SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC584: **Cloud Native Security: Defending Containers and Kubernetes**

3	18	Laptop
Day Course	CPEs	Required

You Will Be Able To

- Use real-world exploits to target key application deployment components
- Understand the risks involved in running cloud native infrastructure
- Explore vulnerabilities to cloud native deployments through authentication, pipeline, and supply chain exploits
- Exploit and then secure application deployments via Docker and Kubernetes
- Determine how vulnerabilities are exploited and how defenses are designed

> **"Great content. Loads of new things to learn. Relevant to real-world tasks.**
>
> — Nii Akai-Nettey, **6point6**

Deploy securely at the speed of cloud native.

Cloud native infrastructure and service providers are enabling organizations to build and deliver modern systems faster than ever. The end-to-end toolchain supporting the systems includes managed services to create cloud infrastructure, store source code, build containers, and manage clusters. For information security professionals, the attack surface created by these modern systems can be difficult to defend and monitor. SEC584 explores Docker and Kubernetes, key components of the cloud native infrastructure stack, providing in-depth analysis of the attack surface, misconfigurations, attack patterns, and hardening steps. Students will gain hands-on experience building, exploring, and securing real-world modern systems.

SEC584 starts by painting a portrait of the modern cloud-native infrastructure hosted in Google Cloud. After deploying cloud resources, students examine methods of compromise, walk through attack scenarios, and then shift their focus to defending and remediating infrastructure services. This includes hardening Kubernetes orchestrator and workload configuration, deploying security testing and monitoring software in pipelines and clusters, cryptographically signing images and build pipelines, and applying AppArmor and Seccomp profiles to containerized workloads.

The course then shifts its focus to defending a live Kubernetes deployment. After students identify several Kubernetes weaknesses, hands-on exercises attacking and remediating security and network policies and admission controllers will help them lock down the lab environment. Attacks and controls are threat-modeled to ensure they are applied correctly, tested out-of-band to ensure their efficacy, and applied at multiple stages throughout the pipeline to enhance engineers' productivity and feedback loops.

Course Authors' Statement

"The proliferation of containers and the growth of Kubernetes and its supporting ecosystem offer a new opportunity for organizations looking to adopt modern development, deployment, and security practices. Containers share their host's kernel and so are more efficient and lightweight than VMs, but they provide a different set of security guarantees. And as cloud providers have built out their managed offerings, the shared responsibility model puts the ultimate responsibility for the security of users' infrastructure on their shoulders.

"Highly scalable and resilient distributed systems bring additional complexity, and DevSecOps security can only be achieved with a solid DevOps engineering foundation on which to build. Once this is established, automated security verification can prove the absence of known regressions and reduce the likelihood of unknown vulnerabilities.

"Attackers have exploited misconfigured Docker and Kubernetes instances, container and application supply chains, and the cloud infrastructure with which they integrate. This course examines all of these attacks in detail, shows attendees how to undertaken them, and provides detailed remediation and testing steps to ensure cloud native infrastructure is locked down, while still providing value to the business."

— Andy Martin & Eric Johnson

Section Descriptions

SECTION 1: Cloud Native Security

Section 1 covers the cloud native security model, threat model, and associated infrastructure security practices. This includes deploying and rooting Jenkins to gain remote code execution on a Google Cloud virtual machine to illustrate security considerations of container workloads, as well as a corresponding discussion of defending containerized workloads.

TOPICS: What is Cloud Native Security; Modern Infrastructure Security Practices; Container Security

SECTION 2: Container Security and Exploitation

Section 2 covers concepts related to the containerization of applications, including the risks and benefits of deploying applications in containers. This day will focus specifically on Docker containers, examining how they are created and deployed, reviewing the risks associated with deploying applications in Docker containers, and exploring ways that Docker containers can be hardened and secured.

TOPICS: Container Image Security; Container Security Testing; Securing the CI Pipeline

SECTION 3: Moving to Kubernetes

Section 3 covers the use of orchestration tools to manage the deployment of containerized applications. This day will focus on the Kubernetes platform. We will look at the potential risks and vulnerabilities associated with Kubernetes as well as how we can secure it through automated scans, proper policy definitions, and continuous intrusion detection.

TOPICS: Introduction to Kubernetes; Attacking Kubernetes; Hardening Kubernetes; Automated Security Testing and DevSecOps Workflows

"Lots of information and lots of content. I learned a lot, and I thought I knew a lot about dockers and containers."

— SEC584 Student

"Lots of content for the course and all valuable and useful for my learning."

— Jacob Austin

Who Should Attend

- Information security professionals
- DevOps engineers
- System administrators
- Operations engineers
- Developers
- Software architects
- Anyone who is responsible for deploying, managing, and securing modern tools like Docker and Kubernetes in the cloud
- Security practitioners trying to understand the risks associated with these components