Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns unter

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: training.ecs.de@arrow.com
Phone: +49 (0)89 930 99 168

Investigating Incidents with Splunk SOAR

CODE:	LÄNGE:	PREIS:
SPL_IISS	4 Hours (0.5 Tage)	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.

Lernziel

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

Zielgruppe

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Voraussetzungen

Security operations experience.

Inhalt

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

Test und Zertifizierung

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

Weitere Informationen

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

Kurstermine

Auf Anfrage. Bitte kontaktieren Sie uns

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.