Monitoring and Response Overview

James Lord

Rachel Kartch

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM18-0590

Updating the Distribution Statement

To appropriately update the distribution markings in the footer of your presentation, follow these steps:

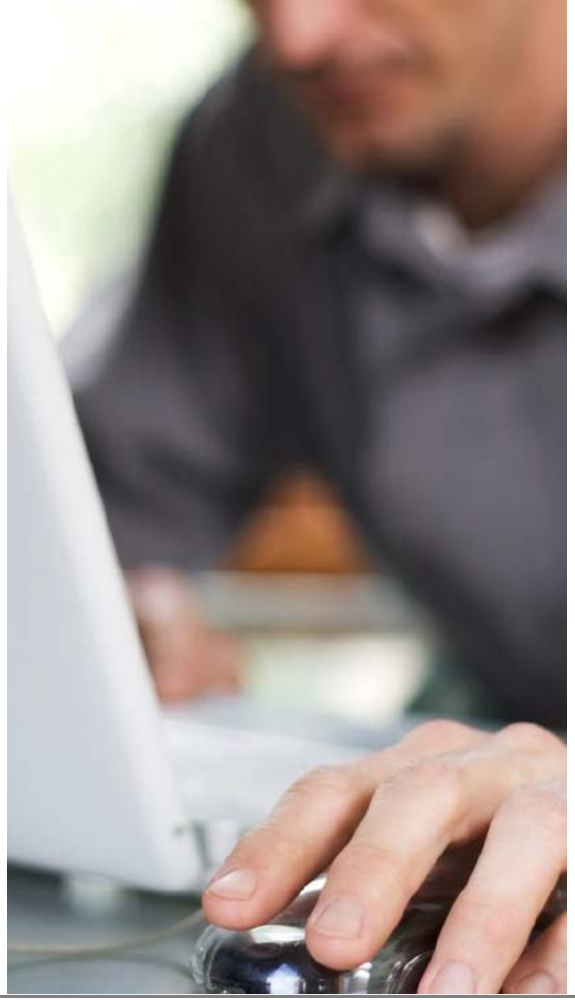
1. From the *Home* tab, select *Replace* at the right side of the tool bar.
2. Paste "[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]" in the *Find what* field.
3. Paste a short version of the distribution statement provided by the Document Marking System (e.g., [DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]), with brackets around it, in the *Replace with* field. See the table on the next slide for the short statements you can use. (If you have questions, send email to DMARR-Team@sei.cmu.edu.)
4. Click the *Replace All* button. Voilà! You're done!

You can use this same *Replace* command to update the title, date, and copyright of your presentation without having to access slide master pages.

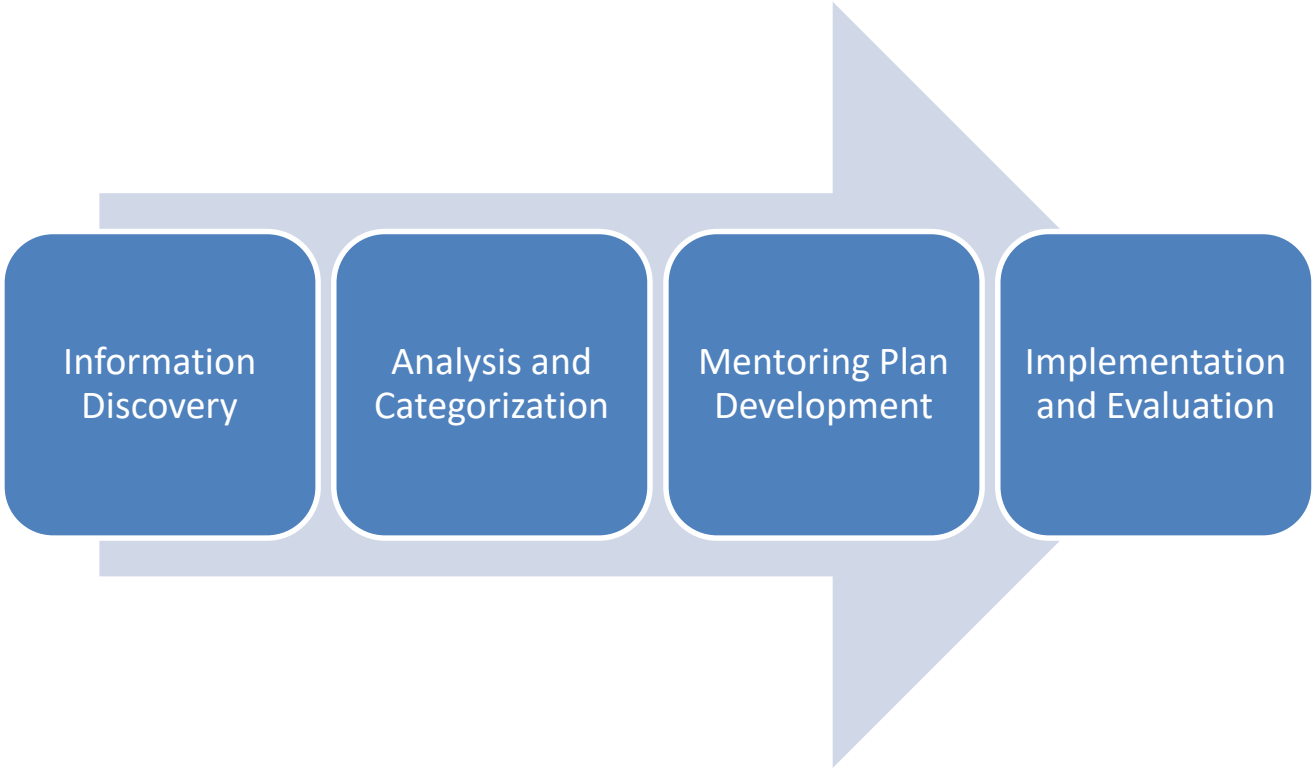
Short Distribution Statements

Statement in Document Markings System	Short Statement You Can Use
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.	[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.
[DISTRIBUTION STATEMENT B] Distribution authorized to U.S. Government Agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT B] U.S. Government Agencies only.
[DISTRIBUTION STATEMENT C] Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT C] U.S. Government Agencies and their contractors only.
[DISTRIBUTION STATEMENT D] Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT D] Department of Defense and U.S. DoD contractors only.
[DISTRIBUTION STATEMENT E] Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT E] DoD Components only.
[DISTRIBUTION STATEMENT F] Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD Authority.	Keep the entire statement. There is no short statement you can use.
[INTERNAL SEI-USE ONLY] Further dissemination requires re-submittal through DM-RRO.	[INTERNAL SEI-USE ONLY] DM-RRO REQUIRED.
[FUNDAMENTAL RESEARCH] This material was created under project [FR ID]; DFARS 252.204-7000 does not apply.	[FR ID]; DFARS 252.204-7000 does not apply.

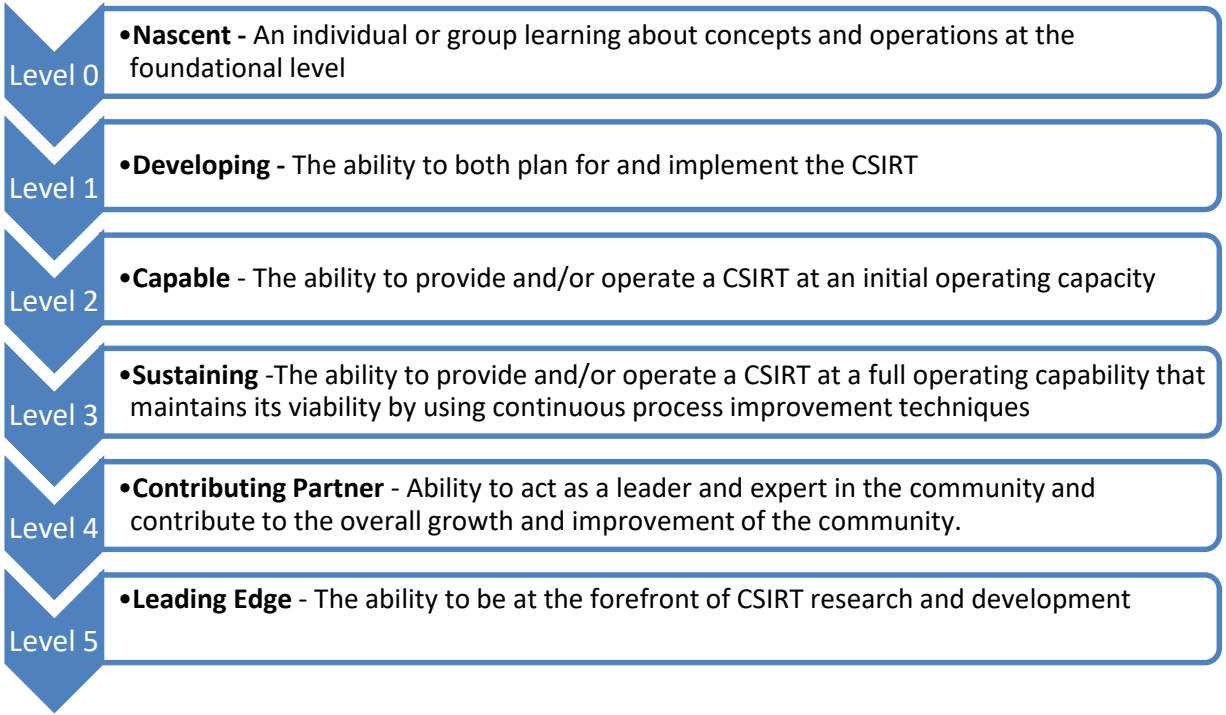
Security Operations Capacity Development



Mentorship Framework



CSIRT Capacity Development Continuum



Engagements in Africa

- **Objectives:**
  - **Promoting Public Awareness**
  - **Facilitate Collaboration**
  - **Conduct Targeted Training**
  - **Provide Institutional Support**
  - **Cyber Workforce Development**
  - **Facilitating increased coordination Among Stakeholders in the Region.**

Cote d' Ivoire National CSIRT (CI-CERT)

Primary Sponsor for FIRST Assessment and Membership

- CI CERT Approved September 2016

Conducted Training Workshops

- Advanced Incident Handling
- DDoS
- Botnets
- Joint Presentations
  - San Juan, Puerto Rico
  - Dar es Salaam, Tanzania

Engagements in East Asia and Pacific

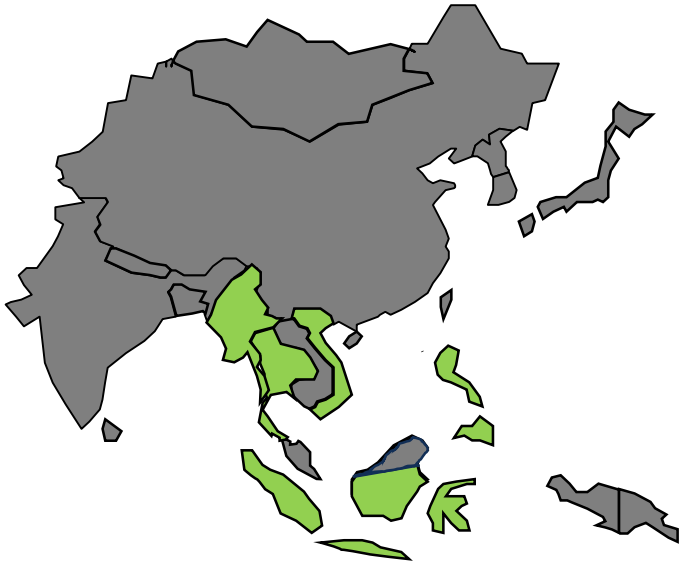
Indonesia

Myanmar

Philippines

Thailand

Vietnam



Vietnam

VN-CERT

FIRST Sponsor

Training Workshops

- Data Sources
- Threat Awareness
- Open Source Tools

Upcoming Workshops

- Cyber Workforce Development
- Train the Trainer

Indonesia
Id-SIRTII/CC

Working with the national CSIRT

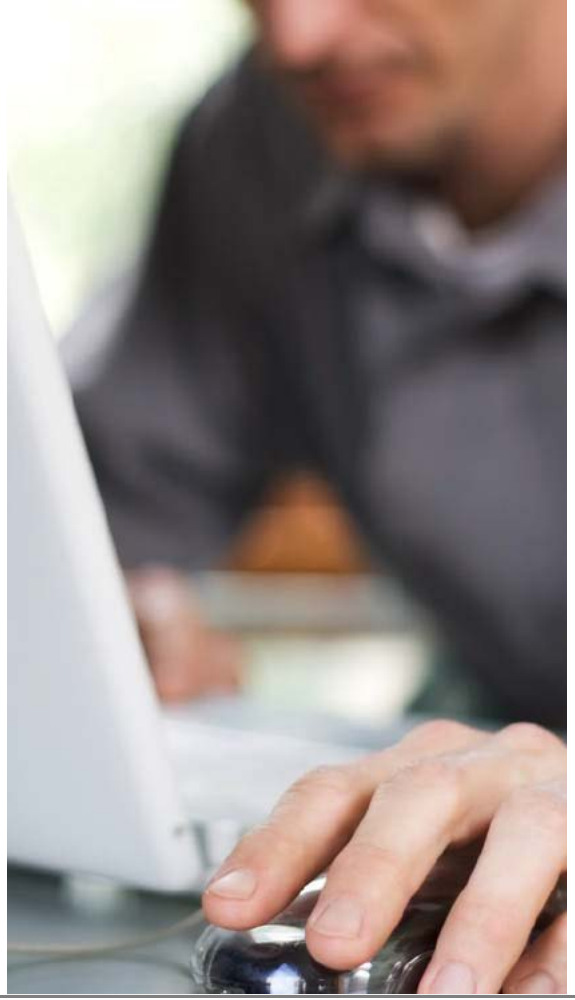
- Intrusion Detection and Prevention Systems
- Analyzing Network Service Traffic

Whole of Government

Perspectives:

- Implementation of national cybersecurity strategy
- Dedicated Funding
- Partnering with critical infrastructure managers
- Capacity building
- Organization of CyberDrills (Exercises with stakeholders) for the strengthening of the operational teams (IT Staff) of the stakeholders

Situational Awareness



Team overview

Solutions (macro)

- Architecture
- Tool evaluation and selection (including RFI support)
- Workflows
- Best practices

Analysis (micro)

- Analytic techniques and methods
- Specifics: data, threats, algorithms

Teamwork and collaboration internally and with other CERT groups

Typical engagements

- Architecture development and recommendations
  - Network architecture
  - Tool deployment/sensing infrastructure (Internet-connected and closed networks)
- Analytic development
  - Signature-based
  - Anomaly detection
- Data analysis
  - Not restricted to network flow or pcap
- RFI support, product evaluation
- Open source and classified research projects
- Training and mentoring (frequent collaboration with Sec Ops)

Recent work

Analytic development

- SiLK analytics to identify clients with low standard deviations for source port of DNS requests—potentially vulnerable to DNS cache poisoning
- Use of Bollinger Bands to measure network volatility for events of interest
- Proof of concept implementations of mean shift algorithm and tensor decompositions to cluster or identify anomalies in Bro log data

Training and mentoring deliveries (in-person or prerecorded videos)

- SQL for Analysts
- SiLK/E1 for Technical Managers
- E1 to Profile Network Services

Recent work (cont.)

Architecture and tools work

- Assessment of and recommendations for methods and locations at which to perform break and inspect of encrypted traffic to maximize security, while minimizing impact on performance
- Initial evaluation of three platforms for full packet capture, based on open source information
- Proof of concept deployment of internal SiLK sensors on a large USG network
- Research and white paper on commercial DNS service providers
- Research and white papers on architecture of cloud-based systems, threats to such systems, and recommended best practices for migrating USG systems and services to the cloud

Current areas of interest

- Increase in encrypted traffic: implications for cybersecurity, privacy, and associated policies
  - TLS 1.3
  - DNS over HTTPS
- Machine learning for cybersecurity
  - How to identify the problems for which ML is an appropriate solution?
  - How to avoid the "hammer looking for a nail" approach?
- Use of IoT/"smart building" capabilities to support cybersecurity

Contact Information

James Lord

Security Operations

Telephone: +1 412.268.3945

Email: jclord@cert.org

Rachel Kartch

Situational Awareness

Telephone: +1 412.268.3998

Email: rakartch@cert.org