MGT520: Leading Cloud Security Design and Implementation

Building and Leading a Cloud Security Program

Cloud adoption is popular across all types of industry, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions. However, an organization’s cloud transition requires numerous key decisions.

This course focuses on what managers, directors, and security leaders need to know to develop their cloud security roadmap, to manage the implementation of cloud security capabilities, as well as how to operate the cloud environment post-transition. Making the right security decisions when adopting the cloud requires understanding the technology, process, and people related to the cloud environment. This complements traditional IT management techniques that managers are accustomed to and helps with making the appropriate informed decisions. We will cover the key objectives of security controls in the cloud environment, including planning, deploying, and running the environment from the starting point to a progressively more mature state. There will be a focus on locking down the environment, securing the data, maintaining compliance, enhancing security visibility to the operations, and managing the security response on a continuous basis. Students will learn the essentials to lead the security effort for the cloud transition journey.

Business Takeaways

- Establish cloud security program supporting the fast pace business transformation
- Make informed decisions on cloud security program
- Anticipate the security capabilities and guardrails to build for the securing the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Hands-on Training

MGT520 uses case scenarios, group discussions, team-based security leadership simulations with embedded real life technical components to help students absorb both technical and management topics. About 60 minutes per day is dedicated to these learning experiences using the Cyber42 leadership simulation game. This web application based game is a continuous exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

- Section 1: Secure Roadmap Development, Migration Preparation, Security IaaS Environment, IAM Secure Setup
- Section 2: Container Security, Logging and Monitoring, Encryption in Cloud
- Section 3: Application Secrets Management, Security Benchmarking, Security Metrics
Section Descriptions

SECTION 1: Security Program Design and Cloud Security Fundamentals

The first section of the course aims to help management professionals develop a migration roadmap to the cloud environment. The goal of the roadmap is to support the business transformation to realize the benefits from the cloud, while maintaining the security of the environment, applications, and data. We will arm you with information on various approaches to migratory and preparatory steps to get you ready for a secure migration journey.

We will then pivot to cloud environment details to help you understand the security targets and maturity journey for the main types of public cloud service offerings. The material will help you advise and lead the security transformation program with the right amount of technical understanding and knowledge on the best practices in the various types of cloud offerings.

Infrastructure as a Service (IaaS) is a common starting point for organizations venturing into the Cloud. We cover the fundamentals of securing these services and discuss an effective, progressive approach to building up security maturity and protection in the IaaS environment.

We end the section covering a new security perimeter paradigm - the Identity and Access Management. With the modern Cloud architecture, we are losing the firewall and network perimeter as our main battle line. The transition from network centric to identity centric security perimeter requires a fundamentally different culture and mindset to effective management. We cover the key objectives and the common paths to gain security maturity.

TOPICS: Building The Roadmap; Managing The Transition To Cloud; Securing IaaS; Identity Access Management

SECTION 2: Cloud Security Features and Capabilities

The second section is dedicated to managing the security of the Cloud Native and SaaS Cloud workloads. The promise of Cloud Native to speed up development, make the workload more secure and reduce the operational burden can be realized given the proper planning and leadership.

Securing the Platform as a Service (PaaS) workloads and the Software as a Service (SaaS) workloads are the core focus for the rest of the second section. These service models form the modern Cloud Native model. The class covers the key decisions on these Cloud service models that have profound impact on overall security posture. We also offer recommended approaches to progressively improve the security in these Cloud based environments.

The rest of the section is dedicated to the advanced technologies, services, and configurations that make the environment more secure than most in-house IT environments. The scale and technology investments of the cloud providers allow them to provide turn-key security capabilities for their customers that are relatively easy to adopt. We will walk through the opportunities offered and the strategies to adopt them in an enterprise context. Not only will you learn the technology that works and strategy that matters, we also cover a maturity model for adopting these technologies so you can start with an easy adoption at the beginning and work towards a highly mature state.

TOPICS: Securing PaaS; Securing Containers and Serverless; Securing SaaS Environments; Cloud Threats and the Adoption of Security Features

Who Should Attend

The primary target audience for this course is managers and directors who are in a position to lead or make key decisions on the IT transformation to cloud environments.

NICE Framework Work Roles:
- Information Systems Security Manager: OV-MGT-001
- Executive Cyber Leadership: OV-EXL-001
- Program Manager: OV-PMA-001
- IT Project Manager: OV-PMA-002
- Cyber Intel Planner: CO-OPL-001

Prerequisites

Students should have three to five years of experience in IT and/or cybersecurity. This course covers the core areas of security leadership in migrating workloads to the cloud environment and assumes a basic understanding of technology, networks, and security.

Notice to Students

This course will have limited overlap with the SANS SEC488: Cloud Security Essentials course because it will provide foundational information on cloud services and cloud security to ensure that students are on the same page. This course focuses on what managers, directors, and security leaders need to know about developing their cloud security plan/roadmap and managing implementation of cloud security capabilities.

“I feel like there was a lot of valuable material and would be very relevant for people creating a cloud security program.”

—Jeff Henderson