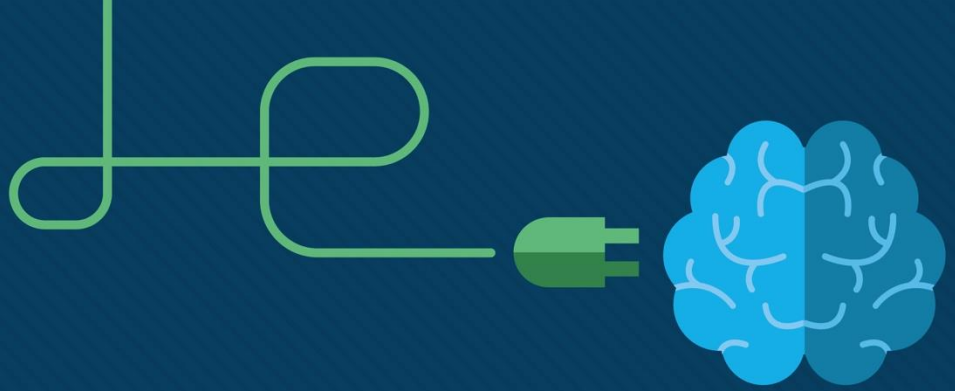


Chapter 1: Cybersecurity and the Security Operations Center

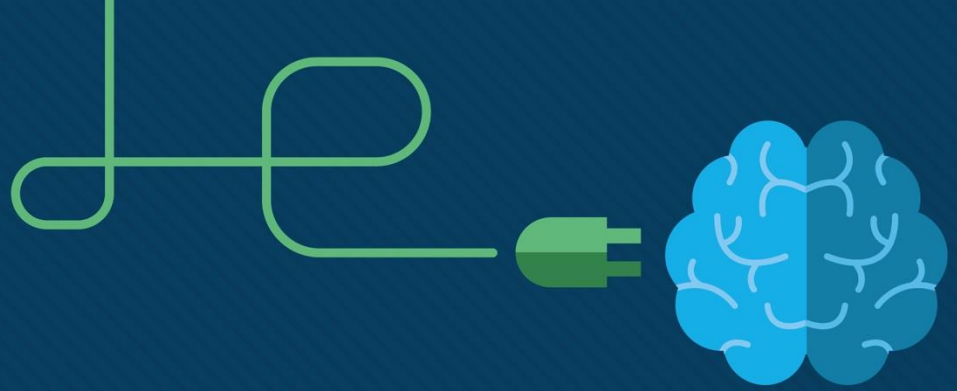
Instructor Materials

Cybersecurity Operations v1.1

Chapter 1: Cybersecurity and the Security Operations Center

Cybersecurity Operations v1.1
Planning Guide

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

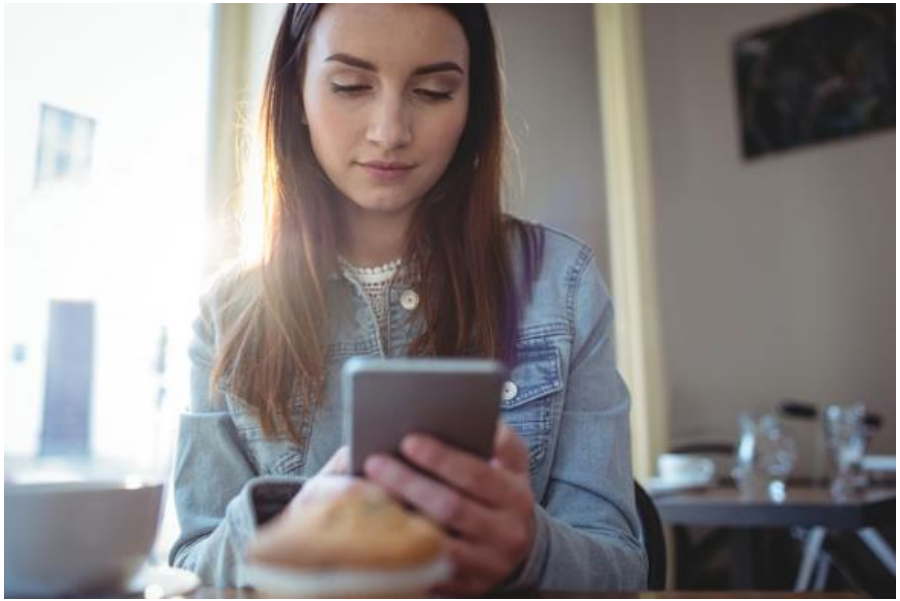
1.1 The Danger

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

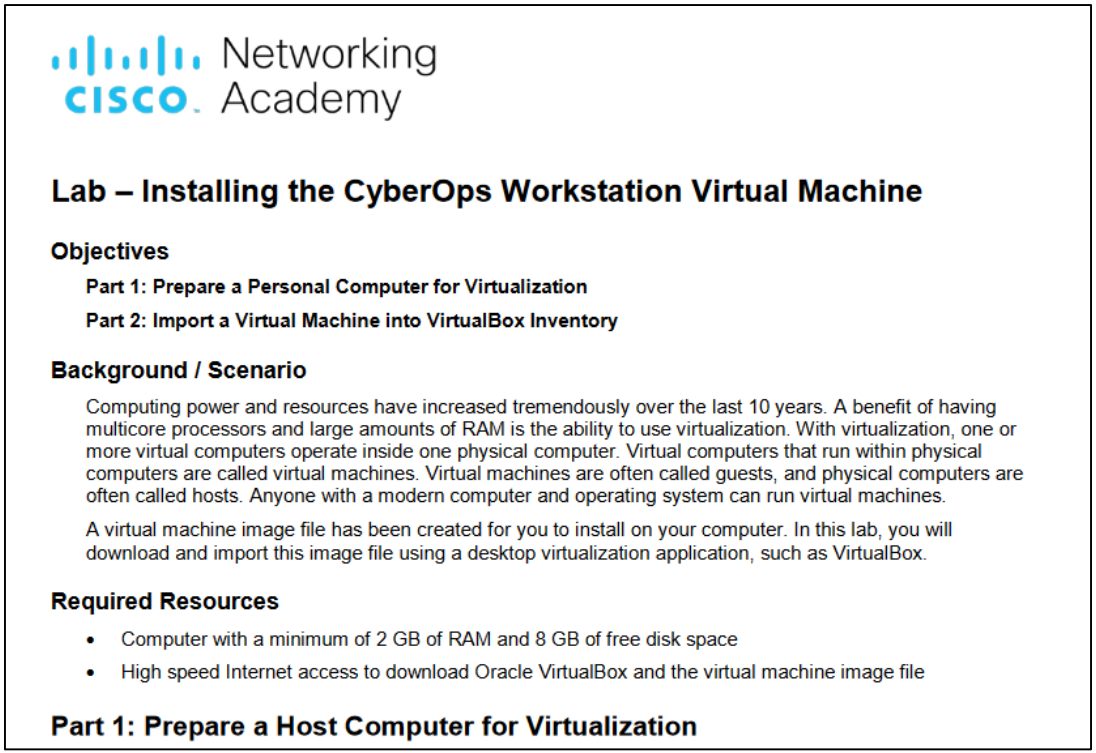
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Installing the CyberOps Workstation Virtual Machine



Networking Academy

Lab – Installing the CyberOps Workstation Virtual Machine

Objectives

Part 1: Prepare a Personal Computer for Virtualization

Part 2: Import a Virtual Machine into VirtualBox Inventory

Background / Scenario

Computing power and resources have increased tremendously over the last 10 years. A benefit of having multicore processors and large amounts of RAM is the ability to use virtualization. With virtualization, one or more virtual computers operate inside one physical computer. Virtual computers that run within physical computers are called virtual machines. Virtual machines are often called guests, and physical computers are often called hosts. Anyone with a modern computer and operating system can run virtual machines.

A virtual machine image file has been created for you to install on your computer. In this lab, you will download and import this image file using a desktop virtualization application, such as VirtualBox.

Required Resources

- Computer with a minimum of 2 GB of RAM and 8 GB of free disk space
- High speed Internet access to download Oracle VirtualBox and the virtual machine image file

Part 1: Prepare a Host Computer for Virtualization

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Cybersecurity Case Studies

Networking Academy

Lab - Cybersecurity Case Studies

Objectives

Research and analyze cyber security incidents

Background / Scenario

Governments, businesses, and individual users are increasingly the targets of cyberattacks and experts predict that these attacks are likely to increase in the future. Cybersecurity education is a top international priority as high-profile cyber-security related incidents raise the fear that attacks could threaten the global economy. The Center for Strategic and International Studies estimates that the cost of cybercrime to the global economy is more than $400 billion annually and in the United State alone as many as 3000 companies had their systems compromised in 2013. In this lab you will study four high profile cyberattacks and be prepared to discuss the who, what, why and how of each attack.

Required Resources

- PC or mobile device with Internet access

Step 1: Conduct search of high profile cyberattacks.

a. Using your favorite search engine conduct a search for each of the cyberattacks listed below. Your search will likely turn up multiple results ranging from news articles to technical articles.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Amateurs

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hacktivists

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Learning the Details of Attacks

Lab – Learning the Details of Attacks

Objectives

Research and analyze IoT application vulnerabilities

Background / Scenario

The Internet of Things (IoT) consists of digitally connected devices that are connecting every aspect of our lives, including our homes, offices, cars, and even our bodies to the Internet. With the accelerating adoption of IPv6 and the near universal deployment of Wi-Fi networks, the IoT is growing at an exponential pace. Industry experts estimate that by 2020, the number of active IoT devices will approach 50 billion. IoT devices are particularly vulnerable to security threats because security has not always been considered in IoT product design. Also, IoT devices are often sold with old and unpatched embedded operating systems and software.

Required Resources

- PC or mobile device with Internet access

Conduct a Search of IoT Application Vulnerabilities

Using your favorite search engine, conduct a search for Internet of Things (IoT) vulnerabilities. During your search, find an example of an IoT vulnerability for each of the IoT verticals: industry, energy systems, healthcare, and government. Be prepared to discuss who might exploit the vulnerability and why, what caused the vulnerability, and what could be done to limit the vulnerability? Some suggested resources to get started on your search are listed below:

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

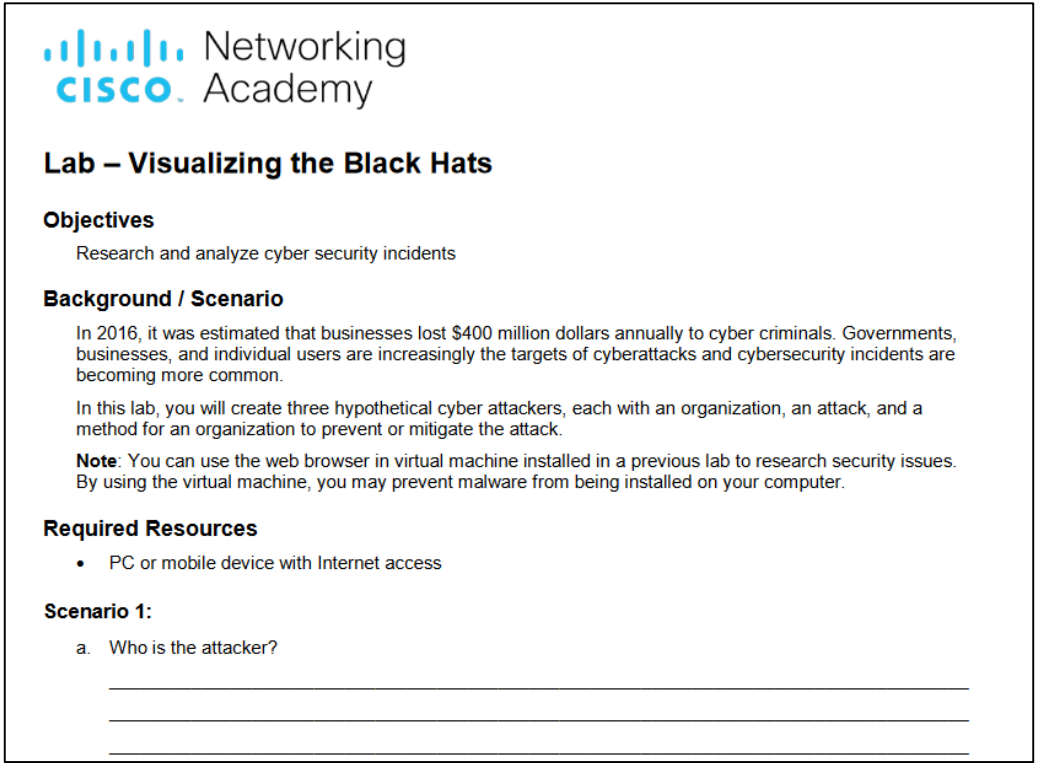
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Visualizing the Black Hats



Networking Academy

Lab – Visualizing the Black Hats

Objectives

Research and analyze cyber security incidents

Background / Scenario

In 2016, it was estimated that businesses lost $400 million dollars annually to cyber criminals. Governments, businesses, and individual users are increasingly the targets of cyberattacks and cybersecurity incidents are becoming more common.

In this lab, you will create three hypothetical cyber attackers, each with an organization, an attack, and a method for an organization to prevent or mitigate the attack.

Note: You can use the web browser in virtual machine installed in a previous lab to research security issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Required Resources

- PC or mobile device with Internet access

Scenario 1:

a. Who is the attacker?

_____

_____

_____

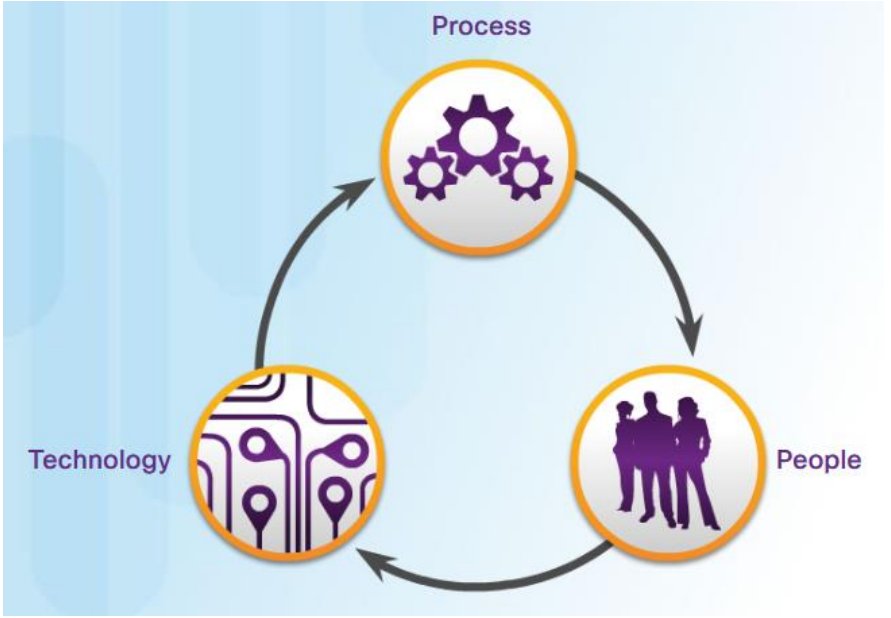
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.2 Fighters in the War Against Cybercrime

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Elements of a SOC

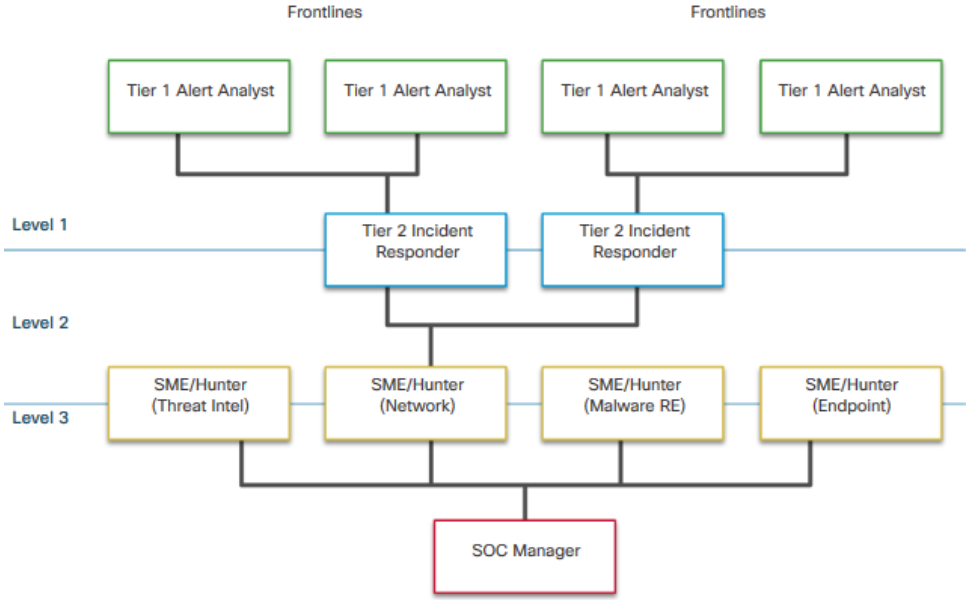
- Security Operations Centers (SOCs) provide a broad range of services:
  - Monitoring
  - Management
  - Comprehensive threat solutions
  - Hosted security
- SOCs can be:
  - In-house, owned and operated by a business.
  - Elements can be contracted out to security vendors.
- The major elements of a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



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

People in the SOC

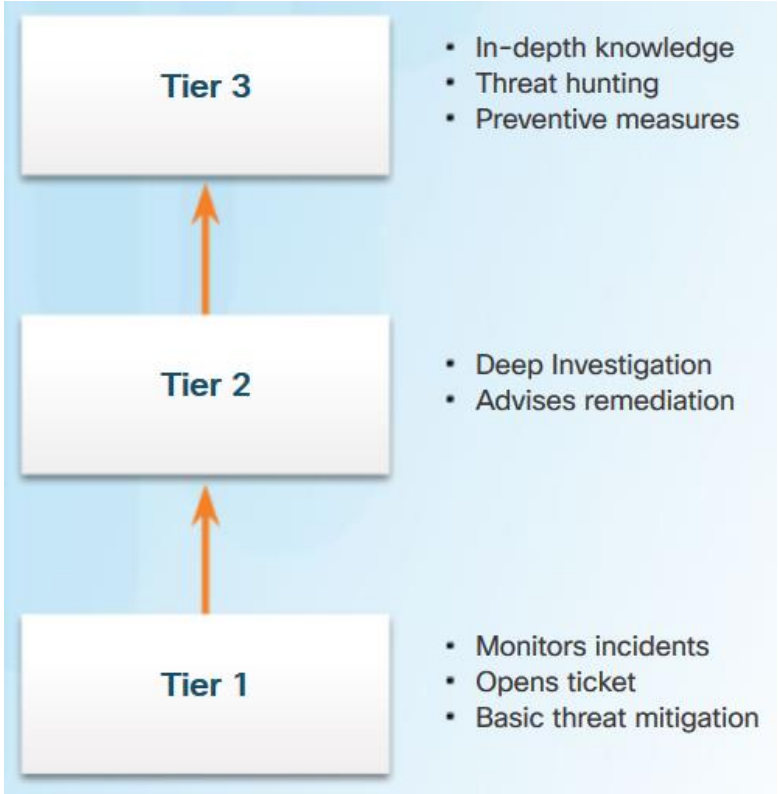
- The SANS Institute (www.sans.org) classifies the roles people play in a SOC into four job titles:
  - **Tier 1 Alert Analyst**
  - **Tier 2 Incident Responder**
  - **Tier 3 Subject Matter Expert (SME)/Hunter**
  - **SOC Manager**
- Can you guess the responsibilities for each of the job titles?



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Process in the SOC

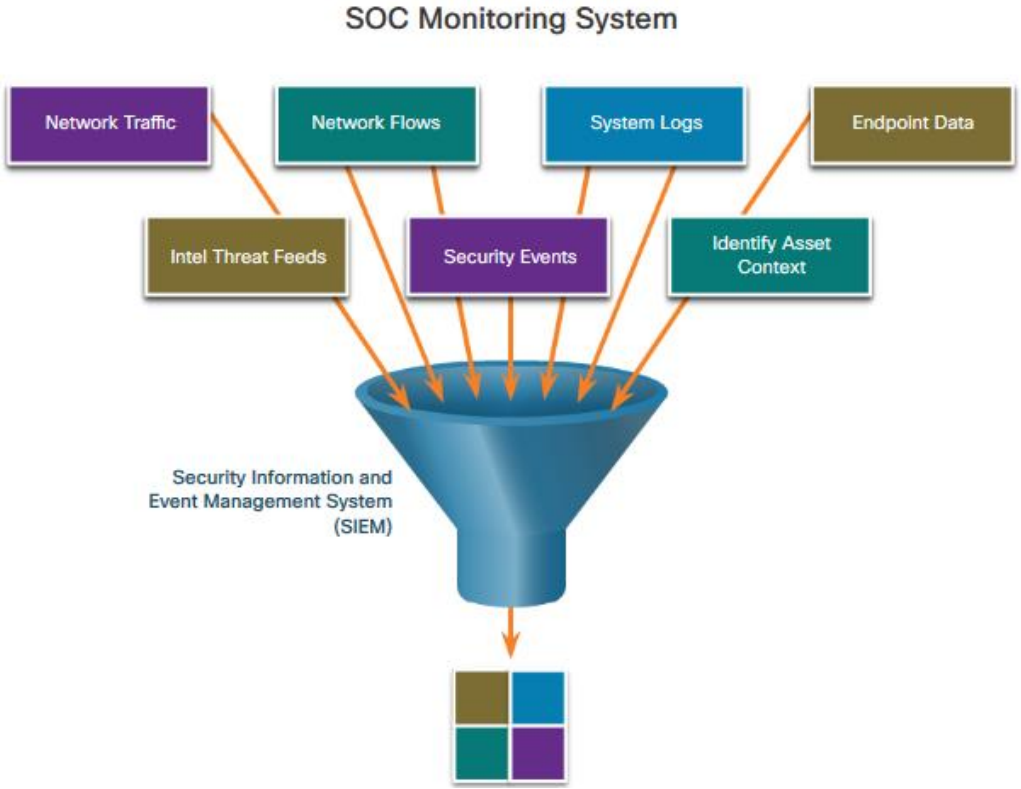
- Tier 1 Alert Analyst begins with monitoring security alert queues.
- Tier 1 Alert Analyst verifies if an alert triggered in the ticketing software represents a true security incident.
- The incident can be forwarded to investigators, or resolved as a false alarm.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Getting Experience

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

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Becoming a Defender

Networking Academy

Lab - Becoming a Defender

Objectives

Research and analyze what it takes to become a network defender

Background / Scenario

In our technology-centric world, as the world gets more connected, it also gets less safe. Cybersecurity is one of the fastest growing and in-demand professions. Individuals in this field perform a wide variety of jobs including but not limited to consultation, investigation and program management services to mitigate risks through both internal and external sources. Cybersecurity professionals are required to evaluate, design and implement security plans, conduct in-depth fraud investigation and perform security research and risk assessment and propose solutions to potential security breaches.

Individuals with good security skills have a great earning potential. To be considered for one of these high paying jobs, it is imperative to have the proper qualifications. To this effect, it is important to consider the industry certificates available for this career path. There are many certifications to choose from, and selecting the right certificate(s) for you individually requires careful consideration.

Note: You can use the web browser in virtual machine installed in a previous lab to research security related issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Required Resources

- PC or mobile device with Internet access

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.3 Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Summary

- A public “rogue” wireless network can be used to gain access personal information.
- Employees of a company can inadvertently download ransomware that could begin the process of gathering and encrypting corporate data.
- Sophisticated malware, Stuxnet worm, is an example of how nations can be targeted to influence nation’s vulnerable infrastructure.
- Amateurs cause damage by using simple tools found online.
- Hacktivists are experienced hackers who work for good causes or malicious purposes.
- Many hackers are only seeking financial gain by stealing money electronically, or stealing corporations’ or nations’ trade secrets and selling this information.
- Defending a nation against cyberespionage and cyberwarfare continues to be a priority.
- Be aware of the insecurities in The Internet of Things.
- PII stands for personally identifiable information. PHI is personal health information. Both PII and PHI can be stolen and used to gain access to private information.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Summary (Cont.)

- The loss of competitive advantage may come from the loss of trust if a company cannot protect the PII of its customers.
- National security can be disrupted by hackers. Stuxnet worm is an example.
- The major elements of a SOC are people, processes, and technology.
- Security Operations Centers work to combat cybercrime.
- The people in a SOC are Tier 1 Analysts (for which this course was developed), Tier 2 Incident Responders, Tier 3 SME/Hunters, and the SOC Manager.
- A Tier 1 Analyst monitors security alert queues. The Tier 1 Analyst may need to verify that an alert represents a true security incident. When verification is established, the incident can be forwarded to investigators, or resolved as a false alarm.
- SIEM systems are used for collecting and filtering data, detecting and classifying threats, analyzing and investigating threats, implementing preventive measures, and addressing future threats.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Summary (Cont.)

- An SOC can be a complete in-house solution or outsource part of the operations to a security solutions provider.
- 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.
- A variety of cybersecurity certifications are available from several different organizations.
- For a career in the cybersecurity field, consider a technical degree or bachelor’s degree. Cybersecurity analysts need to know computer programming. Learning Python is a good place to start.
- A variety of resources provide job search and salary information.
- People prepare for work in a Security Operations Center (SOC) by earning certifications, seeking formal education, and by using employment services to gain internship experience and jobs.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

New Terms and Commands

- distributed denial of service (DDoS)
- hacktivists
- malware
- personally identifiable information (PII)
- protected health information (PHI)
- ransomware
- script kiddies
- security information and event management system (SIEM)
- security Operations Center (SOC)
- SOC Manager
- Tier 1 Alert Analyst
- Tier 2 Incident Responder
- Tier 3 Subject Matter Expert (SME)/Hunter

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 2: Security Concepts**
  - 2.3 Describe the following terms:
    - Threat Actor
    - Reverse engineering
    - PII
    - PHI

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO