Module Objectives

Module Title: Fighters in the War Against Cybercrime

Module Objective: Explain how to prepare for a career as a cybersecurity analyst.

2.1 The Modern Security Operations Center

Topic Title: The Modern Security Operations Center

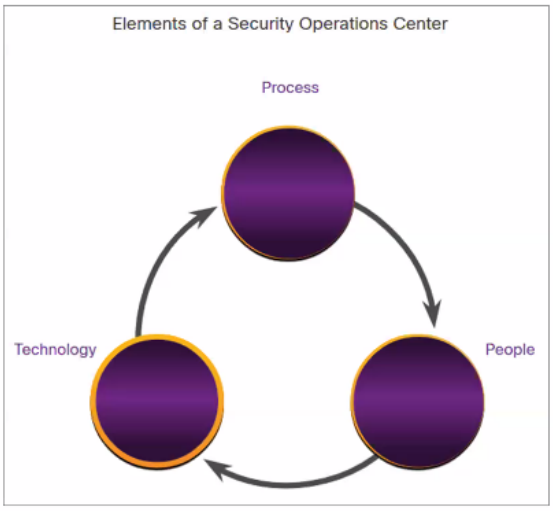
Topic Objective: Describe the role of a cybersecurity analyst.

Becoming a Defender

Fighters in the War Against Cybercrime

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

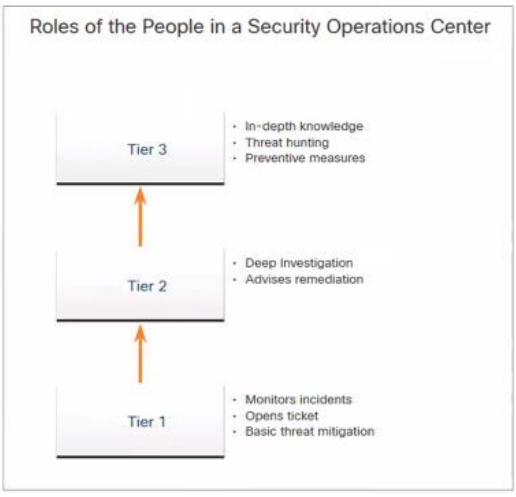
SOCs assign job roles by tiers, according to the expertise and responsibilities required for each.

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

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.