COURSE TABLE OF CONTENTS

Cortex Security Operations Professional Training

OEM: Palo Alto • Duration: 5 Days (40 hrs) • Code: PCSOP

COURSE MODULES & TOPICS

Domain 1: Security Operations Fundamentals (25%)

- Users, Roles, Log Management, Compliance, and Data Protection in Cortex XDR
- Reports and Dashboards
- SOC Components: Roles, Tools/Technologies, and Analytics
- AI vs ML in Security Operations

Domain 2: Threat Intelligence and Incident Response (16%)

- NIST Incident Response Plan
- Incident Management and Response
- Role of Threat Intelligence
- Incident Categorization and Prioritization
- File, IP, Domain, and URL Indicators
- WildFire, Unit 42, and VirusTotal
- False Positive, False Negative, and True Positive
- Basic Threat Hunting

Domain 3: Cortex XDR (23%)

- Key Elements: Sensors, Log Stitching, Causality View, WildFire
- Detection/Response, Behavioral Analytics, Data Sources/Users/Artifacts/Assets
- Agent Management and Deployment
- Cortex XDR vs EDR Use Cases

Domain 4: Cortex XSOAR (16%)

- Marketplace
- Playbooks
- Third-Party Integration
- Indicators/Feeds in Threat Intelligence Management (TIM)
- War Room
- Incident Investigation
- Scripts vs Jobs

Domain 5: Cortex XSIAM (20%)

- Key Components: Sensors, Log Stitching, Automations/Integrations, Content Packs, Playbooks
- XSIAM Processes: Data Ingestion, Investigation Artifacts/Assets
- Threat Management/Detection/Response
- Threat Hunting and Investigation
- IOC, BIOC, and Correlations