Syntho Quest

CERTIFIED SPLUNK TOOL EXPERT

COURSE

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

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

Goal: Equip professionals with the skills to collect, search, analyze, and visualize machine data using Splunk for IT and cybersecurity operations.

Core Domains

1. **Introduction to Splunk (10%)**
   - Overview of Splunk platform and architecture
   - Use cases: IT monitoring, security monitoring, business analytics
   - Splunk components: Forwarders, Indexers, Search Heads
2. **Data Ingestion & Forwarding (15%)**
   - Installing and configuring forwarders
   - Data sources: logs, metrics, APIs, syslog
   - Indexing, parsing, and sourcetypes
3. **Search & Reporting (20%)**
   - Basic and advanced searches using SPL (Search Processing Language)
   - Filtering, transforming, and enriching events
   - Creating reports, alerts, and scheduled searches
4. **Dashboards & Visualizations (15%)**
   - Creating interactive dashboards
   - Panels, charts, maps, tables
   - Drill-downs and data visualizations
5. **Knowledge Objects & Field Extractions (10%)**
   - Event types, tags, lookups
   - Field extraction using regex and KV pairs
   - Calculated fields and workflow actions
6. **Security Use Cases with Splunk (15%)**
   - Monitoring for anomalies, threats, and suspicious activity
   - Security alerts and dashboards
   - Threat intelligence integration and correlation
7. **Splunk Enterprise Security (10%)**
   - Overview of Splunk ES app
   - Notable events, correlation searches, risk scoring
   - Incident review workflow
8. **Splunk Administration & Best Practices (5%)**
   - User roles, authentication, and access control
   - Index management and retention policies
   - Performance tuning and troubleshooting

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