Module 1: The Danger

Instructor Materials

CyberOps Associate v1.0

Module 1: The Danger

Module Objectives

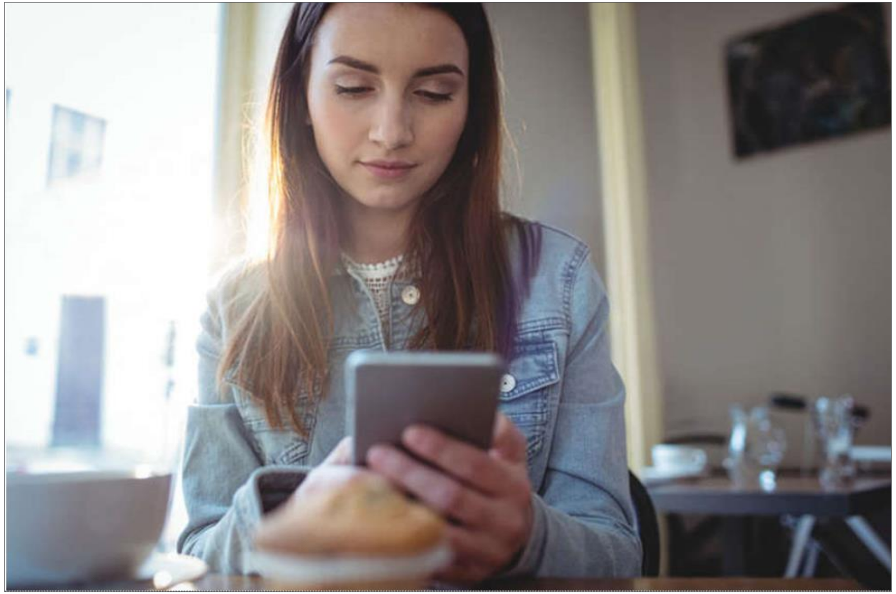
- Module Title: The Danger
- Module Objective: Explain why networks and data are attacked.

Topic Title	Topic Objective
War Stories	Explain why networks and data are attacked.
Threat Actors	Explain the motivations of the threat actors behind specific security incidents.
Threat Impact	Explain the potential impact of network security attacks.

1.1 War Stories

Hijacked People

- Hackers can set up open "rogue" wireless hotspots posing as a genuine wireless network.
- Rogue wireless hotspots are also known as "evil twin" hotspots.



Example: Victim

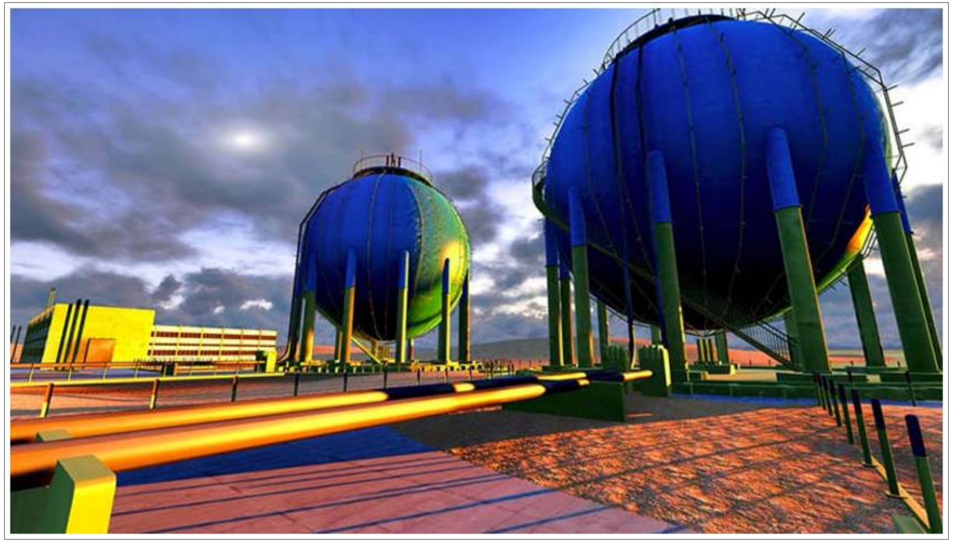
Ransomed Companies

- Employees of an organization are often lured into opening attachments that install ransomware on the employees' computers.
- This ransomware, when installed, begins the process of gathering and encrypting corporate data.
- The goal of the attackers is financial gain, because they hold the company's data for ransom until they are paid.

Example: Czech Hospital

Targeted Nations

- Some of today's malware is so sophisticated and expensive to create that security experts believe only a nation state or group of nations could possibly have the influence and funding to create it.
- Such malware can be targeted to attack a nation's vulnerable infrastructure, such as the water system or power grid.



Example: StuxNet

- One such malware was the Stuxnet worm
  that infected USB drives and infiltrated Windows operating systems. It then targeted Step 7 software that was developed by Siemens for their Programmable Logic Controllers (PLCs).

The Danger
Video - Anatomy of an Attack

Lab - Installing the Virtual Machine

- In this lab, you will complete the following objectives:
- Install VirtualBox on your personal computer
- Download and install the CyberOps Workstation Virtual Machine (VM).

Homework - Cybersecurity Case Studies

- Send me examples preferably with detail technical description of cyberattacks from your home country!

1.2 Threat Actors

Terms

- **Threat actors** are individuals or groups of individuals who perform cyberattacks
- **Cyberattacks** are intentional malicious acts meant to negatively impact another individual or organization.

Threat Actors

Amateurs

- They are also known as script kiddies and have little or no skill.
- They often use existing tools or instructions found on the internet to launch attacks.
- Even though they use basic tools, the results can still be devastating.

Hacktivists

- These are hackers who publicly protest against a variety of political and social ideas.
- They post articles and videos, leaking sensitive information, and disrupting web services with illegitimate traffic in Distributed Denial of Service (DDoS) attacks.

Financial Gain

- Much of the hacking activity that consistently threatens our security is motivated by financial gain.
- Cybercriminals want to gain access to bank accounts, personal data, and anything else they can leverage to generate cash flow.

Trade Secrets and Global Politics

- At times, nation states hack other countries, or interfere with their internal politics.
- Often, they may be interested in using cyberspace for industrial espionage.
- The theft of intellectual property can give a country a significant advantage in international trade.

How Secure is the Internet of Things?

- The Internet of Things (IoT) helps individuals connect things to improve their quality of life.
- Many devices on the internet are not updated with the latest firmware. Some older devices were not even developed to be updated with patches. These two situations create opportunity for threat actors and security risks for the owners of these devices.

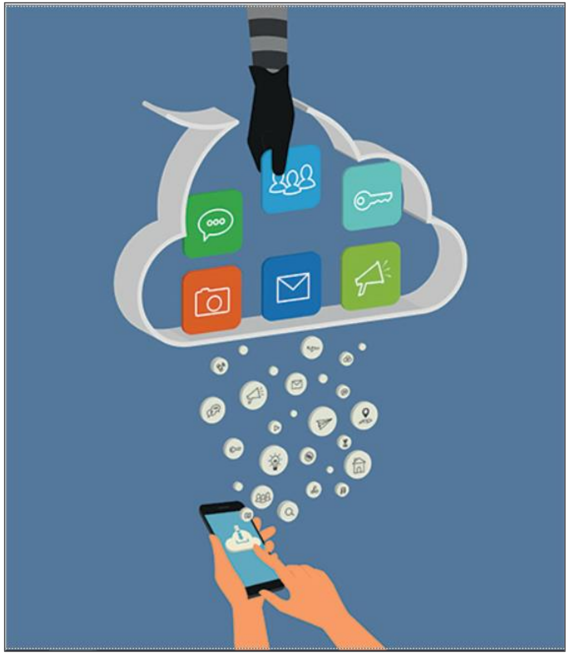
Lab - Learning the Details of Attacks

In this lab, you will research and analyze IoT application vulnerabilities.

1.3 Threat Impact

PII, PHI, and PSI

- **Personally Identifiable Information (PII)** is any information that can be used to positively identify an individual, for example, name, social security number, birthdate, credit card numbers etc.
- Cybercriminals aim to obtain these lists of PII that can then be sold on the dark web. Stolen PII can be used to create fake financial accounts, such as credit cards and short-term loans.
- The medical community creates and maintains **Electronic Medical Records (EMRs)** that contain **Protected Health Information (PHI)**, a subset of PII.
- **Personal Security Information (PSI)**, another type of PII, includes usernames, passwords, and other security-related information that individuals use to access information or services on the network.



Lost Competitive Advantage

- The loss of intellectual property to competitors is a serious concern.
- An additional major concern is the loss of trust that comes when a company is unable to protect its customers’ personal data.
- The loss of competitive advantage may come from this loss of trust rather than another company or country stealing trade secrets.

Politics and National Security

- It is not just businesses that get hacked.
- State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation.
- The internet has become essential as a medium for commercial and financial activities. Disruption of these activities can devastate a nation’s economy.

Thank you! Questions?

Vladimír Veselý

updated: 2023-02-01

https://www.fit.vutbr.cz/research/groups/nes@fit

Module 2: Fighters in the War Against Cybercrime

Instructor Materials

CyberOps Associate v1.0

Module 2: Fighters in the War Against Cybercrime

CyberOps Associate v1.0

Module Objectives

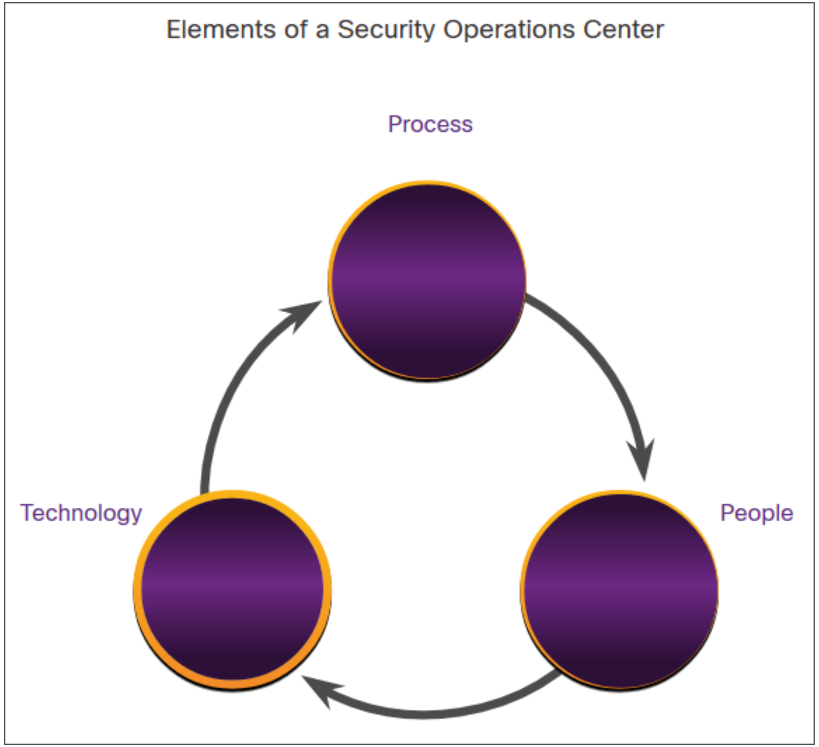
- Module Title: Fighters in the War Against Cybercrime
- Module Objective: Explain how to prepare for a career in cybersecurity operations.

Topic Title	Topic Objective
The Modern Security Operations Centre	Explain the mission of the Security Operations Center (SOC).
Becoming a Defender	Describe resources available to prepare for a career in cybersecurity operations.

2.1 The Modern Security Operations Center

Elements of a SOC

- To use a formalized, structured, and disciplined approach for defending against cyber threats, organizations typically use the services of professionals from a Security Operations Center (SOC).
- SOCs provide a broad range of services, from monitoring and management, to comprehensive threat solutions and customized hosted security.
- SOCs can be wholly in-house, owned and operated by a business, or elements of a SOC can be contracted out to security vendors, such as Cisco's Managed Security Services.



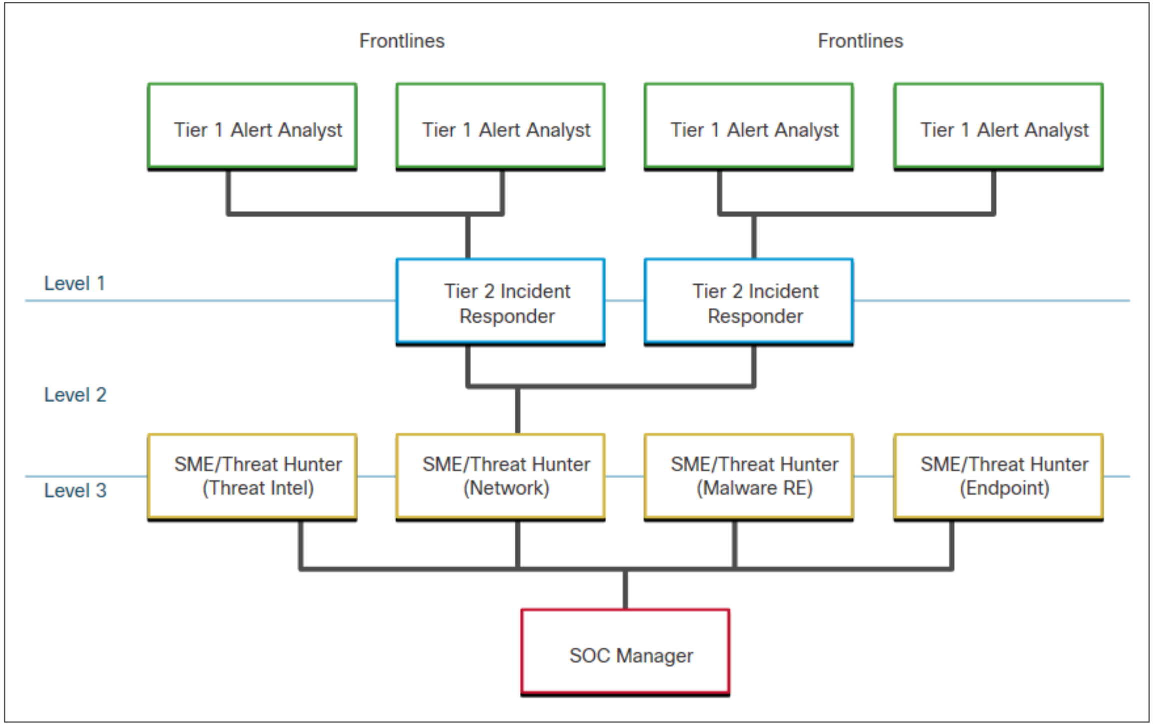
People in the SOC

- SOCs assign job roles by tiers, according to the expertise and responsibilities required for each.

Tiers	Responsibilities
Tier 1 Alert Analyst	Monitor incoming alerts, verify that a true incident has occurred, and forward tickets to Tier 2, if necessary.
Tier 2 Incident Responder	Responsible for deep investigation of incidents and advise remediation or action to be taken.
Tier 3 Threat Hunter	Experts in network, endpoint, threat intelligence, malware reverse engineering and tracing the processes of the malware to determine its impact and how it can be removed. They are also deeply involved in hunting for potential threats and implementing threat detection tools. Threat hunters search for cyber threats that are present in the network but have not yet been detected.
SOC Manager	Manages all the resources of the SOC and serves as the point of contact for the larger organization or customer.

People in the SOC (Contd.)

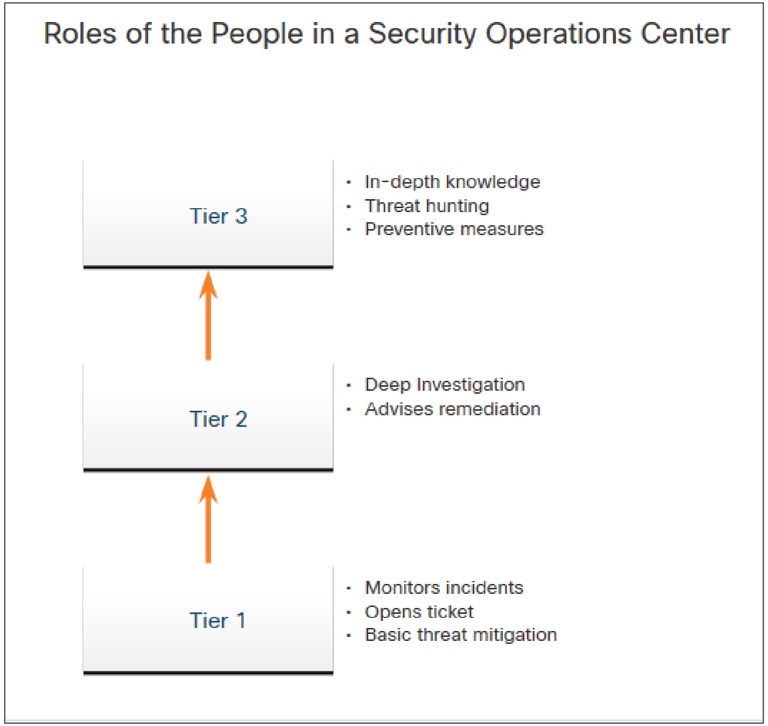
- First tier jobs are more entry level, while third tier jobs require extensive expertise.
- The figure, which is originally from the SANS Institute, graphically represents how these roles interact with each other.


Frontlines
Frontlines
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Tier 1 Alert Analyst
Level 1
Tier 2 Incident Responder
Tier 2 Incident Responder
Level 2
SME/Threat Hunter (Threat Intel)
SME/Threat Hunter (Network)
SME/Threat Hunter (Malware RE)
SME/Threat Hunter (Endpoint)
Level 3
SOC Manager

Process in the SOC

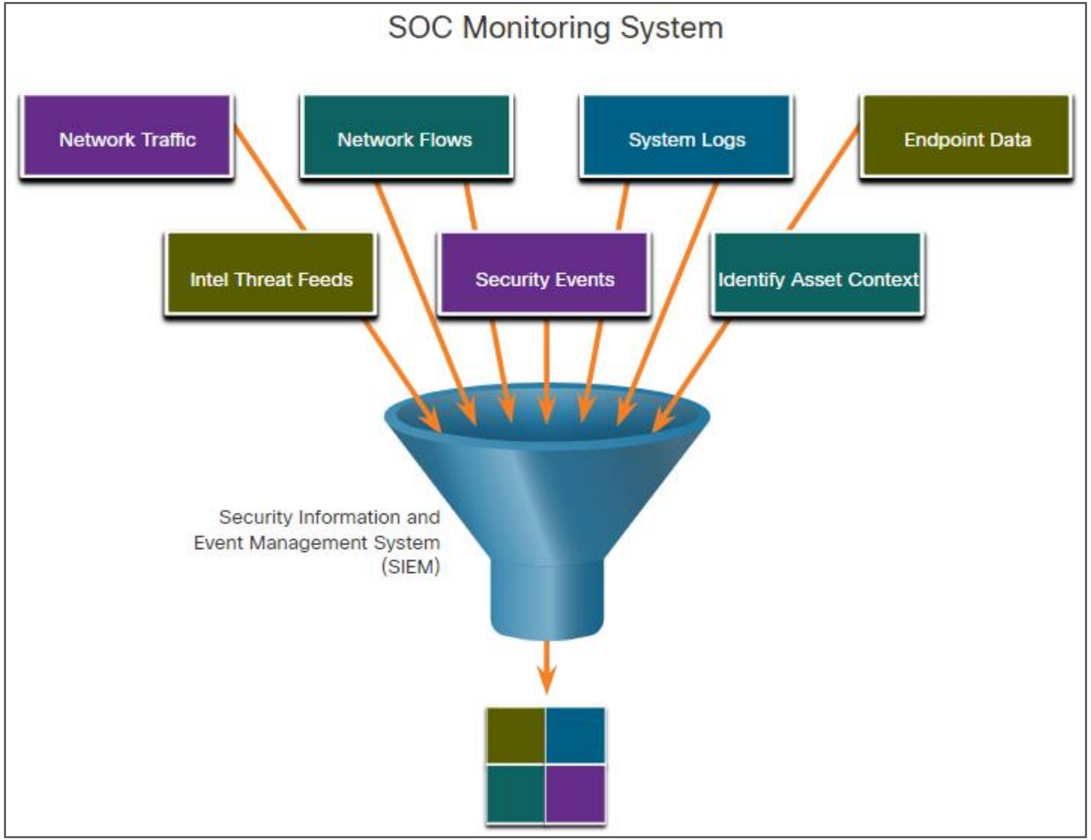
- A Cybersecurity Analyst is required to monitor security alert queues and investigate the assigned alerts. A ticketing system is used to assign these alerts to the analyst's queue.
- The software that generates the alerts can trigger false alarms. The analyst, therefore, needs to verify that an assigned alert represents a true security incident.
- When this verification is established, the incident can be forwarded to investigators or other security personnel to be acted upon. Otherwise, the alert is dismissed as a false alarm.
- If a ticket cannot be resolved, the Cybersecurity Analyst forwards the ticket to a Tier 2 Incident Responder for deeper investigation and remediation.
- If the Incident Responder cannot resolve the ticket, it is forwarded it to a Tier 3 personnel.

Roles of the People in a Security Operations Center



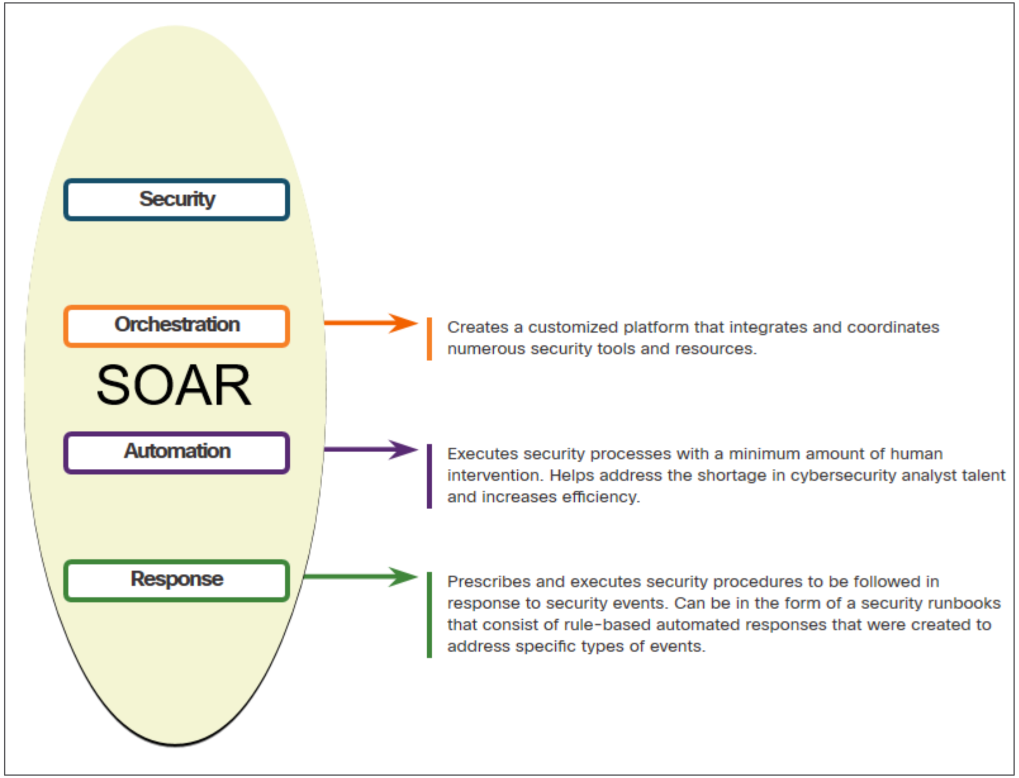
Technologies in the SOC: SIEM

- An SOC needs a Security Information and Event Management (SIEM) system to understand the data that firewalls, network appliances, intrusion detection systems, and other devices generate.
- SIEM systems collect and filter data, and detect, classify, analyze and investigate threats. They may also manage resources to implement preventive measures and address future threats.



Technologies in the SOC: SOAR

- SIEM and Security Orchestration, Automation and Response (SOAR) are often paired together as they have capabilities that complement each other.
- Large security operations (SecOps) teams use both technologies to optimize their SOC.
- SOAR platforms are similar to SIEMs as they aggregate, correlate, and analyze alerts. In addition, SOAR technology integrate threat intelligence and automate incident investigation and response workflows based on playbooks developed by the security team.



Creates a customized platform that integrates and coordinates numerous security tools and resources.

Executes security processes with a minimum amount of human intervention. Helps address the shortage in cybersecurity analyst talent and increases efficiency.

Prescribes and executes security procedures to be followed in response to security events. Can be in the form of a security runbooks that consist of rule-based automated responses that were created to address specific types of events.

Technologies in the SOC: SOAR (Contd.)

- SOAR security platforms:
  - Gather alarm data from each component of the system.
  - Provide tools that enable cases to be researched, assessed, and investigated.
  - Emphasize integration as a means of automating complex incident response workflows that enable more rapid response and adaptive defense strategies.
  - Include pre-defined playbooks that enable automatic response to specific threats. Playbooks can be initiated automatically based on predefined rules or may be triggered by security personnel.

SOC Metrics

- Whether internal to an organization or providing services to multiple organizations, it is important to understand how well the SOC is functioning, so that improvements can be made to the people, processes, and technologies that comprise the SOC.
- Many metrics or Key Performance Indicators (KPI) can be devised to measure different aspects of SOC performance. However, five metrics are commonly used as SOC metrics by SOC managers.

Metrics	Definition
Dwell Time	The length of time that threat actors have access to a network before they are detected, and their access is stopped
Mean Time to Detect (MTTD)	The average time that it takes for the SOC personnel to identify valid security incidents have occurred in the network
Mean Time to Respond (MTTR)	The average time it takes to stop and remediate a security incident
Mean Time to Contain (MTTC)	The time required to stop the incident from causing further damage to systems or data
Time to Control	The time required to stop the spread of malware in the network

Security vs. Availability

- Security personnel understand that for the organization to accomplish its priorities, network availability must be preserved.
- Each business or industry has a limited tolerance for network downtime. That tolerance is usually based upon a comparison of the cost of the downtime in relation to the cost of ensuring against downtime.
- Security cannot be so strong that it interferes with the needs of employees or business functions. It is always a tradeoff between strong security and permitting efficient business functioning.

2.2 Becoming a Defender

Certifications

- A variety of cybersecurity certifications that are relevant to careers in SOCs are available:
  - Cisco Certified CyberOps Associate
  - CompTIA Cybersecurity Analyst Certification
  - (ISC)² Information Security Certifications
  - Global Information Assurance Certification (GIAC)
- Search for “cybersecurity certifications” on the
  Internet to know more about other vendor and vendor-neutral certifications.

CyberOps Certification

Lab – Becoming a Defender

In this lab, you will research and analyze what it takes to become a network defender.

Thank you! Questions?

Vladimír Veselý

updated: 2023-02-01

https://www.fit.vutbr.cz/research/groups/nes@fit