



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Vous pouvez nous joindre ici

Email: training.ecs.fr@arrow.com
Phone: 01 49 97 50 00



Investigating Incidents with Splunk SOAR

| | | |
|--------------|---------------------|-------------------|
| CODE: | DURÉE: | PRIX H.T.: |
| SPL_IISS | 4 Hours (0.5 Jours) | Prix sur demande |

Description

This 3.5 hour course prepares security practitioners to use SOAR to respond to security incidents, investigate vulnerabilities, and take action to mitigate and prevent security problems.

Objectifs

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

Audience

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Prérequis

Security operations experience.

Programme

- SOAR concepts
- Investigations
- Running actions and playbooks
- Case management & workflows

Test et Certification

Certification Tracks Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

Informations supplémentaires

Course Format Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Dates de session

Sur demande. [Merci de nous contacter](#)

Informations Complémentaires

[Cette formation est également disponible sous forme de formation sur site. Veuillez nous contacter pour en savoir plus.](#)