multisoft
Systems

Splunk SIEM Security Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

Splunk SIEM Security Training by Multisoft Systems is designed to equip IT professionals, SOC analysts, and cybersecurity enthusiasts with in-depth knowledge of Splunk's powerful Security Information and Event Management (SIEM) capabilities. This comprehensive training covers the entire Splunk ecosystem, from data collection and indexing to search, correlation, and visualization.

Module 1: Introduction to Splunk security

- ✓ Understanding the fundamentals of Splunk security, details of traditional security threats, and describing correlation searches and the security data model

Module 2: Investigation & Monitoring

- ✓ How to monitor the dashboard and brief on each panel, investigating notable events with incident review dashboards, workflow investigation, and the relative action on the identified flow

Module 3: Investigations

- ✓ Deploying ES investigation timelines for managing, visualizing and coordinating incident investigations, using journals and timelines for documenting breach analysis, and efforts needed to mitigate issues

Module 4: Risk & Network Analysis

- ✓ Deploying risk analysis and identification, risk dashboard utilization, and how to manage risk scores for objects and users

Module 5: Web Intelligence

- ✓ Using HTTP category analysis, HTTP user agent analysis, analyzing a new domain, analyzing the traffic size for spotting new threats, and highlighting investigable events

Module 6: User Intelligence

- ✓ Accessing the anomaly dashboards for user role and access logs and understanding identity and asset concepts

Module 7: Threat Intelligence

- ✓ Monitoring malicious sites with the threat activity dashboard and inspecting the threat intelligence content with the threat artifact dashboard