

## ArcSight Enterprise Security Manager Advanced Analyst (2-7309)

ID 2-7309 Prix sur demande Durée 4 jours

### A qui s'adresse cette formation

This course is intended for Analysts and Content Engineers who:

- Define their organization's security objectives
- Build or using advanced content to correlate, view and respond to those security objectives

### Objectifs

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

- Navigate ArcSight ESM console and command center to correlate, investigate, analyze, and remediate both exposed and obscure threats.
- Construct ArcSight variables to provide advanced analysis of the event stream.
- Develop ArcSight lists and rules to allow advanced correlation activities.
- Optimize event-based data monitors to provide real-time viewing of event traffic and anomalies.
- Design new report templates and create functional reports.
- Find events through the search tools.

### Contenu

- Create ArcSight Variables
- Develop ArcSight Lists and Rules
- Create Data Monitors and Dashboards

## 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](mailto:info@flane.ch), <https://www.flane.ch>