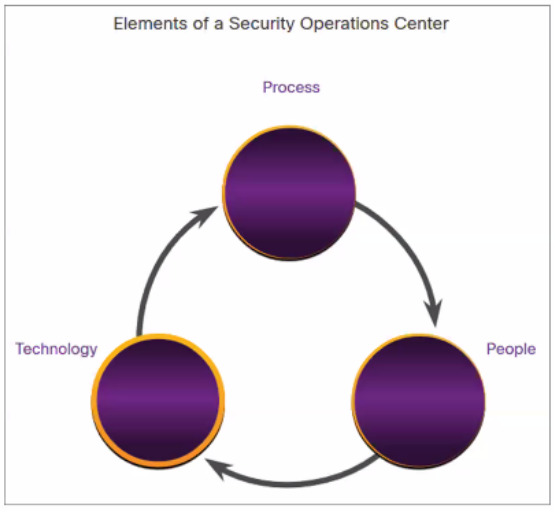
Module 2: Fighters in the War Against Cybercrime

CyberOps Associate v1.0

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.



Fighters in the War Against Cybercrime

People in the SOC

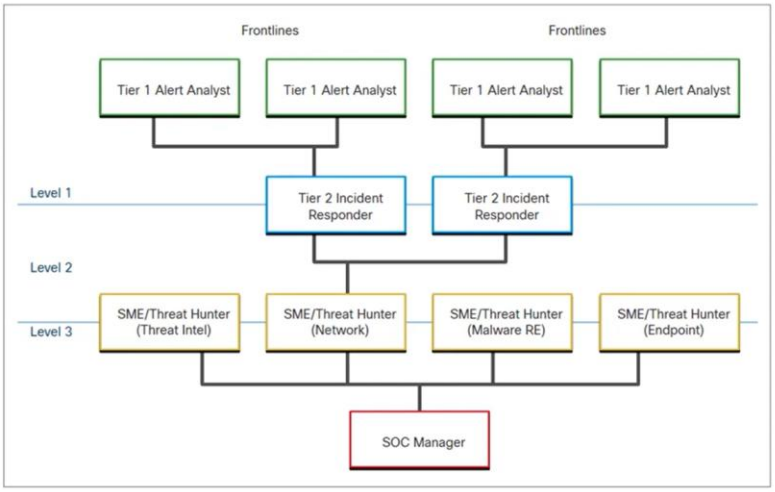
SOCs assign job roles by tiers, according to the expertise and responsibilities required for each.

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.

Fighters in the War Against Cybercrime

People in the SOC (Contd.)

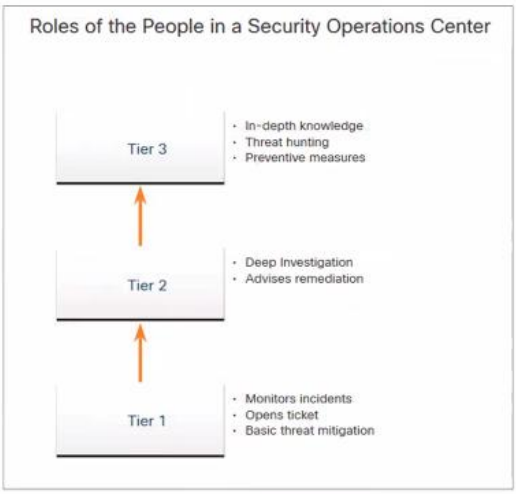
- First tier jobs are more entry level, while third tier jobs require extensive expertise.
- The figure, which is originally from the SANS Institute, graphically represents how these roles interact with each other.



Fighters in the War Against Cybercrime

Process in the SOC

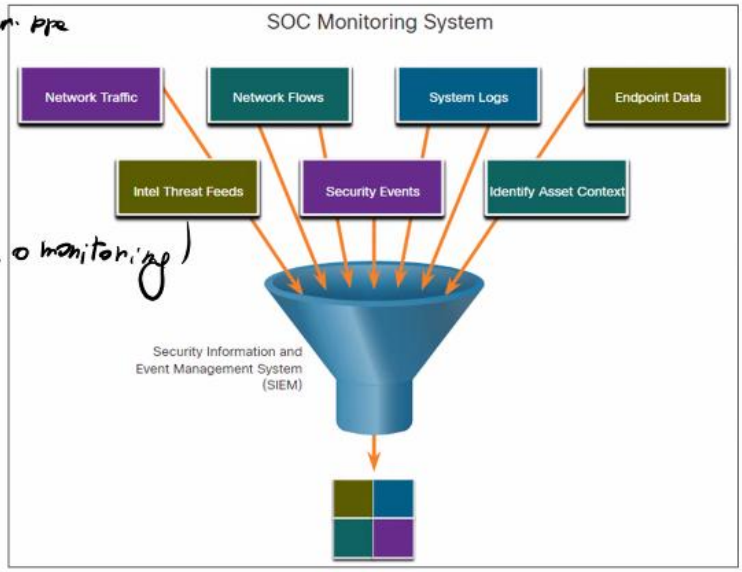
- A Cybersecurity Analyst is required to monitor security alert queues and investigate the assigned alerts. A ticketing system is used to assign these alerts to the analyst's queue.
- The software that generates the alerts can trigger false alarms. The analyst, therefore, needs to verify that an assigned 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.



Fighters in the War Against Cybercrime

Technologies in the SOC: SIEM

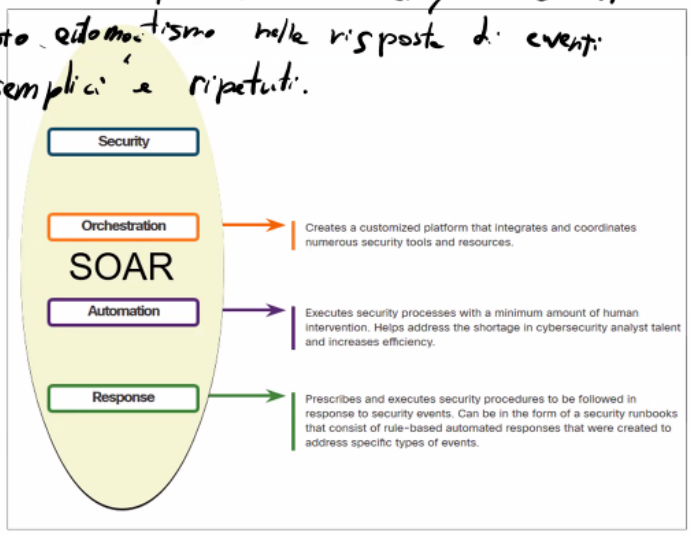
- An SOC needs a Security Information and Event Management (SIEM) system to understand the data that firewalls, network appliances, intrusion detection systems, and other devices generate.
- SIEM systems collect and filter data, and detect, classify, analyze and investigate threats. They may also manage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



Fighters in the War Against Cybercrime

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.



Fighters in the War Against Cybercrime

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

Enterprise and Managed Security

- For medium and large networks, the organization will benefit from implementing an enterprise-level SOC, which is a complete in-house solution.
- Larger organizations may outsource at least a part of the SOC operations to a security solutions provider.
- Cisco offers a wide range of incident response, preparedness, and management capabilities including:
  - Cisco Smart Net Total Care Service for Rapid Problem Resolution
  - Cisco Product Security Incident Response Team (PSIRT)
  - Cisco Computer Security Incident Response Team (CSIRT)
  - Cisco Managed Services
  - Cisco Tactical Operations (TacOps)
  - Cisco's Safety and Physical Security Program

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

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.

Becoming a Defender

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.

Becoming a Defender

Sources of Career Information

- A variety of websites and mobile applications advertise information technology jobs. Each site targets a variety of job applicants and provides different tools for candidates to research their ideal job position.
- Many sites are job site aggregators that gather listings from other job boards and company career sites and display them in a single location.
    - Indeed.com
    - CareerBuilder.com
    - USAJobs.gov
    - Glassdoor
    - LinkedIn

Becoming a Defender

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.

2.3 Fighters in the War Against Cybercrime Summary

What Did I Learn in this Module?

- Major elements of the SOC include people, processes, and technologies.
- The job roles include a Tier 1 Alert Analyst, a Tier 2 Incident Responder, a Tier 3 Threat hunter, and an SOC Manager.
- A Tier 1 Analyst monitors incidents, open tickets, and performs basic threat mitigation.
- SEIM systems are used for collecting and filtering data, detecting and classifying threats, and analyzing and investigating threats.
- SOAR integrates threat intelligence and automates incident investigation and response workflows based on playbooks developed by the security team.
- KPIs are devised to measure different aspects of SOC performance. Common metrics include Dwell Time, Meant Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), and Time to Control.
- There must be a balance between security and availability of the networks. Security cannot be so strong that it interferes with employees or business functions.
- A variety of cybersecurity certifications that are relevant to careers in SOCs are available from different organizations.

