Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss her

Postboks 6562 ETTERSTAD, 0606 Oslo, Norge

Email: kurs.ecs.no@arrow.com
Phone: +47 22 02 81 00

Investigating Incidents with Splunk SOAR

CODE:	LENGTH:	PRICE:
SPL_IISS	3.36 Hours (0.42 days)	kr5,275.00

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

Ved forespørsel. Vennligst kontakt oss

Tilleggsinformasjon

Denne treningen er også tilgjengelig som trening på stedet. Kontakt oss for å finne ut mer.