



Security Information and Event Management

Introduction to SIEM
Network Threats
SIEM Architecture
SIEM Deployment
Logs and Events
Event Collection and Event Correlation
Correlation Rules
Forensically Ready Data
Intrusion Detection, Prevention and Tolerance
Properties of a Robust SIEM
Installing Alien Vault SIEM
Using Web Interface
Configuring Sensor, Logger and Server
onfiguring Network Inventory
Configuring Vulnerability Scanning
Configuring Signature Updates
Policy Management
Configuring Tickets
Introduction to SPLUNK
Overview of machine data
How Splunk works with machine data
Introduction to Splunk's user interface
Searching and saving results
Creating reports and visualizations