

Investigating Incidents with Splunk SOAR

Summary

This course prepares security practitioners to use SOAR to respond to security incidents, investigate vulnerabilities, and take action to mitigate and prevent security problems.

Prerequisites

- Basic security operations knowledge

Course Outline

Topic 1 – Starting Investigations

- SOAR investigation concepts
- ROI view
- Using the Analyst Queue
- Using indicators
- Using search

Topic 2 – Working on Events




- Use the Investigation page to work on events
- Use the heads-up display
- Set event status and other fields
- Use notes and comments
- How SLA affects event workflow
- Using artifacts and files
- Exporting events
- Executing actions and playbooks
- Managing approvals

Topic 3 – Cases: Complex Events

- Use case management for complex investigations
- Use case workflows
- Mark evidence
- Running reports

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit <http://www.splunk.com/education>.

	Format: <ul style="list-style-type: none">• Instructor led class with labs
	Duration: 3 Hours
	Audience: <ul style="list-style-type: none">• SOC analysts, SOAR Administrators, Automation Engineers

To contact us, email education@splunk.com.

