Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Investigating Incidents with Splunk SOAR

CODE:	LENGTH:	PRICE:
SPL_IIWSS	0.96 Hours (0.12 days)	€500.00

Description

This 3 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

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

Programme

Topic 1 – Starting Investigations

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

Topic 2 – Working on Events

- Using 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

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.