Elastic Security for SIEM

Duration: 3 days (8 hrs/day)

Version: Elasticsearch 9.x

Lab Requirement: 3-node Cluster (Centos 10)

Prerequisites

- Basic networking knowledge
- Common Network Monitoring Tools
- Understanding of logs and security concepts
- Familiarity with Linux/Windows

Course Objectives

This course is built for analysts who utilize Elastic Security for SIEM solutions. Elastic Security for SIEM walks you through the architecture behind the Elastic Stack, Fleet, and Elastic Agent. You will then learn how to create visualizations and dashboards and how to use Lens before diving into the Security App. Finally, you will conduct a threat hunting capstone exercise to tie everything together.

Module 1: Elastic Stack Overview

Lesson 1: Introduction to Elastic Stack

- Overview of Elastic Stack Components
- Elasticsearch, Kibana, Logstash, Beats
- SIEM fundamentals and use cases
- Security analytics overview

Lesson 2: Architecture & Data Flow

- Elastic Stack architecture
- Data ingestion pipeline
- Data sources for security use cases
- Indexing and storage concepts

Lesson 3: Fleet and Elastic Agent

- Fleet architecture and components
- Elastic Agent installation and configuration
- Managing integrations at scale
- Data collection strategies

Lab:

- Explore Elastic Stack components
- Install and configure Elastic Agent

Module 2: Elastic Common Schema (ECS)

Lesson 1: ECS Fundamentals

- Purpose of ECS
- Normalization of security data
- Field structure and naming conventions

Lesson 2: Working with ECS Data

- Mapping data to ECS
- ECS in security analytics
- Best practices

Lab:

- Normalize sample data using ECS

Module 3: Data Exploration with Discover

Lesson 1: Discover Interface

- Navigating Kibana Discover
- Searching and filtering data
- Querying with KQL

Lesson 2: Data Analysis

- Field analysis
- Time-based exploration
- Saving searches

Lab:

- Investigate logs using Discover

Module 4: Visualizations

Lesson 1: Visualization Basics

- Types of visualizations
- Creating charts and graphs
- Aggregations

Lesson 2: Advanced Visualizations

- Custom visualizations
- Filtering and drilldowns
- Visualization best practices

Lab:

- Create security-focused visualizations

Module 5: Kibana Lens

Lesson 1: Introduction to Lens

- Drag-and-drop analytics
- Creating quick visualizations

Lesson 2: Advanced Lens Usage

- Combining datasets
- Advanced metrics and formulas
- Time series analysis

Lab:

- Build visualizations using Lens

Module 6: Dashboards

Lesson 1: Dashboard Creation

- Building dashboards
- Adding visualizations
- Layout and customization

Lesson 2: Dashboard Analysis

- Interactive dashboards
- Filters and controls
- Sharing dashboards

Lab:

- Create a SIEM dashboard

Module 7: Elastic Security App

Lesson 1: Security App Overview

- SIEM interface in Kibana
- Hosts, Network, Users views

- Security workflows

Lesson 2: Detection & Alerts

- Detection rules
- Alerts and case management
- Rule tuning

Lesson 3: Threat Hunting

- Investigating security events
- Timeline analysis
- Correlation techniques

Lesson 4: AI & Advanced Capabilities

- AI-driven workflows
- Attack discovery
- Security analytics

Lab:

- Detect and investigate threats

Module 8: Capstone Exercise

Lesson 1: End-to-End SIEM Implementation

- Data ingestion setup
- Visualization and dashboards
- Detection configuration

Lesson 2: Threat Hunting Scenario

- Real-world attack simulation
- Investigation workflow
- Incident response

Lab:

- Perform full threat hunting exercise