Syntho Quest

CERTIFIED IBM QRADAR SIEM EXPERT

COURSE

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

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

Goal: Equip professionals with the knowledge and skills to monitor, detect, analyze, and respond to security events using QRadar SIEM.

Core Domains

1. **Introduction to SIEM & QRadar (10%)**
   - Overview of SIEM and its role in cybersecurity
   - QRadar architecture: Console, Event Processor, Flow Processor, DSMs
   - Use cases: threat detection, compliance, operational monitoring
2. **Event Collection & Log Sources (15%)**
   - Onboarding log sources (Windows, Linux, network devices, cloud)
   - Protocols: Syslog, SNMP, JDBC, API integrations
   - Device Support Modules (DSM) and log normalization
3. **QRadar Console & Navigation (10%)**
   - QRadar user interface: dashboards, offenses, and events
   - Navigation, filters, and search capabilities
   - Event vs flow views
4. **Offenses & Rules (20%)**
   - Offense creation and management
   - Rules engine: building and tuning custom rules
   - Event correlation, priority, and offense lifecycle
5. **Custom Searches & Ariel Query Language (AQL) (10%)**
   - Performing searches using AQL
   - Filtering, grouping, and aggregating events
   - Custom reporting using AQL
6. **Dashboards & Reporting (10%)**
   - Creating custom dashboards and visualizations
   - Scheduled and on-demand reporting
   - KPI & security metrics tracking
7. **Threat Intelligence & Integrations (15%)**
   - QRadar threat intelligence feeds
   - Integration with STIX/TAXII and other threat feeds
   - Mapping to MITRE ATT&CK and SIEM correlation
8. **Administration & Tuning (10%)**
   - User roles, permissions, and authentication
   - Data retention, index management, and log sources tuning
   - System health monitoring, performance tuning, and troubleshooting

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