



Enterprise Computing Solutions - Education Services

## OFERTA FORMATIVA

---

### Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: [formacion.ecs.es@arrow.com](mailto:formacion.ecs.es@arrow.com)

Phone: +34 91 761 21 51



# IBM QRadar SIEM Advanced Topics

<b>CÓDIGO:</b>	<b>DURACIÓN:</b>	<b>Precio:</b>
BQ203G	2 días	€1,100.00

## 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.

## Objetivos

- 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

## Público

Audience

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

## Requisitos Previos

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.

## Programa

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

## Más información

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/BCSVTEenrl.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.

## Fechas Programadas

A petición. Gracias por [contactarnos](#).

## Información Adicional

[Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.](#)