MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Create, implement, or improve your vulnerability management program
- Establish a secure and defensible enterprise and cloud computing environment
- Build an accurate and useful inventory of IT assets in the enterprise and cloud
- Identify existing vulnerabilities and understand the severity level of each
- Prioritize vulnerabilities for treatment
- Effectively report and communicate vulnerability data within your organization
- Engage treatment teams and make vulnerability management fun

The course is based on the PIACT Model:

- **Prepare:** Define, build, and continuously improve the program
- **Identify:** Identify vulnerabilities present in our operating environments
- **Analyze:** Analyze and prioritize identified vulnerabilities and other program metrics to provide meaningful assistance and guidance to stakeholders and program participants
- **Communicate:** Present the findings from analysis appropriately and efficiently for each stakeholder group
- **Treat:** Implement, test, and monitor solutions to vulnerabilities, vulnerability groups, and broader issues identified by the program

Vulnerabilities are everywhere. There are new reports of weaknesses within our systems and software every time we turn around. Directly related to this is an increase in the quantity and severity of successful attacks against these weaknesses.

Managing vulnerabilities in any size organization is challenging. Enterprise environments add scale and diversity that overwhelm many IT security and operations organizations. Add in the cloud and the increasing speed with which all organizations must deliver systems, applications, and features to both their internal and external customers, and security may seem unachievable.

This course highlights why many organizations are still struggling with vulnerability management today and shows students how to solve these challenges. How do we manage assets successfully and analyze and prioritize vulnerabilities? What reports are most effective? How do we deal with vulnerabilities in our applications, and how do we treat them? We'll examine how the answers to these questions change as we move to the cloud or implement a private cloud or DevOps within our organizations. How do we make vulnerability management fun and get everyone to engage in the process? These are just some of the important topics we will cover in this course.

The primary goal of this course is to help you succeed where many are failing and to present solutions to the problems many are experiencing or will experience. Whether your vulnerability management program is well established or just starting, this course will help you mature your program and think differently about vulnerability management.

By understanding common issues and the solutions to them, you will be better prepared to meet the challenges you are facing or will face, and to determine what works best for your organization. Through class discussions and other exercises, you will learn specific analysis and reporting techniques so that you will be able to discuss the problems you and your peers are facing and how to solve those problems.

Knowing that our environments are adopting cloud services and becoming more tightly integrated with them, we'll look at both cloud and non-cloud environments simultaneously throughout the course, highlighting the tools, processes, and procedures that can be leveraged in each environment and presenting new and emerging trends.

A capstone exercise on the final course day of MGT516 features a business scenario that includes both enterprise and cloud-based environments. The exercise allows students to analyze and discuss how best to implement and maintain a vulnerability management program and leverage some of the information they have learned throughout the course. The group solutions are then reviewed in class so participants can learn what others outside their group have determined would best help the organization in the scenario succeed.

"Great course, great content. MGT516 is essential for both well-established and developing vulnerability management teams."

— KRobert Adams, **CBC**

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Section Descriptions

SECTION 1: Overview and Identify

Section 1 begins with a discussion of how to make vulnerability management fun and improve engagement within your organization. Then, we dive into the cloud and discuss how cloud design and architecture can impact vulnerability management. We discuss how to discover and manage assets and what context is critical to the success of the program. Finally, we begin our discussion of how to find or identify vulnerabilities in our environments.

TOPICS: Course Introduction and Overview; Cloud Overview; Cloud Design and Architecture; Asset Management; Finding Vulnerabilities

SECTION 2: Identify and Analyze

Section 2 wraps up our discussion on how to identify vulnerabilities and then moves into how to deal with all of the results. We will go over a variety of analysis and prioritization techniques that can be used to more effectively and efficiently deal with the data that are generated during identification.

TOPICS: Finding Vulnerabilities; Analyzing Vulnerabilities; Introduction to Solution Grouping

SECTION 3: Communicate and Treat

Section 3 begins with how to communicate vulnerabilities, including what metrics are common or useful, and how to generate meaningful reports. We'll examine communication strategies and the different types of meetings that can facilitate communication and program participation. Then, we dive into how to treat vulnerabilities by discussing how change and patch management programs can impact vulnerability management.

TOPICS: Communication; Treatment

SECTION 4: Treatment, Buy-in, and Program

Section 4 discusses the treat phase of the PIACT model. Successful treatment of vulnerabilities should be the primary goal of vulnerability management. Throughout the section we will discuss the common operational processes that are used to treat vulnerabilities. We will also look at some of the technology solutions available to assist with some of these processes, and discuss different and emerging operating models that may impact our treatment methodology.

TOPICS: Treatment; Buy-in; Program

SECTION 5: Managing Vulnerabilities: Capstone Lab Exercise

Section 5 begins with a review of a scenario that triggers the group capstone exercise. The section is broken up into various sections and scenarios that stem from the main case study, which enables students to delve into various aspects of the PIACT model. A review of findings and conclusions will follow each section of the exercise, allowing each team to present its findings to the other teams and to engage in class discussions on the topics covered. The instructor will also present a potential solution for the scenarios discussed.

Who Should Attend

- 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 members
- 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 professional 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

"An understanding of vulnerability management and cloud security is becoming not only valuable but a necessity to keep one's organization secure in this constantly changing and dynamic environment."

— Kae David, **EY**