Powering Security Operations with Cisco XDR (ESOXDR)

Modality: Virtual Classroom

Duration: 3 Days

CLC: 30 Units

About this Course:

The Powering Security Operations with Cisco XDR (ESOXDR) 3-day training guides you through the main aspects and challenges of traditional SOC. You will learn the Cisco XDR security platform and how it can simplify security operations in today's hybrid, multi-vendor, multi-threat landscape. Overview of all the main integration possibilities and components, including APIs discovery, Endpoint and Network Telemetry and ITSM, SIEM systems, and Public Cloud. Through expert instruction and hands-on lab exercises, you will learn how to read the components and work with Incident Manager for effective threat prioritization, streamlined investigations, and evidence-backed recommendations. In this training, you will discover how to elevate productivity with automation capabilities and boost your security resources for optimal value.

Course Objectives:

- Understand the architecture of Cisco Secure Client/XDR.
- Understand the Identification, Containment, Eradication, and Recovery Workflows.
- Understand the XDR Remote Connector and how to accomplish arbitrary integrations.
- Learn how to create automation using Automation APIs.
- Recognize the types and sequence of Orchestration Workflows.
- Understand the fundamentals of working with Public Cloud through XDR Orchestration.
- Explain how to initiate Cisco XDR investigations from Splunk.

Audience:

- Cisco integrators, resellers, and partners
- Network administrators
- Security administrators
- Security consultants
- Systems engineers
- Cybersecurity engineers
- Cybersecurity investigators
- SOC analysts
- Network design engineers
- Solution architects

Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- Working knowledge of the Windows and Linux operating systems.
- Familiarity with basics of networking security concepts.
- Technical understanding of TCP/IP networking and network architecture.
- Technical understanding of security concepts and protocols.

The recommended Cisco offering may help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

Course Outline:

Module 1: Evolution and Introduction to Cisco XDR

- Lesson 1: Detection and Response and the challenges of traditional SOC
- Lesson 2: What is the OODA loop?
- Lesson 3: Overview of Cisco XDR
- High-level Architecture
- Associating SOC profiles to XDR
- Integrations and Response
- XDR/EDR/MDR/SOAR/SIEM – Shared Use cases
- Analytics and Correlation Engine

Module 2: Threat Detection and Incident Response Workflow

- Lesson 1: Understanding Threat Detections with Diverse Intelligence
- Lesson 2: How to read components: Judgement / Indicators / Feeds / Events
- Lesson 3: Cisco XDR: Incident Manager
- Threat inspection captured Incidents
- Infrastructure-based Incident Prioritization: Detection Risk and Asset Value
- MITRE
- Correlated pictorial representation of the threat summary
- Severity Management based on Event types
- Identification/Containment/Eradication and Recovery Workflows

Module 3: Enrichment from Third-Party Integrations

- Lesson 1: Overview of the third-party security landscape
- Lesson 2: Built-in Integrations
- EDR: Crowdstrike, Sentinel One, MSFT Defender, and more...
- NDR: Dark Trace, Extrahop, and more...
- Lesson 3: What is a Relay Module?
- Lesson 4: XDR: Remote Connector
- Lesson 5: Accomplishing arbitrary integrations

Module 4: XDR APIs

- Lesson 1: Northbound and Southbound APIs
- Lesson 2: Threat Intelligence APIs: Private and public databases of threat intel

- Lesson 3: Investigation APIs: Enrich data using your integrated products
- Lesson 4: Response APIs
- Lesson 5: OAuth APIs: Use credentials and get access tokens
- Lesson 6: Automation APIs: Trigger workflows in XDR to do just about anything you want!

Module 5: XDR Automation and Orchestration

- Lesson 1: Understanding Orchestration Workflows: Types and sequence
- Lesson 2: Workflows Components: Targets, Account Keys, Triggers, Variables, Events, Schedules & Reports
- Lesson 3: Constructing a basic workflow
- Lesson 4: Exploring built in cisco and third-party service activities and logics
- Lesson 5: Customizing out of the box workflows to fit the business use case
- Lesson 6: Nesting workflows
- Lesson 7: Using Microsoft APIs to investigate/detect suspicious email with Cisco Secure Email
- Lesson 8: Enforcing DLP policy on outgoing email using Cisco XDR automation

Module 6: Endpoint and Network Telemetry

- Lesson 1: Network and Endpoint Visibility Together: Telemetry + Device Insights
- Lesson 2: Network Visibility Module
- Lesson 3: Cisco Secure Client/XDR: Architecture
- Lesson 4: Reports and Audit logs
- Lesson 5: Asset Tag Device Management

Module 7: Cisco XDR with ITSM, SIEM systems and Public Cloud

- Lesson 1: Overview translation of Splunk CIM to XDR CTIM
- Lesson 2: Initiating Cisco XDR investigation from Splunk
- Lesson 3: Splunk and Cisco XDR Webhooks or Atomic Actions
- Lesson 4: Overview of Cisco XDR and Service Now Integration
- Lesson 5: Adding Context to ServiceNow incident – Using XDR Automate
- Lesson 6: Fundamentals of working with Public Cloud with XDR Orchestration

---

Lab Outline:

Labs are designed to assure learners a whole practical experience, through the following practical activities:

- Accessing Cisco XDR
- Overview of Cisco XDR
- Validate an Attack and Determine the Incident Response
- Perform Threat Hunting
- Discover Third Party integrations
- Query and Recognize XDR API
- Explore Cisco XDR Orchestration
- Evaluate Assets in a Typical Enterprise Environment

- Work with Endpoint and Network Telemetry
- Explain how to initiate Cisco XDR investigations from Splunk
- Explore the integration of Splunk and Cisco XDR through Webhooks or Atomic Actions