SANS Cloud Security focuses the deep resources of SANS on the growing threats to The Cloud by providing training, certification, research, and community initiatives to help security professionals build, deploy and manage secure cloud infrastructure, platforms, and applications.

SANS Cloud Security Curriculum provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and applications in the cloud against the most dangerous threats. The courses are full of important and immediately useful techniques that you can put to work as soon as you return to your office. The curriculum has been developed through a consensus process involving industry leading engineers, architects, administrators, developers, security managers, and information security professionals, and address public cloud, multicloud, and hybrid-cloud scenarios for the enterprise and developing organizations alike.

**SANS Cloud Security Curriculum**

- **SEC488: Cloud Security Essentials**
  - License to Learn Cloud Security

- **SEC505: Public Cloud Security: AWS, Azure, and GCP**
  - Multiple clouds require multiple solutions.

- **SEC522: Defending Web Applications Security Essentials**
  - It’s not a matter of “if” but “when.”
  - Be prepared for a web attack.
  - We’ll teach you how.

- **SEC534: Secure DevOps: A Practical Introduction**

- **SEC540: Cloud Security and DevSecOps Automation**
  - The cloud moves fast. Automate to keep up.

- **SEC541: Cloud Security Monitoring and Threat Detection**
  - Attackers can run but not hide.
  - Our radar sees all threats.

- **SEC557: Continuous Automation for Enterprise and Cloud Compliance**
  - Using Cloud Security and DevOps Tools to Measure Security and Compliance

- **SEC584: Cloud Native Security: Defending Containers & Kubernetes**
  - Deploy securely at the speed of cloud native.

- **SEC588: Cloud Penetration Testing**
  - Aim your arrows to the sky and penetrate the cloud.

- **FOR509: Enterprise Cloud Forensics and Incident Response**
  - Find the Storm in the Cloud

- **MGT516: Managing Security Vulnerabilities: Enterprise and Cloud**
  - Stop treating the symptoms.
  - Cure the disease.

- **MGT520: Leading Cloud Security Design and Implementation**
  - Building and leading a cloud security program.
SEC488: Cloud Security Essentials

License to Learn Cloud Security
SEC488 covers Amazon Web Services, Azure, Google Cloud, and other cloud service providers (CSPs). Like foreign languages, cloud environments have similarities and differences, and this course will introduce you to the language of cloud security. Upon completion of this course, you will be able to advise and speak about a wide range of cybersecurity topics and help your organization successfully navigate the challenges and opportunities presented by cloud service providers.

Daily Topics:
1. Identity and Access Management
2. Compute and Configuration Management
3. Data Protection and Automation
4. Networking and Logging
5. Compliance, Incident Response, and Penetration Testing
6. CloudWars

SEC510: Public Cloud Security: AWS, Azure, and GCP

Multiple clouds require multiple solutions.
SEC510 is an in-depth analysis of the security of managed services for the Big 3 cloud providers: Amazon Web Services, Azure, and Google Cloud Platform. Students will leave the course confident that they have the knowledge they need when adopting services and Platform as a Service (PaaS) offerings in each cloud. Students will launch unhardened services, analyze the security configuration, validate that they are insufficiently secure, deploy patches, and validate the remediation.

Daily Topics:
1. Cloud Credential Management
2. Cloud Virtual Networks
3. Encryption, Storage, and Logging
4. Severless Platforms
5. Cross-Account and Cross-Cloud Assessment
SEC522: Defending Web Applications Security Essentials

It’s not a matter of “if” but “when.” Be prepared for a web attack. We’ll teach you how.

This is the course to take if you have to defend web applications! The quantity and importance of data entrusted to web applications is increasing, and defenders need to learn how to secure these critical data. Traditional network defenses such as firewalls fail to secure web applications. In covering the OWASP Top 10 Risks and beyond, SEC522 will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization’s web assets.

**Daily Topics:**
1. Web Fundamentals and Security Configurations
2. Defense Against Input-Related Threats
3. Web Application Authentication and Authorization
4. Web Services and Front-End Security
5. Cutting-Edge Web Security
6. Capture-and-Defend-The-Flag Exercise

“**This training is essential for anyone who needs to understand web protocol and application security and their limitations. This course provides a practical approach to many theoretical scenarios with relevant POCs within the course work.”**
—Joel Samaroo, Visa Inc.

SEC534: Secure DevOps: A Practical Introduction

**Principles! Practices! Tools! Oh my. Start your journey on the DevSecOps road here.**

SEC534 explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. You will learn how DevOps principles, practices, and tools can be leveraged to improve the reliability, integrity, and security of systems.

**Daily Topics:**
1. Introduction to Secure DevOps
2. Secure Infrastructure and Operations

“**Very informative and up-to-date with tools and processes used in today’s development environments.”**
—Thomas Dison, Patterson Dental
SEC540: Cloud Security and DevSecOps Automation

The cloud moves fast. Automate to keep up.

SEC540 provides security professionals with a methodology for securing modern Cloud and DevOps environments. Students learn how to implement over 20 DevSecOps Security Controls for building, testing, deploying, and monitoring cloud infrastructure and services. Immersive hand-on labs ensure students not only understand theory, but how to configure and implement each security control. By embracing the DevOps culture, you will walk away battle tested and ready to build to your organization's Cloud & DevOps Security program.

Daily Topics:
1. Introduction to DevSecOps
2. Cloud Infrastructure and Orchestration
3. Cloud Security Operations
4. Cloud Security as a Service
5. Compliance as Code

SEC541: Cloud Security Monitoring and Threat Detection

Attackers can run but not hide. Our radar sees all threats.

SEC541 is a cloud security course that looks at how attackers are attacking the Amazon Web Services (AWS) and Microsoft Azure environments, what their characteristics are, and how to detect them and investigate suspicious activity in your cloud infrastructure. Every day, the class will analyze a real world set of attacks, break down how it happened, how they would detect it in their environment, and then dive into the AWS and Azure services analyzing logs, behaviors and building analytics that the students can bring back to their own cloud infrastructure.

Daily Topics:
1. Management Plane and Network Logging
2. Compute and Cloud Services Logging
3. Cloud Service and Data Discovery in AWS

“SEC540 helped me understand the complex ecosystem of DevOps. I came away with a well-rounded understanding of how the different technologies work together and how security needs to be tied into the CI/CD aspect. More than that, I found a new enthusiasm to learn and explore DevOps.”
—Uday Pothakamury, Citi

“This had the right mix of AWS infrastructure background and methods of using AWS log data for threat hunting.”
—Brad Schonhorst, Sony
SEC557: Continuous Automation for Enterprise and Cloud Compliance

Using Cloud Security and DevOps Tools to Measure Security and Compliance

SEC557 teaches professionals tasked with ensuring security and compliance how to stop being a roadblock and work at the speed of the modern enterprise. You’ll learn how to measure and visualize security data using the same tools that developers and engineers are using, as well as how to extract, load, and visualize data from cloud services, on-premise systems, and security tools. The course includes PowerShell scripting, automation, time-series databases, dashboard software, and even spreadsheets to present management with the strategic information it needs and to facilitate the work of your operations staff with sound tactical data.

Daily Topics:
1. Scripting, Data Acquisition, and Visualization Tools
2. Acquiring and Visualizing Cloud Service Data
3. Acquiring and Visualizing Data from OSes, Virtualization, and Containers

SEC584: Cloud Native Security: Defending Containers and Kubernetes

Deliver securely at the speed of cloud native.

SEC584 will perform a deep-dive into defending key infrastructure deployment components, focusing on containerization and orchestration exploits. Students will be thrust directly into detailed issues related to misconfiguration and known attack patterns and will learn how to properly harden and protect against these exploits.

Daily Topics:
1. Cloud Native Security
2. Container Security and Exploitation
3. Moving to Kubernetes
SEC588: Cloud Penetration Testing

Aim your arrows towards the sky and penetrate the Cloud.

SEC588 will equip you with the latest in cloud focused penetration testing techniques and teach you how to assess cloud environments. In this course we dive into topics like cloud based microservices, in-memory data stores, serverless functions, Kubernetes meshes, and containers, as well as identifying and testing in cloud-first and cloud-native applications. You will also learn specific tactics for penetration testing in Azure and AWS, particularly important given that Amazon Web Services and Microsoft account for more than half of the market. It’s one thing to asses and secure a datacenter, but it takes a specialized skill-set to truly assess and report on the risk that an organization faces if their cloud services are left insecure.

Daily Topics:
1. Discovery, Recon, and Architecture at Scale
2. Mapping, Authentication, and Cloud Services
3. Azure and Windows Services in the Cloud
4. Vulnerabilities in Cloud Native Applications
5. Exploitation and Red Team in the Cloud
6. Capstone

FOR509: Enterprise Cloud Forensics and Incident Response

Find the Storm in the Cloud

The world is changing and so is the data we need to conduct our investigations. New platforms change how data is stored and accessed. They remove the examiner’s ability to put their hands directly on the data. Many examiners are trying to force old methods for on-premise examination onto cloud hosted platforms. Rather than resisting change, examiners must learn to embrace the new opportunities presented to them in the form of new evidence sources.

Daily Topics:
1. Cloud Forensics Fundamentals and Microsoft 365
2. Amazon AWS
3. Microsoft Azure
4. Google Cloud (GCP)
MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

Stop treating the symptoms. Cure the disease.

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. The Cyber42 game that forms part of the course puts students in the driver’s seat for the fictional Everything Corporation (“E-Corp”) and allows them to select certain initiatives that will mature E-Corp's VM program. Students will also need to choose how to respond to 13 realistic events that are sure to have an impact on their program. Depending on how students respond, E-Corp’s security culture and the maturity of the different components of its VM program will be impacted. These tabletop exercises will enable students to put the skills they are learning into practice when they return to work at their own organizations.

Daily Topics:
1. Overview: Cloud and Asset Management
2. Identify
3. Analyze and Communicate
4. Treat
5. Buy-in, Program, and Maturity

MGT520: Leading Cloud Security Design and Implementation

Building and Leading a Cloud Security Program

MGT520 teaches students how to build, lead, and implement a cloud security transition plan and roadmap, and then execute and manage ongoing operations. An organization’s cloud transition requires numerous key decisions. This course provides the information security leaders need to drive a secure cloud model and leapfrog on security by leveraging the security capabilities in the cloud.

Daily Topics:
2. Cloud Security Features: Adoption and Maturing the Security Program
3. Cloud Security Features: Adoption and Maturing the Security Program

“I like how the content builds and progresses. Jason clearly thought a lot about how to sequence the information to make it easy to digest.”
—Jim Pruitt, Revolutionary Security
### Level Definitions

- **Baseline** – Courses that impart the baseline skills required of any information security professional involved in Cloud Security, whether active practitioner or manager.

- **Foundational** – Courses that provide the basic knowledge to introduce students to a required skill set for the Cloud Security industry specifically.

- **Core** – Courses that prepare professionals for more focused job functions in Cloud Security, including manager, architect, engineer, analyst, and developer.

- **Specialization** – Courses for critical, advanced skills, or specialized roles in Cloud Security.

- **Management** – Courses that prepare leaders to make sound strategic business decisions in regards to cloud security planning and implementation.

### Role Descriptions

- **DevOps Professional** – Responsible for code creation.

- **Cloud Security Analyst** – Responsible for deciphering.

- **Cloud Security Engineer** – Responsible for building.

- **Cloud Security Architecture** – Responsible for designing.

- **Cloud Security Manager** – Responsible for leading.

### Flight Plan to Becoming a Cloud Ace

<table>
<thead>
<tr>
<th>Level</th>
<th>Courses</th>
<th>DevOps Professionals</th>
<th>Cloud Security Analyst</th>
<th>Cloud Security Engineer</th>
<th>Cloud Security Architect</th>
<th>Cloud Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>COMING SOON</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foundational</td>
<td>SEC488: Cloud Security Essentials (GCLD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECS34: Secure DevOps: A Practical Introduction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECS10: Public Cloud Security: AWS, Azure, and GCP (GPCS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECS22: Defending Web Applications Security Essentials (GWEB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECS40: Cloud Security and DevSecOps Automation (GCSA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core</td>
<td>SECS41: Cloud Security Monitoring and Threat Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECS54: Cloud Native Security: Defending Containers and Kubernetes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECS58: Cloud Penetration Testing (GCPN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FOR509: Enterprise Cloud Forensics and Incident Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specialization</td>
<td>MGT516: Managing Security Vulnerabilities: Enterprise and Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MGT520: Leading Cloud Security Design and Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SECS57: Continuous Automation for Enterprise and Cloud Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• **Security focused** – Providing technical training to properly secure services and workloads in the cloud

• **Multicloud Approach** – Providing training and comparisons on the Big Three public cloud providers

• **Hands-on Labs** – Extensively focuses on “the how” to properly deploy and secure a cloud environment using virtual machines, lab environments, and repeatable exercises

• **Instructors** – Versatile, real-world security practitioners

• **Courseware** – Providing access to slides, notes, and audio files for future reference

---

**RESOURCES**

- **Landing Page** – [www.sans.org/cloud-security](http://www.sans.org/cloud-security)
- **Twitter** – @SANSCloudSec
- **LinkedIn** – [www.linkedin.com/showcase/sanscloudsec](http://www.linkedin.com/showcase/sanscloudsec)
- **YouTube** – [www.youtube.com/c/SANSCloudSecurity](http://www.youtube.com/c/SANSCloudSecurity)