



Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com

Phone: 0870 251 1000

CODE:	LENGTH:	PRICE:
SPL_IISS	3.36 Hours (0.42 days)	€500.00

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.

Objectives

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.

Prerequisites

Security operations experience.

Programme

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

Test and Certification

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

Further Information

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

Session Dates

Aikataulutamme kiinnostuksen mukaan. [Ota yhteyttä](#)

Additional Information

[This training is also available as onsite training. Please contact us to find out more.](#)