Configuring ArcSight SOAR for Effective Threat Response (CASFETR)

ID CASFETR **Prix** sur demande **Durée** 3 jours

A qui s'adresse cette formation

Administrators and Content Engineers responsible for configuring ArcSight security content.

Pré-requis

This course assumes a familiarity working with ArcSight ESM but it is not required

Objectifs

On completion of this course, participants should be able to:

- Configure SOAR to receive alerts from ESM
- Describe the SOAR workflow
- Configure integrations
- Configure filtering, classifying, consolidating
- and dispatching rules
- Create workflow playbooks
- Review system status
- Run, schedule, and export reports

Contenu

Module 1: Introduction to ArcSight SOAR

- Challenges Faced by Organizations
- What Is ArcSight SOAR?
- ArcSight SOAR Features.
- Deployment Overview of ArcSight SOAR.
- Accessing ArcSight SOAR

Module 2: Setting Up SOAR to Receive Alerts

- Installing a Forwarding Connector on ESM
- Configuring a Forwarding Connector User and Web User on ESM
- Configuring a Pre-persistent Rule to Tag the Events Forwarded to SOAR
- Adding an ESM Alert Source on SOAR
- Adding an ESM Integration on SOAR

Module 3: Understanding the SOAR Workflow

- Processing ESM Alerts with SOAR
- Rule Name Filters
- Classification
- Consolidation
- Dispatching Cases
- Automating Case Handling by Using Playbooks

Module 4: SOAR Integrations Overview

- SOAR Integrations Capabilities
- Use Cases Benefits
- Integrating SOAR with MISP
- Integrating SOAR with VirusTotal

Module 5: SOAR Users, Groups, SSO

- Creating User Groups in Fusion
- Creating Users in Fusion
- Importing Existing Users from ESM
- User Roles and Assigning Permissions
- ACLs in SOAR

Module 6: SOAR Case Management

- Understanding the SOAR Cases User Interface
- Viewing Case Details
- Managing Cases in SOAR

Module 7: Filtering, Classifying, Consolidating, and Dispatching Cases

- Filtering Alerts for Case Creation
- Classifying Cases on SOAR
- Consolidating Alerts to Create Cases
- Dispatching Cases

Module 8: Automating Responses with Workflow Playbooks

- What are Playbooks?
- Working with Playbooks
- Workflow Playbooks
- Scheduled Playbooks
- Managing Triggers
- Handling Manual Processes Through Tasks
- Out of The Box Workflows
-

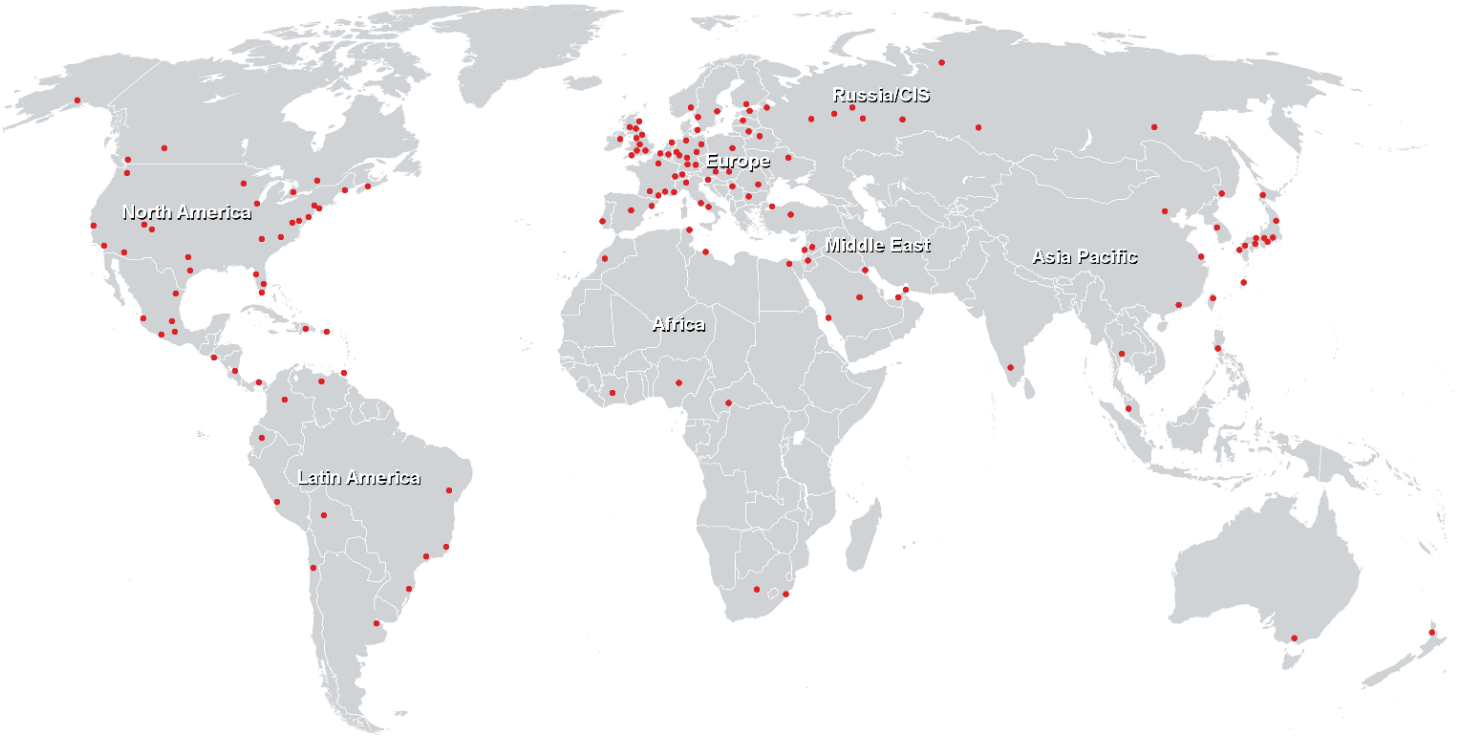
Module 9: SOAR System Status

- Alerts
- Action and Rollback Queues
- Action History
- Enrichment History
- Process Queues
- Troubleshooting

Module 10: Monitoring Using SOAR Dashboards and Reports

- Reports in Fusion
- ArcSight SOAR Standard Content Resources
- Scheduling and Exporting Reports
- Running SOAR Legacy Reports (Jasper Reports)

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch