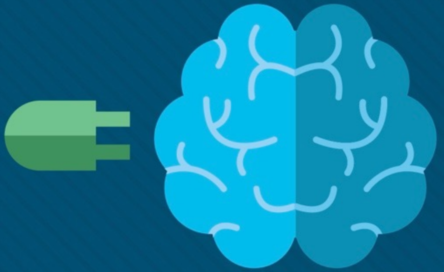


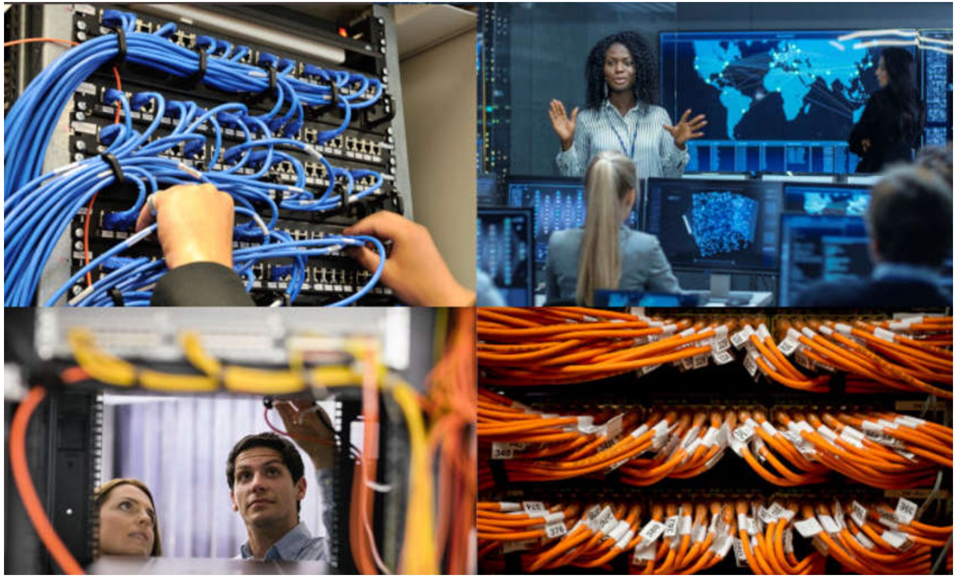
Chapter 1: Cybersecurity and the Security Operations Center

Information Security

Dr. Ayman Aljarbouh

Course Overview

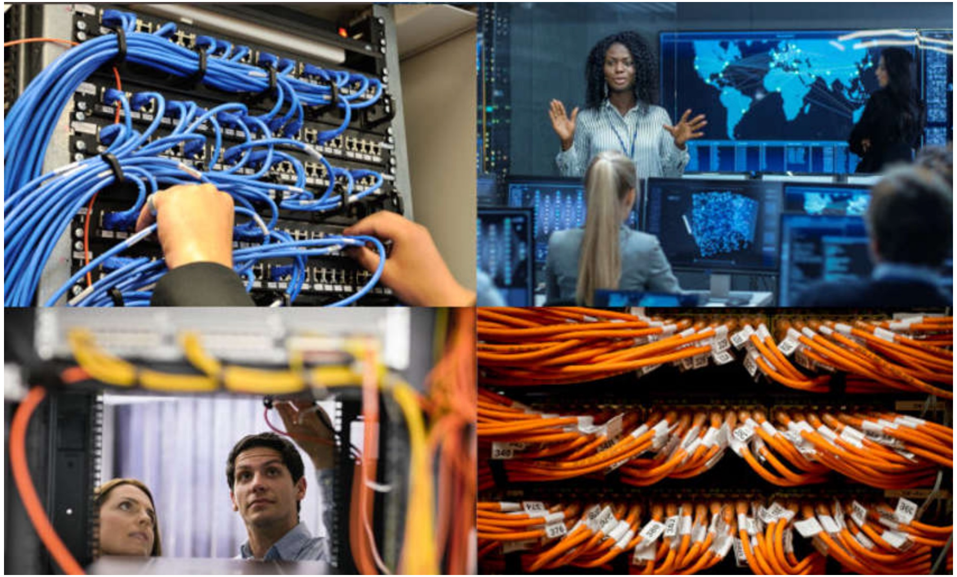
- This course covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).
- Upon completion of the course, you will be able to perform the following tasks:
  - Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
  - Explain the role of the Cybersecurity Operations Analyst in the enterprise.
  - Explain the features and characteristics of the Linux Operating System.



Course Overview

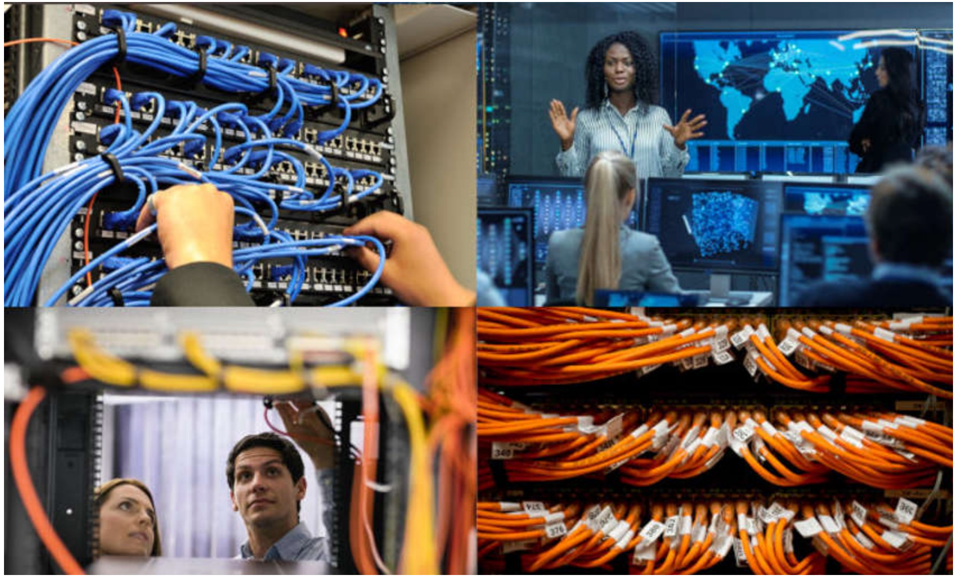
- This course covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).

- Upon completion of the course, you will be able to perform the following tasks:
  - Analyze the operation of network protocols and services.
  - Explain the operation of the network infrastructure.
  - Classify the various types of network attacks.
  - Use network monitoring tools to identify attacks against network protocols and services.



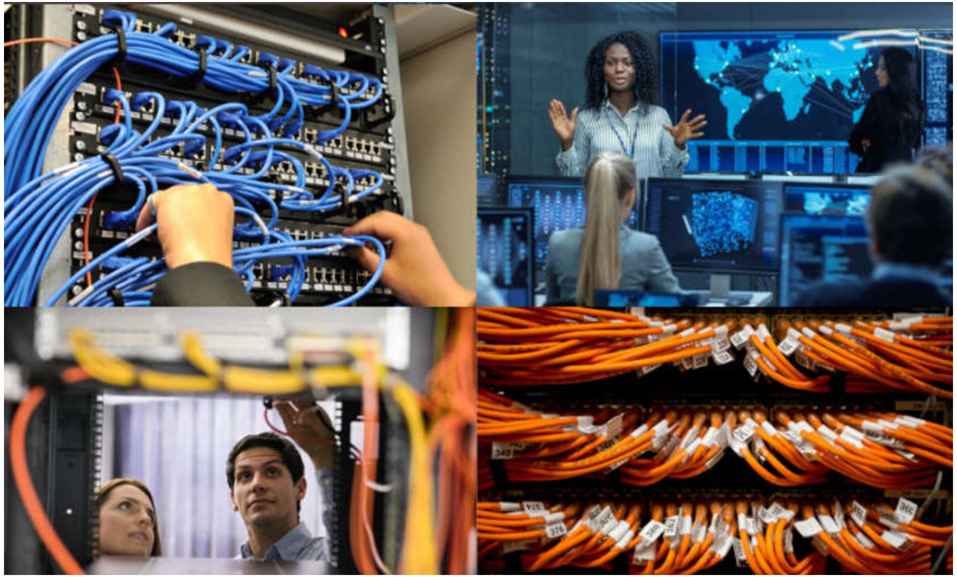
Course Overview

- This course covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).
- Upon completion of the course, you will be able to perform the following tasks:
  - Explain how to prevent malicious access to computer networks, hosts, and data.
  - Explain the impacts of cryptography on network security monitoring.
  - Explain how to investigate endpoint vulnerabilities and attacks.



Course Overview

- This course covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).
- Upon completion of the course, you will be able to perform the following tasks:
    - Evaluate network security alerts.
    - Analyze network intrusion data to identify compromised hosts and vulnerabilities.
    - Apply incident response models to manage network security incidents.

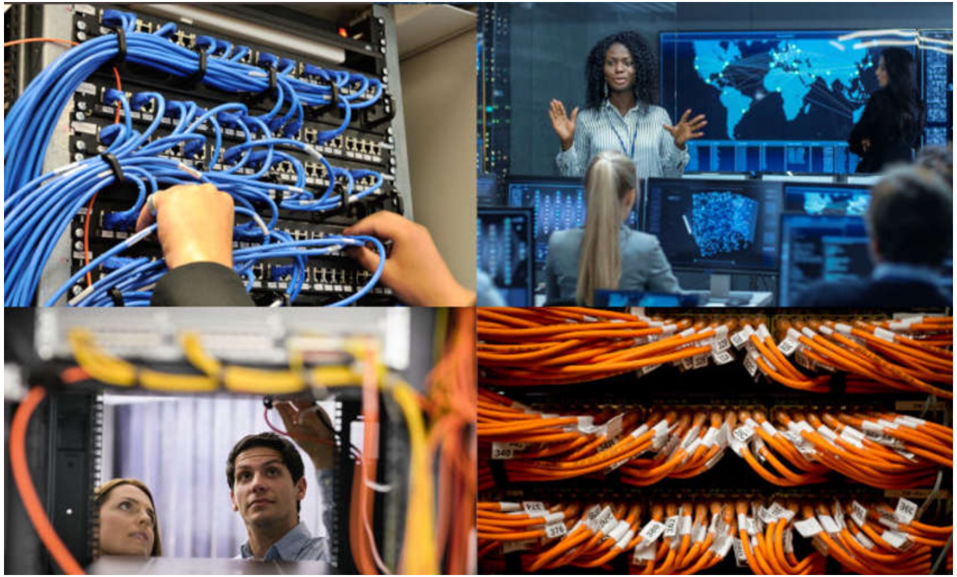


Course Overview

- This course covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).
- Upon completion of the course, you will be able to perform the following tasks:
  - Complete the requirements for Cisco CCNA CyberOps Associate Certification.

Cisco Networking Academy
Verified
CyberOps Associate

CISCO CERTIFIED
CyberOps
Associate



Student Resources

- There are several tools and resources that are available to you that will help you in your journey as you develop your Cyber Security skills and prepare for job opportunities:
  - **Lab Environment**

    Two virtual machines (VM) are used:

    CyberOps Workstation and Security Onion.

1 GB minimum RAM memory requirement

4 GB minimum RAM memory requirement

The virtual machines (VM) provide all the applications and latest security monitoring and network intrusion analysis capabilities needed for the course

Student Resources

- There are several tools and resources that are available to you that will help you in your journey as you develop your Cyber Security skills and prepare for job opportunities:
  - **Cisco Packet Tracer**

    An innovative simulation and visualization tool, helps you to practice networking, IoT and cybersecurity skills from your desktop.

    - Minimum requirement:
      - 4GB of free RAM (64bit)
      - 2GB of free RAM (32bit)
      - 1.4 GB of free disk space
    - Tutorial: http://tutorials.ptnetacad.net/.

Cisco Packet Tracer requires authentication with your email and password when you first use it and for each new OS login session.

Ethical Hacking Statement

- In this course, you will use tools and techniques in a “sandboxed”, virtual machine environment that allows you to create, implement, monitor, and detect various types of cyber attacks.
- Security holes and vulnerabilities that are created in this course should only be used in an ethical manner and only in this “sandboxed” virtual environment.
- Experimentation with these tools, techniques, and resources outside of the provided sandboxed virtual environment is **strictly prohibited**.
- Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator’s motivations.
- It is your responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

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.

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.

Today

1.1 The Danger

Module Objectives

Module Title: The Danger

Module Objective: Explain why networks and data are attacked.

Topic Title	Topic Objective
War Stories	Explain why networks and data are attacked.
Threat Actors	Explain the motivations of the threat actors behind specific security incidents.
Threat Impact	Explain the potential impact of network security attacks.

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.
- A customer logged onto her bank’s website.
- The hacker hijacked her session.
- The hacker gained access to her bank accounts.
- Search the internet on “evil twin hotspots” to learn more about this security threat.

War Stories

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.

War Stories

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).

Zero Days:

https://www.youtube.com/watch?v=ooRSmkn-WfM

War Stories

Video - Anatomy of an Attack

Watch this video to view details of a complex attack.

https://www.youtube.com/watch?v=jK0oG-cDF4Y

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 (Contd.)

Amateurs

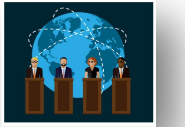
- They are also known as script kiddies and have little or no skill.
- They often use existing tools or instructions found on the internet to launch attacks.
- Even though they use basic tools, the results can still be devastating.

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.

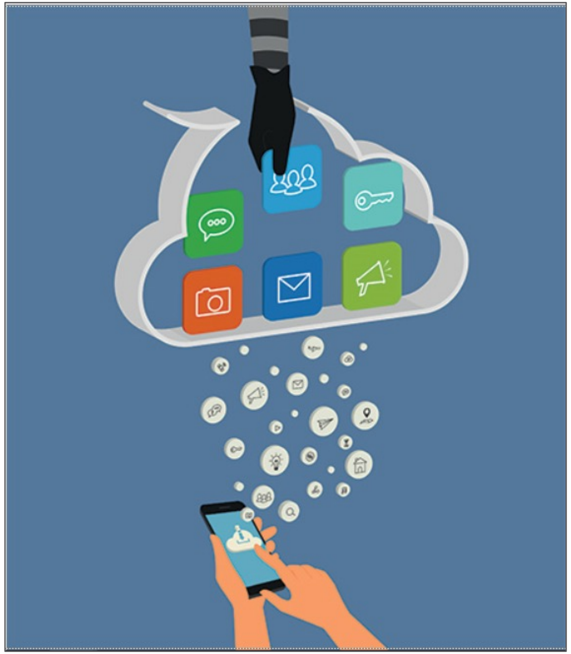
How Secure is the Internet of Things?

- 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 Impact

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.



Threat Impact

Lost Competitive Advantage

- 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.

Threat Impact

Politics and National Security

- It is not just businesses that get hacked.
- State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation.
- The internet has become essential as a medium for commercial and financial activities. Disruption of these activities can devastate a nation’s economy.

In February 2016, a hacker published the personal information of 20,000 U.S. Federal Bureau of Investigation (FBI) employees and 9,000 U.S. Department of Homeland Security (DHS) employees. The hacker was apparently politically motivated.

Threat Impact

Politics and National Security

- It is not just businesses that get hacked.
- State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation.
- The internet has become essential as a medium for commercial and financial activities. Disruption of these activities can devastate a nation’s economy.

The Stuxnet worm was specifically designed to impede Iran’s progress in enriching uranium that could be used in a nuclear weapon. Stuxnet is a prime example of a network attack motivated by national security concerns. Cyberwarfare is a serious possibility.

Threat Impact

Politics and National Security

- It is not just businesses that get hacked.
- State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation.
- The internet has become essential as a medium for commercial and financial activities. Disruption of these activities can devastate a nation’s economy.

Controllers, similar to those attacked by Stuxnet, also are used to control the flow of water at dams and the switching of electricity on the power grid. Attacks on such controllers can have dire consequences.

Cybersecurity and the Security Operations Center

New Terms and Commands

- Evil twin hotspots
- Programmable Logic Controllers (PLCs)
- Threat Actors
- Hacktivists
- Cyberattacks
- Distributed Denial of Service (DDoS)
- Internet of Things (IoT)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Electronic Medical Records (EMRs)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR
- Personal security information (PSI)
- Cyberwarfare

Cybersecurity and the Security Operations Center

Lab 1 - Installing the Virtual Machines

In this lab, you will complete the following objectives:

- Install VirtualBox on your personal computer.
- Install the CyberOps Workstation Virtual Machine (VM).