ArcSight ESM Administrator and Analyst (ASEAAA)

ID ASEAAA **Prix** sur demande **Durée** 5 jours

A qui s'adresse cette formation

Analysts, Content Engineers, Business Administrators

Pré-requis

None

Objectifs

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

- Make ArcSight ESM operational upon initial installation
- Describe how ESM works in the context of your network
- Create user accounts
- Implement built-in content
- Populate ESM with your network and assets to identify endpoints involved in an event
- Create site-specific business-oriented views
- Investigate, identify, analyze, and remediate exposed security issues
- Use workflow management to provide real-time incident response and escalation tracking
- Modify and run standard reports to provide situational awareness and network status
- Establish ESM peering across multiple ESM instances
- Perform distributed event search and content management

Contenu

Module 1: ESM Overview

- Discuss what ArcSight ESM is and how it fits into a SOC
- List the problems ESM can solve
- Discuss basic processes to make an ESM installation successful
- Describe the basic ArcSight components (10' - 100,000' view)
- Identify basic user roles within an ArcSight Installation

Module 2: Command Center

- Discuss an overview of the Command Center
- Describe how to use the Site Map
- Describe how to monitor usage
- Discuss how to configure Dashboards and the different Dashlets you can add
- Describe how to use the Security Operations Center Dashboards
- Explain how to configure and view MITRE Dashboards
- Discuss how to monitor events with Active Channels
- Discuss how to view and use Field Sets
- Discuss how to view, export, and filter Active Lists

Module 3: ESM Console

- Install the ArcSight ESM Console
- Start the ArcSight ESM Console
- Use the Console Panels and Features
- Customize the ESM console

Module 4: Installing and Configuring ArcSight Connectors

- Describe a connector
- Describe normalization
- Describe a network model
- Describe SmartConnectors
- Deploy and configure SmartConnectors

Module 5: ArcSight Marketplace

- Describe what is the Marketplace
- Define Marketplace packages/use cases

Module 6: Schema, Fieldsets, and Active Channels

- Describe the ArcSight Event Schema
- Describe an Active Channel
- Describe what a field set is
- Describe the Event Life Cycle

Module 7: Filters

- Describe Filters and Filter Types
- Create and Modify Filters
- Debug Filters

Module 8: Dashboards & Data Monitors

- Identify Data Monitor types and functions
- Access and Use Dashboards
- Modify Dashboard Data Monitor Layouts

Module 9: Rules & Lists

- Describe rules and rule types
- Describe rule triggers and actions
- Describe Active Lists and Session Lists
- Create and validate rule behavior
- Create and validate Brute Force Login Attempt and Successful rules
- Create and validate Active and Session List integration rules

Module 10: User Administration

- Create, edit, rename, delete user groups
- Create, edit, move, delete users
- Manage resource permissions
- Access and modify global user password properties

Module 11: Notifications

- Describe the operation of ArcSight notifications
- Configure ArcSight notifications

Module 12: Incident Response and Automation with SOAR

- Understand SOAR
- Triage cases with SOAR
- Respond to Cases with Playbooks
- Close a case

Module 13: Queries and Query Viewers

- Explain Queries
- Define Query Viewers
- Explain the advantages of using Query Viewers
- Create the following functions with Query Viewers: Drilldowns, Baselines, Reports, Dashboard views

Module 14: Reports

- Define a report
- Run, view, and save a report
- Manage archived reports

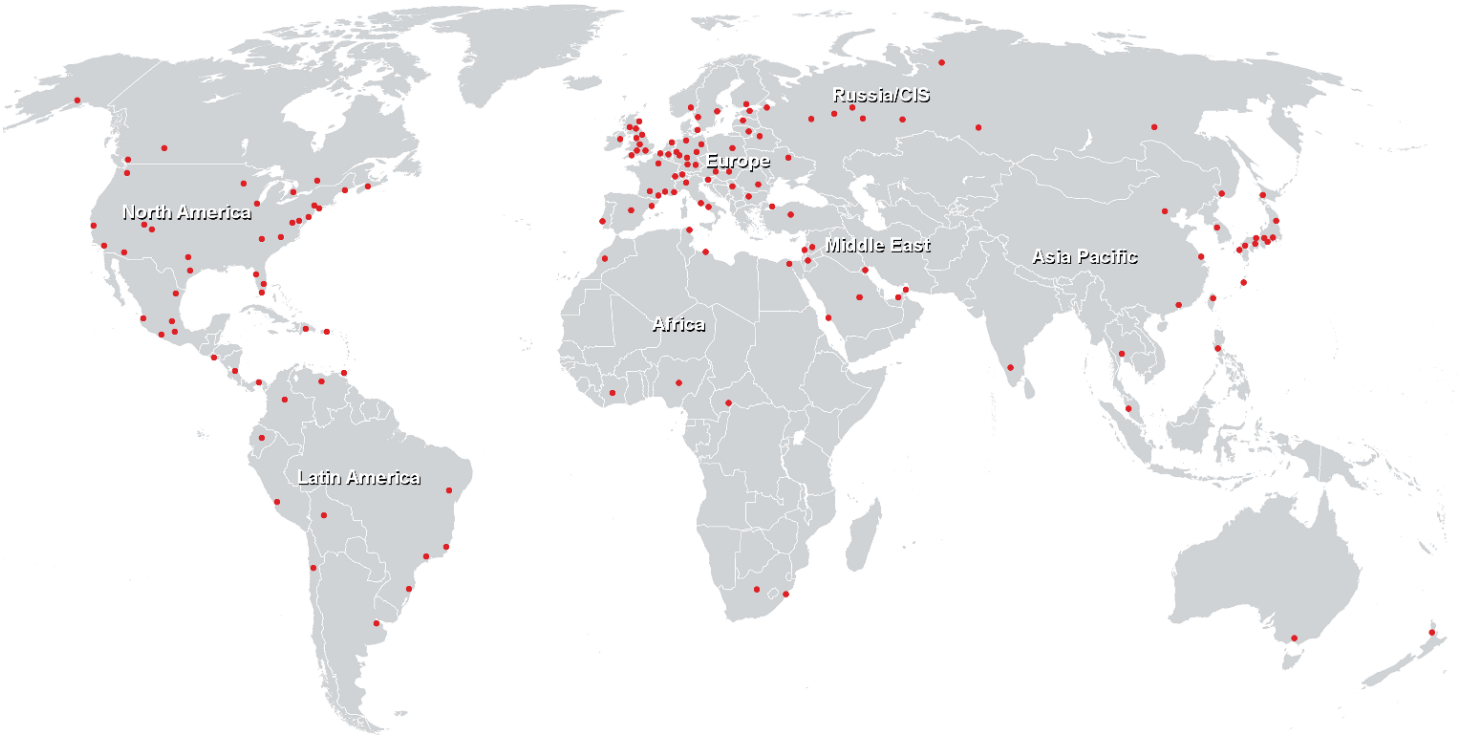
Module 15: Content Management and Peering

- Peer ESMs
- Perform a search on a peer
- Create a package and sync to a peer
- Manually push a package
- Verify successful distribution of a package

Module 16: Event Search

- how keyword, field-based and pipeline searches are performed
- Describe how search results are displayed
- Use the unified Search page to initiate any type of search
- Use Search Helper and Search Builder features to save time constructing search expressions
- Load, modify, and save search filters and saved searches
- Enable peer ESM and Logger instances for searching

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