Syntho Quest

CERTIFIED ALIEN VAULT SECURITY OPERATIONS ANALYST

COURSE

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

Duration: 45 days × 2 hrs/day = 90 hrs

Goal: Equip professionals with the skills to monitor, detect, analyze, and respond to security incidents using AlienVault USM.

Core Domains

1. **Introduction to SOC & AlienVault USM (10%)**
   - SOC concepts, roles, and responsibilities
   - AlienVault USM architecture: USM Appliance, USM Anywhere
   - Use cases: threat detection, incident response, compliance
2. **Asset Discovery & Inventory (10%)**
   - Network and host discovery
   - Asset inventory management and classification
   - Identifying critical assets for monitoring
3. **Log Collection & Event Correlation (15%)**
   - Onboarding log sources (Windows, Linux, network devices, cloud)
   - Event collection methods (agents, syslog, APIs)
   - Normalization and correlation for offense generation
4. **Threat Detection & Analysis (20%)**
   - Detection methods: IDS, behavioral monitoring, signature-based
   - Event triage and prioritization
   - Investigating anomalies, incidents, and potential breaches
5. **Vulnerability Assessment & Management (10%)**
   - Built-in vulnerability scanning in USM
   - Risk assessment and prioritization
   - Integration with threat intelligence feeds
6. **Threat Intelligence & OTX Integration (10%)**
   - AlienVault Open Threat Exchange (OTX)
   - Threat intelligence collection, enrichment, and correlation
   - Mapping indicators of compromise (IoCs)
7. **Incident Response & Workflow (15%)**
   - Incident investigation, containment, and response
   - Offense lifecycle management
   - Reporting incidents and documentation
8. **Reporting, Dashboards & Compliance (10%)**
   - Custom dashboards and visualizations
   - Automated and scheduled reporting
   - Compliance monitoring (PCI, ISO, GDPR)
9. **Administration & Tuning (10%)**
   - User roles, permissions, and authentication
   - Log source tuning, alarm thresholds, system health monitoring
   - Performance optimization and best practices

Business Associate: vivek
Email: contact@synthoquest.com
Mobile: +91-8333801638 (whats app)