Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

FortiSOAR Design and Development

CODE:	LENGTH:	PRICE:
FNT_FT-FSR-DEV	24 Hours (3 days)	Request Price

Description

In this course, you will learn how to use FortiSOAR to design simple to complex playbooks, examine the role of FortiSOAR in mitigating malicious indicators, and learn how to create interactive dashboards to display relevant information about alerts and incidents. You will also learn how to integrate FortiSOAR with FortiGate, FortiSIEM, and FortiMail.

Objectives

After completing this course, you will be able to:

- Identify the role of FortiSOAR in a SOC environment
- Plan a FortiSOAR deployment
- Manage incidents and alerts in a SOC environment
- Explore, create, and customize dashboards
- Explore the structure of a template
- Create, customize, and analyze dashboard widgets
- Create, customize, and publish modules
- Search for records and filter search records
- Analyze field-type options in the field editor
- Build a user prompt from a manual trigger step
- Define variables and dictionaries in Jinja
- Configure step utilities within a playbook step
- Configure various core steps of a playbook
- Configure different modes of data ingestion
- Install/configure connectors and apply to a playbook
- Configure various utility steps
- Configure referenced playbooks
- Configure and use dynamic variables and values
- Use expressions to customize playbook input and outputs
- Use common Jinja filters and functions
- Use filters to extract data from complex data structures
- Build loop functions and conditional statements

Audience

This course is intended for cybersecurity professionals responsible for planning, designing, and customizing FortiSOAR deployments, integrating FortiSOAR with FortiGate, FortiSIEM, and FortiMail, and FortiSOAR playbook design and development.

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- NSE 4 FortiGate Security
- NSE 6 FortiSOAR Administrator

It is recommended that you have an understanding of Python programming and Jinja2 templating language, and familiarity with email security and SIEM technologies is also beneficial.

System Requirements

If you take the online format of this class, you must use a computer that has the following:

- A high-speed internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones
- One of the following:
  HTML5 support;
  An up-to-date Java Runtime Environment (JRE) with Java Plugin enabled on your web browser

You should use a wired Ethernet connection, not a Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connection to the online labs.

Programme

1. Introduction to FortiSOAR
2. Dashboard Templates and Widgets
3. Module Templates and Widgets
4. Application Editor
5. Dynamic Variable and Values
6. Jinja Filters, Functions, and Conditions
7. Introduction to Playbooks
8. Playbook Core Steps
9. Playbook Evaluate Steps
10. Playbook Connectors, Data Ingestion, and Execution Steps

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.