Pipeline

Pipeline is a Leading Learning Partners Association Member

IBMBQ104G - IBM QRADAR SIEM FOUNDATIONS

CORSO CON DOCENTE

Durata	Prezzo	Orari	Calendario
3 giorni	2.400,00€ + IVA	9:00 – 13:00 | 14:00 – 17:00	

Questo corso IBMBQ104G - IBM QRadar SIEM Foundations è dedicato ad approfondire l'architettura di questa soluzione. IBM Security QRadar consente una visibilità approfondita sulle attività di rete, endpoint, utenti e applicazioni. Fornisce raccolta, normalizzazione, correlazione e archiviazione sicura di eventi, flussi, risorse e vulnerabilità. Gli attacchi sospetti e le violazioni dei criteri vengono evidenziati come reati. In questo corso si impara a conoscere l'architettura della soluzione, a navigare nell'interfaccia utente e a indagare sulle infrazioni. Si ricercano e si analizzano le informazioni da cui QRadar ha concluso un'attività sospetta. Esercitazioni pratiche rafforzano le competenze apprese.

Questo corso è **erogato in collaborazione con TD Synnex,** centro autorizzato all'erogazione di corsi ufficiali IBM.

Contenuti del corso

Unit 0: IBM Security QRadar 7.4 – Fundamentals

Unit 1: QRadar Architecture

Unit 2: QRadar UI – Overview

Unit 3: QRadar – Log Source

Unit 4: QRadar flows and QRadar Network Insights

Unit 5: QRadar Custom Rule Engine (CRE)

Unit 6: QRadar Use Case Manager app

Unit 7: QRadar – Assets

Unit 8: QRadar extensions

Unit 9: Working with Offenses

Unit 10: QRadar – Search, filtering, and AQL

Unit 11: QRadar – Reporting and Dashboards

Unit 12: QRadar – Admin Console

Partecipanti

Questo corso è rivolto ad analisti della sicurezza, security technical architects, offense managers, amministratori di rete e amministratori di sistema che utilizzano IBM QRadar SIEM.

Prerequisiti

Per partecipare con profitto al corso **IBMBQ104G – IBM QRadar SIEM Foundations** è necessario possedere competenze nei seguenti ambiti:

- Infrastruttura IT
- Fondamenti di sicurezza informatica
- Linux
- Windows
- Rete TCP/IP
- Syslog

Obiettivi

Al termine del corso **IBMBQ104G – IBM QRadar SIEM Foundations** gli allievi saranno in grado di:

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

Pipeline

Pipeline is a Leading Learning Partners Association Member

Lingua

Lingua utilizzata nel corso/dal docente: Italiano
Il materiale didattico e l'ambiente di laboratorio sono in lingua Inglese

Materiali e Bonus

Ogni partecipante al corso IBM BQ104G – IBM QRadar SIEM Foundations riceve l'accesso alla documentazione didattica digitale in lingua inglese e ai laboratori didattici.

Hai bisogno di chiarimenti o ulteriori informazioni?
Vuoi organizzare un corso personalizzato?
Chiamaci: 02/6074791 Scrivici: formazione@pipeline.it