PALO ALTO NETWORKS: CORTEX XDR: SECURITY OPERATIONS AND INTEGRATION

Course Code: 842009

Designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and engineering roles, to use Cortex XDR

This 3-day instructor-led course provides in-depth training on Cortex XDR, Palo Alto Networks' powerful extended detection and response platform. You will gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments.

The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop workflows, manage indicators, and optimize dashboards for enhanced security operations.

What You'll Learn

- Describe the role of Cortex XDR components, including endpoint agents, XDR collectors, NGFWs, and Broker VMs, in securing networks and devices.
- Utilize XQL to query and analyze logs for effective data ingestion and threat detection.
- Design and implement workflows to streamline security operations.
- Apply External Dynamic Lists and indicator rules to enforce security policies.

Who Needs to Attend

- SOC/CERT/CSIRT/XDR engineers and managers
- MSSPs and service delivery partners/system integrators
- Security consultants and sales engineers.

Prerequisites

- Attendees should possess a solid understanding of cybersecurity principles, including network and endpoint security concepts.

PALO ALTO NETWORKS: CORTEX XDR: SECURITY OPERATIONS AND INTEGRATION

Course Code: 842009

VIRTUAL CLASSROOM LIVE	$3,000 USD	3 Day

Virtual Classroom Live Outline

Course Modules

1. Course Overview
2. Overview of Cortex XDR
3. Software Components
4. Integrations
5. XQL
6. Detection Engineering
7. System Optimization
8. Dashboards and Reports

Feb 2 - 4, 2026 | 8:30 AM - 4:30 PM EST

Apr 13 - 15, 2026 | 8:30 AM - 4:30 PM EDT

Jul 13 - 15, 2026 | 8:30 AM - 4:30 PM EDT

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.