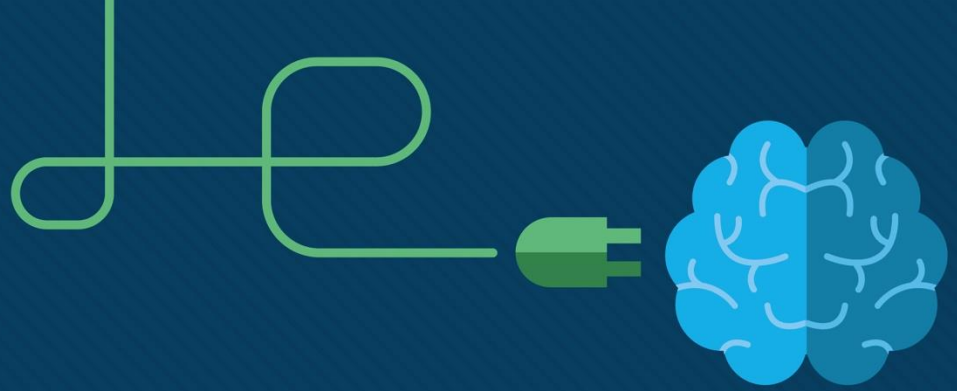


Chapter 1: Cybersecurity and the Security Operations Center

Cybersecurity Operations v1.1

Chapter 1 - Sections & Objectives

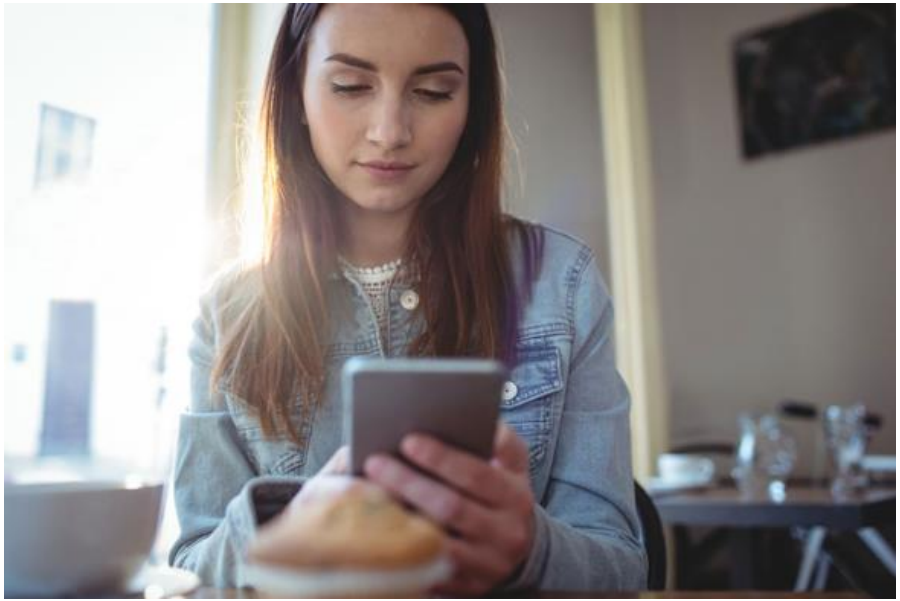
- 1.1 The Danger
  - Explain why networks and data are attacked.
    - Outline features of examples of cybersecurity incidents.
    - Explain the motivations of the threat actors behind specific security incidents.
    - Explain the potential impact of network security attacks.
- 1.2 Fighters in the 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.

1.1 The Danger

War Stories

Hijacked People

- A hacker set up an open “rogue” wireless hotspot posing as a legitimate wireless network.
- A customer logged onto her bank’s website.
- The hacker hijacked her session.
- The hacker gained access to her bank accounts.



War Stories

Ransomed Companies

- An employee receive an email from his CEO, containing an attached PDF.
- Ransomware is installed on the employee's computer.
- Ransomware gathers and encrypts corporate data.
- The attackers hold the company's data for ransom until they are paid.

Targeted Nations

- Stuxnet Worm
  - Infiltrated Windows operating systems.
  - Targeted Step 7 software that controls programmable logic controllers (PLCs) to damage the centrifuges in nuclear facilities.
  - Transmitted from the infected USB drives into the PLCs eventually damaging many cetrifuges.

Amateurs

- Known as script kiddies.
- Have little or no skill.
- Use existing tools or instructions found on the Internet to launch attacks.

Hacktivists

- Protest against organizations or governments
  - Post articles and videos.
  - Leak information.
  - Disrupt web services with DDoS attacks.

Financial Gain

- Much hacking activity is motivated by financial gain.
- Cybercriminals want to generate cash flow
  - Bank accounts
  - Personal data
  - Anything else they can leverage

Trade Secrets and Global Politics

- Nation states are also interested in using cyberspace
  - Hacking other countries
  - Interfering with internal politics
  - Industrial espionage
  - Gain significant advantage in international trade

How Secure is the Internet of Things

- The Internet of Things (IoT)
  - Connected things to improve quality of life.
  - Example: fitness trackers
- How secure are these devices?
  - Firmware
  - Security flaws
  - Updatable with patch
- DDoS attack against domain name provider, Dyn
  - Took down many websites.
  - Compromised webcams, DVRs, routers, and other IoT devices formed a botnet.
  - The hacker controlled botnet created the DDoS attack that disabled essential Internet services.

PII and PHI

- Personally identifiable information (PII) is any information that can be used to positively identify an individual.
  - Examples of PII include: Name, Social security number, Birthdate, Credit card numbers, Bank account numbers, Government-issued ID, Address information (street, email, phone numbers)
  - This information is sold on the dark web.
  - Create fake accounts, such as credit cards and short-term loans.
- Protected Health Information (PHI) – A subset of PII:
  - Creates and maintains electronic medical records (EMRs)
  - Regulated by Health Insurance Portability and Accountability Act (HIPAA)

Lost Competitive Advantage

- Could result in lost competitive advantage.
  - Corporate espionage in cyberspace.
  - Loss of trust that comes when a company is unable to protect its customers' personal data.

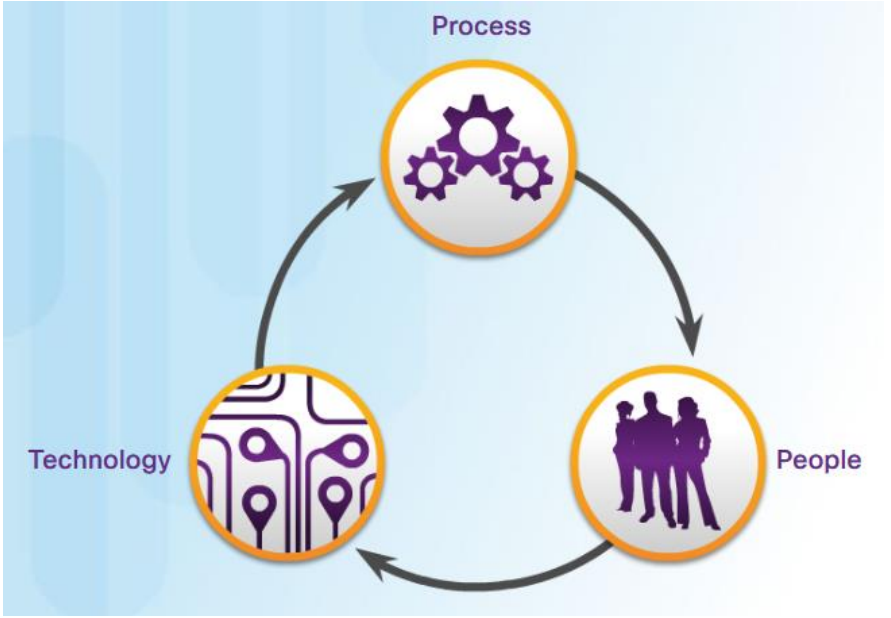
Political and National Security

- 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.

1.2 Fighters in the War Against Cybercrime

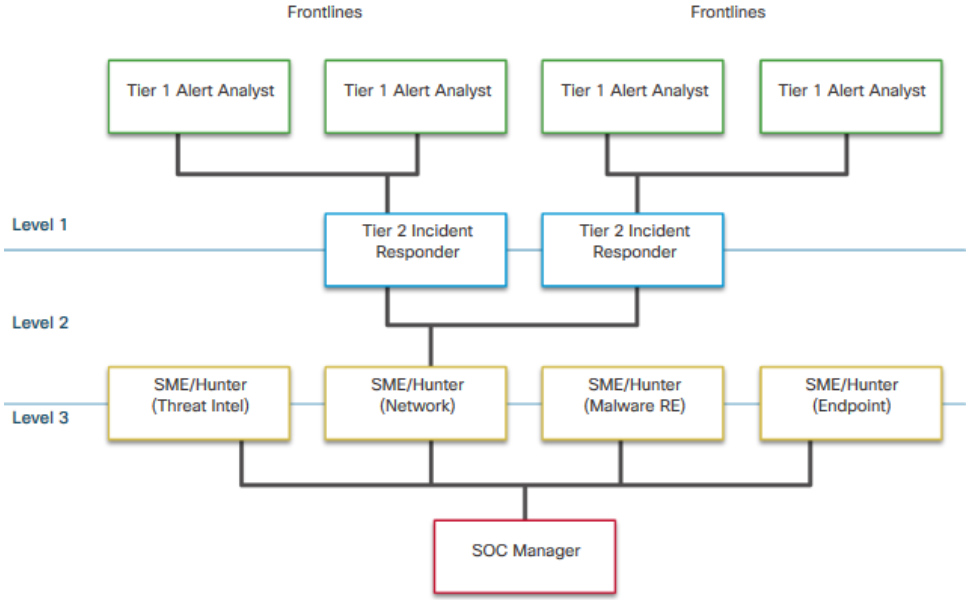
Elements of a SOC

- 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



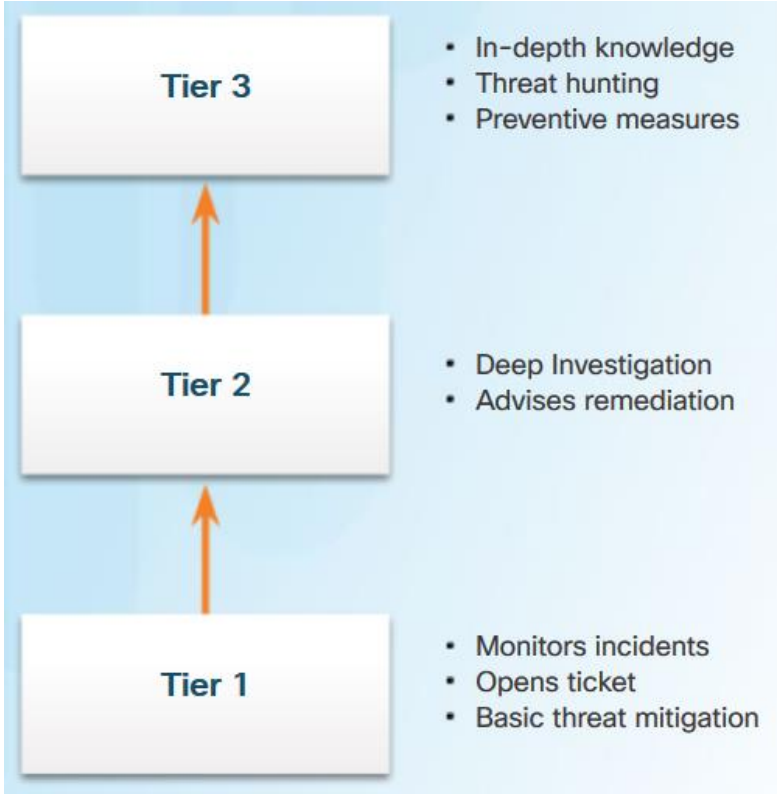
People in the SOC

- 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**
- Can you guess the responsibilities for each of the job titles?



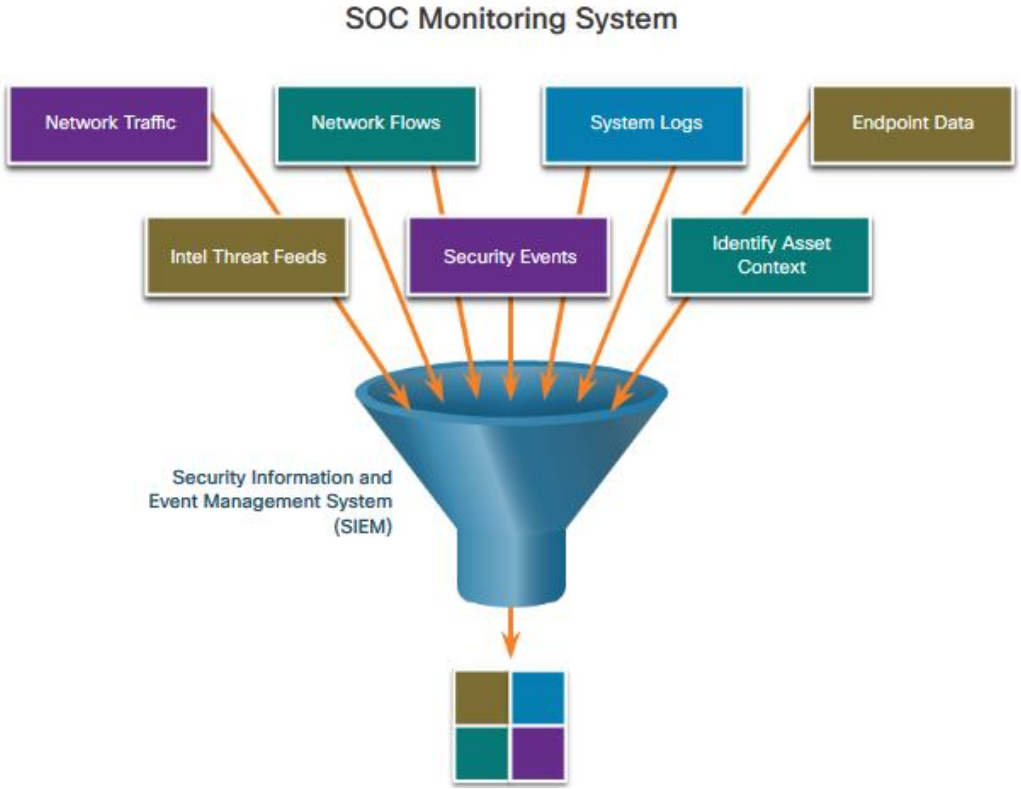
Process in the SOC

- Tier 1 Alert Analyst begins with monitoring security alert queues.
- Tier 1 Alert Analyst verifies if an alert triggered in the ticketing software represents a true security incident.
- The incident can be forwarded to investigators, or resolved as a false alarm.



Technologies in the SOC

- Security Information and Event Management (SIEM) systems:
  - Collect and filter data.
  - Detect and classify threats.
  - Analyze and investigate threats.
  - Implement preventive measures.
  - Address future threats.



Enterprise and Managed Security

- Organizations may implement an enterprise-level SOC.
- The SOC can be :
  - A complete in-house solution
  - Outsourced at least part of the SOC operations to a security solutions provider.

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")	31.5 seconds
99.99999% ("seven nines")	3.15 seconds

Certifications

- A variety of cybersecurity certifications are available:
  - CCNA Cyber Ops
  - CompTIA Cybersecurity Analyst Certification (CSA+)
  - (ISC)² Information Security Certifications (including CISSP)
  - Global Information Assurance Certification (GIAC)

Further Education

- Consider pursuing a technical degree or bachelor's degree in computer science, electrical engineering, information technology, or information security.
- Computer programming is an essential skill in cybersecurity.
- Python is an object-oriented, open-source programing language. It is routinely used by cybersecurity analysts

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

- Ways to gain experience:
  - Internships
  - Cisco Cybersecurity Scholarship
  - Temporary Agencies
  - Your first job


CISCO