RICARDO RIVERA AGUILERA

+41 77 276 17 09
ricardo.rivera.aguilera@gmail.com
https://www.linkedin.com/in/ricardriv
Location: Zúrich, Switzerland
Work eligibility: **EU citizen with Swiss residence permit (B)**
Nationality: Spanish & Chilean

SUMMARY

Dynamic Cybersecurity Engineer with 13+ years of international experience across EU and LATAM. Strong background in cybersecurity operations with expertise in SIEM/SOAR engineering, monitoring, incident response, and vulnerability management. Skilled in aligning security programs with international standards (ISO 27001, IEC 62443) and EU regulatory frameworks (GDPR, NIS2). Experienced in secure development lifecycles (NIST SSDF, IEC 62443-1), risk assessment (ISO 27005, NIST RMF), and vulnerability management governance. Certified in CISM, CEH, CASP+, and AZ-500, bridging technical expertise with compliance to ensure resilience and regulatory alignment.

COMPETENCY SUMMARY

Cybersecurity & SOC Architecture
Incident Response & Threat Hunting
Vulnerability Management & Risk Assessment
Security Automation & Detection Engineering
Cloud Security & SecDevops
Machine Learning & AI for Cybersecurity
Security Data Engineering & Threat Intelligence Enrichment
Collaborative mindset in multicultural environments
Disciplined with attention to detail
Critical and analytical thinking
Complex problem solving and decision making
Presenting, influencing and negotiating
Prioritisation, time and work management
Stakeholder communication and management

EMPLOYMENT HISTORY

Grupo MOK - Madrid, Spain

Cybersecurity Engineer (04/2023 - 12/2024)

Served as Security Engineer for Grupo MOK's first European expansion, leading the design and implementation of the cybersecurity hybrid infrastructure. Ensured compliance with client requirements and regulatory standards

Achievements

- Implemented and secured a hybrid infrastructure across two EU data centers (Frankfurt & Amsterdam) and LATAM/EU cloud environments, protecting 120+ critical servers and 1,500 users.
- Integrated a comprehensive security stack, including Splunk/Elastic SIEM, Sophos XDR, PAM, NAC, and WAF, strengthening monitoring, threat detection, and compliance, and enabling ISO 27001 audit readiness and certification.
- Designed and deployed pipelines of events from Filebeat → Logstash cluster (using Splunk HEC plugin) → Splunk Cluster across LATAM/EU operations, enabling scalable log ingestion and centralized visibility for threat detection.
- Implemented an enrichment data strategy with Logstash (MISP dictionary plugin) and Splunk Ingest Actions, using Python scripts and a Jenkins pipeline to automate API-based IOC enrichment, enabling threat-context tagging (TLP, threat level, tags) and ensuring coverage across heterogeneous log sources, which improved detection accuracy and investigation speed.
- Led evidence preparation and client coordination with BNP Paribas, resulting in due diligence approval and the go-live of Grupo MOK's first EU ecosystem, enabling 1M+ operations/day across interconnected systems between multiple providers. Aligning security practices with GDPR requirements and NIST frameworks.
- Implemented secure development and vulnerability management workflows using Ansible for CIS hardening and configuration management, SonarQube (SAST/DAST) for applications and Qualys across hybrid infrastructure (Cloud and on-premise) servers, enhancing scanning coverage, automation schedules by risk, reporting C-Level, and compliance.
- Secured SaaS application access by combining Sophos Endpoint Protection with Genian NAC, enforcing Zero Trust policies based on device posture and identity.

- Designed and maintained RASCI responsibility matrices to clarify roles, accountability, and governance across security and IT operations.
- Prepared and documented Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP), ensuring operational resilience and compliance with client and regulatory requirements, in coordination with teams in LATAM and EU.

CyberProof - Barcelona, Spain

SIEM Architect CyberProof (05/2021 - 04/2023)

Led and managed SIEM projects for international SOC environments, covering migration, deployment, and continuous optimization. Developed performance measurement methodologies to enhance detection and improve operational efficiency. Provided Tier 3 support, collaborating with the SOC Manager to optimize detection, response, and cross-functional coordination.

Achievements

- Directed large-scale SIEM project (LogRhythm to Qradar) for international SOC services major energy provider in Germany, integrating 250 log sources and redesigning 150+ use cases aligned with business critical policies.
- Developed scalable log ingestion pipelines processing over 20K EPS, and implemented structured alert validation across CTI, Threat Intel, and Vulnerability Management teams.
- Improved detection accuracy by 40% and reduced false positives through continuous tuning, mapping detections to MITRE ATT&CK techniques and aligning them with business requirements.
- Collaborated with global-cross functional teams (Israel, UK, EU, USA) to align SOC operations with business objectives and SLA, including international compliance requirements.
- Defined and implemented a SIEM Use Case Maturity Model (UCMM) to classify detection rules by validation level, ensuring structured promotion from testing to production.
- Designed a SIEM Maturity Framework with quarterly KPIs on detection , efficiency, compliance, and performance. Guaranteeing 100% contractual SLA compliance with clients.
- Integrated eBPF-based runtime security (Tetragon) with SIEM pipelines to provide kernel-level visibility in Docker/Kubernetes environments, enabling critical business use cases for detection and compliance
- Implemented and integrated AWS security findings (Guarduty, Security Hub) with SOC processes, aligning cloud-native posture (security controls) with SIEM correlation, incident response workflows and compliance frameworks.
- Provided mentorship to Tier 1 and Tier 2 analysts and acted as Tier 3 escalation point, overseeing a 25+ member SOC team to enhance detection maturity, threat hunting, incident triage and analyst career development.

EY (Ernst & Young) - Barcelona, Spain

Senior IV Security Specialist (06/2018 - 05/2021)

Led complex cybersecurity initiatives for critical clients across government and automotive sectors, including SEAT (Volkswagen Group) and the Government of Catalonia. Focused on large-scale SIEM implementations, vulnerability management transformation, and detection engineering.

Achievements

- Directed and implemented a $3M budget of a multi-SIEM ecosystem project for Spain's largest automotive manufacturer (SEAT, Volkswagen Group), integrating Elastic and IBM QRadar to strengthen threat detection and response across hybrid environments.
- Migrated vulnerability management system for SEAT (Volkswagen Group) from McAfee MVM to Nessus across 1,500 production servers, improving scan coverage and aligning with ISO/IEC 27001 and NIST CSF.
- Implemented a threat intelligence workflow aligned with the ENISA framework, applying a structured lifecycle to validate and contextualize IOCs via MISP clusters, ensuring relevance to emerging TTPs and supporting SOC operations.
- Designed specific taxonomies to standardize the intake of diverse log sources, establishing a dedicated framework to unify and normalize all data ingestion.
- Implemented API-based monitoring and DLQ mechanisms in high-volume SIEM pipelines, achieving 0% event loss and full data integrity by validating log delivery across distributed environments and ensuring reliable ingestion.
- Implemented ML-driven analytics in Elastic SIEM to monitor 40+ production Jump Servers, enhancing anomaly detection and delivering high-value detection use cases for threat hunting and compliance.
- Integrated QRadar Risk Manager with 30+ Check Point firewalls, enabling automated policy analysis and real-time compliance alignment across perimeter defenses.
- Developed a cyber threat heatmap dashboard for the largest automotive plant in Spain, offering C-level visibility by physical site; later adopted globally.
- Managed the Proof of Concept for NDR solution at SEAT Company, evaluating ExtraHop with gigamon for network traffic capture.

- Led a team of 5 security engineers, delivering and maintaining critical cybersecurity projects for the Government of Catalonia (CESICAT).

NECSIA - Barcelona, Spain

Senior Security Specialist (3/2018 - 6/2018)

Specialized in SIEM implementation and optimization using IBM QRadar and Splunk to enhance security operations for clients. Provided cybersecurity consulting services, focusing on improving security tools and processes to align with industry standards.

Achievements

- Supported Splunk Enterprise deployments (ES) (v7.x) including indexer clusters, search head clusters, and deployment servers for enterprise customers, ensuring reliable log ingestion and high availability

Davinci - Barcelona, Spain

IT Security Consultant (12/2017 - 02/2018)

Conducted SIEM audits (QRadar, RSA, Splunk) ensuring best practices compliance, and provided GDPR technical consulting.

Ibermática - Barcelona, Spain

Infrastructure and systems technician (05/2017 - 07/2017)

Managed and supported security solutions (L3). Ensured the integrity and reliability of distributed system infrastructures.

Makros SPA - Santiago, Chile, Security Specialist Engineer (01/2013 - 12/2016)

Delivered security network infrastructure projects across Latin America, specializing in the design, deployment, and management of NGFWs, endpoint protection,network protection, email security, IDS/IPS systems, and related technologies in complex enterprise and government environments.

ST Computación - Santiago, Chile, Network Administrator (10/2010 - 5/2012)
Quintec - Santiago, Chile, Helpdesk Technician (01/2010 - 08/2010)n

CERTIFICATIONS

Splunk Core Certified User (SPLK-1001)	2025
CEH *(Certified Ethical Hacker, EC-Council)*	2025
AZ-500 *(Azure Security Engineer Associate, Microsoft)*	2025
CISM *(Certified Information Security Manager)*	2025
Intensive Plus Speaking English Skills English (B2) - Emerald Institute, Dublin, Eire	2025
CASP+ *(CompTIA Advanced Security Practitioner (CAS-004)*	2024
IBM Security QRadar SIEM V7.2.8 – Fundamental Administration (C2150-624-ENU)	2018

LANGUAGES

- Languages - Spanish (native), English (proficient), Italian (proficient), Catalan (intermediate)
- Currently learning German (A1)

EDUCATION

- Bachelor's of Science in Telematics Engineering - Institute of Technical Studies CIISA 2010-2014
- Mid-Level Telecommunications Technician - School of Science and Technology 2006-2009

ACTIVITIES

- Delivered a masterclass at IEBS Institute: How to generate an attack and how to detect IT from the SOC.
- Researching new trends in cybersecurity, AI and IT generally.
- Technical volunteer in WAF Open Source Coraza solution.

REFERENCES

Alejandro Sanchez CISO and IT CCO at **SEAT Volkswagen Group** Phone: +34 616 71 56 96 Email: alejandro.sanch@gmail.com
Bernat Canadell Cyber Defence Engineering Lead at **Swiss Re** Phone: +34 609 97 26 12 Email: bernatcanadell@gmail.com
Marc Arderius Campos Cyber Security Director at **EY** Phone: +34 630 48 13 77 Email: m.arderius@gmail.com