

Managing Security Vulnerabilities; Enterprise and Cloud

Course Summary

Description

This course will show you the most effective ways to mature your vulnerability management program and move from identifying vulnerabilities to successfully treating them. You will learn how to move past the hype to successfully prioritize the vulnerabilities that are not blocked, then clearly and effectively communicate the risk associated with the rest of the vulnerabilities in your backlog that, for a variety of reasons, cannot currently be remediated. You'll also learn what mature organizations are doing to ease the burden associated with vulnerability management across both infrastructure and applications as well as across both their cloud and non-cloud environments.

Objectives

At the end of this course, students will be able to:

- Create, implement, and mature your vulnerability management program
- Establish secure and defensible enterprise and cloud computing environments
- Build an accurate and useful inventory of IT assets in the enterprise and the cloud
- Identify existing vulnerabilities and understand how to meaningfully use this information
- Better analyze the output of VM tools and related technology to make the data more actionable
- Prioritize vulnerabilities for treatment based on a variety of techniques
- Effectively report and communicate vulnerability data within your organization
- Understand treatment capabilities and better engage with treatment teams
- Make vulnerability management more fun and engaging for all those involved

Topics

- Overview
- Identify
- Analyze and Communicate
- Treat
- Buy-in, Program, and Maturity

Audience

This course is designed for:

- CISOs
- Information security managers, officers, and directors
- Information security architects, analysts, and consultants
- Aspiring information security leaders
- Risk management professionals
- Business continuity and disaster recovery planners and staff
- IT managers and auditors
- IT project managers
- IT/system administration/network administration professionals
- Operations managers
- Cloud service managers and administrators
- Cloud service security and risk managers
- Cloud service integrators, developers, and brokers
- IT security professionals managing vulnerabilities in the enterprise or cloud
- Government IT professionals who manage vulnerabilities in the enterprise or cloud (FedRAMP)
- Security or IT professionals who have team-lead or management responsibilities
- Security or IT professionals who use or are planning to use cloud services

Prerequisites

A basic understanding of risk management objectives and IT systems and operations is recommended for this course.

Duration

Five days

Managing Security Vulnerabilities; Enterprise and Cloud

Course Outline

I. SECTION 1: Overview:

Cloud and Asset Management In this section we look at why vulnerability management is important and introduce the course. We then provide an overview of the cloud and how different cloud service types and architectures can impact the way we manage vulnerabilities. We'll also look at how to choose technologies and tools for our cloud environments. Finally, we'll dig into why asset management is so important and foundational for effective vulnerability management, and the different ways that gaining additional context can help us succeed.

TOPICS: Course Overview; Cloud and Cloud Vulnerability Management; Asset Management

II. SECTION 2: Identify

Identifying vulnerabilities continues to be a major focus for our security programs, as it can provide insight into the current risks to our organization. It also provides the data for our analysis and for the measures and metrics we use to guide the program and track our maturity. In this section, we will look at common identification pitfalls and discuss identification architecture and design across both infrastructure and applications. We'll also look at where we might require permission to perform identification and how we safely grant permission to third parties to test our systems and applications and responsibly disclose any

III. SECTION 3: Analyze and Communicate Gone are the days when we can just scan for vulnerabilities and send the raw output to our teams for remediation. We need to help reduce the burden by analyzing the output to reduce inaccuracies and identify root-cause issues that may be preventing remediation. Once we have identified the issues that cannot be resolved, we should prioritize the rest to ensure that we are having the greatest impact and provide targeted reports or dashboards to system and platform owners. In this section, we will look at some common inaccuracies in the output of our identification processes, discuss prioritization, and then look at what metrics are commonly used to measure our program and the related operational capabilities. We will also discuss how to generate meaningful reports, communication strategies, and the different types of meetings that should be held to increase collaboration and participation. TOPICS: Analyze; Communicate

IV. SECTION 4: Treat

Treating vulnerabilities and reducing risk is the ultimate goal of all that we do in vulnerability management. It is important for program managers and all participants to understand the typical processes and technologies that exist and how to leverage them to increase positive change within the organization. Most organizations will have some type of change, patch, and configuration management program. In this course section, we will look at how we interface with these processes to streamline change and increase consistency. We'll also examine some unique challenges we face in the cloud, how to better deal with application vulnerabilities, and some alternatives we can look to when traditional treatment methods are not available.

TOPICS: Treatment of Vulnerabilities

V. SECTION 5: Buy-in, Program, and Maturity

Vulnerability management is not the easiest job in an organization, and there are many challenges that can hold us back. From split responsibility and accountability to reliance on shared personnel, much of the work done in this space goes unrecognized. In this section, we'll summarize much of what we have learned and discussed throughout the course and look at how we can use this information to improve the program. We'll discuss how we can make VM more fun and successful within the organization, how we can identify and collaborate more effectively with various stakeholders, and how we can build out and mature a robust vulnerability management program.

TOPICS: Buy-In, Program; Maturity