multisoft
Systems

Open Source SIEM Tools 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

Open Source SIEM (Security Information and Event Management) Tools are crucial for organizations seeking to improve their cybersecurity posture without the hefty cost of proprietary solutions. This training program from Multisoft Systems provides a comprehensive introduction to these powerful, cost-effective tools used to monitor, detect, and respond to security incidents.

Module 1: Introduction to SIEM

- ✓ Overview of SIEM concepts and importance in cybersecurity
- ✓ How SIEMs fit into the overall security operations ecosystem
- ✓ Components of a SIEM system (Data collection, normalization, correlation, etc.)
- ✓ Differences between commercial and open-source SIEM solutions

Module 2: Overview of Open Source SIEM Tools

- ✓ Introduction to popular open-source SIEM tools
- ✓ OSSIM (Open-Source Security Information Management)
- ✓ ELK Stack (Elasticsearch, Logstash, Kibana)
- ✓ Wazuh
- ✓ Graylog
- ✓ SecurityOnion
- ✓ Key features and benefits of using open-source SIEM
- ✓ Challenges with open-source SIEM and how to overcome them

Module 3: Installing and Configuring OSSIM

- ✓ Installation of OSSIM on a virtual machine or physical hardware
- ✓ Basic configuration of OSSIM for data collection
- ✓ Integrating data sources (e.g., syslog, SNMP, etc.)
- ✓ Setting up and customizing alerts
- ✓ Dashboard and report generation

Module 4: ELK Stack (Elasticsearch, Logstash, Kibana)

- ✓ Overview of ELK components for SIEM
- ✓ Installation and configuration of Elasticsearch, Logstash, and Kibana
- ✓ Collecting and parsing logs with Logstash
- ✓ Using Elasticsearch for storing and searching log data
- ✓ Creating dashboards and visualizations in Kibana

- ✓ Integrating ELK Stack with other security tools

Module 5: Wazuh SIEM Setup and Configuration

- ✓ Introduction to Wazuh as a SIEM tool
- ✓ Installation and configuration of Wazuh manager and agents
- ✓ Integrating Wazuh with Elastic Stack for enhanced threat detection
- ✓ Using Wazuh for log analysis, threat hunting, and compliance monitoring
- ✓ Configuring rules and decoders for custom use cases

Module 6: Using Graylog for Security Event Management

- ✓ Introduction to Graylog's architecture and features
- ✓ Installation and configuration of Graylog server and agents
- ✓ Collecting and managing logs from various sources
- ✓ Setting up alerts and notification systems
- ✓ Analyzing logs and creating custom dashboards

Module 7: SecurityOnion Setup

- ✓ Introduction to SecurityOnion as an open-source security platform
- ✓ Installation and configuration of SecurityOnion for SIEM capabilities
- ✓ Configuring SecurityOnion for network monitoring (IDS/IPS)
- ✓ Integrating SecurityOnion with other open-source security tools
- ✓ Reviewing and analyzing alerts and events in SecurityOnion

Module 8: Threat Detection and Correlation in SIEM

- ✓ Understanding correlation rules and their role in threat detection
- ✓ Creating custom correlation rules across different open-source SIEM tools
- ✓ Real-world case studies of threat detection using open-source SIEM
- ✓ Incident response workflows and use of SIEM in investigations

Module 9: Advanced SIEM Features and Techniques

- ✓ Integrating threat intelligence feeds into open-source SIEM
- ✓ Automating tasks using scripts and custom tools
- ✓ Developing custom plugins and integrations for SIEM tools
- ✓ Using Machine Learning and AI in advanced SIEM configurations
- ✓ Optimizing performance and scaling SIEM deployments