Azure Security Center/Defender for Cloud Mastery Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the rapidly evolving landscape of multi-cloud environments, ensuring robust and proactive security is paramount. The Microsoft Defender for Cloud Mastery Training is the definitive program for mastering the Cloud-Native Application Protection Platform (CNAPP) capabilities essential for modern security operations. Azure Security Center/Defender for Cloud Mastery Training Course provides a deep dive into Cloud Security Posture Management (CSPM) and advanced Cloud Workload Protection (CWP), equipping security professionals with the skills to defend hybrid and multi-cloud resources against emerging threats. By focusing on practical deployment, security automation, and seamless integration with Microsoft Sentinel and other XDR components, we ensure participants become expert practitioners in maintaining a Zero Trust security model.

The program emphasizes hands-on labs and real-world case studies to bridge the gap between theoretical knowledge and practical application. Participants will learn to leverage the powerful Secure Score to prioritize and remediate critical risks, implement DevSecOps security controls directly into the development lifecycle, and manage threats across compute, data, network, and application layers. Mastering Microsoft Defender for Cloud is not just about using a tool; it's about adopting a proactive defense strategy that unifies Cloud Security operations and drives measurable improvements in regulatory compliance and threat resilience. This course is your essential step toward becoming a Cloud Security Engineer or SecOps Analyst leader.

Programme Curriculum

Azure Security Center/Defender for Cloud Mastery Training Course

Introduction

In the rapidly evolving landscape of multi-cloud environments, ensuring robust and proactive security is paramount. The Microsoft Defender for Cloud Mastery Training is the definitive program for mastering the Cloud-Native Application Protection Platform (CNAPP) capabilities essential for modern security operations. Azure Security Center/Defender for Cloud Mastery Training Course provides a deep dive into Cloud Security Posture Management (CSPM) and advanced Cloud Workload Protection (CWP), equipping security professionals with the skills to defend hybrid and multi-cloud resources against emerging threats. By focusing on practical deployment, security automation, and seamless integration with Microsoft Sentinel and other XDR components, we ensure participants become expert practitioners in maintaining a Zero Trust security model.

The program emphasizes hands-on labs and real-world case studies to bridge the gap between theoretical knowledge and practical application. Participants will learn to leverage the powerful Secure Score to prioritize and remediate critical risks, implement DevSecOps security controls directly into the development lifecycle, and manage threats across compute, data, network, and application layers. Mastering Microsoft Defender for Cloud is not just about using a tool; it's about adopting a proactive defense strategy that unifies Cloud Security operations and drives measurable improvements in regulatory compliance and threat resilience. This course is your essential step toward becoming a Cloud Security Engineer or SecOps Analyst leader.

Course Duration

5 days

Course Objectives

1. Successfully plan, deploy, and configure Microsoft Defender for Cloud across Azure, AWS, GCP, and on-premises resources.
2. Utilize Defender CSPM and Secure Score to continuously assess, prioritize, and remediate security misconfigurations and vulnerabilities at scale.
3. Configure and manage Cloud Workload Protection for key assets, including Containers, Servers, Databases, and Storage accounts.
4. Enforce the principle of "never trust, always verify" using features like Just-in-Time VM access and adaptive network hardening.
5. Map and monitor organizational compliance against industry standards and Azure Security Benchmark.
6. Embed security scanning for Infrastructure as Code templates and container images into CI/CD pipelines
7. Design and implement Security Orchestration, Automation, and Response workflows using Azure Logic Apps to auto-remediate security alerts.
8. Connect and manage the security of non-Azure and Multi-Cloud environments using Azure Arc integration.
9. Analyze and triage high-fidelity security alerts, investigating attacks using the Microsoft Defender XDR and Sentinel portals.
10. Implement data security controls, including malware scanning on Azure Storage and sensitive data protection using Defender for Storage.
11. Utilize Defender External Attack Surface Management (EASM) to discover and prioritize risks for internet-facing assets.
12. Understand how AI-Driven Threat Detection and machine learning are utilized within Defender for Cloud for behavioral anomaly detection.
13. Formulate an organization-wide CNAPP strategy that unifies security controls from code deployment to runtime protection.

Target Audience

1. Cloud Security Engineers.
2. Security Operations (SecOps) Analysts.
3. Azure Administrators/Engineers.
4. DevSecOps Professionals.
5. Compliance and Risk Managers.
6. Security Architects.
7. Threat Hunters.
8. IT Managers/C-Suite.

Course Modules

Module 1: Foundational Microsoft Defender for Cloud & CSPM

- Introduction to Cloud-Native Application Protection Platform and the shift from Azure Security Center to Microsoft Defender for Cloud.
- Deep dive into Cloud Security Posture Management principles, including Secure Score and security recommendations.
- Onboarding and configuration for Multi-Cloud and Hybrid environments via Azure Arc.
- Customizing and managing Security Policies and the Azure Security Benchmark.
- Remediation and governance using Azure Policy and Azure Logic Apps for automated enforcement.
- Case Study: A global financial firm used Secure Score to reduce their public-facing risk by 45% in one quarter by prioritizing high-impact misconfigurations on their critical AWS and Azure subscriptions.

Module 2: Cloud Workload Protection for Compute and Networking

- Implementing Defender for Servers for comprehensive server protection on Azure and non-Azure machines.
- Configuring Just-in-Time VM access and adaptive network hardening for Zero Trust network security.
- Securing Container environments using Defender for Containers for Kubernetes and image scanning.
- Threat detection and advanced controls for Defender for App Service and Defender for Key Vault.
- Vulnerability assessment and remediation using integrated scanning tools.
- Case Study: An e-commerce company used JIT access with Defender for Servers to eliminate RDP brute-force attacks on their development VMs, shrinking their attack window from always-open to a few minutes a day.

Module 3: Data, Storage, and Database Protection

- Enabling and configuring Defender for Storage for malware scanning and sensitive data activity monitoring.
- Advanced threat protection for Azure SQL Database and open-source databases with Defender for Databases.
- Utilizing Defender for Key Vault to secure cryptographic keys and secrets from threats and unauthorized access.
- Implementing data governance and data loss prevention related to cloud storage.
- Auditing and monitoring data access patterns for anomalies and suspicious activities.
- Case Study: A healthcare provider deployed Defender for Storage, which successfully flagged and prevented a suspicious internal script from exfiltrating patient data stored in an Azure Blob container, leading to a quick incident response.

Module 4: Regulatory Compliance and Governance

- Mapping and assessing adherence to industry and regulatory compliance standards
- Creating custom regulatory initiatives to enforce specific organizational security requirements.
- Generating compliance reports and leveraging the Compliance Manager integration.
- Continuous monitoring of compliance drift and automating corrective actions.
- Integrating compliance data with enterprise GRC tools.
- Case Study: A retail organization achieved a critical PCI DSS compliance milestone 60% faster by using Defender for Cloud's built-in regulatory standards and automated continuous compliance checks.

Module 5: DevSecOps and Code-to-Cloud Security

- Integrating Defender for Cloud with CI/CD platforms like GitHub and Azure DevOps.
- Scanning Infrastructure as Code templates for misconfigurations before deployment.
- Implementing container image vulnerability scanning in the container registry.
- Visualizing Code-to-Cloud security risks and tracing findings back to the source code repository.
- Empowering developers with direct, contextual security feedback and automated pull-request annotations.
- Case Study: A software development team adopted DevSecOps integration, preventing five critical cloud misconfigurations from reaching production in the first month by scanning their Terraform templates at the source.

Module 6: Threat Detection, Alert Triage, and Investigation

- Understanding the different types of security alerts and the high-fidelity threat intelligence powering them.
- Effective alert triage, filtering, and suppression techniques to manage alert fatigue.
- Using the Microsoft Defender XDR portal for unified incident investigation and correlation.
- Deep-dive log analysis using Azure Log Analytics and Kusto Query Language for threat hunting.
- Connecting Defender for Cloud alerts and recommendations to Microsoft Sentinel for centralized SIEM/SOAR.
- Case Study: A SOC team used the combined insights of Defender for Cloud and Microsoft Sentinel to correlate a suspicious VM login with a newly deployed vulnerable container image, leading to a successful and rapid containment of a zero-day exploit attempt.

Module 7: Security Automation and Orchestration (SOAR)?ÜÖ??Å

- Designing and implementing Security Orchestration, Automation, and Response playbooks using Azure Logic Apps or Power Automate.
- Automating the remediation of common misconfigurations
- Creating custom automation workflows for incident enrichment and ticket creation in platforms like ServiceNow.
- Managing exceptions and suppressing low-priority alerts with automated rule-based logic.
- Leveraging Workbooks and custom dashboards for operational reporting and security visibility.
- Case Study: A corporate IT department automated the response to 'High Severity' non-compliant resources, saving their SecOps team an estimated 15 hours per week on manual remediation tasks.

Module 8: Advanced Scenarios and Strategic CNAPP Design

- Exploring Defender External Attack Surface Management to identify unknown or unmanaged organizational assets.
- Utilizing Defender for APIs to discover and protect APIs and their data plane.

- Best practices for integrating Defender for Cloud with third-party security solutions and Cloud Access Security Brokers
- Strategic planning for a holistic CNAPP implementation across a complex, multi-cloud enterprise.
- AI-driven security and evolving Zero Trust models in the cloud.
- Case Study: A large enterprise used Defender EASM to discover several forgotten, public-facing developer portals, which were quickly brought under management and secured using Defender for Cloud recommendations, mitigating a significant shadow IT risk.

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.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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