

# ESM320

## ArcSight-ESM-Advanced Analyst with exam

This course provides you with the knowledge required to use advanced ArcSight ESM content to find and correlate event information, perform actions such as notifying stakeholders, graphically analyze event data, and report on security incidents. You will familiarize and/or reinforce your understanding of the advanced correlation capabilities within ArcSight ESM that provide a significant edge in detecting active attacks.

This course covers ArcSight security problem solving methodology using advanced ESM content to find, track, and re-mediate security incidents. During the training, you will use variables and correlation activities, customize report templates for dynamic content, and customize Dashboards to monitor incidents.

The last day of class offers a hands-on exam. Passing the exam awards you with Certified Expert badge.

### Kursinhalt

- Module 1: ESM Overview
- Module 2: Command Center
- Module 3: ArcSight Console
- Module 4: Active Channels
- Module 5: Filters
- Module 6: Variable Customization
- Module 7: Data Monitors and Dashboards
- Module 8: ESM Lists
- Module 9: ESM Rules
- Module 10: Query Viewers Authoring
- Module 11: ESM Reports
- Module 12: Unifited Event Search Tools

**E-Book** Sie erhalten englischsprachige Unterlagen von HPE als E-Book.

### Zielgruppe

This course is intended for analysts responsible for:

- Defining their organization's security objectives
- Building or using advanced content to correlate, view and respond to those security objectives.

### Voraussetzungen

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

- Common security devices such as IDS and firewalls
- Common network device functions, such as routers, switches, and hubs
- TCP/IP functions such as CIDR blocks, subnets, addressing, and communications
- Basic Windows operating system tasks and functions
- Possible attack activities, such as scans, man in the middle, sniffing, DoS, and possible abnormal activities, such as worms, Trojans, and viruses 3
- SIEM terminology, such as threat, vulnerability, risk, asset, exposure, and safeguards
- Completed the ArcSight ESM Administrator and Analyst course or 6 months experience administering ArcSight ESM

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.expertech.ch/go/ES32](http://www.expertech.ch/go/ES32)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Stand 28.04.2024

Training		Preise zzgl. MwSt.
<b>Termine in der Schweiz</b>	<b>5 Tage</b>	
<b>Online Training</b>	<b>5 Tage</b>	<b>CHF 4.125,-</b>
<b>Termin/Kursort</b>	09.09.-13.09.24	☑ Online
		Kurs Sprache Englisch 



EXPERTeach



## Unser Trainingsangebot für Sie:



### Classroom Training

Das Live-Trainingserlebnis in unseren Training Centern oder bei Ihnen vor Ort.



### Online Training

Nehmen Sie online am Kurs teil – ohne Reise- und Hotelaufwände.



### Hybrid Training

Classroom & online in einem Kurs – Sie wählen, wie Sie teilnehmen möchten.



### Inhouse-Schulungen

Für Ihr Projekt erstellen wir genau passende Trainingskonzepte.



### Garantierte Kurstermine

Die ExperTeach Garantietermine geben Ihnen Sicherheit für Ihre Planung.

## Auszeichnungen für ExperTeach



ExperTeach AG

Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch