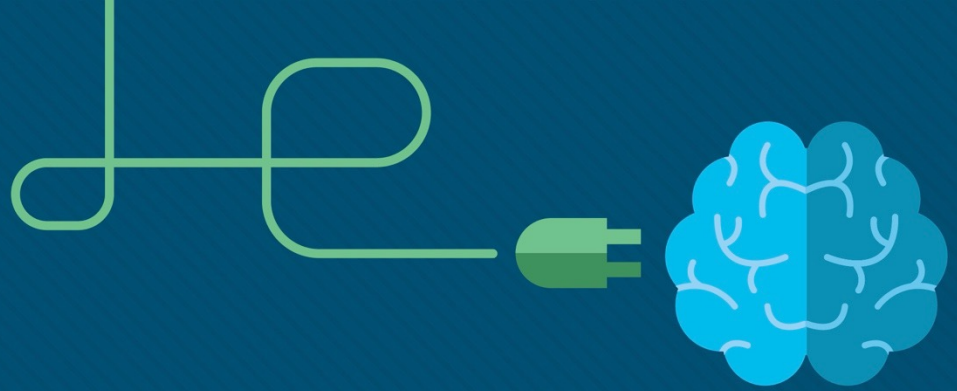


Chapter 1: Cybersecurity and the Security Operations Center

Information Security

Dr. Ayman Aljarbouh

Chapter 1 - Sections & Objectives

- 1.1 The Danger
  - Explain why networks and data are attacked.
    - Outline features of examples of cybersecurity incidents.
    - Explain the motivations of the threat actors behind specific security incidents.
    - Explain the potential impact of network security attacks.
- 1.2 Fighters in the War Against Cybercrime
  - Explain how to prepare for a career in Cybersecurity operations.
    - Explain the mission of the security operations center (SOC).
    - Describe resources available to prepare for a career in Cybersecurity operations.

Chapter 1 - Sections & Objectives

- 1.1 The Danger
  - Explain why networks and data are attacked.
    - Outline features of examples of cybersecurity incidents.
    - Explain the motivations of the threat actors behind specific security incidents.
    - Explain the potential impact of network security attacks.
- 1.2 Fighters in the War Against Cybercrime
  - Explain how to prepare for a career in Cybersecurity operations.
    - Explain the mission of the security operations center (SOC).
    - Describe resources available to prepare for a career in Cybersecurity operations.

Today

1.2 Fighters in the War Against Cybercrime

Module Objectives

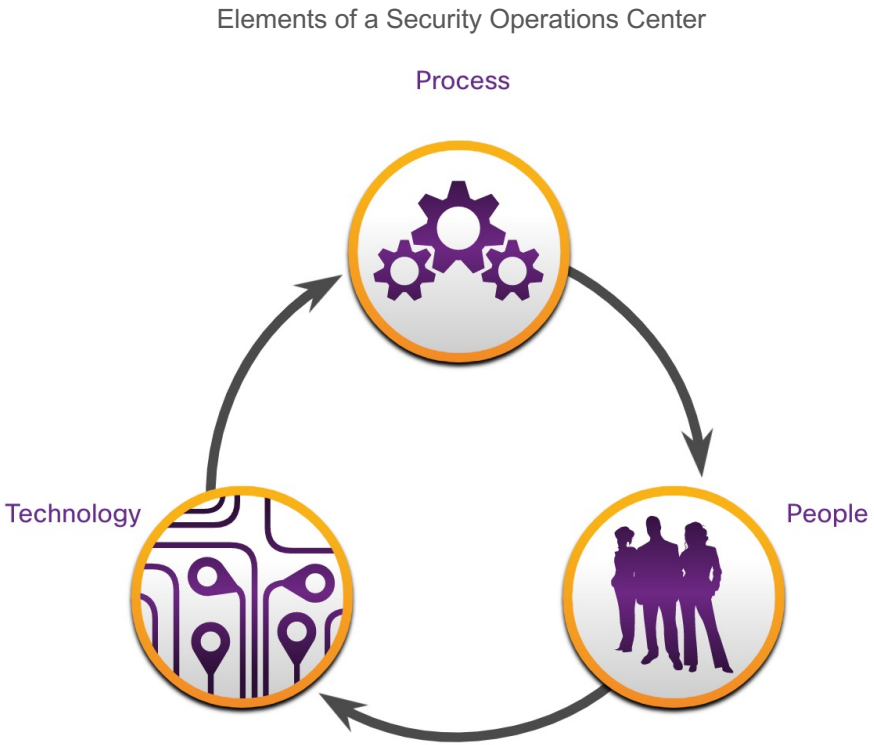
Module Title: Fighters in the War Against Cybercrime

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.

Elements of a SOC

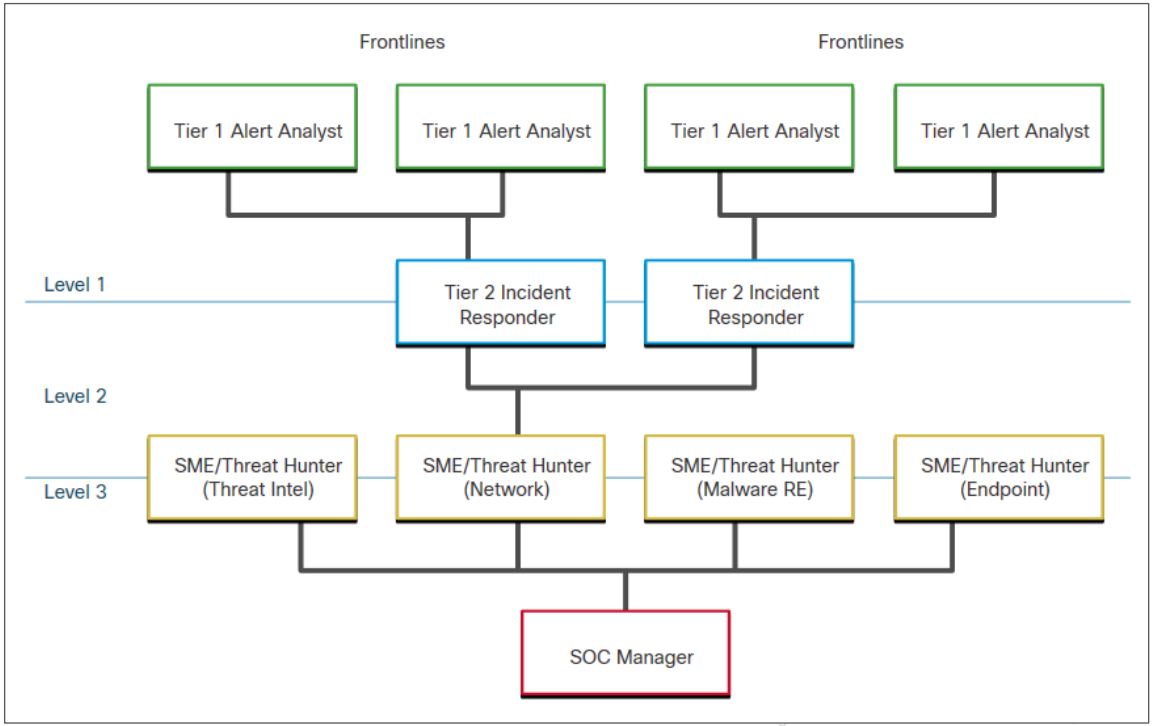
- Security Operations Centers (SOCs) provide a broad range of services:
  - Monitoring
  - Management
  - Comprehensive threat solutions
  - Hosted security
- SOCs can be:
  - In-house, owned and operated by a business.
  - Elements can be contracted out to security vendors.
- The major elements of a SOC:
  - People
  - Processes
  - Technology



People in the SOC

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

- 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.



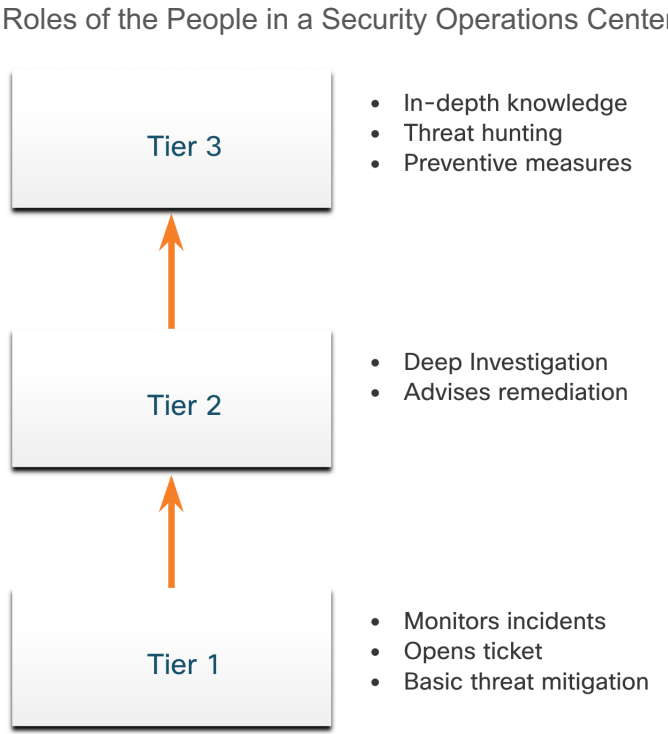
People in the SOC (Contd.)

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.

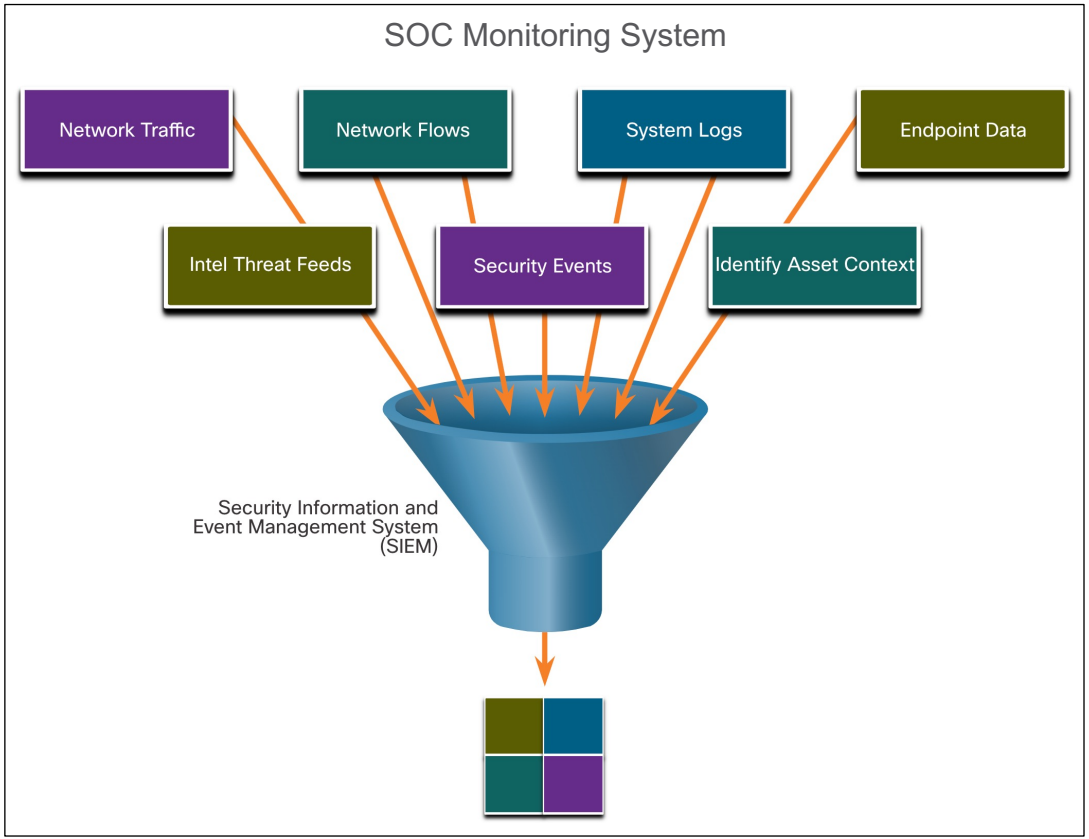
Process in the SOC

- 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.



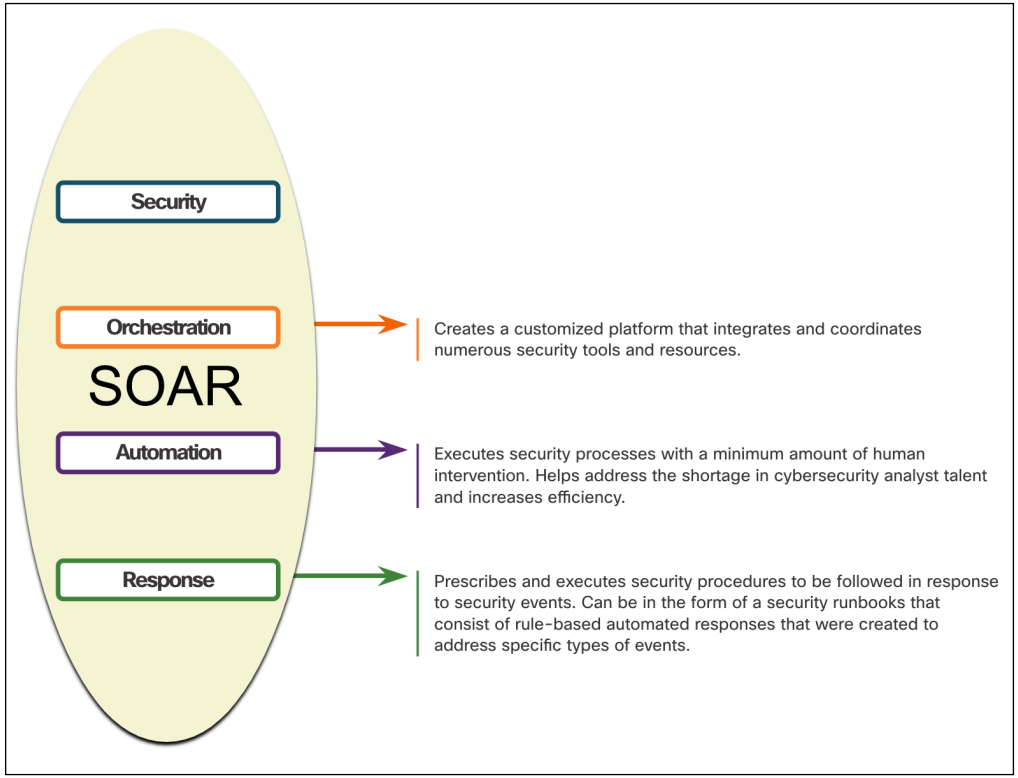
Technologies in the SOC: SIEM

- 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.
  - Detect and classify threats.
  - Analyze and investigate threats.
  - Implement preventive measures.
  - 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.



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

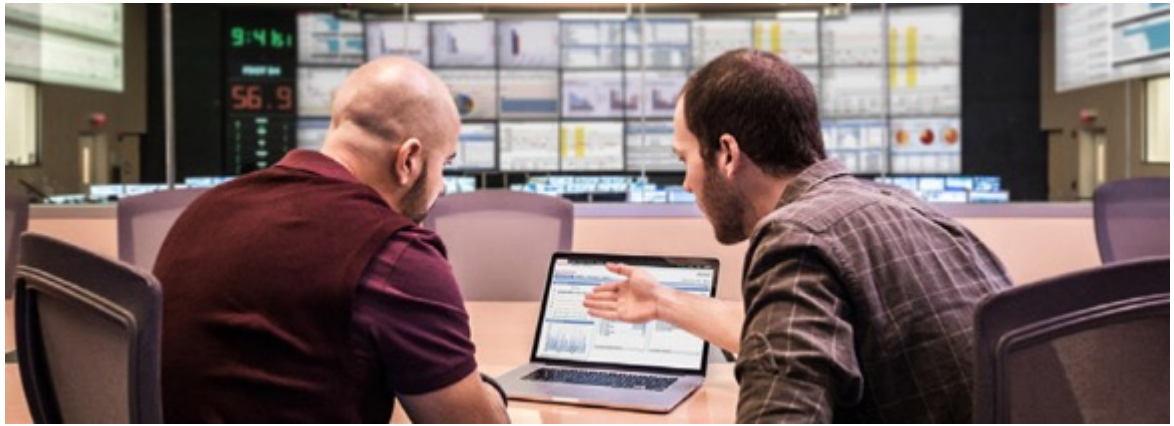
Security vs. Availability

- Most enterprise networks must be up and running at all times.
- Preferred uptime is often measured in the number of down minutes in a year. A “five nines” uptime means that the network is up 99.999% of the time (or down for no more than 5 minutes a year).
- Trade off between strong security and permitting business functions.

Availability %	Downtime
99.8%	17.52 hours
99.9% (“three nines")	8.76 hours
99.99% (“ four nines")	52.56 minutes
99.999% (“five nines")	5.256 minutes
99.9999% (“six nines“)	31.56 seconds
99.99999% (“seven nines“)	3.16 seconds

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)



Further Education

- **Degrees**: When considering a career in the cybersecurity field, one should seriously consider pursuing a technical degree or bachelor's degree in computer science, electrical engineering, information technology, or information security.
- **Python Programming**: Computer programming is an essential skill for anyone who wishes to pursue a career in cybersecurity. If you have never learned how to program, then Python might be the first language to learn.
- **Linux Skills**: Linux is widely used in SOCs and other networking and security environments. Linux skills are a valuable addition to your skillset as you work to develop a career in cybersecurity.

Sources of Career Information

- A variety of websites and mobile applications advertise information technology jobs:
  - Indeed.com
  - CareerBuilder.com
  - USAJobs.gov
  - Glassdoor.com - salary information
  - LinkedIn – professional network

Getting Experience

- **Internships:** Internships are an excellent method for entering the cybersecurity field. Sometimes, internships turn into an offer of full time employment. However, even a temporary internship allows you the opportunity to gain experience in the inner workings of a cybersecurity organization
- **Scholarships and Awards**: To help close the security skills gap, organizations like Cisco and INFOSEC have introduced scholarship and awards programs.
- **Temporary Agencies**: Many organizations use temporary agencies to fill job openings for the first 90 days. If the employee is a good match, the organization may convert the employee to a full-time, permanent position.
- **Your First Job:** If you have no experience in the cybersecurity field, working for a call center or support desk may be your first step into gaining the experience you need to move ahead in your career.

New Terms and Commands

• Security Operations Center (SOC) • Cybersecurity Analyst • CyberOps Associate • Tier 1 Alert Analyst • Tier 2 Incident Responder • Tier 3 Threat Hunter • SOC Manager	• Security Information and Event Management (SIEM) system • Security Orchestration, Automation and Response (SOAR) • Key Performance Indicators (KPI)	• Dwell Time • Mean Time to Detect (MTTD) • Mean Time to Respond (MTTR) • Mean Time to Contain (MTTC) • Time to Control • Job site aggregators • Temporary agencies

Lab 2 - Learning the Details of Attacks

In this lab, you will conduct a Search of IoT Application Vulnerabilities.