Enterprise Computing Solutions - Education Services

# TRAINING OFFERING

**Du kan nå os her**

.

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

# Investigating Incidents with Splunk SOAR

| CODE: | LENGTH: | PRICE: |
| --- | --- | --- |
| SPL_IISS | 4 Hours (0.5 dage) | kr 3,625.00 |

## 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

På anmodning. Kontakt os venligst

## Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.