NSM Operation

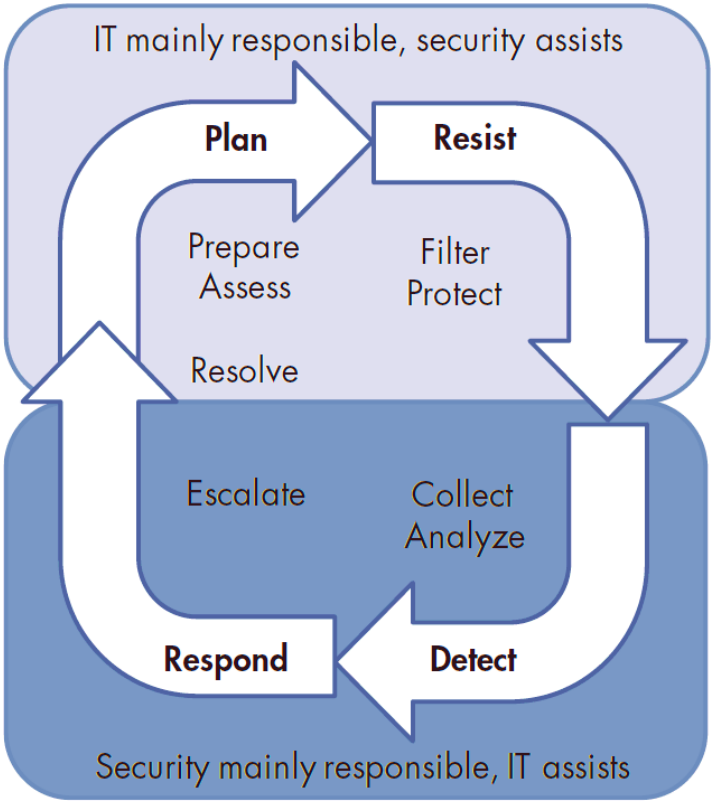
INFO-6081 – Monitoring & Incident Response

Learning Outcomes

- The Enterprise Security Cycle
- Collection
  - Technical and Non-Technical Sources
- Analysis
  - Event Classification
- Escalation
  - Documentation and Notification
- Resolution
  - Containment

The Enterprise Security Cycle

- NSM is characterized as the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions
- This does not specifically address planning or resist phases
- All phases are required to protect an organization from threats
- In fact, it is quite normal for all phases to occur simultaneously



The Enterprise Security Cycle

Planning

- The goal of planning is to prepare the organization's assets to effectively resist intrusion
- In this phase, the security and IT departments prepare the assets to prevent known attacks or vulnerabilities
- The controls that are enabled are measured for effectiveness
- Elements of the planning phase include budgeting, auditing, compliance and training
- Security and penetration testing are considered to be assessments of the planning phase

The Enterprise Security Cycle

Resistance

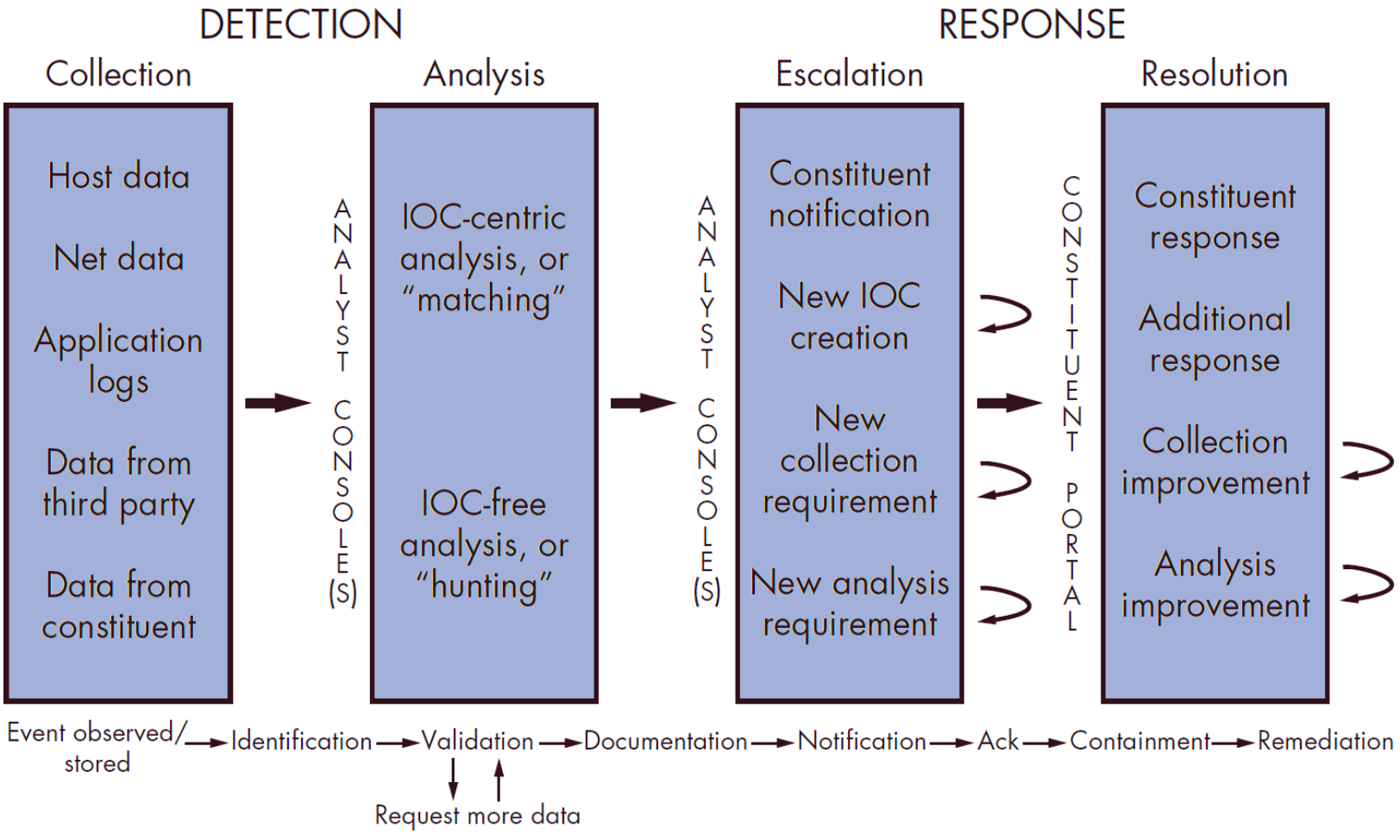
- The goal of the resistance phase it to prevent or delay the attacker entry into the organization's information systems
- In resistance, automated countermeasures filter undesired traffic and prevent access to attackers
- Elements of the resist phase include antivirus, firewalls, intrusion detection and prevention, data-loss prevention, access controls, whitelisting, etc.
- Security education and awareness training (SETA), configuration and vulnerability management are employed to harden the human element in the resist phase

The Enterprise Security Cycle

Detection and Response

- The detection and response phases include three elements of NSM, collect analyze and escalate
- Analysts perform these actions to have enough information about the intrusion to prepare a response
- The fourth element, resolve is a component of the response phase

The Enterprise Security Cycle



Collection, Analysis, Escalation & Resolution

Collection

- Gathering data to determine if an activity is normal, suspicious or malicious

Analysis

- Validating the nature of an event
- Analysis can be focused on indicators of compromise (IOC) (matching) or not (hunting)

Escalation

- Documenting the event and notifying a stakeholder about the status of a compromised asset

Resolution

- The actions taken by the CSIRT to prevent of reduce the risk of loss

Collection

- Collection includes various processes that gather information both technical and nontechnical sources

Technical Sources:

  - Data from hosts, network logs, and information systems
  - There are many commercial and non-commercial platforms to collect endpoint data and analyze potential IOC
  - Network-centric collection takes bulk-collection and adds additional layers of interpretation to identify potential IOC
  - Application logs are another invaluable source of technical information
  - Antivirus systems provide information about filesystem detection

Collection

Nontechnical Sources:

- Stakeholders, partners, law enforcement, intelligence agencies, etc.
- Nontechnical sources can be more important to NSM than technical sources
- Reports from users are often critical
- Properly trained users can often identify new attacks long before evidence becomes apparent in network logs
- External nontechnical sources can provide context about emerging threats to an organization

Analysis

- Analysis is the process of identifying and validating normal, suspicious and malicious events that are observed
- IOCs can expedite this process
- IOC codify intruders' activities so technical systems can identify those events in digital evidence
- Examples can include IP addresses, domain names, message content, etc.
- Matching known IOC to evidence allows analysts to identify suspicious or malicious events and validate their findings

Analysis

- Advanced threat analysis includes “hunting”, which relies on the knowledge and experience of the analyst to detect possible intrusion into the system that have not been detected through traditional means
- Upon validating the presence of an intruder (and responding accordingly), the new detection method is added to the IOC-centric operations

Analysis

- Analysts use data to identify and verify intrusions
- Intrusions are just one type of incident that a CSIRT may need to respond to
- Intrusions usually indicate a breach of security policy and often fall into one or more categories, based on the type of intrusion, or the damage it causes
- The following slide depicts the intrusion categories popularized by the US Department of Defense

Name	Description
Cat 6	Intruder conducted reconnaissance against asset with access to sensitive data
Cat 3	Intruder tried to exploit asset with access to sensitive data, but failed
Cat 2	Intruder compromised asset with access to sensitive data but did not obtain root or administrative access
Cat 1	Intruder compromised asset with ready access to sensitive data
Breach 3	Intruder established command-and-control channel from asset with ready access to sensitive data
Breach 2	Intruder exfiltrated non-sensitive data or data that will facilitate access to sensitive data
Breach 1	Intruder exfiltrated sensitive data or is suspected of exfiltrating sensitive data based on volume, etc.
Crisis 3	Intruder publicized stolen data online or via mainstream media
Crisis 2	Data loss prompted government or regulatory investigation with fines or other legal consequences
Crisis 1	Data loss resulted in physical harm or loss of life

Analysis

Example 1

- An intruder convinced a user to execute malware, but host IDPS prevented the download of a command-and-control application

Example 2

- The organization was contacted by law enforcement regarding several of the organization's customers reporting that they were the victim of identity theft

Analysis

Event Classification

- CSIRTs classify events within their analysis console or event management system
- Classification and recording should include the analyst making the decision, the time of identification, the classification type or identifier and as much relevant information as possible
- Counting and classifying events creates one of the two key metrics that CSIRTs collect
  - The other is the total event time from detection to containment

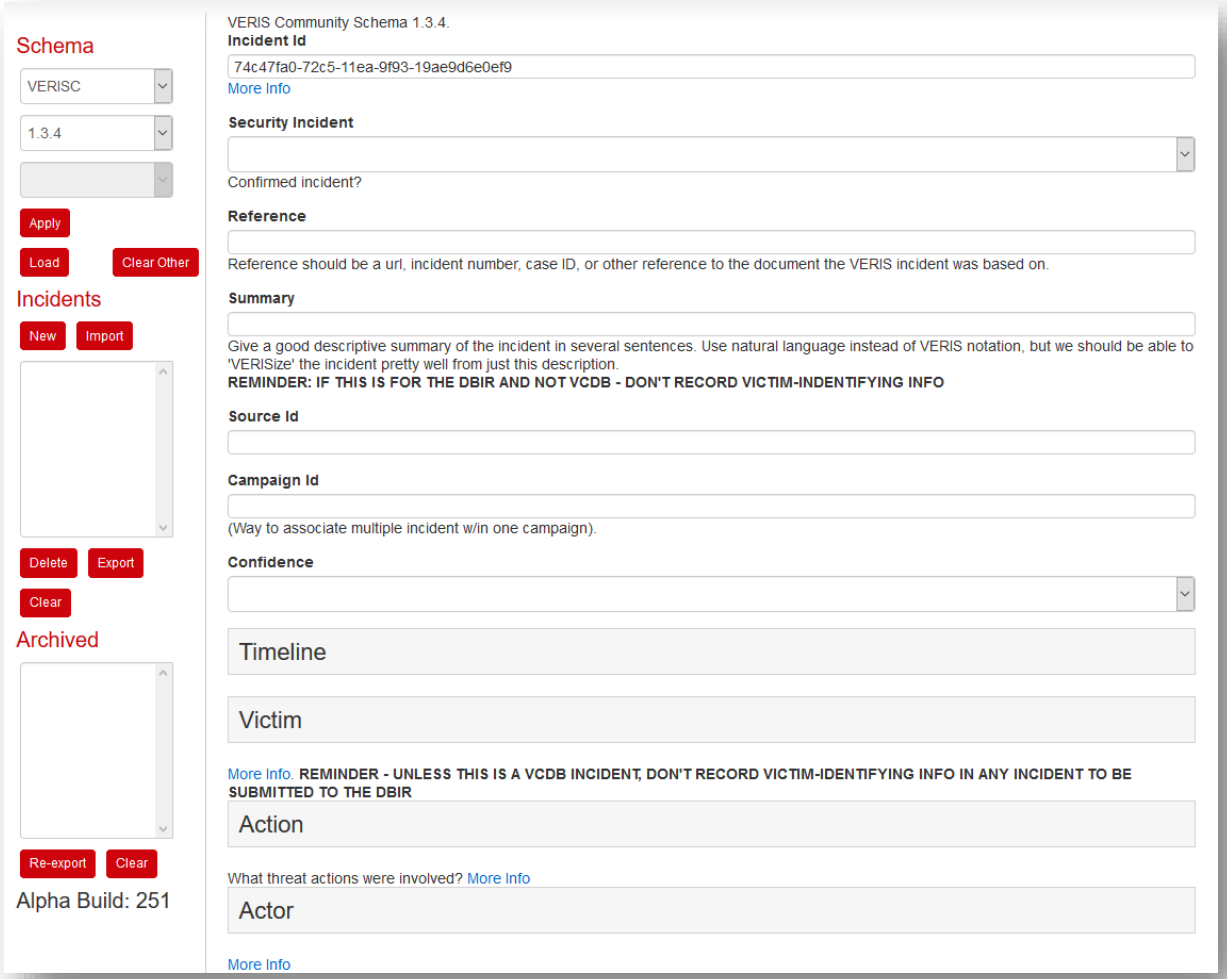
Escalation

- Escalation refers to the process the CSIRT takes to document their findings, notify the stakeholders and receive acknowledgment of the incident response
- Escalation and documentation are often the most challenging aspects of the NSM process
- When documenting, it is important to assign a single incident number to each compromised asset
- This number will be used to report the metrics of the incident response process later

Escalation

- Documentation is a critical, but often undervalued aspect of the IR process
- Individual teams will often capture different amounts of data regarding incidents, often the volume of investigations can dictate the level of documentation
- When process allows, a community standard like the Vocabulary for Event Recording and Incident Sharing (VERIS) should be adopted, which provides common language for describing security related incidents
- More details can be found at: http://veriscommunity.net

VERIS Community Schema



Escalation

- Notifying the stakeholder that the asset in their possession has been compromised can be a difficult task
- In a poorly managed environment, asset inventory is often non-existent or lacking update, which makes identifying the user of the asset a challenge
- If the CSIRT cannot map an IP address to a hardware device or a user, notification is impossible, and the network remains at risk
- Additionally, the severity of the incident may limit the urgency of informing the user

Escalation

- If an incident is urgent, the communication medium should be appropriate for the severity of the incident
- Acknowledgement of an incident can also be a challenge, as some users may not care that their device has been compromised, or they may not understand the implications of compromise
- Sometimes the user is so caught up in their work that they delay acknowledging the incident
- When they do respond, log the response time in the official record

Escalation

- If the attacker has gained persistence in a system, they may have access to the user's email, and may have the ability to read (or remove) information about the incident
- Ensure that you communicate any sensitive or confidential information in a secure manner (in person/by phone)
- Like email, an attacker may target any internal messaging platform that the organization uses, so don't rely on this as a secure communication tool

Resolution

- Resolution describes the process used to transition compromised assets to a trustworthy state
- The process used for this transition varies based on the nature of the incident, as well as the capabilities of the CSIRT
- The CSIRT will push to have the device removed from the network as soon as possible, often in opposition with the departmental team, who will not want to lose the functionality of the asset

Resolution

- When working to contain an intrusion begin with the compromised asset and consider at least some of the following actions:
  - Put the device into hibernation mode
  - Disable or disconnect network access
  - Add a local firewall rule that prevents the device from communicating with other devices
  - Add an access control list that prevents the device from communicating with other devices
  - Add a firewall rule that prevents the device access to the internet

Resolution

- Once containment is complete, the scope of the attack should be determined, and any other potential victims investigated
- When deciding what containment actions to take, the CSIRT can take a threat-centric or asset-centric approach
  - A threat-centric approach focuses on the adversary and may track one or more potential threats at a time
  - An asset-centric approach focuses on the sensitivity of the data on the network and works to move quickly to respond to threats to those resources

Resolution

- Mature CSIRTs often track criminal groups in terms of adversary campaigns, realizing a single intrusion is likely a small element of a much larger campaign
- CSIRTs fighting persistent intrusions organize their response actions into waves, which are an effort to detect and respond to an intrusion type
- It is important to realize that you will never have full visibility of the intruder's intent, so it is recommended to document what you think the intruder is doing
- Remediation/Recovery is the final step of the process

Summary

- NSM is a component of the Enterprise Security Cycle, focusing mainly on the detection and response phases
- Collection gathers data from both technical and non-technical sources to determine if the data is normal, suspicious, or malicious
- Analysis is performed on suspicious and malicious traffic to determine the nature of the event
- Escalation is the process of documenting the incident and notifying the stakeholder of the compromise
- Resolution involves actions taken to reduce or remove the risk of further loss

References

- Bejtlich, R. (2013). Chapter 9: NSM Operation. In The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch Press.
- Elemind.com. (n.d.). The VERIS WebApp. Retrieved March 30, 2020, from http://veriscommunity.net/webapp.html