MGT520: **Leading Cloud Security Design and Implementation**

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Define a strategy for securing a workload in the cloud for medium-size and large enterprises that can support their business objectives
- Establish a security roadmap based on the security strategy that can support a fast-paced cloud adoption and migration path while maintaining a high degree of security assurance
- Understand the security basics of the cloud environment across different types of service offerings, then explain and justify to other stakeholders the decisions within the security roadmap
- Build an effective plan to mature a cloud security posture over time, leveraging security capabilities offered by cloud providers to leapfrog in security capabilities
- Explain the security vision of the organization in the cloud domain to your Board Directors and executives, collaborate with your peers, and engage your workforce, driving the security culture change required for the cloud transformation

"This type of training, i.e., cloud security from a management perspective, is rare and the quality of this one is definitely amazing."

—Benoit Ramillon, **UEFA**

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, while the cloud environment may appear similar to running a traditional IT environment on the premises, the cloud solutions protection requirements are in fact very different because the traditional network perimeter is no longer the best line of defense and the threat vectors are not the same. Effective defense of the organization's cloud environment requires significant planning and governance by a well-informed management team.

The SANS MGT520: Leading Cloud Security Design and Implementation course focuses on what managers, directors, and security leaders need to know to develop their cloud security roadmap and 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 walk through the key aspects of managing cloud transition and ensuring security in the continuous operations post-migration that are common across organizations on the same journey. 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.

Author Statement

"Cloud transition is common in many organizations these days, but many security leaders feel overwhelmed and underprepared for the security aspects of the cloud. When organizations accept security as an integral part of the transformation path, they can not only achieve the same level of security as their in-house IT environment, but also take advantage of a huge opportunity to leapfrog in security using cloud capabilities. In MGT520, we discuss industry-proven techniques to plan for the security aspects of cloud transformation. This course will arm students with the necessary information to confidently lead their organization towards securing the cloud workload and leveraging cloud capabilities to further enhance their security maturity in the IT environment."

—Jason Lam

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 ll then pivot to cloud environment details to help you understand the security targets and maturity journey for the main types of public cloud services 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 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.

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

SECTION 3: Cloud Security Features: Adoption and Maturing the Security Program

The third course section covers 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 begging and work towards a highly mature state.

Cloud adoption is a long-term process. We will arm you with the information to drive the changes required by measuring the cloud security posture and using metrics to aid in making the right decisions.

TOPICS: Cloud Threats and the Adoption of Security Features; Cloud Security Assurance and Assessment; Maturing the Cloud Security Program

SECTION 2: Cloud Infrastructure and Orchestration

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, making the workload more secure and reduce the operational burden can be realized given the proper planning and leadership. We first walk through the 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.

Securing the Platform as a Service (PaaS) workloads and also 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 get improved security in these Cloud based environments.

TOPICS: Identity Access Management; Securing PaaS; Securing Containers and Serverless; Securing SaaS Environments

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.

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