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

Administering Splunk SOAR

CODE:	LÄNGE:	PREIS:
SPL_ASS	4 Hours (0.5 Tage)	€500.00

Description

This 3 hour course prepares IT professionals to configure and manage SOAR.

Lernziel

- SOAR concepts
- Initial configuration
- Apps and assets
- Configuring automation
- User management
- Ingesting Data
- Customization and monitoring

Voraussetzungen

Classes:

- Investigating Incidents with Splunk SOAR

Inhalt

Topic 1 –Initial Configuration

- Describe SOAR operating concepts
- Identify documentation and community resources
- SOAR & Splunk Architecture
- Product settings
- Access control
- Authentication settings
- Response settings
- Understanding roles
- Creating users
- Managing user access

Topic 2 – Apps, Assets and Playbooks

- Add and configure apps and assets
- Manage playbooks
- Ingesting Data
- Labels and tags
- Event settings

Topic 3 – Customization and Monitoring

- Create custom severity levels
- Create custom status levels
-
- Add custom fields and CEF settings
-

- Create custom workbooks
-
- Run reports
-
- Use SOAR audit tools
-
- Monitor system health

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.