Role-Based Course Descriptions

The goal of Optiv's role-based awareness training is to educate employees on security-aware behaviors specific to their role. Depending on the nature of the company, all employees may have a specialized role and would benefit from applicable training. Courses align with common compliance-related training obligations and/or security concerns related to specific responsibilities or positions within organizations.

Role-Based Courses

Business Stakeholders

AI Security for Business Stakeholders

10-15 minutes	Business Stakeholders
While artificial intelligence (AI) can yield significant benefits for an enterprise, it can also pose a number of unforeseen challenges and even security risks for those that aren't fully prepared to adopt it. This course outlines key considerations for business stakeholders surrounding the secure adoption and integration of AI technology.	• Identify the characteristics and best practices of a secure, AI-enabled organization • Describe the various steps to becoming a secure, AI-enabled organization • Understand key concepts and topics concerning AI security for enterprises

Cybersecurity Foundations for Businesses

10-15 minutes	Business Stakeholders
Cybersecurity touches every part of the business ecosystem. A basic understanding of cybersecurity concepts and terms can help bridge the gap between business stakeholders and the technical teams carrying out cybersecurity strategies and initiatives.	• Define common cybersecurity terms and the CIA Triad • Identify common cyber threats • Outline the people and components involved in organizational cybersecurity

Cybersecurity Implications for Businesses

15 minutes	Business Stakeholders
Individuals in non-cybersecurity roles are often tasked with making decisions about their organization's cyber strategy that directly affect the organization's security posture. This course helps stakeholders understand the implications and impacts of the cybersecurity decisions they make.	• List five types of implications businesses should consider • Summarize three non-financial implications of cybersecurity • Describe how security culture impacts security posture

Cybersecurity Incident Management and Preparedness

10 minutes	Business Stakeholders
A cybersecurity incident can be costly, but organizations can minimize the impact by preparing resources, plans, and procedures in advance. This course defines incident management, introduces roles involved, and provides best practices for assembling incident management teams.	• Explain goals and purposes of incident management • Identify types of incident response teams and roles within them • Outline what should be included in an organization's policies

Third-Party Risk Management Basics

15 minutes	Executives, Risk Managers, Finance, Supply Chain and Logistics, Systems Administrators, IT Staff
Risks introduced by business relationships with vendors can be just as damaging and costly as internal risks. This course describes a framework for recognizing, prioritizing, and reducing risks introduced by third parties.	• Define third-party risk management and its lifecycle • Summarize the third-party risk management framework • Identify methods for classifying and tiering third-party risks

Cloud Infrastructure Security

Commonly Used Cloud Services and Risks

10-15 minutes	Cloud Administrators, IT Staff, Security Staff, Developers
Services in the cloud can enhance security, user experience, and performance. Unfortunately, they can also introduce threats to the environment. This course examines common services, related risks, and best practices for their use.	• Identify the six categories of common cloud services • Paraphrase risks introduced by cloud services • Describe best practices to mitigate services-related risks

Compliance, Regulatory, and Data Handling

Data Privacy and Protection Regulations

10-15 minutes	All Employees and Contractors
As organizations are subject to more data privacy and protection laws, it's imperative that all employees, regardless of their role in compliance, have a basic understanding of regulations and their obligations.	• Explain why your organization requires this training • Identify common components of data privacy laws • Provide examples of how organizations typically comply with regulations

HIPAA Privacy and Security Basics

15 minutes	All employees and contractors of organizations required to comply with HIPAA
The Health Insurance Portability and Accountability Act requires businesses handling Electronic Patient Health Information to take steps to keep this data secure. This introductory course, presented in a framework of cybersecurity, is intended for general end users.	• Define protected health information • Recognize entities covered by HIPAA • Identify key HIPAA requirements

Protecting Privacy in Customer Service Roles

10 minutes	All employees and contractors in customer-facing roles
Individuals in customer service roles often collect or have access to a vast amount of customer information. This access can make these employees a prime target for information theft. This course outlines risks and best practices for protecting customer information.	• Paraphrase why customer service roles are targets for information theft • Analyze methods used to obtain customer information fraudulently • Restate best practices to protect customer information

IT and Security

Security Awareness for Users with Privileged Access

15 minutes	Users with Privileged Access
Not all users within an organization have the same level of access to resources and systems. Those with elevated access are known as users with privileged access. This elevated access also involves elevated risk. This course explores these risks and methods to reduce, mitigate, and remediate them.	• Summarize why privileged access involves additional risk • Paraphrase strategies for managing vulnerabilities that place sensitive data at risk • Identify security measures that prevent data breaches stemming from misconfigured privileges

Operational Technology

Introduction to Operational Technology

15 minutes	IT Staff, Security Staff
Operational technology (OT) allows organizations to monitor, control, and manage manufacturing equipment, industrial processes, and critical infrastructure. But what is OT? This course provides an overview of common OT terminology, use cases, and industries where OT is found.	• Differentiate between operational technology and information technology • Identify industries that frequently use OT systems • List common devices and components present in OT systems

Understanding Security in Operational Technology

15 minutes	Executives, Systems Administrators, IT Staff, Security Staff
Operational technology (OT) can optimize industrial processes. But the highly specialized and physical nature of OT systems introduces risk and makes them difficult to protect. This course reviews challenges and best practices related to securing OT systems.	• Identify threat actors that commonly target OT systems • Paraphrase characteristics that contribute to increased risk in OT systems • Describe strategies organizations can adopt to protect OT systems

Payment Card Industry

Introduction to the Payment Card Industry

10-15 minutes	End users in organizations that are subject to PCI compliance
This course guides employees through the complicated world of the Payment Card Industry with a wide, yet focused range of knowledge from identity theft and fraud to types of cardholder data and basic security guidelines.	• Identify cardholder data that can be stored • Summarize six control objectives of the PCI Data Security Standard • Order the flow of cardholder data in a transaction

Your Role in PCI: Payment Card Handling

10-15 minutes	Payment Card Handlers
Individuals and organizations that handle and process payment card transactions must do so securely. By understanding the personally identifiable information associated with payment cards and how to secure it, these entities can perform safer transactions. This course helps every type of entity better understand their obligations with respect to payment card security.	• Describe different types of personally identifiable information • Identify the security features present on modern payment cards • Compare and contrast handling requirements for contact and contactless payment cards

OWASP Courses

OWASP API Top 10

10 minutes	Developers
Application programming interfaces (APIs) are an increasingly common way to connect systems, applications, and services. This course highlights common API security mistakes and recommends secure coding practices. A general understanding of coding practices and APIs is strongly recommended.	• Explain the 10 most prevalent API vulnerabilities • Understand the risks of unsecure APIs • Detect and mitigate API vulnerabilities

OWASP IoT Top 10

10 minutes	Developers, Systems Administrators, IT Staff, Users with Privileged Access
The adoption of Internet of Things (IoT) technology is a trend that continues to grow. This course highlights common IoT security issues to help organizations understand IoT vulnerabilities and secure IoT technologies.	• Identify common vulnerabilities associated with IoT • Explain the root cause of common IoT vulnerabilities • Describe techniques for preventing common IoT vulnerabilities

OWASP Mobile Top 10

10-15 minutes	Developers of Mobile Applications
In today's increasingly mobile environment, there is a drive for developers to quickly and efficiently create mobile applications for a variety of devices while following security best practices for the next generation of mobile applications. This course covers 10 important security topics that apply regardless of development platform or programming language.	• List OWASP's top 10 mobile application security risks • Summarize threats presented by each risk type • Recall strategies that protect against risks identified in the course

OWASP Proactive Controls

15 minutes	Developers
OWASP Top 10 Proactive Controls describe the 10 most critical security concerns for software developers. Complementing the risk mitigation focus of OWASP Web/Mobile Top 10, these controls contribute to an informed foundation for a secure development process.	• Identify the 10 most critical security concerns for software developers • Connect OWASP risk categories with proactive development strategies that protect applications

OWASP Top 10 Privacy Risks

10-15 minutes	Developers, Web Application Administrators, Roles overseeing application development
Privacy issues are near the forefront of risks associated with web applications. This course highlights privacy risks identified by OWASP from a technological and organizational perspective to help learners understand, improve, and address privacy in web applications.	• Identify and define each of the OWASP Top 10 Privacy Risks • Describe examples of and options for assessing and addressing potential privacy risks in web applications

OWASP Web Top 10

60 minutes (11-part program)	Developers

OWASP, the Open Web Application Security Project, regularly lists the 10 most frequent and dangerous security vulnerabilities and attacks being used on the internet. This program covers the attacks on OWASP's 2021 list, exploring examples, remediation, and best practices to incorporate into development and coding work.

Introduction to OWASP

The developer's role in securing applications is critical in today's vulnerable web environment, but trusted resources are available to guide secure development. This course introduces learners to the Open Web Application Security Project (OWASP), its resources, and the structure of the OWASP Web Top 10 2021 list.

- Describe the purpose of OWASP and its top 10 lists
- Summarize the structure of the OWASP Web Top 10 2021 list

OWASP Web Top 10: Broken Access Control #1

Broken access controls fail to govern what users are permitted to do or access in an application. This course examines how these flaws are exploited and provides best practices for configuring and strengthening the access controls used within applications.

- Identify common flaws that may permit unauthorized access to applications
- Paraphrase policies and configurations that can strengthen access controls

OWASP Web Top 10: Cryptographic Failures #2

Weak or non-existent cryptography (encryption) within many web applications can expose sensitive data. This course describes known weak cryptographic practices and protocols and explores strategies for protecting the data stored, transferred, and processed by applications.

- List known weak or outdated cryptography protocols
- Describe practices and configurations that protect sensitive data

OWASP Web Top 10: Injection #3

Injection occurs when untrusted input is not properly sanitized by the application. This course illustrates how injected data compromises applications and reviews how safe APIs, input validation, sanitization, escaping, and SQL controls can prevent attacks.

- Outline how injection attacks occur
- Identify methods to prevent successful injection attacks

OWASP Web Top 10: Insecure Design #4

Insecure design encompasses any weakness in an application caused by ineffective security control design processes. This course examines how undefined requirements, ineffective refinement strategies, poor change management, and insecure development lifecycles affect the security of applications.

- Summarize common characteristics of insecure design
- Recognize effective processes for security control design

OWASP Web Top 10: Security Misconfiguration #5

Security misconfigurations are pervasive and frequently allow attackers unauthorized access to systems and data. This course defines the most common security misconfigurations affecting web applications and describes strategies development teams can implement to confirm secure configurations are in place.

- Provide examples of how security misconfiguration can occur
- Identify best practices to verify and validate secure configurations

OWASP Web Top 10: Vulnerable and Outdated Components #6

Attackers can easily locate and exploit vulnerable components in applications, with threats ranging from minor damage to full server takeover. This course covers potential areas of vulnerability and offers best practices for sourcing, configuring, and documenting components securely.

- Describe how inventory and tracking can uncover vulnerable components
- Compare and contrast component sources as safe and unsafe

OWASP Web Top 10: Identification and Authorization Failures #7

Weak authentication and session management can be leveraged to expose passwords, keys, or session tokens to exploit user identities. This course explores these flaws and suggests prevention techniques such as strong credential requirements, multi-factor authentication, and appropriate session management.

- Summarize scenarios that can permit identification and authorization failures
- Identify policies and security controls that can limit user-created failures

OWASP Web Top 10: Software and Data Integrity Failures #8

When the integrity of software and data within an application is not verified, malicious content may be unknowingly added. This course reveals strategies to protect against flaws introduced by untrusted sources, insecure CI/CD pipelines, and insecure deserialization.

- Explain how inappropriate software sourcing can introduce vulnerabilities
- Paraphrase the role of secure CI/CD pipelines for integrity verification

OWASP Web Top 10: Security Logging and Monitoring Failures #9

Applications that do not actively detect unusual events or patterns can allow vulnerabilities and attacks to remain undiscovered. This course examines the reactive role of logging and monitoring in secure applications and describes best practices for using logs to respond rapidly to security events.

- Contrast the reactive role of logging and monitoring with proactive controls
- Describe how log context and format can affect the ability to detect events

OWASP Web Top 10: Server-Side Request Forgery #10

Server-side request forgery (SSRF) is an attack that uses the application's server as a proxy to bypass security controls. This course outlines how SSRF attacks occur and describes network and application layer security controls to prevent successful attacks.

- Summarize the steps involved in an SSRF attack
- Identify security controls at the network and application layer to prevent SSRF

Web 3.0 Secure Coding

60 minutes (Five 10-15 minute courses)

Developers

Web 3.0 is the next evolutionary phase of the internet with a shift from the centralized platforms of Web 2.0 to decentralized networks, blockchain technology, artificial intelligence, and semantic web principles. This program compares the benefits of user-centricity, privacy, and interoperability in Web 3.0 with the evolving challenges of securing the "decentralized web."

Introduction to Web 3.0

This course guides learners through the foundational elements of Web 3.0, helping them understand how it differs from its predecessors, its core technologies, and its potential to reshape our digital world.

- Explain how Web 3.0 differs from Web 1.0 and 2.0
- Identify the core principles of Web 3.0
- Summarize Web 3.0's impact on data ownership, privacy, and internet applications

Web 3.0 - Open Standards and Protocols

Explore the pivotal role of open standards and protocols in shaping the decentralized web. This course delves into how these principles foster innovation, inclusivity, and user empowerment, paving the way for a more accessible and democratic internet.

- Define open standards and protocols in Web 3.0
- Describe key protocols driving the decentralized web
- Analyze challenges and best practices of open standards and protocols

Web 3.0 - Understanding Decentralization

This course explores the transformative concept of decentralization, its foundational elements, real-world applications, challenges, and cybersecurity best practices within the Web 3.0 ecosystem.

- Identify key elements enabling decentralization
- Analyze applications and impacts of decentralization
- Describe cybersecurity challenges and best practices for implementing decentralized systems

User-Centricity in Web 3.0

In this course, learners will discover how placing users at the center of Web 3.0 not only enhances their experience but also contributes to a more secure, open, and democratic internet.

- Explain the concept of user-centricity and key elements that contribute to user-centricity
- Identify cybersecurity challeneges and best practices for designing secure, user-centric web services

Interoperability, Connectivity, and Ubiquity in Web 3.0

This course aims to equip users with an understanding of foundational principles, challenges, and best practices for navigating the cybersecurity landscape in the era of decentralized web technologies.

- Describe the role and importance of interoperability, connectivity, and ubiquity in Web 3.0
- Identify key cybersecurity challenges and best practices to enhance security in Web 3.0 applications