QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1937

Zero Trust Identity & Access Security Training Course

IDENTITY & ACCESS MANAGEMENT
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Zero Trust Identity & Access Security Training Course provides a comprehensive and practical framework for designing, implementing, and managing identity and access security within a Zero Trust security architecture. The course focuses on the principle of continuously verifying users, devices, applications, and access requests rather than relying on traditional perimeter-based security models.

Participants will explore the strategic role of identity as a core security control and examine authentication, authorization, identity lifecycle management, privileged access, adaptive access policies, multi-factor authentication, device trust, application access, and continuous monitoring. The program emphasizes how identity-centric security can reduce unauthorized access, credential-based attacks, lateral movement, and excessive privileges.

The course addresses practical Zero Trust implementation across cloud, hybrid, on-premises, remote, and distributed environments. Participants will learn how to assess identity risks, establish appropriate access controls, apply least-privilege principles, strengthen privileged identities, and integrate identity security with endpoint, application, data, and network security controls.

Through practical scenarios, architecture exercises, security assessments, access-control simulations, and incident-based case studies, participants will develop the capability to build identity and access security strategies aligned with Zero Trust principles. The course also addresses governance, monitoring, risk management, compliance, identity threat detection, and continuous improvement.

Objectives

- By the end of the course, participants will be able to:
- Analyze the principles and security objectives of Zero Trust identity and access security.
- Assess identity-related risks across users, devices, applications, and organizational resources.
- Design identity-centric security controls based on Zero Trust principles.
- Apply least-privilege and need-to-know access models.
- Strengthen authentication and authorization mechanisms.

- Implement multi-factor and risk-based authentication approaches.
- Develop effective identity lifecycle management processes.
- Protect privileged accounts and administrative identities.
- Design adaptive access policies based on identity, device, location, behavior, and risk.
- Integrate identity security with cloud, endpoint, application, network, and data security.
- Detect and respond to identity-based threats and suspicious access activities.
- Establish identity governance, monitoring, and access review mechanisms.
- Evaluate Zero Trust identity architectures and identify security gaps.
- Develop practical implementation priorities and security roadmaps.
- Establish metrics for measuring identity and access security effectiveness.

Who Should Attend

This course is designed for cybersecurity managers, information security professionals, identity and access administrators, security architects, infrastructure managers, IT managers, network and systems administrators, cloud security professionals, and technology specialists responsible for protecting organizational identities and access.

It is also suitable for risk and compliance professionals, security governance teams, internal auditors, enterprise architects, security operations personnel, cloud administrators, and technical decision-makers involved in Zero Trust, identity security, access governance, or cybersecurity transformation initiatives.

The course is particularly valuable for organizations operating hybrid and cloud environments, supporting remote workforces, managing privileged access, or seeking to strengthen protection against credential theft, unauthorized access, insider threats, and identity-based attacks.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the core principles of Zero Trust architecture and identity-centric security.
- Map identities, resources, applications, devices, and access relationships.
- Assess identity and access risks using structured risk-based approaches.

- Design secure authentication and authorization architectures.
- Apply least-privilege principles across organizational environments.
- Configure and evaluate multi-factor and adaptive authentication strategies.
- Establish effective identity lifecycle and access provisioning processes.
- Implement stronger controls for privileged and high-risk identities.
- Design conditional access policies based on contextual risk.
- Integrate identity controls with endpoint, cloud, application, network, and data security.
- Identify indicators of identity compromise and suspicious access behavior.
- Support identity-related incident detection, investigation, and response.
- Establish access review, governance, monitoring, and audit mechanisms.
- Evaluate Zero Trust maturity and identify opportunities for improvement.
- Develop a phased roadmap for implementing Zero Trust identity and access security.
- Define meaningful security metrics and performance indicators.

Course Outline

DAY 01

Zero Trust Principles and Identity-Centric Security

- Evolution from perimeter-based security to Zero Trust.
- Core principles and security objectives of Zero Trust.
- Identity as a primary security control.
- Users, devices, applications, workloads, and resources as security entities.
- Continuous verification and explicit trust decisions.
- Least privilege and need-to-know access.
- Identity threats and credential-based attacks.
- Identity attack surfaces in cloud and hybrid environments.
- Mapping identities, resources, and access relationships.
- Assessing organizational readiness for Zero Trust identity security.

DAY 01 — CONTINUED

> **PRACTICAL APPLICATION**
>
> Conduct a Zero Trust identity security assessment for a representative hybrid organization and identify major identity risks and security gaps.

DAY 02

Authentication, Authorization, and Adaptive Access

- Authentication and authorization fundamentals.
- Password security and credential protection.
- Multi-factor authentication strategies.
- Strong authentication and phishing-resistant approaches.
- Single sign-on and federated identity concepts.
- Role-based and attribute-based access control.
- Conditional and risk-based access decisions.
- Device identity and device trust.
- Context-aware access based on identity, device, location, behavior, and risk.
- Designing secure access policies for high-risk scenarios.

> **PRACTICAL APPLICATION**
>
> Design an adaptive access-control framework for employees, administrators, contractors, and remote users with different levels of security risk.

DAY 03

Identity Lifecycle, Privileged Access, and Access Governance

- Identity lifecycle management from onboarding to offboarding.
- Identity provisioning and deprovisioning.
- Joiner, mover, and leaver processes.
- Role management and access entitlement design.
- Least-privilege implementation.
- Privileged account security.

DAY 03 — CONTINUED

- Administrative identity protection.
- Privileged access management principles.
- Periodic access reviews and entitlement certification.
- Segregation of duties and excessive privilege risks.
- Identity governance and accountability.

PRACTICAL APPLICATION

Develop an identity lifecycle and privileged access model that reduces excessive privileges and improves control over administrative accounts.

DAY 04

Zero Trust Integration, Monitoring, and Identity Threat Detection

- Integrating identity security with endpoint protection.
- Cloud and application access security.
- Network and data security integration.
- Identity telemetry and security monitoring.
- Detecting anomalous authentication and access behavior.
- Credential theft and account compromise scenarios.
- Identity-based lateral movement.
- Insider and compromised-account risks.
- Investigation and response to suspicious identity activity.
- Security automation and continuous verification.
- Strengthening identity resilience and recovery capabilities.

PRACTICAL APPLICATION

Analyze a simulated identity compromise involving suspicious authentication, privilege escalation, and unauthorized resource access, then develop an investigation and response plan.

DAY 05

Zero Trust Identity Architecture, Governance, and Implementation

- Designing an enterprise Zero Trust identity architecture.
- Integrating identity security across hybrid and multi-cloud environments.
- Identity governance and security policies.
- Security standards, controls, and compliance considerations.
- Continuous access evaluation and monitoring.
- Measuring Zero Trust identity security maturity.
- Key performance and security indicators.
- Identifying implementation gaps and technology dependencies.
- Prioritizing security initiatives according to risk and business impact.
- Building a phased Zero Trust implementation roadmap.
- Continuous improvement and security optimization.

FINAL WORKSHOP

Design an integrated Zero Trust Identity & Access Security Strategy covering identity architecture, authentication, authorization, least privilege, privileged access, adaptive access, identity lifecycle management, monitoring, threat detection, governance, maturity assessment, security metrics, priorities, and an implementation roadmap.

Register or Request More Information

Course page: https://quest-training.com/courses/zero-trust-identity-access-security-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440