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

Advanced SOAR Implementation

CODE:	LÄNGE:	PREIS:
SPL_ASI	15.36 Hours (1.92 Tage)	€1,500.00

Description

This 13.5 hour (3 days a 4,5 hours) course is intended for experienced SOAR consultants who will be responsible for complex SOAR solution development, and will prepare the attendee to integrate SOAR with Splunk as well as develop playbooks requiring custom coding and REST API usage.
Potential attendees have received a passing grade in all prerequisite courses, and must ensure they can devote all of their attention to the class, as the course work is very challenging. Students will develop a custom solution with SOAR, Splunk and custom Python code. The labs provide requirements for the solution; the student must plan and execute the development. This will require thoughtful focus, experimentation and problem-solving skills.

Lernziel

- Using external search in SOAR
- Sending events from Splunk to SOAR
- Updating Splunk events from SOAR
- Running SOAR reports on Splunk
- Executing SOAR playbooks from Splunk
- Searching Splunk from SOAR playbooks
- Writing custom code in SOAR playbooks
- Using the SOAR REST API in Phantom playbooks

Voraussetzungen

Attendees for this class must ensure that they meet all course pre-requisites. This is a challenging, advanced class that draws on technical knowledge from many areas in Splunk and SOAR, and the demanding labs and course schedule leave little time to learn the basics.
Classes:

- Experience with Python programming
- Adminstering Splunk SOAR
- Developing Splunk SOAR Playbooks
- Enterprise Splunk Data Administration
- Enterprise Splunk System Administration

Either
Using *or* Administering Splunk Enterprise Security

Inhalt

Module 1 – Implementing Splunk and SOAR

- Review of SOAR UI and concepts
- Describe interactions between Splunk and SOAR
- Identify key concepts and data flows
- Pre-requisites for integration

Module 2 – Configuring External Splunk Search

- Describe the benefits of externalizing search to Splunk
- Configure the SOAR instance for externalization

- Configure the Splunk instance for externalization
- Use the Splunk app for SOAR Reporting

Module 3 – Sending Splunk Events to SOAR

- Configure the SOAR Add-on for Splunk
- Map CIM fields to CEF
- Send Enterprise Security notables to SOAR
- Automatically trigger SOAR playbooks for Splunk notables

Module 4 – Accessing Splunk from SOAR

- Install and configure the SOAR App for Splunk
- Ingest Splunk events into SOAR
- Use Splunk search from playbooks
- Update Splunk notable events

Module 5 – Custom Coding in Playbooks

- SOAR coding best practices
- Writing, using and managing custom functions
- Using the SOAR API in custom code
- Store and retrieve persistent data

Module 6 – Using SOAR REST

- Use Django queries to search for data in SOAR
- Use REST to access SOAR data
- Use the HTTP app to execute REST from playbooks

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.