Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Administering Splunk SOAR

CODE:	LENGTH:	PRICE:
SPL_ASS	1.12 Hours (0.14 days)	€500.00

Description

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

Objectives

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

Prerequisites

Classes:

- Investigating Incidents with Splunk SOAR

Programme

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

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.