

Javier Foriscot Llorca

SIEM Administrator · IBM QRadar

CURRICULUM VITAE · EUROPASS

Email: javi.foris@hotmail.com Web: javierforiscot.dev LinkedIn: linkedin.com/in/javier-foriscot-llorca-539876140

ABOUT ME

Cybersecurity specialist with over five years in SOC and SIEM environments. Currently an IBM QRadar Administrator at Kyndryl, working on the migration from RSA NetWitness and on the administration, integration and evolution of the platform. Hands-on experience with QRadar, RSA NetWitness, ArcSight, Splunk and Azure Sentinel. Previously nearly ten years in television (Mediaset España, Zeppelin TV), combining production, directing and video editing roles, with additional training as a full-stack developer.

WORK EXPERIENCE

05/2024 – CURRENT

QRADAR ADMINISTRATOR

Kyndryl

RSA NetWitness to IBM QRadar migration project

- Log source migration across an environment of 20,000+ sources.
- Infrastructure migration.
- Use case and report migration.
- Automation and script migration.

QRadar administration & maintenance

- User and group management.
- Rule and use case maintenance, including new deployments.
- New integrations: API, Syslog, JDBC, Logfile, WinCollect...
- Bash and Python scripting for ad-hoc reporting. Automation through the QRadar API.
- Version upgrades across PRE and PRO environments.
- Financial audit support, providing evidence from the SIEM.

2022 – 2024

L2 ANALYST · ADVANCED CYBER DEFENCE

UST · CyberProof — Client: Banc Sabadell

- Threat modeling and detection procedure modeling.
- Correlation rule development in RSA NetWitness.
- Detection gap review with Darktrace.

2022

CYBERSECURITY ANALYST

NTT DATA

- Forensic analysis with Cisco AMP and incident response with CrowdStrike Falcon.
- Direct reporting to clients and users.
- Vulnerability management (CPE & CVE).

2021 – 2022

CYBERSECURITY ANALYST

Telefónica SOC — via Alten

- Multidisciplinary SOC working with: 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, perimeter WAF, Symantec Cloud and Sandas.

2021

SOC OPERATOR

Sermicro · Evolutio — CISOC

- Operations in a SIEM environment.
- Monitoring with Arbor, Zabbix and Imperva; ticketing with TheHive, Remedy, Jira and ServiceNow.

12/2018 – 12/2019 · MADRID

VIDEO EDITOR

LA MÁQUINA Producciones

07/2015 – 06/2021 · MADRID

ASSISTANT DIRECTOR

Mediaset España

02/2017 – 09/2020

ASSISTANT DIRECTOR

Zeppelin TV

2012 – 2020

TV PRODUCER

Mediaset España

Concurrent roles. Live TV production and directing: team coordination, tight deadlines and real-time problem solving.

EDUCATION AND TRAINING

CERTIFICATION

IBM QRADAR SIEM · C1000

IBM

- Rule and dashboard implementation.

2020 – 2021

CYBERSECURITY BOOTCAMP

The Bridge · Digital Talent Accelerator

- Networking, cryptography, SIEM operations, vulnerability analysis, web and mobile application attacks, exploitation, defence evasion and asset protection.

2020

FULL-STACK WEB DEVELOPMENT BOOTCAMP

The Bridge · Digital Talent Accelerator

- Node.js, Express, React, MongoDB and version control with Git.

2011 – 2015

BACHELOR'S DEGREE IN AUDIOVISUAL COMMUNICATION

European University of Madrid — EQF level 6

LANGUAGE SKILLS

Mother tongue: Spanish

Other languages:

	Understanding		Speaking		Writing
	Listening	Reading	Spoken production	Spoken interaction	
English	C1	C1	C1	C1	C1

Levels: A1 and A2: Basic user · B1 and B2: Independent user · C1 and C2: Proficient user.

DIGITAL SKILLS

Specialisation

IBM QRadar: administration, migration, integrations, rules & use cases, API and version upgrades

Other SIEMs

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

Integration & automation

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

Network & perimeter

Akamai, Imperva, WAF, Arbor, Darktrace, Zabbix

Ticketing

TheHive, ServiceNow, Jira, Remedy, Sandas

Development

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

COMMUNICATION AND ORGANISATIONAL SKILLS

- Working under pressure and real-time problem solving, developed in live TV production and SOC environments.
- Coordination of multidisciplinary teams and direct client communication.