieces of data from various sources often provides better understanding.

In the cyber realm, these types of information are often useful

- registry and whois data (www.iana.org, www.iana.org/whois)
- domain and IP address history (www.robtex.com)
- known bad databases or black lists (www.virustotal.com)

Macroanalysis Example 1

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts from multiple (100+) sources to 10.127.77.135 port TCP/22, for accounts “root”, “admin”, and “fsmithe”. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

Example 1: Story so far…

Web server supports a number of citizen interactions with Country1

Attackers targeting credentials (dictionary attack), Ministry of Foreign affairs

Quiet attack, no claim of responsibility, no defacement

Human-oriented timing of attack

Web activity (voter change of address forms) and login access to voter registration records

Example 1: Macroanalysis

Does not appear to be hacking for host compromise

- Technical attack
- Impact beyond technical (sociopolitical)
- No change in site configuration, no software installation or removal

Voter registration

- Faking new voters is relatively hard (identity, in-person activity)
- Changing addresses is relatively easy (few validation options)
- Disenfranchising or complicating operations at voting locations
- (Reminder – this is a fictitious example)

Country1 is one of the few countries in the region doing change-of-address via web

Analytic Acumen: Mosaic Theory or Not?

Mosaic theory of analysis states

- analysis is like a puzzle
  - You gather as many little pieces as possible and put them together to see the picture.

Analysis really works

- more like a medical diagnosis
  - You look at a few pieces, come up with a theory, and work from there.

Analytic Acumen: Recency Bias

People tend to think of the latest as the best.

Be careful not to disregard information as invalid just because it is "old" information.

Example

An analyst sees an alert on traffic matching a signature for a piece of malware that was prevalent three years ago.

Macroanalysis

Find and tell the story.

- Who, what, when, where, why, and how
- Means, motive, opportunity, and sequence
- Motivations, capabilities, and intentions

Looking at context is key.

Avoid trying to make everything fit one perspective.

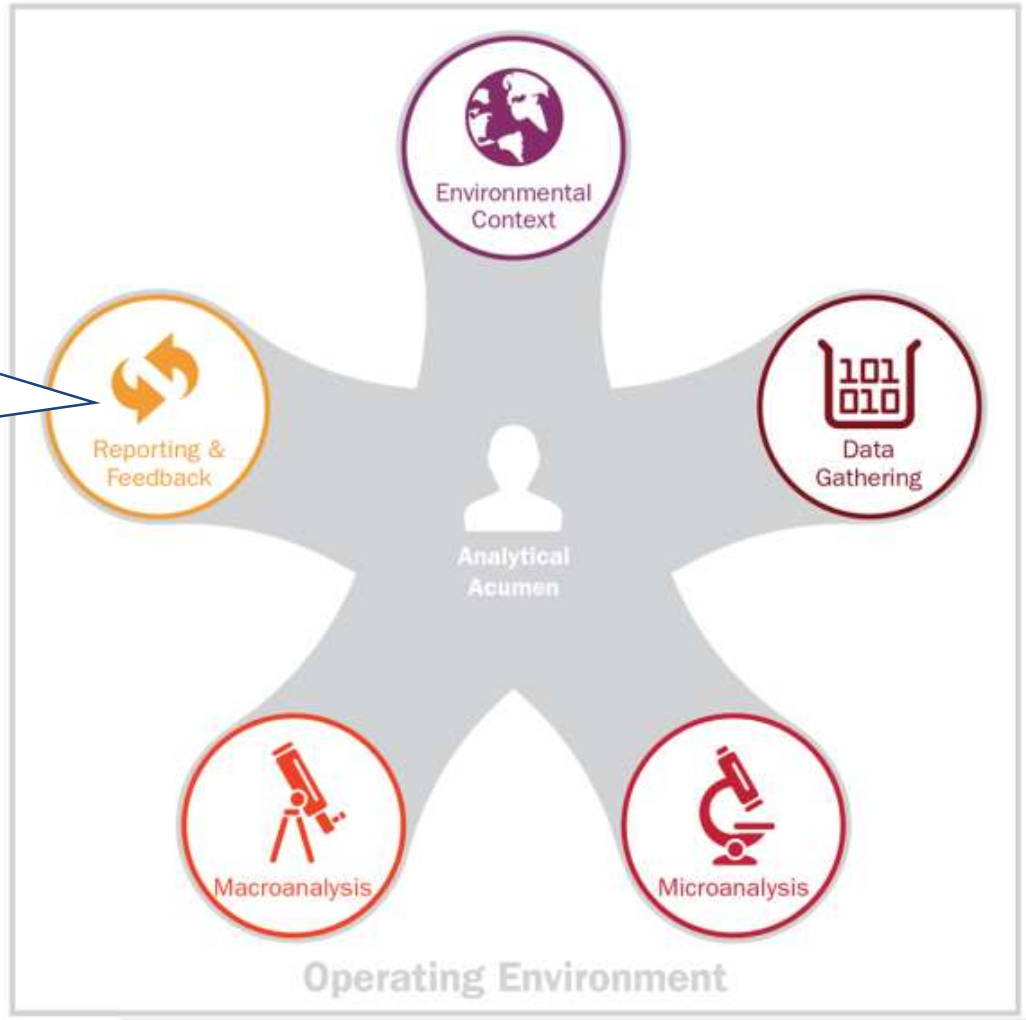
Watch for preponderance of the data.

Thinking Like An Analyst: Reporting

- Sharing
- Interpretation
- Blind-spot bias

Analysis Framework – Reporting and Feedback

To:
Management
Automata
Engineering
History



Sharing is important!

Incident ticket documentation, IR reports, and talking to other analysts or managers are all forms of reporting.

When reporting

- Know your audience.
- Make your point clear and provide evidence to support it.
- Acknowledge the limitations of your analysis and any other possibilities.

Incremental Reporting

Report what you know – but express any uncertainty

Revise prior reporting – explain the unfolding story

Use data to express

- scope of activity
- hypotheses being explored
- conclusions

Capture the report through the analysis

- Details and assumptions can be lost if not documenting throughout
- Keep the focus on data and on dealing with activity

Bottom Line Up Front

Keep the focus on supporting defense.

- Is action needed?
- If needed, what are possible courses of action?
- Based on results, which is the preferable action?

Report the data, then the interpretation.

Bring in relevant outside activity or information.

Ensure explicit statement of potential range of impact.

If you cannot articulate how and why, then you may be on the wrong track.

Macroanalysis Example 1

From: Country1 CSIRT (csirt@country1.c1)
Date: September 11, 2018 16:25:38 (-05:00)
Subject: [INC#14687915] Strange logins
To: csirt@country2.c2

We have been receiving (since Sept 4, 2018) persistent login attempts from multiple (100+) sources to 10.127.77.135 port TCP/22, for accounts “root”, “admin”, and “fsmithe”. The first account is blocked from remote login, the second is not present, and the third is a user account, but no successful login has occurred. The host in question is public-facing and used for citizen access to the Country1 Ministry of Foreign Affairs, but is also remotely administered by our support contractor. Attempts to block the attack by restricting port 22 access have not been successful to this point. Assistance in dealing with this activity is requested.

Example 1: Reporting

Is the attack real (action needed)?

- Some activity is happening on this server
- Change of common behavior
- Compromise of credentials

What can be done?

- Incident response (hot spare, change credentials, investigate and restore)
- Hold recent change of address as advisory (leave system in place)
- Increased monitoring
- Advise management and affected users

What should be done?

- Minimum disruption during critical period
- Monitor developing situation
- Advise other parties under threat

Analytic Acumen: Facts Require Interpretation

Contrary to popular belief,
facts do not speak for themselves.

Everyone interprets what they see based on their

- knowledge
- experience
- biases

Analysts must be aware of how these three things influence their interpretations and account for them in their findings and reporting.

Analytic Acumen: Blind-spot Bias

People tend to not recognize their own biases.

Analysts should have someone review their findings, especially for those that are very important or go to upper management or external entities.

Example

An analyst selected a new security appliance and is conducting a pilot test. Other analysts should review the test to ensure the analyst is not influenced by personal biases such as choice-supportive bias, pro-innovation bias, and halo effect.

Reporting

Reporting is important.

- No organization can deal with all threats completely on their own.
- There may be legal requirements that certain notification or disclosure must occur.
- Without sharing information, no accurate understanding of government-wide threats can occur.

Describe as fully as possible when reporting: avoid dropping details that may be important.

Include interpretation to place observations in proper context.

Summary: Bias

Anchoring bias

Selective perception bias

Information bias

Recency bias

Confirmation bias

Conservatism bias

Blind-spot bias

Shameless Plug for Our FloCon Conference

Join us at FloCon 2020

FloCon: Using Data to Defend

January 6-9, 2020

Savannah, GA

www.flocon.org

Course References

SEI Cyber Intelligence Research Consortium. Cyber Intelligence Conceptual Framework. https://www.sei.cmu.edu/about/organization/etc/upload/CyberInt-Conceptual-Framework.pdf

Heuer, Richards J. Psychology of Intelligence Analysis. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis

Lee, Robert M. & Bianco, David. Generating Hypotheses for Successful Threat Hunting. SANS Institute Website. https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172

Lubin, Gus & Lebowitz, Shana. 58 cognitive biases that screw up everything we do. Business Insider Website. http://www.businessinsider.com/cognitive-biases-2015-10/

Thinking Like An Analyst Part 2 Participation Scenario 1

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Department of State 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 sponsored by the United States Department of Defense.

DM18-1124

Overview

Introduction

Rules of the game

Scenario 1

Scenario 2

Scenario 3

How did we do, what did we learn

Course objectives

Describe a model of the analysis process, with distinct stages

Identify selected processes and results associated with each stage

Characterize key thinking issues (biases) that can affect analysis results

Apply the analysis process to a body of data

Introduction

These scenarios have been created to illustrate various concepts covered in the “How to be an analyst” morning session.

For all scenarios, the background is described in the

“Rules of the Game” handout

- You are an employee of the same company.
- You are described in “Who am I”.
- The company is described in “Company Info”.

Introduction

The goal of each scenario is to work through a cyber event and achieve a reasonable outcome.

Throughout the scenario, there will be several tasks and decisions.

To keep things simple and not require any special knowledge of tools, some tasks will be partially completed for you.

Choosing which tasks to complete is part of the exercise.

We will run through the scenarios as a group with as much input from you as possible.

Introduction

As we go through each scenario we may do some or all of

- Develop several hypotheses regarding the situation
- List and decide on which course(s) of action to take
- Discuss how to avoid bias in our hypotheses and decisions

Look at each decision point with that in mind.

Do you remember all of the Biases we covered this morning?

Can you recall how many we discussed?

OK, fine…

Seven Deadly Biases

1. Anchoring Bias
2. Selective Perception Bias
3. Information Bias
4. Recency Bias
5. Confirmation Bias
6. Conservatism Bias
7. Blind-spot Bias

Who am I

Name: **Alex Smith**

Role: **SOC team lead, day-shift; tier-3 analyst**

Team mates: **Four tier-1 analysts**

one tier-2 analyst

one threat intel analyst

Boss: **Jody Jones**, SOC manager

Favorite color: **Yellow**

Coffee: **Dark and black**

Quirk: **Color codes everything**

Company Info

Size: **500+ employees**

Locations: **Omaha, NE; Lexington, KY**

(both of which are in the US Central Time, DST, UTC-6)

Industry: **Legal services**

Culture: **Laid-back,**

managers are approachable

expectation that employees take initiative

when they see things that need to be done

they do them

Let’s get started

You’ve worked through your morning routine.

- reading the morning reports
- getting coffee
- checking your email
- going over all your dash-boards

You have discovered three potential issues that you need to address.

You have prioritized them

Here’s the first one

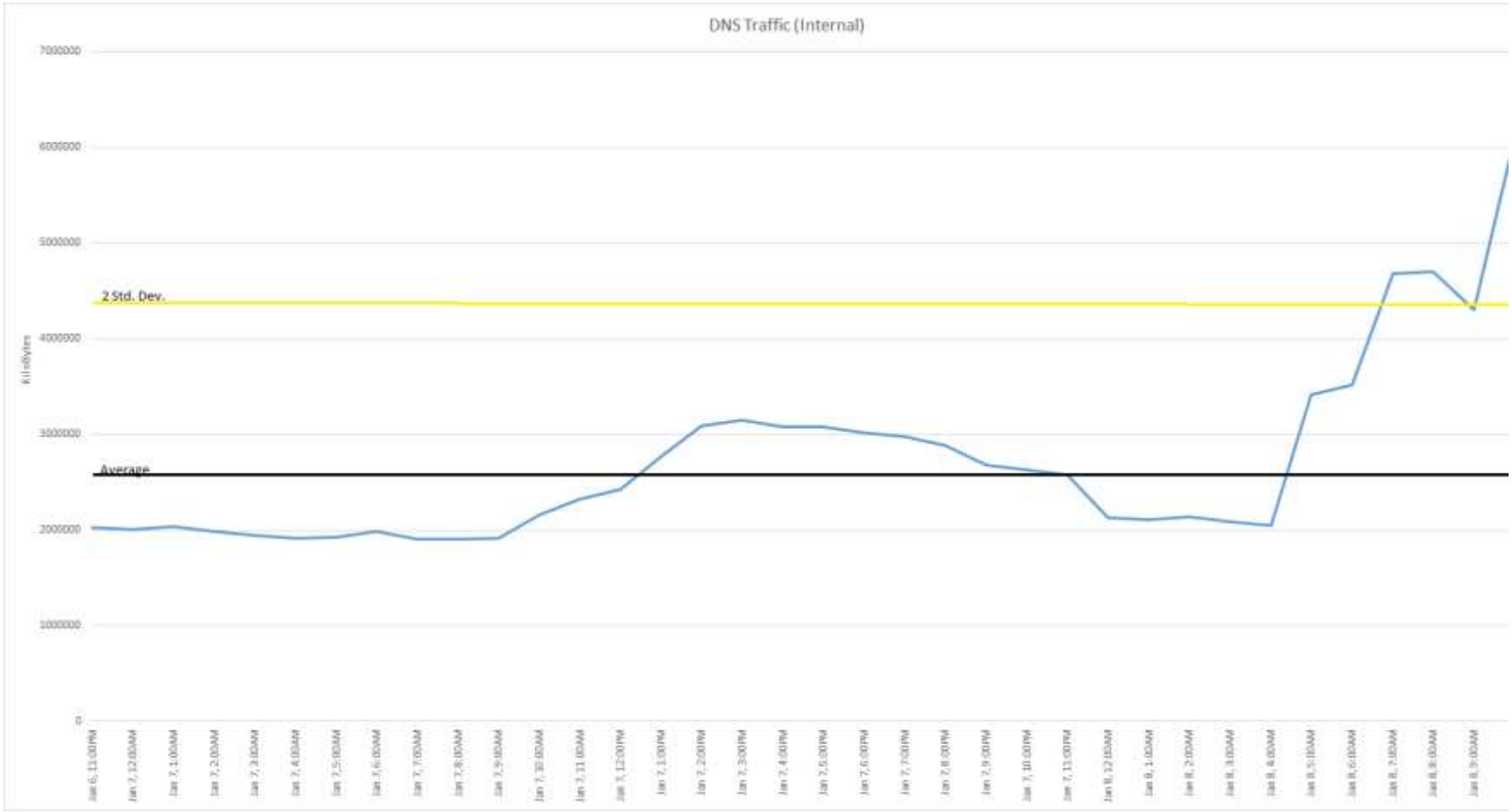
Scenario 1
DNS

Most of your dashboards are nominal

except the DNS server dashboard

which catches your attention

DNS Traffic (Internal)



Task 1 Problem Statement

The volume of internal DNS requests to your DNS resolver more than doubled around 0730 this morning.

Employees are beginning to complain that they cannot connect to various news or social media sites. These include:

- www.socialskilz.com
- www.connectingthere.com

You want to figure out where the problem is.

Task 1 Steps

How do you determine the location of the problem?

- Confirm the problem
- Narrow it down
- Develop one or more hypotheses
  - And methods of testing

Task 1.1

From your desktop, check if you can get to any of the sites mentioned by users.

```
(1)$ ping www.socialskilz.com
 ping: unknown host www.socialskilz.com
(2)$
(2)$ ping www.connectingthere.com
 ping: unknown host www.connectingthere.com
(3)$
```

Task 1.2

From your smartphone, check if you can get to any of the sites mentioned by users.

```
https://www.socialskilz.com
Network error (dns unresolved hostname)

https://www.connectingthere.com
Network error (dns unresolved hostname)
```

Task 1.3

From your desktop, check if you can get to other sites on the Internet

```
 (3) $ ping example.com
PING example.com (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=1 ttl=56 time=11.1 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=2 ttl=56 time=11.2 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=3 ttl=56 time=11.2 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=4 ttl=56 time=11.2 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=5 ttl=56 time=11.2 ms
64 bytes from 93.184.216.34 (93.184.216.34): icmp_seq=6 ttl=56 time=11.2 ms
^C
--- example.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 11.188/11.234/11.287/0.127 ms
(4) $
```

Hypotheses

1. This is an **external** problem that I cannot help.
2. This is an **internal** problem that I cannot help.
3. This is an **external** problem that I may be able to mitigate
4. This is an **internal** problem that I can resolve.

Decision 1.1

1. This is an **external** problem that I cannot help.
2. This is an internal problem that I cannot help.
3. This is an external problem that I may be able to mitigate
4. This is an internal problem that I can resolve.

Decision 1.2

1. This is an external problem that I cannot help.
2. This is an **internal** problem that I cannot help.
3. This is an external problem that I may be able to mitigate
4. This is an internal problem that I can resolve.

Decision 1.3

1. This is an external problem that I cannot help
2. This is an internal problem that I cannot help
3. This is an **external** problem that I may be able to mitigate
4. This is an internal problem that I can resolve

Decision 1.4

1. This is an external problem that I cannot help
2. This is an internal problem that I cannot help
3. This is an external problem that I may be able to mitigate
4. This is an **internal** problem that I can resolve

Decision 1

Which do you choose?

Decision 1 Score

	Decision	Score
1	This is an **external** problem that I cannot help.	0
2	This is an **internal** problem that I cannot help.	0
3	This is an **external** problem that I may be able to mitigate	2
4	This is an **internal** problem that I can resolve.	1

Bias

Did we fall prey to any of the seven biases we've discussed?

Task 1.1 Anchoring Bias: there is a problem it must be ours

Task 1.2 Shows it is not just our problem

Task 1.3 Shows it is not Internet wide

Task 2

Managers need answers as to what is going on.

The Public Relations team is unable to do their job.

Internet traffic is sluggish, which is interfering with work for several other departments.

You need to figure out what is going on.

First you need to determine if you should restart your internal DNS server.

How might you do that?

Task 2.1 Check memory and CPU usage on server

```
top - 20:54:03 up 694 days,  1:54,  2 users,
load average: 2.61, 2.78, 2.64
Tasks: 745 total, 4 running, 740 sleeping, 0 stopped, 1 zombie
Cpu(s): 8.4%us, 0.3%sy, 0.0%ni, 91.3%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem:  132125540k total, 114625092k used, 17500448k free, 15139432k buffers
Swap:  4193276k total,  2842228k used,  1351048k free, 93274368k cached
```

Task 2.2 Check the Network

```
(7) $ netstat -su
IcmpMsg:
    InType0: 4
    InType3: 21758
    InType8: 219193
    InType11: 1
    OutType0: 219193
    OutType3: 2303
    OutType8: 132
Udp:
    2528550068 packets received
    8719 packets to unknown port received.
    430 packet receive errors
    1804811989 packets sent
UdpLite:
IpExt:
    InBcastPkts: 224
    InOctets: 93973245041736
    OutOctets: 129672772630325
    InBcastOctets: 74313
(8) $
```

Decision 2 Which do you choose?

1. Yes, restart the DNS server
2. No, don't restart the server

Decision 2.1

1. Yes, restart the DNS server
2. No, don't restart the server

Decision 2.2

1. Yes, restart the DNS server
2. No, don't restart the server

Decision 2 Score

	Decision	Score
1	Yes, restart the DNS server	0
2	No, don’t restart the server	1

Bias

Did we fall prey to any Biases we've discusses?

Information Bias

- People tend to seek information even when that information will not change the end results.

Did we really learn anything we didn't already know from the results of Tasks 2.1 and 2.2?

Not really

While we could not get to some Web sites

We did get a response from *example.com*

Task 3 Event or Incident?

We have an “Event” on our hands

If it is an actionable “Incident” we must act

Decision 3 Incident Response

Next, determine if you need to implement an incident response plan.

What goes into this decision?

- What would be the desired outcome of implementing the plan?
- What steps would be taken as part of the plan?
- When would the plan be completed?

Decision 3

1. Yes, implement an Incident Response plan
2. No, don't implement an Incident Response plan

Decision 3.2

1. Yes, implement an Incident Response plan
2. No, don't implement an Incident Response plan

Decision 3 Score

	Decision	Score
1	Yes, implement an Incident Response plan	0
2	No, don’t implement an Incident Response plan	1

Task 4

Next, you need to find out what is going on to explain to Acme's managers.

How do we do this?

We know what it looks like from our vantage point

But is anyone else affected?

Where can we find that sort of information?

Task 4.1 Read *OnTopOCyber.org*

OnTopOCyber
By: Meg A. Byte

DNS provider ReLyCDN is currently being attacked using a very aggressive DDoS attack. If you use them for your website DNS you probably have experienced outages today.
This attack affects any website or online service that uses ReLyCDN for DNS resolution. So far this attack has affected:

- PayMeThisWay
- SocialSkillz
- Tixetz ticket sales were affected earlier today according to WP Slack #community-team channel.
- GiterDone
- CloudySound
- ConnectingThere
- NileBuy

Task 4.1 Read *OnTopOCyber.org* continued

This attack may affect your website shopping cart checkout if you use a service provider who has been affected by the attack. It may also affect other features or services you provide to customers that rely on being able to contact a site affected by the attack.

If your website is affected by this attack, you should consider setting up another DNS provider as your secondary DNS or temporarily moving all DNS to another provider. You will need to exactly duplicate your DNS configuration on the new provider before making it the authoritative DNS for your domain and this may take some time. The transfer may take up to 48 hours, by which time this may all be over.

The attack appears to be an attack on ReLyCDN's infrastructure according to their technical updates. They are working continuously to mitigate the attack.

Task 4.1 Read *OnTopOCyber.org*

What do we know?

-
-

Relevant facts we learned

-
-
-

Task 4.2 Read *CyberSecTimes.com*

CyberSecTimes

Several major websites have reported outages today. Other sources, have reported that DNS provider ReLyDNS is suffering a DDOS attack. DDoS is short for a denial of service attack. Hackers use DDoS attacks to prevent the internet server from giving service to a website. A user will not be able to access a website where ever it is being hosted. How are they able to accomplish?

Hackers get hundreds (or thousands) of internet users to download a specialized software with the intent of utilizing a denial of service attack. The users who download this type of software may know that they are downloading it with a full intent on being a part of a denial of service attack. All of the users with the downloaded denial of service attack software on their computers attack the targeted websites may execute the attack at the will of the hacker. These hundreds (or thousands) of computers will send multiple request (thousands of times) within milliseconds, flooding the server that hosts the website.

The server will then become overloaded with all these requests and have no choice but to shut down. The server shutting down will force the website to no longer be on the web.

Task 4.2 Read *CyberSecTimes.com*

What do we know?

-
-

Relevant facts we learned

-
-
-

Task 4.3 Read *Industry-ISAC.com*

Industry-ISAC

ReLyCDN is unable to resolve domains.
Indicators of the issue include:

- Traffic to RyLyCDN domain servers:
  - 711.0.0.53, 711.0.1.53, 711.0.2.53, 711.0.53.0.
- Slow load times for
  - PayMeThisWay.com
  - SocialSkillz.com
  - Tixetz.net
  - GiterDone.org
  - CloudySound.com
  - ConnectingThere.com
  - NileBuy.net

Task 4.3 Read *Industry-ISAC.com*

What do we know?

-
-

What relevant facts did we learn?

-
-
-

Task 4.4 Read *Round-about-security.net*

Network Error (dns_unresolved_hostname)

Your requested host "round-about-security.net" could not be resolved by DNS.

For assistance, contact your network support team.

Task 4.4

What do we know

- *Round-about-security.net* isn't the best source of intel
-

Relevant facts we learned

- Only that we can't get to the web site
-
-

Decision 4

What do you do to explain what is happening?

Decision 4.1

What do you do to explain what is happening?

1. Send an email to managers, the intranet bulletin board, and employee notice alias.
2.
3.

Decision 4.1

What do you do to explain what is happening?

1. Send an email to managers, the intranet bulletin board, and employee notice alias.
2. Talk individually to all managers about what is happening.
3.

Decision 4.1

What do you do to explain what is happening?

1. Send an email to managers, the intranet bulletin board, and employee notice alias.
2. Talk individually to all managers about what is happening.
3. Post a notice to the intranet bulletin board.

Decision 4 Score

	Decision	Score
1	Send an email to managers, the intranet bulletin board, and employee notice alias.	2
2	Talk individually to all managers about what is happening.	0
3	Post a notice to the intranet bulletin board.	1

Task 5 Network Problem?

While working on communicating out what is going on, you notice that internal resources are getting sluggish.

You wonder if this is due to internal DNS response issues or network bandwidth issues.

Task 5.1 Check overall network traffic volumes.

Summary:

type	average	peak	peak sTime	>2Std.Dev.
in	7495038583	9724114903	01/08/2018T06:00:00	N/A
out	5283093470	8195335893	01/08/2018T07:00:00	01/08/2018T07:00:00 01/08/2018T08:00:00
int2int	8365641358	10579703283	01/07/2018T10:00:00	N/A

Task 5.2 Check network traffic volumes by service to the server.

Summary:

type	port	average	peak	peak sTime	>2Std.Dev.
in	53	1510227542	1944822981	01/08/2018T06:00:00	N/A
in	80	1132670656	1458617235	01/08/2018T06:00:00	N/A
in	123	226534131	291723447	01/08/2018T06:00:00	N/A
out	53	1023424607	1639067179	01/08/2018T07:00:00	01/08/2018T07:00:00 01/08/2018T08:00:00 01/08/2018T10:00:00
out	80	790646034	1131298521	01/08/2018T09:00:00	N/A
out	123	156757778	218259704	01/08/2018T09:00:00	N/A
int2int	53	1667858259	2115940657	01/07/2018T10:00:00	N/A
int2int	80	1250893694	1586955493	01/07/2018T10:00:00	N/A
int2int	123	250178738	317391098	01/07/2018T10:00:00	N/A

Task 5.2 Check internal DNS server logs

```
tail emergency.log
  <empty>
tail alert.log
 <empty>
tail critical.log
 <empty>
tail error.log
 <empty>
```

Decision 5

How do you remediate the internal traffic issues?

1. Restart the DNS server.
2. Let the network administrator know what you have found.
3. Do nothing.

Decision 5 Score

	Decision	Score
1	Restart the DNS server	0
2	Let the network administrator know what you have found	2
3	Do nothing	1

Task 6 Check for Updates

OnTopOCyber
By: Meg A. Byte
...
[Updated at 12:18pm Pacific Time]
This attack has largely been mitigated by ReLyCDN. Residual network slowdowns may affect your:
External assets like fonts, style-sheets, javascript (like jQuery), images or any external page component you load from an outside server. These may become inaccessible and stall the page load. The fix in this case is to move that asset onto your own server and reference it locally.

Social media integration. ConnectingThere was not available earlier today and if it's API becomes unavailable, it may affect certain pages loading and may affect user's ability to share posts.

Backups. If your backups are stored off-server on an external domain, make sure that domain stays accessible or backups may not be copied over.

Checkout. Already mentioned, but if your payment processor goes offline, it will stall all transactions on your site and may even make certain pages inaccessible. PayMeThisWay has been affected by this but appears to be back.

Task 7 Report

Create a single report of the incident

- executive summary
- detailed section that can be provided to managers on request
- used by analysts to update and close all their related open tickets

Primary Report on the Event

This morning RyLyCDN experienced a successful denial of service attack against their DNS services. This meant that people throughout the world that were trying to visit websites that use RyLyCDN's services were not able to find the websites. These included SocialSkillz.com and ConnectingThere.com, which are used by our employees on a day to day basis.

Due to the problems with these and other high-use websites, our internal DNS server experienced an increase in requests. At one point this morning this resulted in our internal resources (i.e. intranet) having slower than normal response times. These issues have been resolved.

The RyLyCDN attack appears to have terminated and the impacted websites are back to normal.

Questions?

Comments?

Thinking Like An Analyst Part 2 Participation Scenario 2

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Department of State 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 sponsored by the United States Department of Defense.

DM18-1124

Overview

Introduction

Rules of the game

Scenario 1

Scenario 2

Scenario 3

How did we do, what did we learn

Let’s get started

You successfully managed a DNS outage

Now on to the one you listed as the second priority

Scenario 2: Phishing Email

Check email…

While going through your email, you noticed an odd message from the IT department.

Email Message Text

Alex,

We have sent you this email, because we have reason to believe your Active Directory account has been used for dissemination of sensitive company info. In order to absolve you of any fraudulent activity, we are required to open an investigation into this matter. You have 1 business day to verify that you did not violate company policy or we will lock your account and begin termination proceedings.

To confirm your account please click this link and enter your credentials when prompted:
confirming-account.acme.com.link

Sincerely,

Acme IT

Task 1 What to do about the suspicious email

Form one or more hypotheses

Test them

Hypotheses

What is *your* Hypothesis?

1. This is a policy violation by IT.
2. This is a phishing attempt targeting yourself.
3. This is a phishing attempt targeting multiple individuals.
4. This is a legitimate request.

You need to determine what, if anything, needs to be done regarding the email.

Task 1 Determine the following

1.1 Is this a policy violation by IT (perhaps an IT policy violation)

1.2 Am I the target?

1.3 Are multiple Acme employees targeted?

1.4 Is this a legitimate request?

Task 1.1

Hypothesis 1 (This is a policy violation by IT)

Try the obvious first

Which is…?

Ask them

Ask the IT Department : Transcript of chat session

Smith: Hey Terry you there?

Terry: Hello Alex! What's up?

Smith: Did IT send out an email earlier today with a link to verify active domain creds?

Terry: Are you kidding me?

Smith: I know

Smith: but I had to ask.

Terry: No... IT would never do that. That is a policy violation.

Task 1.2

1.2 This is a phishing attempt targeting yourself.

Possible courses of action

- Examine the email header
- Ask others if they got one

Task 1.2 Examine the email header

What do we want to find out?

Where do we look?

Will we know when we found it?

Phishing Email Header

```
Received: from EMAIL.ACME.ORG ([10.64.28.250]) by
 EMAIL2.ACME.ORG ([10.64.28.249]) with mapi id 14.03.0361.001; Mon, 26 May 2019 11:57:11
-0400
Received: from AMCE.XYZ ([654.122.11.8]) by EMAIL.ACME.ORG ([10.64.28.250])
 with mapi id 14.04.0531.001; Mon, 26 May 2019 11:57:11 -0400
From: Acme IT <IT@AMCE.XYZ>
To: <ASmith@ACME.org>
Subject: Potential data leaking-confirm it is not so
Date: Mon, 26 May 2019 11:57:10 -0400
Message-ID: <AA35F3AFCE38674FBD8087DC90B55C070104400408@EMAIL>
References: <AA35F3AFCE38674FBD8087DC90B55C070104400227@EMAIL>
 <DBA07B8EB519C549AE2B76609997096C613C8307@EMAIL>
In-Reply-To: <DBA07B8EB519C549AE2B76609997096C613C8307@EMAIL>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <AA35F3AFCE38674FBD8087DC90B55C070104400408@EMAIL>
MIME-Version: 1.0
X-MS-Exchange-Organization-AuthSource: AUTH.EMAIL.ACME.ORG
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [10.64.22.6]
X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0
Content-type: multipart/alternative;
          boundary="B_3593579173_1803306192"

> This message is in MIME format. Since your mail reader does not understand
this format, some or all of this message may not be legible.
```

Phishing Email Header

```
Received: from EMAIL.ACME.ORG ([10.64.28.250]) by
 EMAIL2.ACME.ORG ([10.64.28.249]) with mapi id 14.03.0361.001; Mon, 26 May 2019 11:57:11
-0400
Received: from AMCE.XYZ ([654.122.11.8]) by EMAIL.ACME.ORG ([10.64.28.250])
 with mapi id 14.04.0531.001; Mon, 26 May 2019 11:57:11 -0400
From: Acme IT <IT@AMCE.XYZ>
To: <ASmith@ACME.org>
Subject: Potential data leaking-confirm it is not so
Date: Mon, 26 May 2019 11:57:10 -0400
Message-ID: <AA35F3AFCE38674FBD8087DC90B55C070104400408@EMAIL>
References: <AA35F3AFCE38674FBD8087DC90B55C070104400227@EMAIL>
 <DBA07B8EB519C549AE2B76609997096C613C8307@EMAIL>
In-Reply-To: <DBA07B8EB519C549AE2B76609997096C613C8307@EMAIL>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <AA35F3AFCE38674FBD8087DC90B55C070104400408@EMAIL>
MIME-Version: 1.0
X-MS-Exchange-Organization-AuthSource: AUTH.EMAIL.ACME.ORG
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [10.64.22.6]
X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0
Content-type: multipart/alternative;
          boundary="B_3593579173_1803306192"

> This message is in MIME format. Since your mail reader does not understand
this format, some or all of this message may not be legible.
```

Results from Email Header

The email was to me rather than to a list

So Hypothesis 2 is good

But could Hypothesis 3 be valid also?

Task 1.3 Did other employees receive one?

Could it be part of a larger campaign?

Possible courses of action

- Check intel feeds
- Find our more about the sender
- Look at incoming email logs

Is it part of a larger campaign?

OnTopOCyber

No results for "IT phishing" in the last 7 days. Please try new search.

Suggested Stories:
* Cloud this and cloud that! What is the cloud? No..seriously...we are asking.
* Ransomware is on the rise. How can you protect yourself?
- PSexec is your friend and your enemy.

Find out more about the sender (amce.xyz)

```
$ whois amce.xyz

Whois Record for amce.xyz
Domain Profile
Registrant Org          Gettin Away With It
Registrar Status
Dates
Created on 2019-05-20
Expires on 2021-05-19
Updated on 2019-05-24

Tech Contact    Host Master
IP Address      654.122.11.8 is hosted on a dedicated server

IP Location     United States - Not Here Rd, NY, NY
ASN
Whois Record ( last updated on 2019-05-24 )
$
```

Find out more about the sender (amce.xyz)

```
$ nslookup amce.xyz
 DNS server handling your query: localhost
 DNS server's address:      127.0.0.1#53

 ** server can't find amce.xyz: NXDOMAIN

$
```

How many reported the message

```
<Check IT abuse mailbox for user reports>

Results:
 13 with sender 'IT@AMCE.XYZ' earliest data ‘May 26, 2019'
  4 with subject
        'Potential data leaking-confirm it is not so'
        earliest data ‘May 27, 2019‘
```

How many received a message from the Phisher?

<search email server incoming logs for sender email address>

```
53 messages with sender 'IT@AMCE.XYZ'
earliest data ‘May 25, 2019'
```

At most 17 reported it, but 53 messages were received

What did we learn?

From the intel feed?

From the whois?

From the nslookup?

From the server log queries?

Decision 1 rating

This is a policy violation by IT.

This is a phishing attempt targeting yourself.

This is a phishing attempt targeting multiple individuals.

This is a legitimate request.

Decision 1 Score

	Decision	Score
1	This is a policy violation by IT.	0
1.1	This is an IT policy violation	1
2	This is a phishing attempt targeting yourself.	2
3	This is a phishing attempt targeting multiple individuals.	2
4	This is a legitimate request.	0

Bias?

Did we fool ourselves by being biased?

Did we really learn anything from the header, whois and nslookup?

We know it was not from IT,

Actually, we already knew that, but wanted to make

- Absolutely
- 100%
- Positively
- Certain

And wasted time in the process

Information Bias again

Decision 2 What to do next?

You have the results of the tasks

Which course of action do you take?

Can you take more than one?

1. Delete the email from your inbox
2. Submit block request for email sender and pull the emails from inboxes
3. Submit a block request on the email subject
4. Send company-wide email telling everyone to delete the email if they get it and not respond with the requested information

Decision 2 Score

	Decision	Score
1	Delete the email from your inbox	1
2	Submit block request for email sender and pull the emails from inboxes	2
3	Submit a block request on the email subject	0
4	Send company-wide email telling everyone to delete the email if they get it and not respond with the requested information	1

Hypothesis 3

No one responded to the message

Task: Look for responses to the message

Task: Determine if enough data was transferred to be “dangerous”

Task: Look for responses to the message

<Check for replies to the message>

```
Results: 1 with recipient IT@AMCE.XYZ
         sender:jtoast@acme.com
         earliest data ‘May 26, 2019‘
```

Task: Determine if enough data was transferred to be “dangerous”

<Query NetFlow repository for outgoing connections to the link IP address in the message>

```
$ rwfilter --pass=stdout --start=$START --end=$END \
       --type=out,outweb --daddr=$IP \
   | rwuniq --fields=stime,sip,dip,proto,sport,dport   \
       --values=bytes,packets  \
       stdin
```

```
sTime               sIP          dIP           pro  sPort  dPort   Bytes    Packets
05/27/2019T14:40:21  10.20.0.216  654.122.11.8  6    54238  80        1572     56
05/27/2019T14:40:21  10.20.0.216  654.122.11.8  6    54246  80      129024   1076
```

Decision 3

Which should we do?

1. Nothing, we reset the user's account, we're done
2. Find out what information the user exfiltrated
3. Find out how much damage was actually done
4. Ask the boss for advice

Decision 3

Which should we do?

Nothing, we reset the user's account, we're done

Needed to be done, but not enough

Find out what information the user exfiltrated

Maybe later, not that relevant now

Find out how much damage was actually done

Attacker has user credentials, what was done with them?

Ask the boss for advice

Boss will get annoyed and tell you to get to work

Decision 4 Score

Decision	Discussion
Nothing, we reset the user's account, we're done	Needs to be done, but it is not enough
Find out what information the user exfiltrated	Maybe later, not that relevant now
Find out how much damage was actually done	**Attacker has user credentials, what was done with them?**
Ask the boss for advice	Boss will get annoyed and just tell you to work on it

Find our how much damage was done - 1

Check audit logs for anomalous logins.

```
$ tail audit.log | grep "root"

 type=USER_AUTH msg=audit(1222222222.123:14873): user
pid=7263 uid=372 auid=372 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 msg='op=authentication acct=root exe/bin/su
hostname=? addr-? terminal=pts/0 res=success'
```

Find our how much damage was done - 2

Check audit logs for anomalous logins.

```
$ tail audit.log | grep "root"

 type=USER_AUTH msg=audit(1222222222.123:14873): user
pid=7263 uid=372 auid=372 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 msg='op=authentication acct=root exe/bin/su
hostname=? addr-? terminal=pts/0 res=success'
$
```

Find our how much damage was done - 3

Check application logs for anomalous activity

```
$ tail application.log | grep "Audit Login"

Audit Login  Login failed     master    DB          Admin       1/8/2018
Audit Login  Login failed     master    DB          Admin       1/8/2018
Audit Login  Login failed     master    DB          Admin       1/8/2018
Audit Login  Login failed     master    DB          jtoast      1/8/2018
Audit Login  Login failed     master    DB          jtoast      1/8/2018
Audit Login  Login failed     master    DB          jtoast      1/8/2018
Audit Login  Login failed     master    DB          Guest       1/8/2018
Audit Login  Login failed     master    DB          Guest       1/8/2018
Audit Login  Login failed     master    DB          Guest       1/8/2018
Audit Login  Login failed     master    DB          Root        1/8/2018
Audit Login  Login succeeded  master    DB          Root        1/8/2018
$
```

Decision 4

It looks bad, how to proceed?

1. Initiate incident response.
2. Disable the impacted account.
3. Close the incident as resolved.

Decision 4 Score

Decision	Discussion
Initiate incident response.	**And the sooner the better, because it could get worse**
Disable the impacted account.	Already reset password, but how many more will click?
Close the incident as resolved.	Not even close to being resolved

Questions?

Comments?

Shameless Plug for Our Conference

Join us at FloCon 2020

FloCon: Using Data to Defend

January 6-9, 2020

Savannah, GA

www.flocon.org

Course References

SEI Cyber Intelligence Research Consortium. Cyber Intelligence Conceptual Framework. https://www.sei.cmu.edu/about/organization/etc/upload/CyberInt-Conceptual-Framework.pdf

Heuer, Richards J. Psychology of Intelligence Analysis. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis

Lee, Robert M. & Bianco, David. Generating Hypotheses for Successful Threat Hunting. SANS Institute Website. https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172

Lubin, Gus & Lebowitz, Shana. 58 cognitive biases that screw up everything we do. Business Insider Website. http://www.businessinsider.com/cognitive-biases-2015-10/

Thinking Like An Analyst
Part 2
Scenario 3
Participation

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Department of State 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 sponsored by the United States Department of Defense.

DM18-1124

Overview

Introduction

Rules of the game

Scenario 1

Scenario 2

Scenario 3

How did we do, what did we learn

Let’s get started

You successfully managed a phishing disaster

Now on to the one you listed as the third priority

Scenario 3 Cyber Group Targeting Acme

While talking to your team this morning, your threat intelligence analyst brings to your attention threats that are being made against Acme by the cyber hacker collective COYOTE.

Verbal attacks have been an on-going occurrence for several weeks

But now COYOTE is talking about

“Acme’s coming doomsday”

What do we know?

In further discussion with your team, you find out that

COYOTE has been known to follow through with threats to other organizations in the past.

Decision 1 What to do about COYOTE?

1. This is just a bluff that can be ignored and does not require your attention.
2. They may follow through and you can stop it.
3. They may follow through and you can prepare.

Decision 1 Score

Decision	Yes/ No	Discussion
This is just a bluff that can be ignored and does not require your attention.		
They may follow through and you can stop it.		
They may follow through and you can prepare.		

The plot thickens

Your CEO, Bob Acme, has heard about the threats through a colleague and wants to know what the organization has done to mitigate any attack.

As you haven't yet done anything, you tell him you're on it.

What are some courses of action?

Courses of Action

1. Further discussion with your threat intel analyst
    1. How does COYOTE operate and other questions
2. Read threat feeds
    1. OnTopOCyber.org
    2. Industry-ISAC.com
    3. CyberSecTimes.com
    4. Round-about-security.net

Are there any viable technical courses of action at this time?

Discussion with Mary, the Threat Intel Analyst

Smith: Hi Mary, have time to chat about COYOTE?

Mary: Sure Alex. What do you need to know?

We need to make sure we're protected against attacks. What can you tell me about how COYOTE operates?

Well, they've done some damage with DDoS attacks. Managed to degrade performance of the *XYZZY* website and took *Whoot Delivery* offline for over an hour. They also appear to have had some successful email phishing campaign. Oh, and when *Whoot Delivery* came back online, their website was defaced. Seems COYOTE conducted a successful web injection attack on the website just before the DDoS.

Discussion with Mary, the Threat Intel Analyst

How sophisticated would you say they are?

Technologically, I would say moderate. They seem to use *Low Orbit Ion Cannon* for DDoS. I came across one of their phishing emails--it was pretty good.

What is *Low Orbit Ion Cannon*?

It's an open-source network stress testing tool that is being used for DoS attacks. Get a bunch of them sending traffic to the same target and they can generate a pretty good load.

What is a pretty good load in terms of COYOTE capability?

Not sure. They seem to have a lot of members, but I have not come across any indication that they control any wide-spread botnets.

Ok, thanks. Let me know if you find out anything else.

Sure, no problem, happy to help.

On Top O'Cyber

OnTopOCyber
By: Meg A. Byte
2 search results for COYOTE
Result 1
COYOTE Melts Fud's Fudges
2017/10/13

This past week Fud's Fudges candy company was knocked offline for over a day by several members of COYOTE. A hacker known as K1lzSw1ch and another that goes by the handle TayzorFayse were bragging on several dark web forums and encouraging others to join in the attacks.

K1lzSw1ch has been very vocal in his displeasure with the political backing the candy company has provided to, as he put it, "the wrong candidate".

On Top O'Cyber

So who is this K1lzSw1ch? I've done some research and have a pretty good idea. If you remember, in our last post about COYOTE (COYOTE Delivers Whoot Delivery a Speed Bump) we talked about Harry Jones, AKA Mr. Xaisar.

Since then, Mr. Jones has been arrested and is sitting in a UK prison waiting extradition to the US. According to the extradition request, he worked for Prickle Technology as a sales rep and is accused of bribery and other fraudulent activities in the US.

With this information I began digging into Mr. Jones' activities and acquaintances. What I found lead me to the conclusion that Mr. Jones' (former) coworker Tom Brown is this K1lzSw1ch.

On Top O'Cyber

Result 2
COYOTE Delivers Whoot Delivery a Speed Bump
2017/02/24

Whoot Delivery, and on-demand, ride share taxi service was unable to provide services for over an hour this morning due to a DDoS attack. According to the website defacement discovered on the Whoot website after the attack, the perpetrators were the hacker collective COYOTE. According to the defacement, they were conducting a "protest" of Whoot's management firing their lead counsel who is currently embroiled in a bribery scandal.

Why could COYOTE care about a bribery scandal? I've been doing research to find out.

On Top O'Cyber

It turns out that this particular bribery scandal involves fraudulent activity that has been conducted from both the US and UK. According to reports, Whoot's lead counsel accepted bribes from a sales rep for an unnamed UK company to agree to contracts that critics say were against investor interests.

It appears that the sales rep in question is one Harry Jones. Though I have not yet found out what company Mr. Jones works for, I have found out quite a bit else about him:

- Very vocal on ConnectingThere about contractor pay with companies like Whoot.
- Talks daily about the COYOTE hacker collective.
- Was called Mr. Xaisar once in a response to a posting.

That last item lead me to do some digging. Mr. Xaisar is the handle used on a hacker forum of an admitted member of COYOTE.

Industry-ISAC.com

Industry-ISAC
1 result for "COYOTE"
2017/06/09 (Updated: 2017/11/22)

COYOTE is a cyber hacker collective engaging in hacktivism.
They are best known for attacks on these organizations:
* Fud's Fudges, DDoS
* Whoot Delivery, DDoS and website defacement
* XYZZY, DDoS

Indicators of compromise:
* Large, concurrent amounts of traffic from multiple IP addresses in the ranges
    * 323.9.8.4/30
    * 425.23.68.16/30
    * 516.124.84.0/30
* Email traffic that passed through 425.23.68.100 on the way to the recipient
* Emails containing compressed attachments with COYOTE RAT malware
* Emails containing links to sites dropping COYOTE RAT malware

CyberSecTimes.com

CyberSecTimes

1 search result for COYOTE

COYOTE vs. Fud's Fudges
2017/10/15

Fud's Fudges, the well-known candy company, was caught by the neck by COYOTE. No, not the animal, the hacker collective. According to OnTopOCyber, COYOTE was throwing a fit due to the political endorsement of the "wrong candidate" by the candy making giant.

Industry-ISAC.com states that COYOTE has targeted Whoot Delivery and XYZZY in the past.

Decision 2 Which attacks may you need to mitigate?

1. DDoS against the webserver
2. DDoS against the DNS server.
3. Malware injection attack on public website.
4. Malware studded email.

Relevant Information – 1

What useful information did we gather from the reading we just did?

- They use Low Orbit Ion Cannon for DDoS
  - Degrade or take web sites off line
- Successful web injection attack on a website
- Large, concurrent amounts of traffic from multiple IP addresses in the ranges
  - 323.9.8.4/30
  - 425.23.68.16/30
  - 516.124.84.0/30

Relevant Information – 2

- Email traffic that passed through 425.23.68.100 on the way to the recipient
- Emails containing compressed attachments with COYOTE RAT malware
- Emails containing links to sites dropping COYOTE RAT malware

Decision 2

Mitigate?	Yes/ No	Discussion
DDoS against the webserver		
DDoS against the DNS server.		
Malware injection attack on public website.		
Malware studded email.		

Courses of action

What do we do to protect against COYOTE's threatened attacks?

- Nothing, what will happen will happen
- Nothing, we are invulnerable
- Find out how vulnerable are we?
- Which attacks should we work to mitigate?

Courses of action

What do we do to protect against COYOTE's threatened attacks?

- ~~Nothing, what will happen will happen~~
- ~~Nothing, we are invulnerable~~
- Find out how vulnerable are we?
  - **We pay our service provider, let's find out more**
- Which attacks should we work to mitigate?

Find out about Services provided

(Calling Smoke Screen Providers)

Receptionist of Smoke Screen Providers: Hello this is Robin at Smoke Screen Providers, how can I help you today?

Smith: Hey, this is Alex from Acme Legal Services. I just received a report from our threat analysts here regarding a cyber-hacking collective, who would I speak to regarding the protection you guys provide against threats like DDoS attacks?

Receptionist: Please hold while I connect you to your customer service representative?

(Really bad music while on hold)

Customer Service Representative: Hello Alex, this is Adrienne, Acme's customer service representative. I hear you would like to hear about Smoke Screen's protection against cyber threats such as DDoS attacks, is that correct?

Yes, we have had some threats from a hacker collective famous for DDoS attacks.

Find out about Services provided

Adrienne: Can I just have your account number to pull up your account?

Sure. (keyboard clicks). Its—XXXXXXXXXXXXX.

Okay according to your contract, "Smoke Screen Providers will maintain a 99.95% up-time for web and DNS services, less scheduled maintenance. To achieve this requirement, we monitor the hosted website and DNS server for unauthorized access. We also provide DDoS protection guaranteed to be adequate up to 100Gbps."

If it makes you feel better 80% of DDoS attacks are under 1 Gbps, so you should be safe.

Excellent!

Is there anything else I can help you with?

No that's it. Thanks.

Decision 2

Mitigate?	Yes/ No	Discussion
DDoS against the DNS server.	No	Provided
DDoS against the webserver	No	Provided
Malware injection attack on public website.		
Malware studded email.		

Courses of action

What do we do to protect against COYOTE's threatened attacks?

- ~~Nothing, what will happen will happen~~
- ~~Nothing, we are invulnerable~~
- Find out how vulnerable are we?
  - We pay our service provider, let's find out more
- **Which attacks should we work to mitigate?**

Find out more about our web server

(Visit Acme's Web Administrator)

Smith. Hey I just talked to one our threat analysts and they noted that we have received some threats from a hacker collective---

Web Admin: Cool! Like Anonymous

Yeah, Coyote, they are into DDoS attacks, web injections, and spear phishing, that sort of stuff. Are our websites vulnerable to this type of stuff?

Nope. No user entered content. We don't even have a search function.

That's what I wanted to know, thanks.

Decision 2

Mitigate?	Yes/ No	Discussion
DDoS against the DNS server.	No	Provided
DDoS against the webserver	No	Provided
Malware injection attack on public website.	No	Nothing to hack
Malware studded email.		

Ring, Ring, Ring

Bob Acme contacts you for an update.

You tell him what you have found out about the COYETE modus operandi.

Bob is a high level executive who likes information clear and concise

How will you provide it?

Courses of action

What form should you use for your reply to Bob?

- A small book with all the information you have gathered including your recollection of relevant conversations, let him draw his own conclusions
- Just state the facts
- The five Ws and an H
- BLUF

The five Ws and an H

As an executive, Bob might want to know about his adversary.

This will be a good format

1. Who
2. What
3. Where
4. When
5. Why
6. How

Tell Bob about COYOTE
use this as an outline, fill in relevant details

Five Ws and H	
Who	COYOTE Harry Jones (AKA Mr. Xaisar) Tom Brown (AKA K1lzSw1ch)
What	Threats to Acme
Where	They are somewhere in cyberspace attacking Acme here
When	Unknown, but possibly soon
Why	Politics: one of our clients “backed the wrong candidate” Revenge/protest against friends being fired
How	DDOS, hacking attempts, phishing
Any additional?	Service Provider will protect against DDOS Hacking shouldn’t be a problem Need to address phishing

BLUF: Bottom Line Up Front

State conclusions first

Then back them up

Realizing that he may not actually read past the BLUF content

Bob,
We have been threatened by the hacker collective COYOTE.
Their motivation is political and revenge toward one of our clients.
COYOTE is known to use DDOS, Web hacking and phishing.
Our service provider assures me that we are protected against DDOS, our Web administrator indicates that our web site does not contain the vulnerabilities that COYOTE typically exploits .
We must improve our defenses against phishing email attacks.

… go on to describe in detail…

Conclusion: Alex saves the day

Our hero, Alex

- Keeps in communication with Smoke Screen and the web admin
- Improves phishing defenses, both technical and user training
- The attack starts but is only barely noticeable
  - Smoke Screen tells Alex that they mitigated a peak 2Gbps DDOS
  - Our web admin sees some unsuccessful exploit attempts
  - Most phishing emails are found and quarantined
  - Users report a few that got through as well as some false positives
  - Mary, our threat intel analyst, sees some chatter about COYOTE being frustrated but vowing to renew efforts

Questions?

Comments?

Shameless Plug for Our Conference

Join us at FloCon 2020

FloCon: Using Data to Defend

January 6-9, 2020

Savannah, GA

www.flocon.org

Course References

SEI Cyber Intelligence Research Consortium. Cyber Intelligence Conceptual Framework. https://www.sei.cmu.edu/about/organization/etc/upload/CyberInt-Conceptual-Framework.pdf

Heuer, Richards J. Psychology of Intelligence Analysis. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis

Lee, Robert M. & Bianco, David. Generating Hypotheses for Successful Threat Hunting. SANS Institute Website. https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172

Lubin, Gus & Lebowitz, Shana. 58 cognitive biases that screw up everything we do. Business Insider Website. http://www.businessinsider.com/cognitive-biases-2015-10/