MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Create, implement, and mature your vulnerability management program and get buy-in from your stakeholders
- Implement techniques for building and maintaining an accurate and useful inventory of IT assets in the enterprise and the cloud
- Identify processes and technologies that are effective across both infrastructure and applications and know how to configure them appropriately
- To be aware of common false positives or false negatives in your identification arsenal
- Prioritize unblocked vulnerabilities for treatment based on a variety of techniques
- Effectively report and communicate vulnerability data within your organization
- Identify and report on the risk associated with vulnerabilities that are blocked and cannot currently be prioritized for remediation
- Have a better understanding of modern treatment capabilities and how to better engage with treatment teams
- Make vulnerability management more fun and engaging for all those involved
- Differentiate how to deal with application layer vulnerabilities versus infrastructure vulnerabilities
- Understand how your strategies and techniques might change as you move to the cloud, implement private cloud, or roll out DevOps within your organization

Business Takeaways:

This course will help your organization:

- Understand what is working and what is not working in modern day vulnerability programs
- Anticipate and plan for the impacts related to cloud operating environments
- Realize why context matters and how to gather, store, maintain, and utilize contextual data effectively
- Effectively and efficiently communicate vulnerability data and its associate risk to key stakeholders
- Determine how to group vulnerabilities meaningfully to identify current obstacles or deficiencies
- Know which metrics will drive greater adoption and change within the organization

Stop Treating Symptoms. Cure the Disease.

Whether your vulnerability management program is well established or you are just getting started, this course will help you think differently about vulnerability management. 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. MGT516 is based on the Prepare, Identify, Analyze, Communicate, and Treat (PIACT) Model.

MGT516 helps you think strategically about vulnerability management in order to mature your organization's program, but it also provides tactical guidance to help you overcome common challenges. By understanding and discussing solutions to typical issues that many organizations face across both traditional and cloud operating environments, you will be better prepared to meet the challenges of today and tomorrow. Knowing that many organizations are adopting cloud services in addition to continuing to manage their more traditional operating environments, we'll also look at different cloud service types throughout the course and how they impact the program both positively and negatively. We will highlight some of the tools and processes that can be leveraged in each of these environments and present new and emerging trends.

Hand-On Training

MGT516 uses the Cyber42 leadership simulation game, critical thinking labs based on outlined scenarios, hands-on labs and demonstrations to provide you with the information you need to skillfully fight the VM battle. Cyber42 helps students absorb and apply the content throughout the course. In this web-based continuous tabletop exercise, students play to improve security culture, manage budget and schedule, and improve specific vulnerability management capabilities at the fictional organization, "The Everything Corporation" or "E Corp." This puts you in real-world scenarios that require you to think through various options for improving the organization's maturity by responding to specific events.

"This course is essential for both well-established and developing vulnerability management teams."

—Robert Adams, **CBC**

"A great course to utilize if new to cloud vulnerability management."

—Amaan Mughal

Section Descriptions

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

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 findings.

TOPICS: Identification

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

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

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

"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**

Who Should Attend

- CISOs
- Vulnerability program managers and analysts managing vulnerabilities in the enterprise or cloud
- Information security managers, architects, analysts, officers, and directors
- Aspiring information security leaders
- Risk management, business continuity and disaster recovery professionals
- IT operations managers and administrators
- Cloud service managers, administrators, integrators, developers, and brokers
- Cloud service security and risk managers
- Government IT professionals who manage vulnerabilities in the enterprise or cloud (FedRAMP, NIST CSF)

NICE Framework Work Roles:

- Program Manager OV-PMA-001
- Information Systems Security Manager OV-MGT-001
- Security Architect SP-ARC-001
- Enterprise Architect SP-ARC-002
- Cyber Workforce Developer and Manager OV-SPP-001
- Cyber Policy & Strategy Planner OV-SPP-002
- IT Project Manager OV-PMA-001
- IT Program Auditor OV-PMA-005
- Executive Cyber Leadership OV-EXL-001
- Information Systems Security Developer SP-SYS-001
- Systems Developer SP-SYS-002
- System Administrator OM-ADM-001
- Database Administrator OM-DTA-001
- Research & Development Specialist SP-TRD-001
- Security Control Assessor: SP-RSK-002
- Security Awareness & Communications Manager: OV-TEA-003