Advanced Vulnerability Management in Cloud Workloads Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid Cloud Migration and adoption of DevSecOps practices have expanded the attack surface, making traditional vulnerability scanning inadequate. Advanced Vulnerability Management in Cloud Workloads Training Course is designed to equip security professionals with the cutting-edge knowledge and practical skills required to implement a proactive, Risk-Based Vulnerability Management (RBVM) program across dynamic Multi-Cloud environments. You will move beyond simple CVSS scoring to master Contextual Prioritization, automated remediation, and Shift-Left Security to address the most critical threats, including cloud native misconfigurations, container vulnerabilities, and complex IAM flaws.

This intensive, hands-on training focuses on managing the entire vulnerability lifecycle within cloud-native and hybrid architectures. By mastering Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) tools, you will learn to integrate security seamlessly into CI/CD pipelines and drive continuous, measurable risk reduction. The goal is to transform reactive patch management into a strategic, Automated Remediation process that ensures regulatory Compliance and strengthens the overall Cloud Resilience of the organization.

Programme Curriculum

Advanced Vulnerability Management in Cloud Workloads Training Course

Introduction

The rapid Cloud Migration and adoption of DevSecOps practices have expanded the attack surface, making traditional vulnerability scanning inadequate. Advanced Vulnerability Management in Cloud Workloads Training Course is designed to equip security professionals with the cutting-edge knowledge and practical skills required to implement a proactive, Risk-Based Vulnerability Management (RBVM) program across dynamic Multi-Cloud environments. You will move beyond simple CVSS scoring to master Contextual Prioritization, automated

remediation, and Shift-Left Security to address the most critical threats, including cloud native misconfigurations, container vulnerabilities, and complex IAM flaws.

This intensive, hands-on training focuses on managing the entire vulnerability lifecycle within cloud-native and hybrid architectures. By mastering Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) tools, you will learn to integrate security seamlessly into CI/CD pipelines and drive continuous, measurable risk reduction. The goal is to transform reactive patch management into a strategic, Automated Remediation process that ensures regulatory Compliance and strengthens the overall Cloud Resilience of the organization.

Course Duration

10 days

Course Objectives

Upon completion, participants will be able to:

1. Architect and deploy a modern Risk-Based Vulnerability Management (RBVM) program for Multi-Cloud environments.
2. Master the process of Contextual Prioritization beyond simple CVSS scores using EPSS and business impact.
3. Implement Continuous Monitoring for new and evolving threats in dynamic cloud environments.
4. Apply Shift-Left Security principles to integrate vulnerability scanning into CI/CD Pipelines.
5. Effectively leverage Cloud Security Posture Management (CSPM) tools to identify and remediate Cloud Misconfigurations.
6. Secure Container and Kubernetes Workloads using specialized vulnerability scanning and CWPP.
7. Analyze and mitigate risks associated with over-privileged Identity and Access Management (IAM) policies.
8. Perform in-depth vulnerability assessment of Serverless and Function-as-a-Service (FaaS) components.
9. Develop Automated Remediation and orchestration workflows to reduce Mean Time To Remediation.
10. Integrate Threat Intelligence feeds into the vulnerability management lifecycle for proactive defense.
11. Secure Infrastructure-as-Code templates for security by design.
12. Establish key performance indicators and produce executive-level Risk Reporting for compliance.
13. Address advanced vulnerabilities, including API Security flaws and data exposures in SaaS platforms.

Target Audience

1. Cloud Security Engineers
2. Vulnerability Management Analysts
3. DevSecOps Engineers and Architects
4. IT Risk and Compliance Professionals
5. Security Operations Center Analysts
6. Cloud Architects and Developers with Security Responsibility
7. Penetration Testers
8. Security Managers and Technical Directors

Course Modules

Module 1: Foundations of Advanced Cloud VM (Vulnerability Management)

- The shift from perimeter defense to Cloud-Native risk.

- Understanding the Shared Responsibility Model in a VM context.
- Categorizing cloud workload types
- Asset Discovery and comprehensive inventory across Hybrid Cloud.
- VM lifecycle in the context of Continuous Integration/Continuous Delivery
- Case Study: Analysis of a major public cloud breach caused by inadequate cross-account asset inventory.

Module 2: Risk-Based Prioritization and Contextual Scoring

- Moving beyond CVSS to Risk-Based Vulnerability Management
- Utilizing Exploit Prediction Scoring System and business context.
- Correlating vulnerabilities with actual network exposure and IAM permissions.
- Defining and calculating Mean Time To Exploit and MTTR.
- Creating a tiered remediation Service Level Agreement structure.
- Case Study: Prioritizing 500+ vulnerabilities for a FinTech environment based on data sensitivity and internet-facing assets.

Module 3: Cloud Misconfiguration and Posture Management

- Deep dive into Cloud Misconfigurations
- Implementing and tuning Cloud Security Posture Management tools.
- Policy-as-Code and automated compliance checking
- Remediating overly permissive Identity and Access Management policies.
- Leveraging Cloud Native Tools
- Case Study: Remediating a high-profile data leak due to a misconfigured S3 bucket using a CSPM solution.

Module 4: Vulnerability Scanning in IaaS Workloads

- Agent-based and Agentless Scanning methodologies for Virtual Machines.
- Credentialed and non-credentialed scans and their limitations in IaaS.
- Advanced scanning techniques for gold images and custom AMIs/VM Images.
- Automating patch deployment and configuration drift detection.
- Integrating vulnerability data with Configuration Management Databases
- Case Study: Developing an automated patching and rescan workflow for a large fleet of Linux and Windows IaaS instances across a hybrid network.

Module 5: Container and Image Vulnerability Scanning

- Securing the Container Image Lifecycle
- Scanning container images for OS, library, and application vulnerabilities.
- Integrating image scanning tools into Docker and CI/CD workflows.
- Runtime protection and behavioral analysis using CWPP solutions.
- Addressing misconfigurations in container runtime and orchestrators
- Case Study: Preventing a supply chain attack by enforcing a zero-vulnerability image policy in a container registry before deployment.

Module 6: Kubernetes Security and Vulnerability Management

- Vulnerability assessment of the Kubernetes Control Plane.
- Scanning Kubernetes manifests for security best practices.

- Network policy, Role-Based Access Control, and Secrets management in K8s.
- Utilizing Cloud Workload Protection Platform for runtime security in K8s.
- Advanced remediation: Admission controllers and automatic policy enforcement.
- Case Study: Identifying and mitigating a critical RBAC vulnerability that allowed privilege escalation within a multi-tenant Kubernetes cluster.

Module 7: Serverless and FaaS Vulnerability Assessment

- The unique attack surface of Serverless functions
- Scanning third-party libraries and dependencies in FaaS code.
- Managing over-permissioned function roles and environment variables.
- Runtime Monitoring and securing API Gateway configurations.
- Vulnerability checking for Event-Driven Architectures and queues.
- Case Study: Auditing and hardening a vulnerable AWS Lambda function that had excessive permissions to an organizational database.

Module 8: Infrastructure-as-Code Security and Shift-Left

- Integrating Static Application Security Testing into IaC pipelines.
- Scanning Terraform, CloudFormation, and ARM templates for security flaws.
- Enforcing security policies with tools like Checkov, Kics, and OPA Gatekeeper.
- Pre-deployment validation and Policy Enforcement in Git repositories.
- Automated remediation of security findings before deployment
- Case Study: Blocking a deployment pipeline after an IaC scan detected a policy violation that would have created a publicly exposed database.

Module 9: Cloud Identity and Access Management Vulnerabilities

- Identifying and remediating over-privileged user and service roles.
- Analyzing Lateral Movement attack paths through IAM trust relationships.
- Detecting Stale Credentials and unused access keys.
- Enforcing Least-Privilege and Zero Trust principles through IAM.
- Leveraging IAM Access Analyzer and similar tools for risk detection.
- Case Study: Tracing a privilege escalation attack using a combination of a vulnerable VM and an overly permissive, unmonitored service account role.

Module 10: API and Application-Layer Vulnerability Management

- Advanced vulnerability scanning for cloud-hosted Web Applications and APIs.
- Integrating Dynamic Application Security Testing for runtime flaws.
- Mitigating the OWASP Top 10 in a cloud-native context
- Securing API Gateways and implementing Web Application Firewalls.
- Analyzing API vulnerabilities leading to data exposure and lateral movement.
- Case Study: Discovering and patching an API endpoint vulnerability that allowed unauthorized enumeration of user data from a cloud database.

Module 11: Threat Intelligence and Proactive Defense

- Integrating commercial and open-source Threat Intelligence feeds.
- Using threat data to prioritize vulnerabilities based on active exploitation.
- Understanding the role of Zero-Day and N-day vulnerability tracking.

- Proactive hunting for compromise indicators based on threat actor Tactics, Techniques, and Procedures
- Creating a rapid response process for critical, actively exploited vulnerabilities.
- Case Study: Using a major vendor security advisory and integrated threat feed to prioritize and patch a critical vulnerability within 24 hours of disclosure.

Module 12: Automation and Orchestration for Remediation

- Designing Automated Remediation workflows using Serverless
- Orchestrating remediation across Multi-Cloud environments.
- Integrating VM tools with ITSM for ticket automation.
- Using Security Orchestration, Automation, and Response platforms.
- Developing Automated Rollbacks and validation for failed patches.
- Case Study: Implementing a SOAR playbook that automatically isolates a vulnerable internet-facing VM and triggers an emergency patch.

Module 13: Continuous Monitoring and Auditing

- Establishing Continuous Monitoring for new asset deployment and configuration changes.
- Setting up effective Alerting and notification mechanisms.
- Analyzing logs and events for indicators of attempted exploitation.
- Regular security assessments, Penetration Testing, and bug bounty programs.
- Maintaining audit trails and compliance evidence for vulnerability fixes.
- Case Study: Implementing real-time monitoring that immediately flags and quarantines newly deployed workloads that violate baseline security policies.

Module 14: Governance, Reporting, and Compliance

- Mapping vulnerability management to major frameworks
- Developing executive-level dashboards and Risk Reporting tailored to the business.
- Establishing a Vulnerability Disclosure Policy and coordination process.
- Communicating risk effectively to technical teams, leadership, and auditors.
- Defining and tracking Key Performance Indicators for VM program maturity.
- Case Study: Presentation of a quarterly security posture report to a C-suite, demonstrating significant risk reduction through RBVM implementation.

Module 15: Advanced Topics and Future Trends

- Vulnerability management in Data Lakes and modern data platforms.
- The impact of Generative AI and LLMs on cloud security and scanning.
- Securing Software Supply Chain dependencies
- Advanced Zero Trust integration with vulnerability context.
- Evolution of CWPP and CSPM into unified Cloud-Native Application Protection Platforms
- Case Study: Evaluating the use of a new AI-powered scanner to identify and prioritize vulnerabilities in an organization's proprietary code base.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.

- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com