Operational Cybersecurity 1b: Security and Planning in the Workplace

More and more, companies are under attack by malicious cyber attackers compromising the security of sensitive employee, customer, and societal data. In this course, you will dive into data security in the workplace and will learn ways to mitigate cyber threats that lurk in dark corners. You will step into the familiar shoes of CISO, this time at a startup company, making decisions about access and authentication protocols, security planning, and expanding the business in a safe way. Lastly, you will explore real-world security breaches, how they were solved, and step-by-step instructions to setup robust security policies. Let's continue forging your cybersecurity stronghold against cyber attackers and keep sensitive data secure.

Companion courses listed at the end.

Unit 1: Access Control in a Corporate Context

Threat actors are always looking for ways into corporate networks and systems. Whether these are nation-states, former employees, or disgruntled workers, when they do gain access and bypass the perimeter controls, what is left to stop them? Internal security policies and access controls are the next layers of defense they will encounter. Let's dive into how access controls can be applied at the level of the operating system, individual, or even group. We'll learn how these elements must be well-planned and constantly monitored to ensure that they protect the organization—and ultimately avoid risks from turning into news stories about the latest data breach.

What will you learn in this unit?

1. Explain the components that allow a user to be authorized on a network
2. Understand access control models and their uses
3. Recommend policies to protect against third-party vulnerabilities
4. Discuss the 2019 Capital One data breach

Unit 2: Authentication at Work

Who are you? Prove it! Verifying who you are to a system requires a process known as authentication. Every day, our devices ask us to identify ourselves and prove who we are to access our accounts. Most systems now require something more than just a simple username and password to gain access. Have you ever considered how the system knows who you are (and whether it would even be possible to impersonate someone else)? Let's explore the way devices establish our identity—the authentication process—and some of the newer technologies and protocols that are available to secure our networks and digital assets.

What will you learn in this unit?

1. Explain authentication factors
2. Understand how biometrics are used as authentication factors
3. Identify protocols used in network-level authentication
4. Consider the use of single sign-on (SSO) and the implementation of authentication on switches and routers
5. Think about a perfect protocol scenario

Unit 3: Scenarios: Testing and Troubleshooting

Even if we have some strong cybersecurity measures set up, we can't leave anything to chance. It is important that we continue to monitor and test our defenses. We don't want an active cyberattack to be the first time we realize that our defenses won't hold because, by then, it'll be too late! This means it's time to learn how to conduct vulnerability and penetration tests and how to remediate any issues that we may discover in the course of that testing. This type of testing requires a unique skill set and a dedication to personal integrity. What does integrity have to do with it? It is the only thing that separates a black-hat hacker from an ethical penetration tester. Let’s find out why.

What will you learn in this unit?

1. Explain the need for continuous monitoring
2. Understand the basics of digital forensics
3. Describe the vulnerability scan process
4. Consider the penetration testing process
5. Plan possible post-scan actions

Unit 4: Response and Recovery Planning

“Are you ready?” Think about how many times you have been asked that question. Your response may have been “Ready for what?” Incident response and recovery planning is a large part of operational security. Will we be ready when an attack against our organization is thrown our way? It is not a matter of if, but when, a security incident will impact your organization. So, let’s explore the existing frameworks and best practices to ensure that we aren’t the lead story on the six o’clock news for not being able to recover from a cyberattack!

What will you learn in this unit?

1. Identify the difference between incident response and disaster recovery plans
2. Understand the NIST 800-61 incident response framework
3. Identify the steps in the Cyber Kill Chain®, MITRE ATT&CK, and Diamond model frameworks
4. Respond to a mock security incident
5. Conduct a post-incident analysis

Unit 5: Security Awareness and Training

Don’t talk to strangers, remember your parents’ phone number, don’t touch the stove when it’s hot—all of these are safety awareness tips that your parents, guardians, or teachers may have shared with you when you were growing up. You could probably come up with many more pieces of life advice that you have been given—maybe some more useful than others. The CISO has a responsibility to train every employee to be cyber aware to keep their own personal information and the data the company stores safe. Security awareness training programs are important for explaining in layman’s terms what the responsibilities are for security teams and general users.

What will you learn in this unit?

1. Identify security awareness training frameworks
2. Explain various data classification categories
3. List examples of good workplace security habits
4. Consider positive security habits for sysadmins
5. Understand hands-on learning opportunities in cybersecurity

Unit 6: Ethical Concerns in Cybersecurity

Do we all do the right thing, even when no one is looking? In cybersecurity, we know this isn’t always the case and that threat actors intentionally exploit vulnerabilities they find. We, however, can act ethically as we execute our operational security planning. There are several laws and regulations that have been put into practice all over the world to encourage or even force organizations and individuals to act in a responsible and ethical manner. Let’s explore some of the major regulations and how they help form organizational policies.

What will you learn in this unit?

1. Identify different types of computer crimes and their consequences
2. Explain different types of copyright issues in the digital era
3. Understand how to handle data ethically
4. Consider data laws that are in place in the United States
5. Describe best practices concerning ethical behavior on networks and in personal digital activities

Unit 7: Personal Device Security

Do you have a favorite computing device or maybe an operating system that you are more productive with? On the other hand, have you ever been required to use a computing device that you just didn’t like? This is a common occurrence in the business world, and many employees would rather use their own devices than whatever they are assigned on the job. Enter the bring your own device (BYOD) model of computing! But hold on—while this sounds like a fantastic opportunity to improve employee satisfaction, it can be a massive security hurdle for CISOs. That’s why we need to explore how personal devices can be safely integrated into a corporate network.

What will you learn in this unit?

1. Define different device ownership models
2. Identify various security concerns related to employees bringing personal devices to work
3. Explain the purpose of mobile device management (MDM) platforms
4. List various MDM polices that can be enforced
5. Understand how Cisco Systems selected a new MDM

Unit 8: Gliders Expands

Gliders, Inc., is growing—fast! The company has just acquired its largest competitor, and you have been tasked with combining the technical resources of both companies in the most cost-effective and secure way possible so that this new company will become a seamless part of Gliders. Expansion is always exciting (and stressful) for organizations, and in our digital age, one of the first things companies evaluate when they merge is whether migrating data, processing, and storage to the cloud makes sense. Let’s analyze the benefits and risks that cloud services may bring to the new and expanded Gliders, Inc.

What will you learn in this unit?

1. Define the cloud and discuss why an organization may use these types of platforms
2. Identify different cloud platform security controls
3. Consider cloud application security controls
4. Understand cloud security misconfigurations

Companion courses

Cybersecurity
National Security
Network Security Fundamentals

Principles of Information Technology