Advanced Threat Modeling for Cloud Architecture 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 adoption of multi-cloud and cloud-native technologies has drastically expanded the attack surface for modern enterprises. Traditional security approaches, which often focus on detection and response, are insufficient against Advanced Persistent Threats (APTs) and complex supply chain attacks. Advanced Threat Modeling for Cloud Architecture Training Course provides the advanced architectural security expertise needed to transition from a reactive posture to a secure-by-design philosophy. Participants will master cutting-edge methodologies like PASTA, VAST, and Adversary-Centric Modeling to identify and mitigate design-level flaws, ensuring the resilience of critical cloud workloads, microservices, and serverless architectures across major providers

This specialized program moves beyond fundamental concepts, focusing on automated threat modeling, integrating security into the CI/CD pipeline, and validating Zero Trust architectures. By decomposing complex systems, analyzing cloud configuration risks, and simulating real-world attack chains using frameworks like MITRE ATT&CK Cloud Matrix, security professionals will gain the proficiency to build truly resilient cloud environments. The emphasis is on practical, hands-on application of tools and techniques to create scalable, repeatable, and governance-aligned threat modeling practices that significantly reduce security debt and accelerate DevSecOps maturity.

Programme Curriculum

Advanced Threat Modeling for Cloud Architecture Training Course.

Introduction

The rapid adoption of multi-cloud and cloud-native technologies has drastically expanded the attack surface for modern enterprises. Traditional security approaches, which often focus on detection and response, are insufficient against Advanced Persistent Threats (APTs) and complex supply chain attacks. Advanced Threat

Modeling for Cloud Architecture Training Course provides the advanced architectural security expertise needed to transition from a reactive posture to a secure-by-design philosophy. Participants will master cutting-edge methodologies like PASTA, VAST, and Adversary-Centric Modeling to identify and mitigate design-level flaws, ensuring the resilience of critical cloud workloads, microservices, and serverless architectures across major providers

This specialized program moves beyond fundamental concepts, focusing on automated threat modeling, integrating security into the CI/CD pipeline, and validating Zero Trust architectures. By decomposing complex systems, analyzing cloud configuration risks, and simulating real-world attack chains using frameworks like MITRE ATT&CK Cloud Matrix, security professionals will gain the proficiency to build truly resilient cloud environments. The emphasis is on practical, hands-on application of tools and techniques to create scalable, repeatable, and governance-aligned threat modeling practices that significantly reduce security debt and accelerate DevSecOps maturity.

Course Duration

10 days

Course Objectives

Upon completion, participants will be able to:

1. Master Adversary-Centric Modeling for Cloud-Native Applications.
2. Decompose complex Multi-Cloud and Hybrid Architectures for security analysis.
3. Apply the PASTA and VAST frameworks to secure modern development pipelines.
4. Integrate Threat Modeling as Code (TMC) into DevSecOps workflows for continuous assurance.
5. Utilize the MITRE ATT&CK Cloud Matrix to simulate and mitigate cloud-specific threats.
6. Evaluate and secure Serverless and Containerized environments
7. Identify and remediate Cloud Configuration Risks and Misconfigurations (CSPM).
8. Design and validate Zero Trust Architecture principles in a cloud context.
9. Model threats associated with Cloud Identity and Access Management (IAM).
10. Analyze security implications of Data Flow across Trust Boundaries in distributed systems.
11. Develop robust Attack Trees and Kill Chains for high-risk cloud assets.
12. Prioritize and communicate identified risks using advanced Risk Scoring methodologies (DREAD, CVSS).
13. Drive a Secure-by-Design culture and scale threat modeling enterprise-wide.

Target Audience

1. Cloud Security Engineers/Architects
2. Product Security/Application Security Engineers
3. DevSecOps/Cloud DevOps Engineers
4. Enterprise/Solution Architects
5. Security Consultants/Penetration Testers
6. CISOs and Security Leaders
7. Risk & Compliance Professionals
8. Technical Program Managers

Course Modules

Module 1: Foundational Concepts & Advanced Frameworks

- Shifting from Traditional to Advanced Cloud Threat Modeling.
- Deep-dive into Data Flow Diagram Decomposition for Cloud Architectures.
- Frameworks: Mastering PASTA
- Frameworks: Mastering VAST
- Case Study: Analyzing the Capital One Breach through a DFD and PASTA lens to highlight misconfiguration and data flow flaws.

Module 2: Cloud-Native & Infrastructure-as-Code Modeling

- Modeling Cloud Service Provider Components
- IaC Threat Modeling with tools like Checkmarx KICS and Terraform Security.
- Securing Container Architectures and Kubernetes components
- Threat Modeling for Serverless Functions and API Gateways.
- Case Study: Modeling an EKS/AKS cluster's attack surface, focusing on Container Escape and IaC misconfigurations.

Module 3: Adversary-Centric Modeling with MITRE ATT&CK

- Introduction to the MITRE ATT&CK Cloud Matrix and its application.
- Mapping Adversary Tactics, Techniques, and Procedures to Cloud Infrastructure.
- Developing Attack Trees and Cyber Kill Chains specific to cloud environments.
- Creating realistic Threat Actor Personas and their cloud objectives.
- Case Study: Simulating an APT attack chain using the MITRE ATT&CK Cloud Matrix targeting a high-value S3 bucket or Azure Storage account.

Module 4: Identity and Access Management Threat Modeling

- Modeling Cloud IAM Roles, Policies, and Privilege Escalation vectors
- Advanced threats to Federated Identity and Single Sign-On in the cloud.
- Securing Service Accounts and machine-to-machine communication.
- Applying the Principle of Least Privilege and validating its implementation.
- Case Study: Modeling a "Confused Deputy" attack scenario involving cross-service/account IAM delegation.

Module 5: Data Security & Storage Threat Modeling

- Modeling threats to Data at Rest and Data in Transit
- Threats related to Encryption Key Management and HSM services
- Securing Cloud Databases against exfiltration and unauthorized access.
- Addressing risks from Public Access Misconfigurations and unauthenticated endpoints.
- Case Study: Modeling data exfiltration from an AWS S3 bucket and identifying the necessary preventative and detective controls.

Module 6: Network and Perimeter Threat Modeling

- Modeling Virtual Private Cloud (VPC)/VNet, Subnet, and Network Access Control List boundaries.
- Threats against Cloud Firewalls, Security Groups, and WAFs.
- Advanced modeling of Cloud Load Balancers and DDoS attack vectors.
- Analyzing Ingress/Egress Traffic flows and potential for data tunneling.
- Case Study: Decomposing a multi-region cloud network architecture and modeling the impact of a compromised jump box on network segmentation.

Module 7: Zero Trust Architecture (ZTA) Modeling

- Integrating Zero Trust Principles into Cloud Design.
- Modeling the Policy Enforcement Point and Policy Decision Point in the cloud.
- Threat modeling for Microsegmentation and dynamic access control.
- Validating ZTA controls against Insider Threat and Lateral Movement scenarios.
- Case Study: Designing and threat modeling a full Zero Trust deployment for a microservices application using Istio/Service Mesh.

Module 8: Continuous Threat Modeling & DevSecOps

- Embedding threat modeling into the CI/CD Pipeline
- Practicing Threat Modeling as Code for automated model updates.
- Integrating TM tools with Issue Trackers and Source Control
- Automating threat discovery using security tools and Threat Intelligence Feeds.
- Case Study: Implementing a fully automated check in a GitHub/GitLab pipeline that fails the build if a critical threat is introduced via an IaC change.

Module 9: Advanced Risk Prioritization and Mitigation

- In-depth Risk Scoring methodologies
- Mapping identified threats to Security Controls
- Developing an effective Mitigation Roadmap and communicating risk to stakeholders.
- Post-Mitigation: Validation and Verification of security controls
- Case Study: Prioritizing the top 5 risks for a new financial service cloud application and presenting the mitigation strategy to executive leadership.

Module 10: Multi-Cloud and Hybrid Cloud Threat Modeling

- Addressing unique threats in Hybrid Cloud and multi-cloud environments
- Modeling Cloud Interoperability and Trust Relationships between CSPs.
- Securing Cloud Brokerage and third-party SaaS/PaaS integrations.
- Addressing Cross-Cloud Identity and data flow consistency challenges.
- Case Study: Modeling a critical data pipeline that spans AWS SQS and Azure Service Bus, identifying potential cross-cloud data tampering threats.

Module 11: Insider and Supply Chain Threat Modeling

- Modeling Insider Threats in the context of high-privileged cloud accounts.
- Threats originating from the Software Supply Chain
- Securing the Build Process and container image integrity
- Modeling risks from Third-Party Vendors and managed cloud services.
- Case Study: Analyzing a compromised dependency in a container image and modeling the blast radius on the production cloud environment.

Module 12: Compliance, Governance, and Scalability

- Aligning Threat Modeling with Regulatory Compliance
- Developing a Threat Modeling Governance framework and a Bug Bar for cloud projects.
- Scaling the practice across large Agile development teams and multiple products.
- Measuring the Return on Investment of a mature threat modeling program.

- Case Study: Developing a standardized threat model template and checklist for a new business unit to ensure regulatory compliance from the start.

Module 13: Advanced Cloud Security Posture Management (CSPM) Integration

- Threat modeling for Cloud Security Posture Management tools and findings.
- Automating the correlation of threat models with Cloud Asset Inventory.
- Leveraging threat models to fine-tune Detection and Response rules
- Modeling configuration drift and ensuring security controls remain effective.
- Case Study: Using a CSPM tool's output as a starting point for an on-the-fly threat model.

Module 14: Practical Tools and Automation

- Hands-on with OWASP Threat Dragon and similar open-source tools.
- Utilizing Microsoft Threat Modeling Tool for large-scale enterprise models.
- Exploring commercial solutions like IriusRisk and ThreatModeler for automation.
- Leveraging Generative AI/LLMs for initial threat identification and DFD generation.
- Case Study: Conducting a live, hands-on threat modeling session for a sample GCP Microservices architecture using a collaborative tool.

Module 15: Future of Cloud Threat Modeling

- Modeling threats in emerging areas.
- Securing AI/ML Workloads and model integrity in the cloud.
- The role of Software Composition Analysis in identifying supply chain threats during modeling.
- Integrating Breach and Attack Simulation with threat model validation.
- Case Study: Modeling the potential for Data Poisoning or Model Evasion attacks against a cloud-hosted AI inference service.

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
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