



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Vous pouvez nous joindre ici

Email: training.ecs.fr@arrow.com
Phone: 01 49 97 49 51



IBM QRadar SIEM Advanced Topics

CODE:	DURÉE:	PRIX H.T.:
ZL1_BQ203	2 Jours	€1,590.00

Description

IBM® Security QRadar® enables you to minimize the time gap between when a suspicious activity occurs and when you detect it. Attacks and policy violations leave their footprints in log events and network flows of your IT systems. To connect the dots, QRadar SIEM correlates these scattered events and flows into offenses that alert you to suspicious activities. Using the skills taught in this course, you will be able to configure processing of uncommon events, work with reference data, and develop custom rules, custom actions, and custom anomaly detection rules.

The lab environment for this course uses the IBM QRadar SIEM 7.3 platform.

Objectifs

- Create custom log sources to utilize events from uncommon sources
- Create, maintain, and use reference data collections
- Develop and manage custom rules to detect unusual activity in your network
- Develop and manage custom action scripts to for automated rule reponse
- Develop and manage anomaly detection rules to detect when unusual network traffic patterns occur

Audience

Audience

- Security administrators
- Security technical architects
- Offense managers
- Professional services using QRadar SIEM
- QRadar SIEM administrators

Prérequis

Prerequisites:

- IT infrastructure
- IT security fundamentals
- Linux
- Microsoft Windows
- TCP/IP networking
- Log files and events
- Network flows

You should also have completed the IBM QRadar SIEM Foundations course.

Programme

Module 1: Creating log source types
Module 2: Leveraging reference data collections
Module 3: Developing custom rules
Module 4: Creating Custom Action Scripts
Module 5: Developing Anomaly Detection Rules

Informations supplémentaires

Prior to enrolling, IBM Employees must follow their Division/Department processes to obtain approval to attend this public training class. Failure to follow Division/Department approval processes may result in the IBM Employee being personally responsible for the class charges.

GBS practitioners that use the EViTA system for requesting external training should use that same process for this course. Go to the EViTA site to start this process:

<http://w3.ibm.com/services/gbs/evita/BCSVTEurl.nsf>

Once you enroll in a GTP class, you will receive a confirmation letter that should show:

- The current GTP list price
- The 20% discounted price available to IBMers. This is the price you will be invoiced for the class.

Dates de session

Date	Lieu	Time Zone	Langue	Type	Garanti	PRIX H.T.
27 Jan 2022	Virtual Classroom	CET	English	Instructor Led Online		€1,590.00
10 Mar 2022	Virtual Classroom	CET	English	Instructor Led Online		€1,590.00
14 Apr 2022	Virtual Classroom	CEDT	English	Instructor Led Online		€1,590.00
02 Jun 2022	Virtual Classroom	CEDT	English	Instructor Led Online		€1,590.00
08 Sep 2022	Virtual Classroom	CEDT	English	Instructor Led Online		€1,590.00
13 Oct 2022	Virtual Classroom	CEDT	English	Instructor Led Online		€1,590.00
17 Nov 2022	Virtual Classroom	CET	English	Instructor Led Online		€1,590.00

Informations Complémentaires

[Cette formation est également disponible sous forme de formation sur site. Veuillez nous contacter pour en savoir plus.](#)