

Javier Foriscot Llorca

Administrador SIEM · IBM QRadar

CURRICULUM VITAE · EUROPASS

Correo electrónico: javi.foris@hotmail.com Web: javierforiscot.dev

LinkedIn: [linkedin.com/in/javier-foriscot-llorca-539876140](https://www.linkedin.com/in/javier-foriscot-llorca-539876140)

SOBRE MÍ

Especialista en ciberseguridad con más de cinco años en entornos SOC y SIEM. Actualmente administrador de IBM QRadar en Kyndryl, donde trabajo en la migración desde RSA NetWitness y en la administración, integración y evolución de la plataforma. Experiencia con QRadar, RSA NetWitness, ArcSight, Splunk y Azure Sentinel. Anteriormente, casi diez años en televisión (Mediaset España, Zeppelin TV) compaginando realización, ayudantía de realización y edición de vídeo, con formación adicional como desarrollador full-stack.

EXPERIENCIA LABORAL

05/2024 – ACTUAL

ADMINISTRADOR QRADAR

Kyndryl

Proyecto de migración de RSA NetWitness a IBM QRadar

- Migración de log sources en un entorno de más de 20.000 fuentes.
- Migración de la infraestructura.
- Migración de casos de uso y reports.
- Migración de automatismos y scripts.

Administración y mantenimiento de QRadar

- Gestión de usuarios y grupos.
- Mantenimiento de reglas y casos de uso, incluidas nuevas altas.
- Nuevas integraciones: API, Syslog, JDBC, Logfile, WinCollect...
- Scripting en Bash y Python para reportes ad hoc. Automatización mediante la API de QRadar.
- Upgrades de versión en entornos PRE y PRO.
- Soporte a auditorías financieras, aportando evidencias desde el SIEM.

2022 – 2024

ANALISTA N2 · ADVANCED CYBER DEFENCE

UST · CyberProof — Cliente: Banc Sabadell

- Threat modeling y modelado de procedimientos de detección.
- Creación de reglas de correlación en RSA NetWitness.
- Revisión de gaps de detección con Darktrace.

2022

ANALISTA DE CIBERSEGURIDAD

NTT DATA

- Análisis forense con Cisco AMP y respuesta a incidentes con CrowdStrike Falcon.
- Reporting directo a cliente y usuarios.
- Gestión de vulnerabilidades (CPE y CVE).

2021 – 2022

ANALISTA DE CIBERSEGURIDAD

Telefónica SOC — a través de Alten

- SOC multidisciplinar trabajando con: IBM QRadar, ArcSight (6.9–7.4), Azure Sentinel, Splunk, McAfee SIEM, AlienVault, RSA, CrowdStrike Falcon, Microsoft Defender for Endpoint, Palo Alto EDR, Cisco Secure Endpoint, Check Point Harmony, Akamai, WAF perimetral, Symantec Cloud y Sandas.

2021

OPERADOR SOC

Sermicro · Evolutio — CISOC

- Operación en entorno SIEM.
- Monitorización con Arbor, Zabbix e Imperva; ticketing con TheHive, Remedy, Jira y ServiceNow.

12/2018 – 12/2019 · MADRID

EDITOR DE VÍDEO

LA MÁQUINA Producciones

07/2015 – 06/2021 · MADRID

AYUDANTE DE REALIZACIÓN

Mediaset España

02/2017 – 09/2020

AYUDANTE DE REALIZACIÓN

Zeppelin TV

2012 – 2020

REALIZADOR DE TELEVISIÓN

Mediaset España

Puestos compaginados de forma simultánea. Realización de programas en directo: coordinación de equipos, plazos ajustados y resolución de problemas en tiempo real.

EDUCACIÓN Y FORMACIÓN

CERTIFICACIÓN

IBM QRADAR SIEM · C1000

IBM

- Implementación de reglas y dashboards.

2020 – 2021

BOOTCAMP DE CIBERSEGURIDAD

The Bridge · Digital Talent Accelerator

- Redes, criptografía, operación de SIEM, análisis de vulnerabilidades, ataques a aplicaciones web y móviles, explotación, evasión de defensas y protección de activos.

2020

BOOTCAMP DE DESARROLLO WEB FULL-STACK

The Bridge · Digital Talent Accelerator

- Node.js, Express, React, MongoDB y control de versiones con Git.

2011 – 2015

GRADO EN COMUNICACIÓN AUDIOVISUAL

Universidad Europea de Madrid — Nivel 6 del MEC

COMPETENCIAS LINGÜÍSTICAS

Lengua materna: Español

Otros idiomas:

	Comprensión		Habla		Escritura
	Comprensión auditiva	Comprensión de lectura	Producción oral	Interacción oral	
Inglés	C1	C1	C1	C1	C1

Niveles: A1 y A2: usuario básico · B1 y B2: usuario independiente · C1 y C2: usuario competente.

COMPETENCIAS DIGITALES

Especialidad

IBM QRadar: administración, migración, integraciones, reglas y casos de uso, API y upgrades de versión

Otros SIEM

RSA NetWitness, ArcSight, Splunk, Azure Sentinel, McAfee ESM, AlienVault

Integración y automatización

QRadar API, Python, Bash, REST APIs, Syslog, JDBC, Logfile, WinCollect

EDR / XDR

CrowdStrike Falcon, Microsoft Defender for Endpoint, Palo Alto Cortex, Cisco Secure Endpoint (AMP), Check Point Harmony

Red y perímetro

Akamai, Imperva, WAF, Arbor, Darktrace, Zabbix

Ticketing

TheHive, ServiceNow, Jira, Remedy, Sandas

Desarrollo

JavaScript, Node.js, Express, React, MongoDB, Git

COMPETENCIAS DE COMUNICACIÓN Y ORGANIZACIÓN

- Trabajo bajo presión y resolución de incidencias en tiempo real, adquiridos en la realización de televisión en directo y en entornos SOC.
- Coordinación de equipos multidisciplinares y comunicación directa con cliente.