Cybersecurity Academy Advanced Courses

Cloud Security Automation

Course Description:

Cyber-attacks against cloud network operations are increasing with intensity and have the potential to inflict wide-spread damage to business production and organization's reputation. It is now more important than ever for security practitioners to understand the magnitude of the problem and employ solutions to defend cloud-based networks as well as to maintain trust with customers, partners, and shareholders. This course is designed to enhance student's understanding of securing Cloud Computing technologies using an enterprise suite of services such as Cloud Native Application Protection Platform, with an emphasis on cloud container configurations that provide visibility of risks associated with deployment in public cloud and private data centers.

NIST/NICE Alignment and Work Roles:

- Implementation and Operation – Systems Administration (IO-WRL-005)
- Implementation and Operation – Systems Security Analysis (IO-WRL-006)
- Protection and Defense – Infrastructure Support (PD-WRL-004)
- Potential Job Roles: Systems Administrator; Security Architect; Systems Security Analyst; Cyber Defense Analyst

Course Objectives:

- Evaluate how Cloud-based machine learning aids with anomaly detection.
- Explain how Cloud security services deploy and analyze data security policies.
- Identify container security deployment models and DevOps pipeline.
- Compare container vulnerability and compliance management procedures.

  upgrade procedures.
- Discover single and cluster container defender installation procedures.
- Describe methods used to monitor containers for vulnerabilities.
- Review and analyze the top 10 container vulnerability list.
- Search for and evaluate the container CVE details information.
- Design protection and security best practices for Serverless applications
- Examine the security enhancements provided by Identity-Based Micro-segmentation.
- Explain the value of Cloud-based Infrastructure as Code.
- Review and analyze Identity and Access Management Cloud security services.
- Discover the container compliance status through scans for AWS cloud accounts.
- Describe container monitoring and runtime behavior.
- Describe container model machine learning, patterns, learning states and drips.
- Analyze container model details processes, networking and Trust Audit details.
- List the steps required to develop a new container runtime rule.
- Investigate an incident through compliance, image, snapshots and audit details.
- Evaluate the challenges associated with Cloud Identity and Access Management.
- Identify how SASE architecture integrates Secure Web Gateway, FWAAS, and CASB.
- Discover how Security Posture Management assesses risk of SaaS applications.
- Examine the network security requirement for a Secure Web Gateway SASE solution.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Cloud and Container Security Overview • Cloud Defender - Monitoring Vulnerabilities • Cloud Assessment - Monitoring Behavior • Maintaining Compliance and Identity Access Management • Cloud Incident Management - Runtime Defense	Successful completion of the Cloud Security Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 3 credits – 45 contact hours **Format:** Instructor-Led or Self-Paced	• Introduction to Kubernetes • Configuring Kubernetes: Persistent Storage and YAML Files • Configuring Kubernetes: Microservices and DevSecOps • Reviewing CNAPP Compute Console I • Reviewing CNAPP Compute Console II • Running CNAPP Compute Defense I • Running CNAPP Compute Defense II