Hashicorp PAM Training

Curriculum 5 Days

Day - 1

- **Introduction to Modern PAM**
  - Traditional PAM vs Modern PAM approaches
  - Zero Trust principles and Least Privilege Access
  - Overview of HashiCorp PAM Architecture (Boundary + Vault)
  - Key use cases: Cloud, Hybrid, and On-Prem environments

- **HashiCorp Vault Essentials**
  - Vault architecture and components (Core, Storage, Seal/Unseal, Policies)
  - Types of secrets (Static vs Dynamic)
  - Authentication methods overview (Token, AppRole, Kubernetes, AWS IAM)
  - Vault deployment options (OSS, Enterprise, Cloud)

- **HashiCorp Boundary Essentials**
  - Boundary architecture (Controllers, Workers, Targets)
  - Identity-based access vs network-based access
  - Session brokering and credential injection
  - Deployment models (OSS, Enterprise)

- **Hands-On Lab**
  - Install and configure Vault in dev mode
  - Install Boundary and connect to a demo environment
  - Create simple static secrets in Vault
  - Create basic user and target in Boundary

Day - 2

- **Vault Setup for Secure Secrets Management**
  - Initializing and unsealing Vault securely
  - Configuring persistent storage backends
  - Creating and managing policies (HCL)
  - Enabling authentication methods (LDAP, Kubernetes, AWS IAM)
  - Setting up Audit devices for compliance

- **Dynamic Secrets & Credential Management**
  - Configuring Vault database secret engine (PostgreSQL/MySQL)
  - Generating ephemeral SSH credentials
  - Secrets leasing, TTLs, and revocation
  - Integrating Vault with PKI for certificate issuance

- **Hands-On Lab**
  - Deploy Vault in HA mode (using Consul or integrated storage)
  - Configure AppRole and AWS IAM Auth methods
  - Create dynamic database credentials
  - Configure SSH secrets engine for just-in-time SSH keys

Day - 3

- **Boundary Setup and Access Control**
  - Installing and configuring Boundary controllers and workers
  - Configuring identity providers (OIDC, LDAP, SSO)
  - Defining scopes, roles, grants, and sessions
  - Creating targets (SSH, RDP, Kubernetes, Database)

- **Integrating Boundary with Vault**
  - Enabling Vault credential injection
  - Setting up Boundary to use dynamic Vault credentials
  - Session logging and auditing
  - Implementing just-in-time access workflows

- **Hands-On Lab**
  - Configure Boundary with OIDC (Okta/Azure AD)
  - Create roles, grants, and targets for SSH and RDP access
  - Integrate Boundary with Vault to inject dynamic database credentials
  - Record and review a full user session

Day - 4

- **Advanced Vault Use Cases**
  - Using Vault as Encryption-as-a-Service (EaaS)
  - Vault Agent and Auto-Auth for applications
  - Using Vault for Kubernetes secret injection
  - Enterprise features (namespaces, replication, Sentinel policies)

- **Advanced Boundary Use Cases**
  - Scaling Boundary with multiple workers
  - Boundary Enterprise features (Session Recording, RBAC enhancements)
  - Integrating Boundary with service discovery and Terraform
  - Designing multi-cloud PAM architecture

- **Hands-On Lab**
  - Configure Vault Transit engine for data encryption
  - Deploy Vault + Boundary in Kubernetes
  - Automate Boundary target and role creation with Terraform
  - Record an SSH session with session replay

Day - 5

- **Security Hardening**
    - Vault hardening (Seal/Unseal strategies, Shamir keys, HSM)
    - Boundary hardening (Network segmentation, TLS, Worker security)
    - Rotating keys and secrets automatically
    - Implementing RBAC and policy-as-code

- **Enterprise PAM Integration**
    - Integrating with SIEM and audit systems
    - Incident response with Vault and Boundary
    - Migrating from legacy PAM to HashiCorp PAM
    - Designing HA, DR, and multi-region PAM setups

- **Capstone Project**
    - Design and implement a full PAM solution using Vault + Boundary
    - Secure SSH and database access with just-in-time credentials
    - Enforce identity-based access via SSO
    - Configure complete audit logging and session recording

- **Hands-On Lab**
    - Build a production-grade HashiCorp PAM architecture
    - Test access workflows for admins, developers, and auditors
    - Simulate secret rotation and emergency access scenarios