SP-USES - Using Splunk Enterprise Security

Days: 2

Prerequisites: Students should have a working understanding of Intro to Splunk, Using Fields, Visualizations, Search Under the Hood, Intro to Knowledge Objects, and Introduction to Dashboards.

Audience: Security operations center (SOC) analysts and security professionals who use Splunk Enterprise Security to identify, investigate, and respond to threats.

Description: This two-day instructor-led course prepares SOC analysts to use Splunk Enterprise Security (ES). Students learn to identify and track incidents, analyze security risks, use risk-based alerting and threat intelligence, investigate suspicious activity, and work with the dashboards and response tools used in day-to-day security operations.

Course Objectives: Upon completion of this course, students will:

- Explain the role of a SIEM and the core capabilities of Splunk Enterprise Security.
- Navigate the Analyst Queue and triage findings and finding groups.
- Create and manage investigations using response plans, events, playbooks, and actions.
- Use risk-based alerting, assets and identities, and adaptive responses.
- Analyze security domain and intelligence dashboards.
- Work with threat intelligence and protocol intelligence to investigate network activity.

OUTLINE:

MODULE 1: ES FUNDAMENTALS

- SIEM functions and Splunk Enterprise Security
- Data models, detections, and findings
- Roles, permissions, and ES navigation

MODULE 2: EXPLORING THE ANALYST QUEUE

- Filtering and queue navigation
- Triage findings and finding groups
- Create ad hoc findings
- Suppress findings from the queue

MODULE 3: WORKING WITH INVESTIGATIONS

- Create and manage investigations
- Use response plans
- Add Splunk events
- Use playbooks and actions

MODULE 4: RISK-BASED ALERTING

- Risk and Risk-Based Alerting concepts
- Risk scores and entity risk
- Risk Analysis dashboard
- Annotations and risk findings

MODULE 5: ASSETS AND IDENTITIES

- Assets and Identities framework
- Missing asset or identity data
- Management interface and lookup tables
- Field-matching criteria

MODULE 6: ADAPTIVE RESPONSES

- Adaptive Response concepts
- Default response actions
- Invocation methods
- Troubleshooting response issues

MODULE 7: SECURITY DOMAIN DASHBOARDS

- Inspect incident-related events
- Identify security domains
- Use and launch domain dashboards

MODULE 8: INTELLIGENCE DASHBOARDS

- Web and User Intelligence dashboards
- Filter and highlight events
- Investigators for assets and identities
- Access Anomalies

MODULE 9: THREAT INTELLIGENCE

- Threat Intelligence framework
- Configuration locations
- Threat findings and indicators
- Troubleshooting

MODULE 10: PROTOCOL INTELLIGENCE

- Network data in Splunk events
- Stream events
- Protocol Intelligence dashboards