QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1939

Privileged Access Management (PAM) & Identity Security Training Course

IDENTITY & ACCESS MANAGEMENT
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

Privileged Access Management (PAM) & Identity Security Training Course provides a comprehensive and practical framework for protecting privileged identities, administrative accounts, and high-risk access across modern enterprise environments. The course focuses on reducing the security risks associated with excessive privileges, compromised administrative credentials, unauthorized administrative activity, and uncontrolled access to critical systems and data.

Participants will examine the role of privileged access management as a core component of enterprise identity security and Zero Trust architectures. The program covers privileged account discovery, classification, credential protection, password vaulting, session management, just-in-time access, least privilege, privileged elevation, access approval, monitoring, and auditing.

The course addresses privileged access across on-premises infrastructure, cloud environments, databases, applications, network devices, endpoints, and hybrid technology ecosystems. Participants will learn how to identify privileged accounts and service identities, establish appropriate controls, manage emergency access, and strengthen administrative workflows without unnecessarily disrupting legitimate business operations.

Through architecture exercises, privileged access assessments, attack scenarios, access-control simulations, and practical governance workshops, participants will develop the ability to design and improve PAM programs aligned with organizational risk, cybersecurity requirements, compliance expectations, and Zero Trust principles.

Objectives

- By the end of the course, participants will be able to:
- Analyze the role of privileged access management in enterprise identity security.
- Identify and classify privileged accounts, identities, credentials, and access pathways.
- Assess risks associated with privileged accounts and administrative access.
- Design a comprehensive PAM strategy aligned with organizational security objectives.
- Apply least-privilege and just-in-time access principles.
- Establish secure privileged credential management and password vaulting practices.

- Design effective privileged access request, approval, and provisioning processes.
- Implement controls for privileged session monitoring and recording.
- Strengthen protection of service accounts, machine identities, and non-human identities.
- Manage privileged access across cloud, hybrid, on-premises, and remote environments.
- Detect suspicious privileged activity and indicators of credential compromise.
- Establish emergency and break-glass access controls.
- Develop PAM governance, policies, standards, and accountability mechanisms.
- Define metrics for measuring privileged access security and control effectiveness.
- Develop a practical roadmap for implementing and continuously improving PAM capabilities.

Who Should Attend

This course is designed for cybersecurity professionals, identity and access management specialists, security architects, IT managers, infrastructure managers, systems administrators, network administrators, cloud security professionals, and technology specialists responsible for administrative access and enterprise security.

It is also highly relevant for security operations teams, risk and compliance professionals, internal auditors, governance specialists, enterprise architects, privileged account administrators, and decision-makers responsible for identity security, access governance, cybersecurity transformation, or Zero Trust initiatives.

The course is particularly valuable for organizations seeking to reduce the risk of credential theft, privilege escalation, insider threats, unauthorized administrative activity, and compromise of critical systems.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the principles and architecture of privileged access management.
- Identify privileged identities and high-risk access pathways across an enterprise.
- Conduct a structured privileged access risk assessment.
- Classify privileged accounts according to risk, business function, and level of access.

- Design least-privilege and just-in-time access models.
- Apply secure credential storage, rotation, and management practices.
- Establish effective privileged access request and approval workflows.
- Implement privileged session monitoring and audit mechanisms.
- Protect service accounts and non-human privileged identities.
- Manage privileged access across cloud and hybrid environments.
- Detect and investigate suspicious privileged activity.
- Design emergency access and break-glass procedures.
- Establish PAM governance, policies, standards, and accountability.
- Develop PAM security metrics and management reporting.
- Assess PAM maturity and identify control gaps.
- Develop a phased PAM implementation and improvement roadmap.

Course Outline

DAY 01

Privileged Access Risks and Identity Security Foundations

- Understanding privileged access and administrative identities.
- The relationship between PAM, IAM, cybersecurity, and Zero Trust.
- Privileged accounts and enterprise attack surfaces.
- Types of privileged identities and access.
- Human, service, application, machine, and cloud privileged identities.
- Privilege escalation and credential theft risks.
- Insider threats and unauthorized administrative activity.
- Identifying critical systems and high-risk access pathways.
- Privileged access discovery and inventory.
- Assessing privileged access security maturity.

PRACTICAL APPLICATION

Conduct a privileged access assessment for a representative enterprise and identify high-risk identities, systems, and access pathways.

DAY 02

Privileged Credential Management and Least Privilege

- Principles of least privilege.
- Privileged account classification and risk prioritization.
- Credential protection and secure password management.
- Password vaulting and credential rotation.
- Managing shared and generic administrative accounts.
- Just-in-time and time-bound privileged access.
- Privilege elevation and controlled administrative access.
- Access request and approval workflows.
- Reducing standing administrative privileges.
- Managing privileged access exceptions.
- Aligning privileged access with business requirements.

> **PRACTICAL APPLICATION**
>
> Design a privileged credential management model covering discovery, classification, vaulting, rotation, approval, elevation, and access termination.

DAY 03

Privileged Access Architecture and Technology Controls

- Enterprise PAM architecture and core components.
- Privileged account discovery and onboarding.
- Credential vaults and secure repositories.
- Privileged session management.
- Session recording and monitoring.
- Application and database privileged access.
- Network device and infrastructure administration.
- Endpoint and server privileged access.
- Cloud and hybrid privileged access.
- Service accounts and machine identities.

DAY 03 — CONTINUED

- Integrating PAM with enterprise identity platforms and security operations.

PRACTICAL APPLICATION

Design a PAM architecture for a hybrid enterprise environment covering servers, databases, network devices, cloud platforms, applications, endpoints, and administrative users.

DAY 04

Monitoring, Threat Detection, and Incident Response

- Monitoring privileged access activities.
- Identifying abnormal administrative behavior.
- Detecting compromised privileged credentials.
- Privilege escalation indicators.
- Suspicious sessions and unauthorized access patterns.
- User and entity behavior analysis for privileged activity.
- Security event correlation and investigation.
- Responding to privileged account compromise.
- Emergency access and break-glass procedures.
- Revoking and recovering compromised privileged access.
- Integrating PAM monitoring with security operations and incident response.

PRACTICAL APPLICATION

Investigate a simulated privileged account compromise involving credential theft, unauthorized elevation, suspicious administrative sessions, and access to critical systems.

DAY 05

PAM Governance, Compliance, Measurement, and Implementation

- Developing PAM governance frameworks.
- Defining ownership, responsibilities, and accountability.
- PAM policies, standards, procedures, and access rules.

DAY 05 — CONTINUED

- Access certification and privileged account reviews.
- Segregation of duties and administrative controls.
- Audit evidence and compliance requirements.
- PAM risk indicators and performance metrics.
- Measuring control effectiveness and maturity.
- Building the PAM target operating model.
- Prioritizing PAM initiatives based on risk and business impact.
- Managing implementation risks and organizational change.
- Continuous improvement and PAM optimization.

FINAL WORKSHOP

Develop an integrated Privileged Access Management & Identity Security Strategy covering privileged identity discovery, risk assessment, least privilege, credential protection, just-in-time access, privileged sessions, cloud and hybrid access, monitoring, incident response, governance, compliance, performance measurement, maturity assessment, and an implementation roadmap.

Register or Request More Information

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