SEC541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection

GCTD
Cloud Threat Detection
giac.org/gctd

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Research attacks and threats to cloud infrastructure and how they could affect you
- Break down a threat into detectable components
- Effectively use AWS and Azure core logging services to detect suspicious behaviors
- Make use of cloud native API logging as the newest defense mechanism in cloud services
- Move beyond the cloud-provided Graphic User Interfaces to perform complex analysis
- Perform network analysis with cloud-provided network logging
- Understand how application logs can be collected and analyzed inside the cloud environment
- Effectively put into practice the AWS and Azure security specific services
- Integrate container, operating system, and deployed application logging into cloud logging services for more cohesive analysis
- Centralize log data from across your enterprise for better analysis
- Perform inventory of cloud resources and sensitive data using scripts and cloud native tooling
- Analyzing Microsoft 365 activity to uncover threats
- Ability to leverage cloud native architecture to automate response actions to attacks

Authors' Statement

"Cloud service providers are giving us new tools faster than we can learn how to use them. As with any new and complex tool, we need to get past the surface-level 1how-to in order to radically reshape our infrastructure. This course is an overview of the elements of AWS and Azure that we may have used before but are ready to truly explore. By the end of the class, you ll be confident knowing that you have the skills to start looking for the threats and building a true threat detection program in AWS and Azure."

—Shaun McCullough and Ryan Nicholson

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

SEC541 is a cloud security course that investigates how attackers are operating against Amazon Web Services (AWS) and Microsoft Azure environments, the attacker's characteristics, and how to detect and investigate suspicious activity in your cloud infrastructure. You will learn how to spot the malice and investigate suspicious activity in your cloud infrastructure. In order to protect against cloud environment attacks, an organization must know which types of attacks are most likely to happen in your environment, be able to capture the correct data in a timely manner, and be able to analyze that data within the context of their cloud environment and overall business objectives.

SEC541 starts each day by walking through a real-world attack campaign against a cloud infrastructure. We will break down how it happened, what made it successful, and what could have been done to catch the attackers in the act. After dissecting the attacks, we learn how to leverage cloud native and cloud integrated capabilities to detect, threat hunt, or investigate similar attacks in a real environment, and building our arsenal of analytics, detections and best practices. The course dives into the AWS and Azure services, analyzing logs and behaviors and building analytics that the students can bring back to their own cloud infrastructure.

Key Takeaways

- Decrease the average time an attacker is in your environment
- Demonstrate how to automate analytics, thus reducing time
- Help your organization properly set up logging and configuration
- Decreases risk of costly attacks by understanding and leveraging cloud specific security services
- Lessen the impact of breaches that do happen
- Learn how to "fly the plane", not just the ability to read the manual

Hands-on Training

The labs in this course are hands-on explorations into AWS and Azure logging and monitoring services. **About 75% of labs are AWS and 25% Azure.** Each lab will start by researching a particular threat and the data needed to detect it. In most labs, the students will conduct the attack against their accounts, generating the logs and data needed to perform analysis. Students will use native AWS and Azure services and open-source products to extract, transform, and analyze the threat. The course lecture coupled with the labs will give students a full picture of how those services within AWS & Azure work, the data they produce, common ways to analyze the data, and walk away with the ability to discern and analyze similar attacks in their own cloud environment.

- **SECTION 1:** SEC541 environment deployment, analyzing cloud API logs with CloudTrail, parsing JSON-formatted logs with JQ, network analysis
- **SECTION 2:** Environment setup, application/OS log lab with OpenCanary, CloudWatch agent and customization, strange ECS behavior, finding data exfiltration
- **SECTION 3:** Metadata services and GuardDuty, cloud inventory, discovering sensitive data in unapproved location with Macie, vulnerability assessment with Inspector, data centralization with Graylog
- **SECTION 4:** Microsoft 365 Exchange investigation, introduction to Kusto Query Language, log analytics analysis using Azure CLI, Microsoft Defender for Cloud and Sentinel, Azure network traffic analysis
- **SECTION 5:** Setup the automate forensics workflow, analyze the results, participate in the CloudWars Challenge

Section Descriptions

SECTION 1: Management Plane and Networking Logging

SEC541 starts with an investigation into the attack of the developer services company, Code Spaces. The class will break down the attack and map each action to the MITRE ATT&CK framework. This leads to an investigation of the detection and logging capability most unique to Cloud Services, the Cloud API Service. The Cloud API is at the heart of most activity in the cloud and is the first best place to start for analysis and detection. The class then investigates network analysis options in AWS and Azure cloud services, understanding what data is available, what is missing, and some of the ways that network analysis could have been used to detect Code Spaces and similar attacks.

TOPICS: Debrief: Code Spaces; Cloud API Logging; Cloud-Native Logging Services; Network Flow Logging

SECTION 2: Computer and Cloud Services Logging

Section 2 starts with a dive into the attack against Tesla's Kubernetes management services. As with Section 1, the class will investigate the specific tactics used in the attack and how they map to MITRE's new Container ATT&CK Framework. Containers are becoming ever more common in cloud services, especially when they help common application development in multi-cloud or hybrid architectures. Section 2 starts with looking at how application logs can be gathered in AWS and Azure, at what level, and the types of data typically gathered. The class then looks at Kubernetes, Docker, AWS, and Azure container orchestration services, what data is logged, and how to investigate that log data to detect activity or help with investigations. The section rounds out by looking at proxies that operate in the cloud environment. Proxies have the promise of improving operations and maybe even security, but Cloud-managed proxies lose some visibility. The class will understand what services are available and how to make the most of the logging.

TOPICS: Debrief Tesla Attack; Making Use of Operating System Logs; Gathering Application Generated Logs; Log Agents; Container Logs; Cloud Proxies

Who Should Attend

- Security analysts
- Security architects
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- System administrators
- Cloud administrators

SECTION 3: Cloud Services and Data Discovery

Section 3 starts with an investigation into the Capital One attack. After pulling apart the techniques used by the attacker, the class will look at how AWS cloud's metadata service can be used to gain unauthorized access to cloud infrastructure through application vulnerabilities, and what is different from Azure's implementation. After a discussion of AWS services that help with security monitoring, the section will discuss tools and cloud-managed services that are used to perform an inventory of resources and perform data discovery. Cloud environments are constantly changing, and the investigator needs these discovery tools to pinpoint problems quickly. AWS and Azure provide services to help with application, host, and configuration vulnerabilities that may point to potential intrusion and attacker activities. The class will look at some cloud company services build to help perform and remediate these vulnerabilities. Lastly, this section will discuss the benefits of centralizing the data collected from cloud, host, and application logs. The class will look at AWS and Azure services that help manage data centralization, which one to use, and their benefits.

TOPICS: Debrief: Capital One; AWS Cloud Inventory Techniques and Services; Using Data Discovery Tools; Vulnerability Analysis Services; Data Centralization; AWS Elasticsearch

SECTION 4: Microsoft Ecosystem

Just like the first three sections, Section 4 starts off with a review of the MalwareBytes breach from early 2021 and the major MITRE ATT&CK techniques involved. Afterwards, we will explore Microsoft 365, the components aiding defenders in their detection initiatives, and put our skills to the test using those techniques to discover the beginning of a new attack campaign in the first or five lab exercises. Next, and this is where section 4 differs, we will review a second breach: the SolarWinds supply chain attack from 2021. Afterwards, we dive more—and the proper configuration steps—of Azure Active Directory. This will include a lab analyzing data using a language that was covered previously (but not yet exercised): Kusto Query Language. You will find, in the next few modules that round out the section, a continuation of what makes Azure quite different than most other cloud vendors: how their logging is handled related to cloud storage access, their unique detection services, and how network traffic can be analyzed. Each of these topics include a unique exercise to hone your skills.

TOPICS: MalwareBytes Attack; Microsoft 365; SolarWinds Attack; Azure Active Directory (AD); Storage Monitoring; Detection Services; Network Traffic Analysis

SECTION 5: Automate Response Actions and CloudWars

The commercial cloud services are designed to automate the building and operation of complex workloads. We can leverage those automation design patterns to start automating the data capture, analysis, and security defenses in our environment. In this section, we will discuss some of the workloads we might want to automate in our cloud environment, investigate some of the services for automation, and then work through an example. This section also includes a CloudWars competition to reinforce the topics covered throughout the course. Through this friendly competition, you will answer several challenges made up of multiple choice, fill-in-the-blank, as well as hands-on and validated exercises performed in two CSP environments. You will also be given new cloud resources to deploy and analyze - earning valuable points in the process.

TOPICS: Automated Response Actions; CloudWars Challenge