Threat Actors and Defenders

Md Manirul Islam

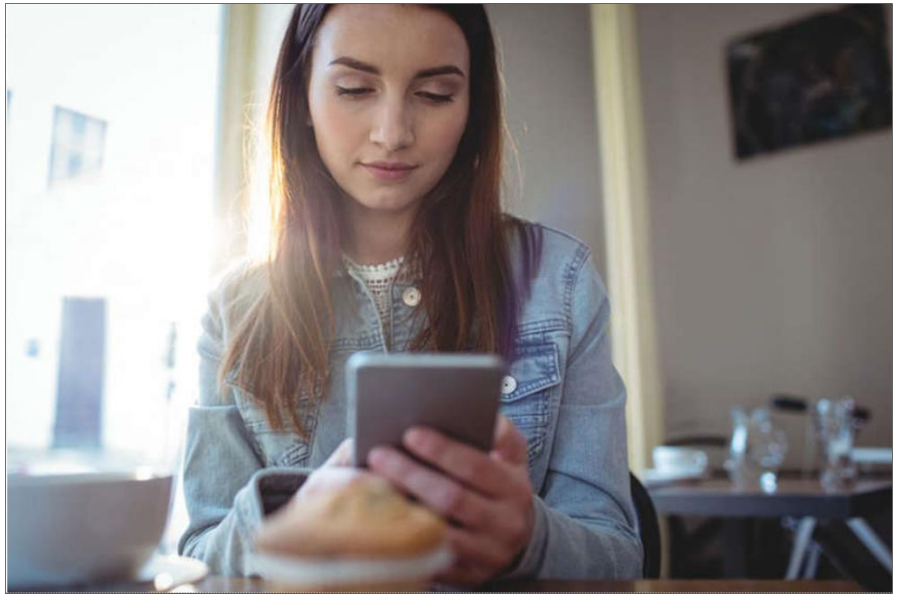
Director, Institute of Continuing Education

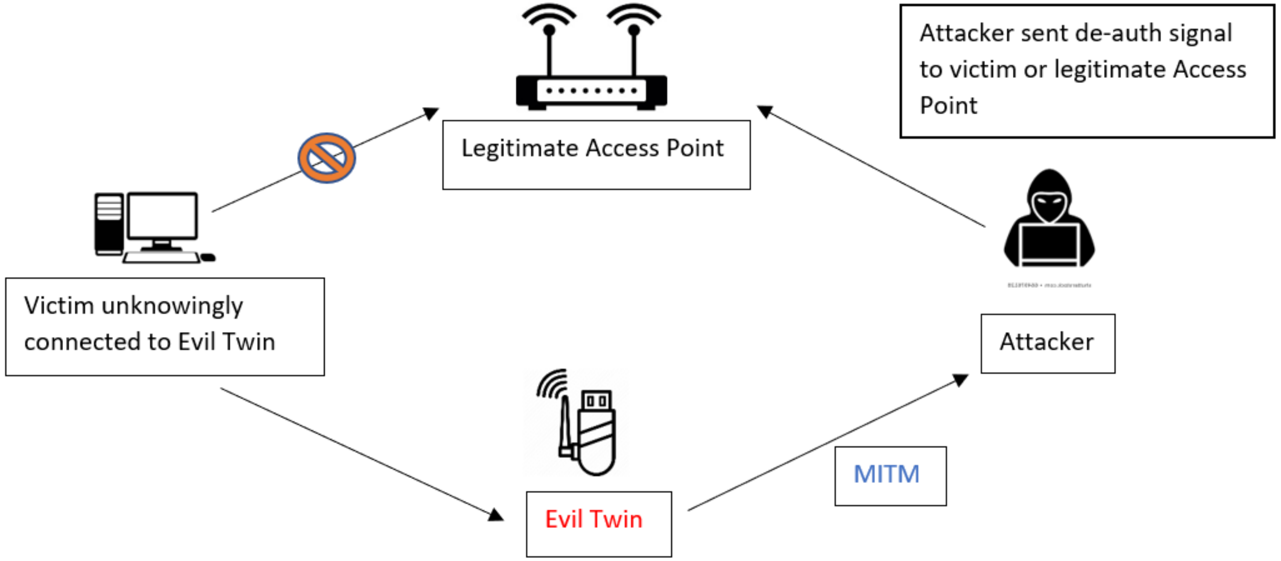
American International University-Bangladesh

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.

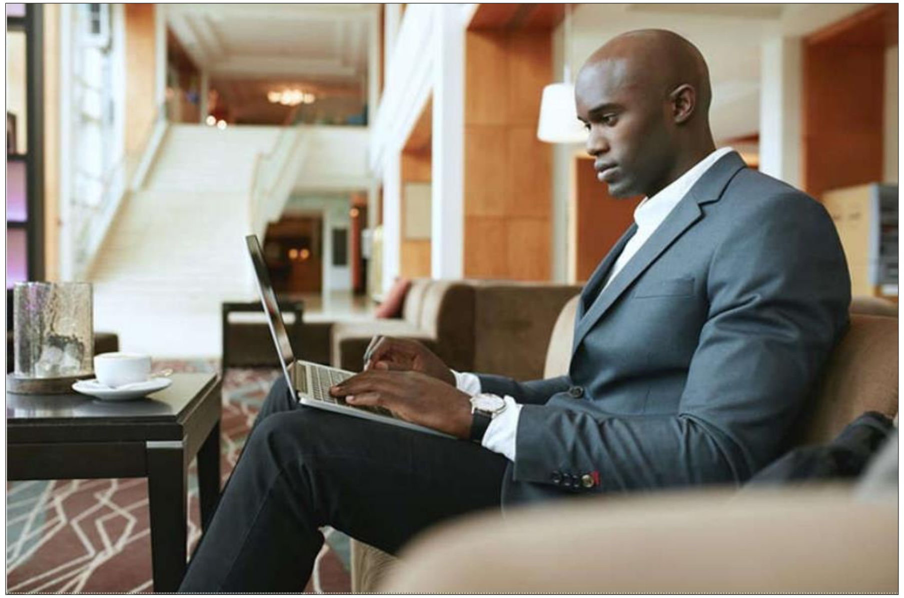




Attacker sent de-auth signal to victim or legitimate Access Point

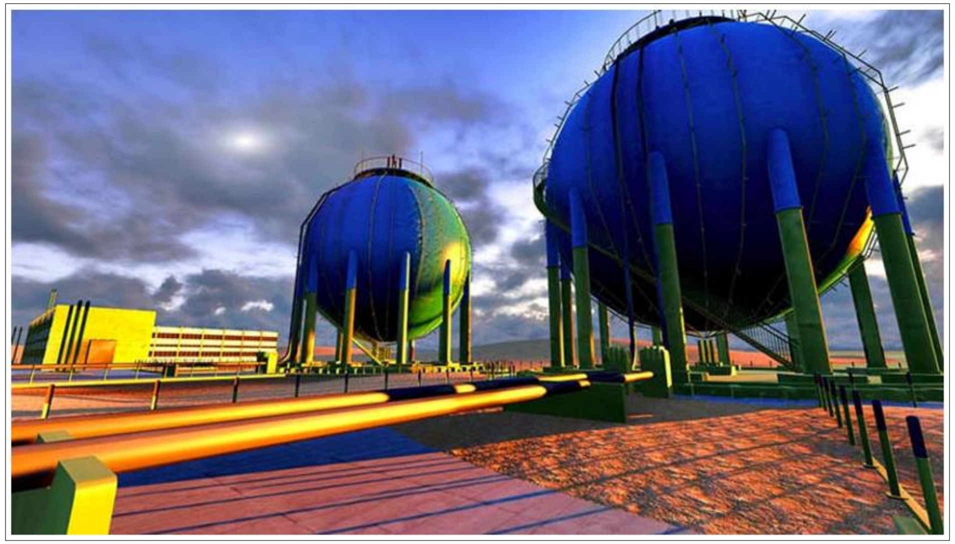
Ransomed Companies

- 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.



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.
- 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).



Threat Actors

Threat Actors

- Threat actors are individuals or groups of individuals who perform cyberattacks. They include, but are not limited to:
  - Amateurs
  - Hacktivists
  - Organized crime groups
  - State-sponsored groups
  - Terrorist groups
- 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.

Threat Impacts

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.

Business Impact

- 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.

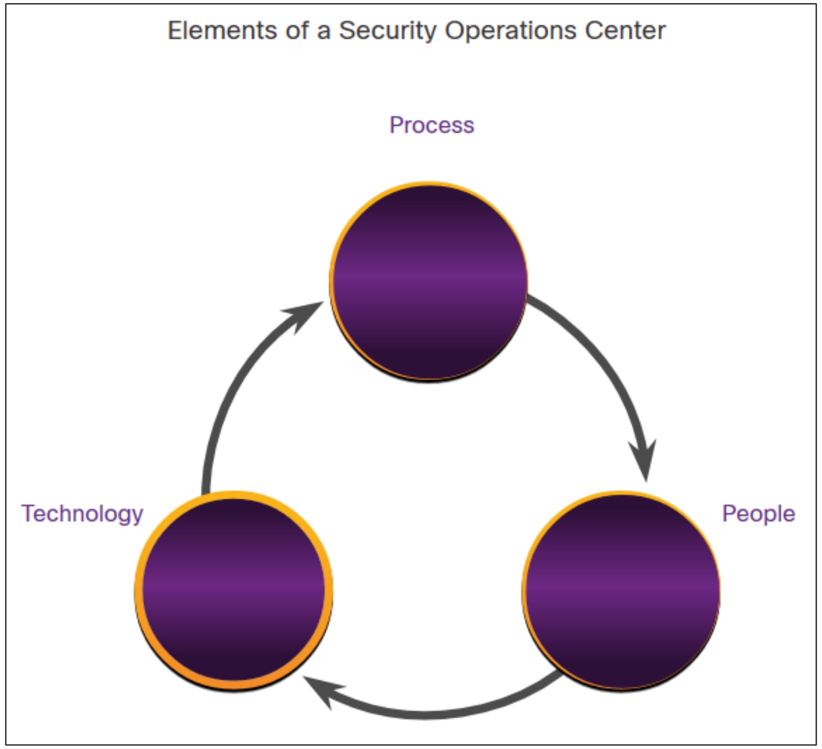
Political and National Security

- In 2016, a hacker published PII of 20,000 U.S. FBI employees and 9,000 U.S. DHS employees.
- Stuxnet worm was designed to impede Iran’s progress in enriching uranium
  - Example of network attack motivated by national security concerns
- Cyberwarfare is a serious possibility.
- The Internet has become essential as a medium for commercial and financial activities.
  - Disruption can devastate a nation’s economy and the safety of its citizens.

Fighters in the War against Cybercrime

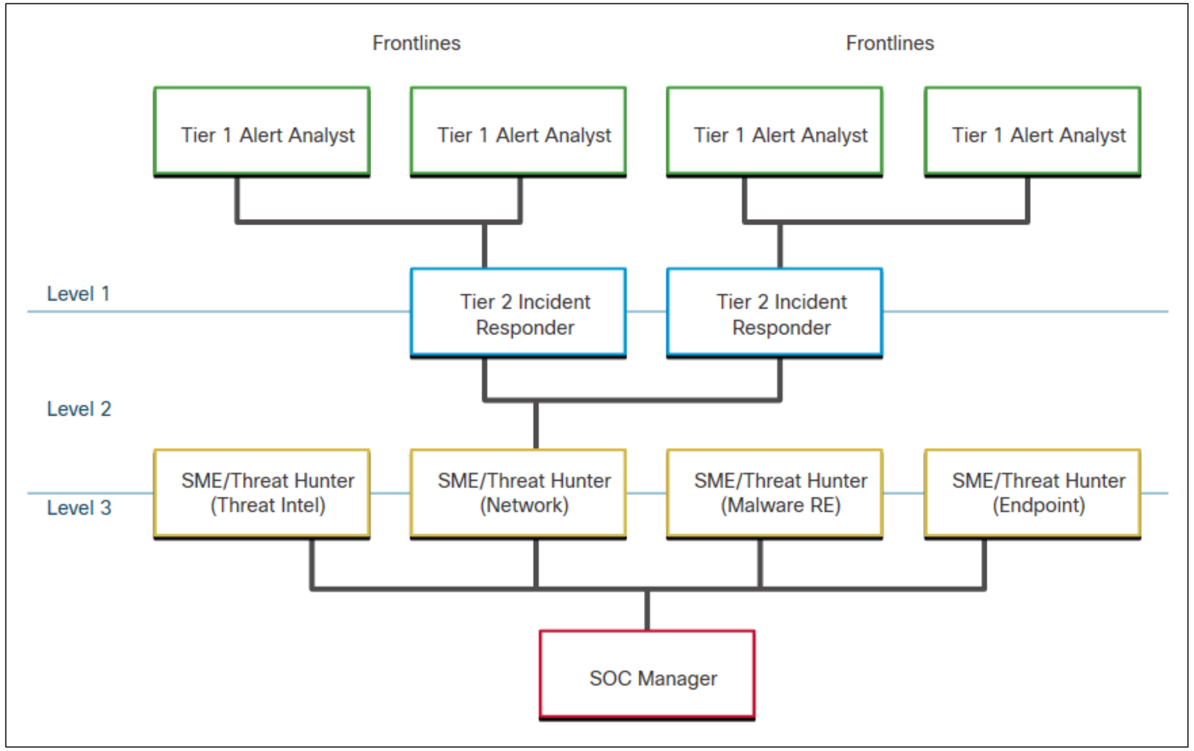
Security Operations Centers

- 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.



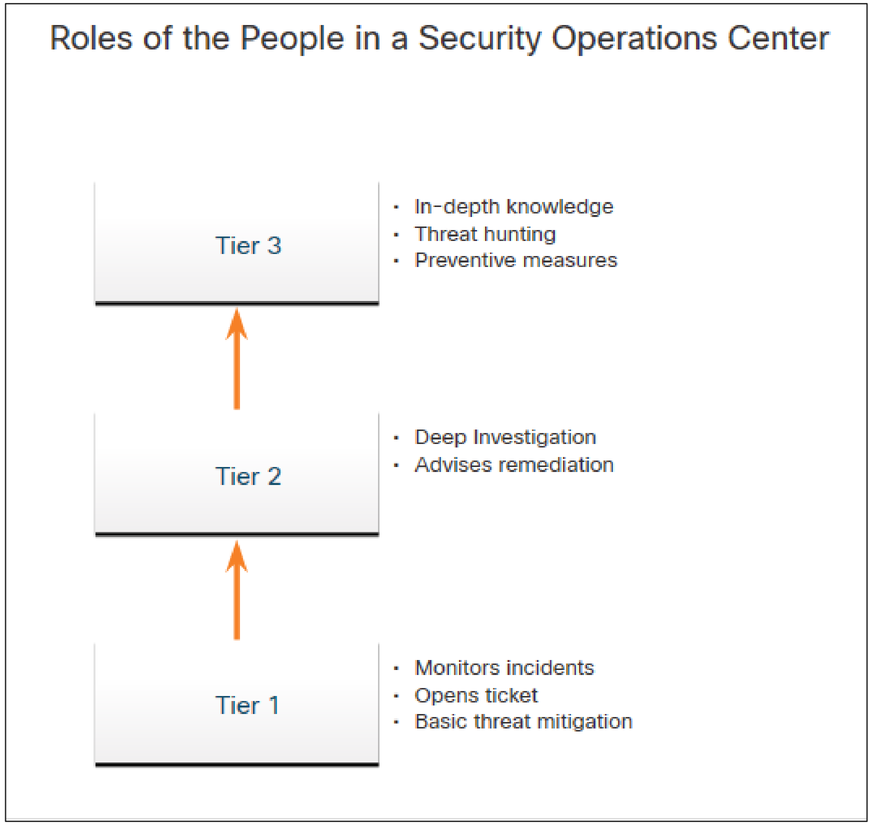
People in the SOC

- SOCs assign job roles by tiers, according to the expertise and responsibilities required for each.
- The SANS Institute (www.sans.org) classifies the roles people play in a SOC into four job titles:
  - **Tier 1 Alert Analyst**
  - **Tier 2 Incident Responder**
  - **Tier 3 Subject Matter Expert (SME)/Hunter**
  - **SOC Manager**


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
Level 3
SME/Threat Hunter (Threat Intel)
SME/Threat Hunter (Network)
SME/Threat Hunter (Malware RE)
SME/Threat Hunter (Endpoint)
SOC Manager

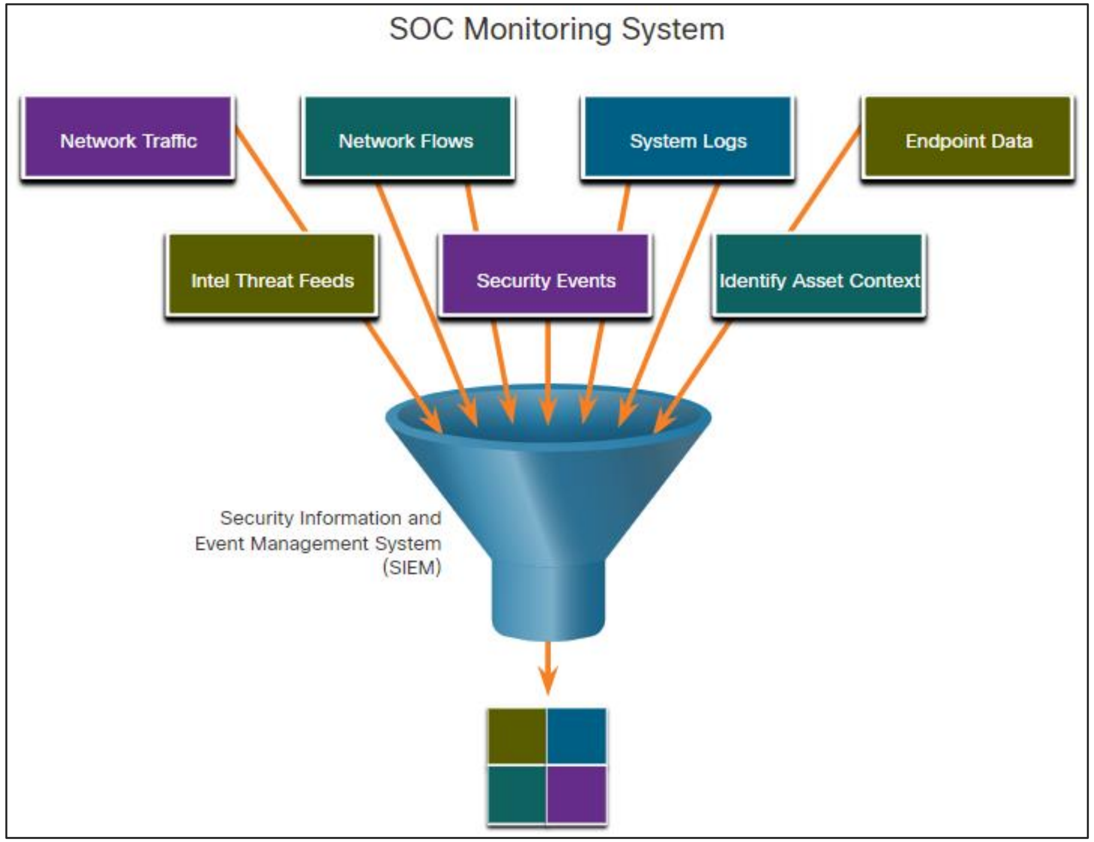
Process in the SOC

- 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.



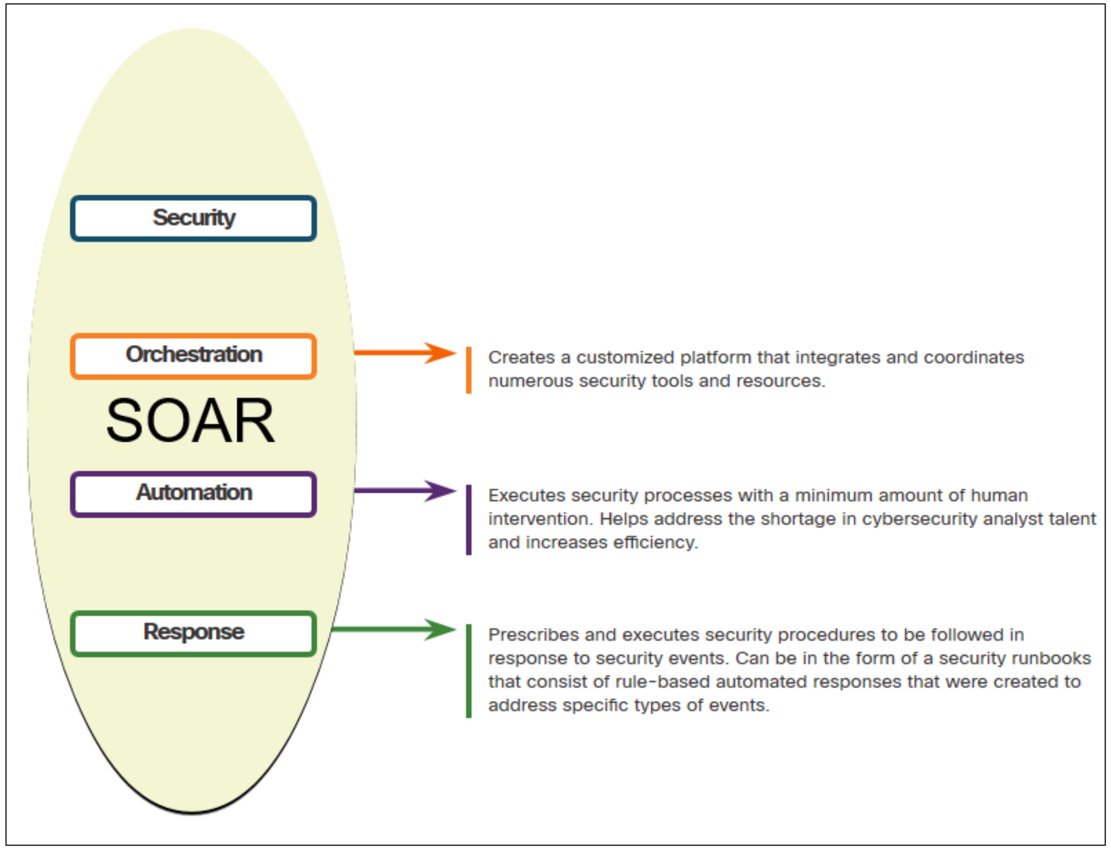
Technologies in the SOC: SIEM

- 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.

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

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)

Further Education

- **Degrees**: 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. 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

AMERICAN INTERNATIONAL UNIVERSITY
PRAESIDIUM
DISCIPLINA CIVITATIS
1994
BANGLADESH

cisco Networking Academy

ice.aiub.edu

ice@aiub.edu

☎ 01630-665666