OKTA Advanced Security

Duration: 2 days (8hrs/day)

Prerequisites: Okta Essentials or minimum experience in Okta.

Course Objective: Learn how to use Okta to create a Zero Trust environment in a landscape where people are the new perimeter. This hands-on course is full of tips for expanding your security footprint with Okta.

Lab Requirement: Koening DC

Module 1 - Zero Trust: Past, Present, and Future

Learn about Zero Trust

Understand Shared Responsibility

Apply Standards to Manage Risk

Module 2 - Protect Cloud Access with Okta's Adaptive MFA

Configure Network Zones

Configure an Okta Sign-On Policy

Configure an Application Sign-On Policy

Module 3 - Move Beyond Passwords with Contextual Access Management

Review and Reduce Attack Surface

Implement Passwordless Authentication

Learn about WebAuthn and DSSO

Module 4 - Implement Risk Based Access

Learn about risk scoring

Configure Behavior Detection

Module 5 - Deploy Managed Devices

Understand Device Trust with Okta Verify

Configure Managed Devices

Module 6 – Configure Role-based Administrators

Determine the least privileges required for an admin

Configure administrators for various common roles

Module 7 – Explore the Okta System Log and Configure Log Forwarding

Export Log Data

Understand SIEM Integrations

Module 8 – Monitor your Okta Components

Explore Okta HealthInsight and ThreatInsight

Learn about monitoring agents, appliances, and related tenants

Module 9 – Streamline Your Path to Compliance

Learn about Okta Workflows for compliance

Implement and Enforce Lifecycle Automation

Learn about compliance standards