



Enterprise Computing Solutions - Education Services

## TRAINING OFFERING

---

**You can reach us at:**

Arrow ECS, Woluwedal 30, 1932 Sint-Stevens-Woluwe

Email: [education.ecs.benelux@arrow.com](mailto:education.ecs.benelux@arrow.com)

Phone: +32 2 332 19 57

# Investigating Incidents with Splunk SOAR

<b>CODE:</b>	<b>LENGTH:</b>	<b>PRICE:</b>
SPL_IISS	4 Hours (0.5 days)	Request Price

## 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**

On request. Please [Contact Us](#)

### **Additional Information**

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