ArcSight Recon Analyst (2-7329)

ID 2-7329 **Prix** sur demande **Durée** 4 jours

A qui s'adresse cette formation

This course is ideal for security analysts who want to enhance their threat detection and investigation capabilities by leveraging ArcSight Recon's event search, reporting, and dashboarding features to identify anomalies, uncover threats, and support proactive security operations.

Pré-requis

To be successful in this course, you should have the following prerequisites or knowledge:

- Familiar with Boolean logic operators and ArcSight Schema groups and fields.
- Basic understanding of Command Shell in Windows and Linux, and familiarity with SIEM concepts

Objectifs

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

- Investigate events using Recon Search tools and Scheduled event searches.
- Explain the usage of Search resources such as Field Sets, Filters, and Operators.
- Describe, access, create and use Reports and Dashboards.
- Describe and use the default Cloud Security Dashboards and Reports.
- Implement Dashboards with Parabox Charts (known as parallel box plots charts).
- Describe and use the default MITRE ATT&CK Dashboards and Reports.
- Describe Threat Hunting types: unstructured and structured
- Create custom Search Queries, Reports and Dashboards to analyze event data using sample scenarios.
- Define Outliers Models and identify suspicious sources using Recon Analytics charts.

Contenu

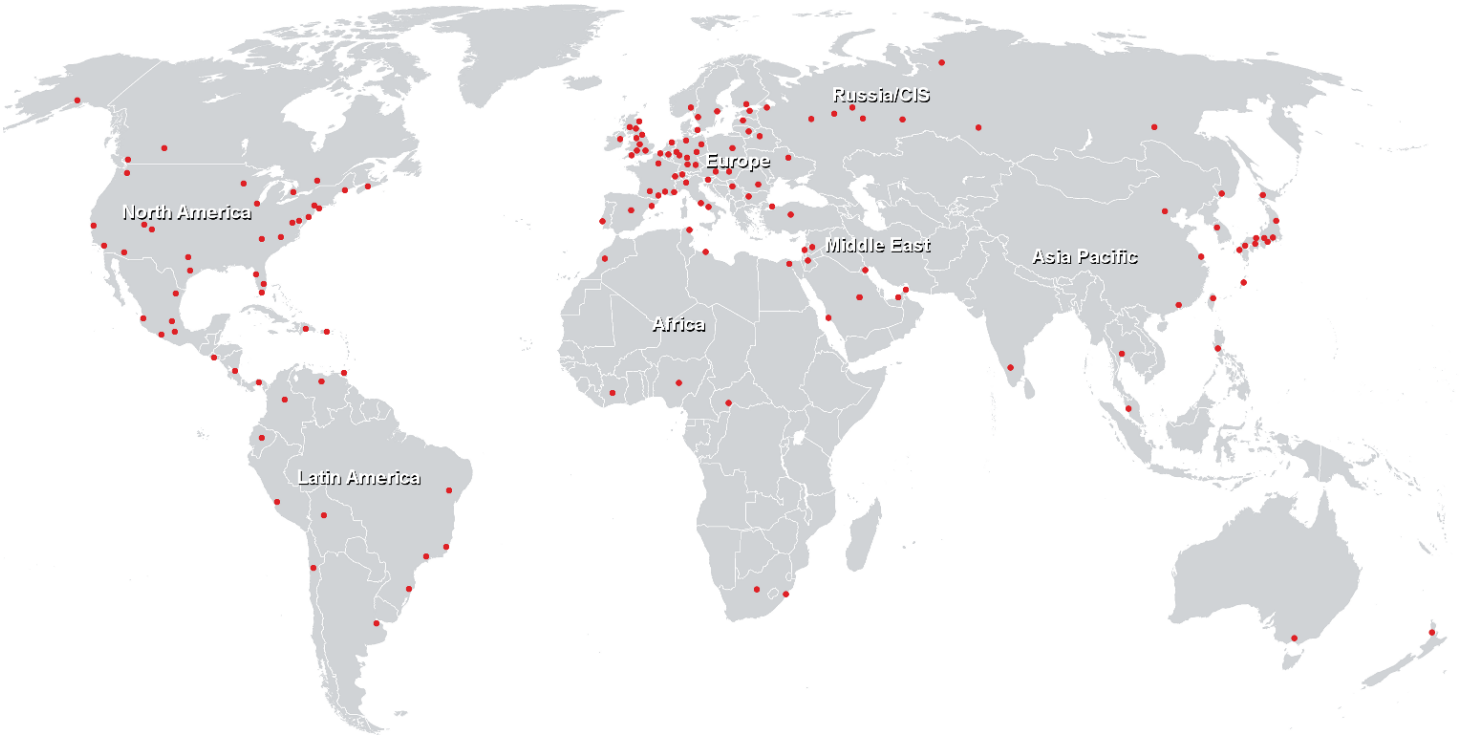
As a learner, you will begin by exploring event search and reporting features using Recon's default content to get familiar with the interface and its core functionalities. As the course progresses, you will engage in hands-on exercises to build more advanced event searches, reports, and dashboards from the ground up.

You will also analyze security events tied to specific use cases, such as detecting threats from former employees, investigating the Log4j vulnerability, and uncovering insider threats related to data exfiltration. By applying your knowledge of Recon, you will examine these scenarios to identify targets, indicators of compromise (IoCs), and potential attackers.

Highlights:

- Create search queries using ArcSight schema fields, keywords, field sets, search operators, and hashtags.
- Use default content reports and dashboards to analyze events of interest, including MITRE ATT&CK content.
- Create reports and dashboards using data worksheets from scratch.
- Analyze event data using Recon tools in sample scenarios, such as uncovering ex-employee threats and detecting Log4j vulnerability.
- Use Recon tools to analyze historical events and identify undetected threats in a sample unstructured threat-hunting scenario.
- Build and score the outlier model and explain outlier's analytics charts.

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