Operational Cybersecurity 1A: Introduction

Even when we use the strongest bricks, Firewalls can be breached and other security measures can be exploited by malicious cyberattackers. In Operational Cybersecurity 1a: Introduction, you will assume your role as Chief Information Security Officer (CICO) responsible for a data network's design, maintenance, and end-user training. You will explore essentials of keeping networks safe and secure through the use of cryptology, keys, and certificates before moving into the important practice of risk assessment. In the end, your attention will shift to mitigating and managing identified risks and working with key stakeholders to improve the organization's security posture and disaster response. Are you ready to help businesses protect personal information and outsmart cyber attackers? Grab your white hat, BYOD, and let's get started!

Companion courses listed at the bottom.

Unit 1: Advanced Networking Concepts

In all likelihood, the device you are using at this very moment is connecting you to the internet over a wireless connection. Perhaps you are at home, in an office building, in a coffee shop, or at an airport. Is the wireless network you are connected to secure? Do you know if anyone is capturing your data? Have you entered a username or password into any webpages? The reality is that most personal and professional computing devices in use today connect to wireless networks. But how do we begin to analyze risks and then secure and protect our wireless networks against those risks? This unit will introduce you to the OPSEC framework and how it is applied to protect users, data, and the wireless networks we all use.

What will you learn in this unit?

1. Define OPSEC and its five components
2. Understand wireless security design
3. Describe how NAT assists with network security
4. Explain the use of network analysis tools
5. Identify a variety of VPN configurations and how to implement them

Unit 2: Virtual Local Area Networks

We've already seen the critical role played by the physical data network in providing access to data for organizations, employees, and customers. In this unit, we dive a little deeper to see how a specific network configuration tool allows CISOs and network administrators to separate network systems from their data. Once the team has used the OPSEC framework, identified what systems are on the network, and determined how they should be allowed to communicate, the team can employ virtual local area networks (VLANs) as part of a layered defense. To bring these concepts to life, we will go through a case analysis of an attack waged on the 25th largest school district in the United States.

What will you learn in this unit?

1. Define what a VLAN is and how it can be used
2. Explain the security benefits of VLANs
3. Understand the use of specialized VLANs
4. Apply best practices to network configuration

Unit 3: Cryptology, Keys, and Certificates

Encryption is one of the most effective tools available to secure both the files on our systems and the packets that flow across data networks. Encryption is the tool that facilitates the use of digital keys and certificates that are applied to servers and network protocols. You interact with all of these in your everyday use of digital devices while browsing the internet but very likely never realized they were being utilized in the background. For a CISO, this is a best-case scenario. The end user's equipment and their data are secure, and little or no effort is required on their part. In this unit, we will explore how these technologies work and how to deploy them in a production network. Then, we will look at how encryption technologies power and account for new forms of digital currency.

What will you learn in this unit?

1. Define cryptography, cryptology, and encryption
2. Understand public key infrastructure
3. Discuss the use and management of certificates
4. Explain cryptocurrencies and blockchain

Unit 4: Assessing Risk

Every day, we make choices in our lives, and naturally, some of these are riskier than others. In this unit, we will be taking a fresh look at risk through a new lens. To start, consider that each business that utilizes technology invites an element of risk into its environment. This is because risks aren't just about hackers; they include factors such as hardware reliability and the policies that determine how technology should and should not be used in the workplace. When analyzed through a formal risk assessment, these factors provide management teams with actionable information on how to make decisions. The results reveal to companies what their risks are and how they can best invest their time and resources to avoid those risks.

What will you learn in this unit?

1. Explain the risk assessment formula
2. Distinguish between quantitative and qualitative risk analysis
3. Demonstrate an understanding of the process of technical analysis
4. Identify and employ network risk assessment tools
5. Summarize policies developed for operational controls and risk

Unit 5: Risk Mitigation and Management

Once the process for a security risk assessment concludes, you will enter the risk mitigation phase. Learning how to mitigate and manage identified risks in the organization is an important part of the CISO's role. This task incorporates a wide array of skills that are needed to understand the variety of technology platforms involved and the risks associated with each of them. In addition to supporting both legacy and current technologies, the CISO must keep an eye on emerging technologies. The reality is that users begin to operate new devices in the office before a strategy has been developed to manage them safely. The other harsh reality is that, even with exceptional planning implemented to manage risk, there is the constant threat that an attacker will find a way into the network. When it happens, you must be ready!

What will you learn in this unit?

1. Explain change management
2. Mitigate technical risks
3. Understand business continuity planning
4. Summarize how hardware risks are mitigated

5. Describe the process of managing an active attack

Unit 6: Assessing and Mitigating Network Attacks

Networks are the objects of constant reconnaissance performed by actors looking for vulnerabilities to exploit. Sometimes, these actors are the good guys looking for a way in so that holes in the network can be patched, but at other times, they are bad guys finding a way into the network before those holes are secured. In either case, the methods employed to gain access to a network are the same. In this unit, we'll take a deep dive into the technical mitigations that should be considered to minimize these types of network attacks. From physically locking the network closet door to writing the proper firewall rule, there is much to consider when trying to secure a network. This unit will require you to explore the technical part of your CISO brain.

What will you learn in this unit?

1. Describe the impact of low-level network attacks
2. Identify network protocol attacks and mitigation techniques
3. Summarize the roles that routers play in security planning
4. Assess how different types of firewalls protect networks
5. Explain how to protect network clients from being attacked

Unit 7: Social Engineering, Email, and File Attacks

The world is an increasingly complicated place. Communications have moved almost completely to digital platforms, and coworkers can now collaborate via phone, video, and email, virtually removing the need to meet in person at all. However, email has an inherent fault: There is an implied trust that what people read on a screen was created by the sender identified in the "From" field. Likewise, we trust that what a "friend" sends us on social media is a genuine message. This is important because, today, digital platforms such as these form a trusted part of our lives. But what happens when threat actors exploit that trust and use these platforms to launch campaigns to gather information about your company's employees as well as your personal life? It's time to explore that question by covering the techniques that cybercriminals use and the ways you must continue to build layered defenses to protect information.

What will you learn in this unit?

1. Differentiate between types of social engineering techniques
2. Describe measures employed to counter social engineering attacks
3. Explain how to harden SMTP servers from attack
4. Understand vulnerabilities presented by legacy file-sharing services
5. Evaluate a social engineering case study

Unit 8: Assessing and Mitigating Malware Attacks

Even though malware has been around since the 1970s, we still frequently hear about malicious software attacks being launched against major organizations. It seems logical enough to think of this as a problem that should have been solved by now, so why hasn't it been? As you progress through this unit, you will discover why malware attacks continue to occur and what next-generation attacks will look like. Along this journey, we will explore how to detect that a system has been infected and investigate the possible recovery strategies. As you now know, even when the OPSEC framework is followed at every step, every connected device represents a potential malware infection.

What will you learn in this unit?

1. Identify common malware attack types
2. Evaluate the severity of different malware attacks
3. Explain how to identify indicators of compromise
4. Cite evidence of next-generation malware attacks
5. Summarize the use of secure application development techniques
6. Understand the Cobalt Kitty malware attack

Companion courses:

Cybersecurity

National Security

Principles of Information Technology

Coding