Evanildo Ribeiro

SOC Analyst | Detection Engineer | AI Security Research

London, UK · +44 7411 269534 · contact@evanildoribeiro.com · linkedin.com/in/evanildoribeiro · www.evanildoribeiro.com
Work Authorisation: UK | EU | Brazil · Languages: English (Fluent) | Portuguese (Native) | Spanish (Intermediate)

PROFESSIONAL SUMMARY

SOC Analyst and Detection Engineer with hands-on experience building and tuning detections in Splunk and Elastic, analysing endpoint and network telemetry, and supporting ATT&CK-mapped incident response across Linux, Windows, and network environments. Delivered project, internship, and academic work, including a First-Class final-year IoT anomaly detection project using convolutional autoencoders. Earlier IT support and management experience adds breadth across enterprise systems, access control, and team leadership. Currently pursuing CompTIA Security+ (Sep 2026) and Microsoft SC-200. Actively researching AI security, with a focus on adversarial robustness, model integrity, and the intersection of machine learning and threat detection.

TECHNICAL SKILLS

SIEM & Detection:
Splunk (SPL), Elastic Stack (KQL/EQL)

Scripting:
Python, Bash

Network Analysis:
Zeek, Wireshark, PCAP analysis

Frameworks:
MITRE ATT&CK, Incident Triage, Vulnerability Assessment

Endpoint:
Sysmon, Windows Event Logs, Linux Auditd

General:
Excel, Google Sheets, Technical Documentation

PROFESSIONAL EXPERIENCE

Applied Cryptography: Secure File Sharing

Dec 2025 – Mar 2026

Independent Security Project · London, UK

- Designed and built a Flask-based encrypted file-sharing system enforcing a verify-then-decrypt model to eliminate decryption oracle risks, applying cryptographic best practices throughout the full request lifecycle.
- Implemented AES-256-GCM for symmetric encryption, RSA-OAEP for key encapsulation, and RSA-PSS for digital signatures, ensuring authentication, encryption and non-repudiation across all file transfers.
- Integrated ECDH P-256 with HKDF-derived session keys to achieve Perfect Forward Secrecy, preventing retrospective decryption of captured sessions even in the event of long-term key compromise.
- Validated the system with rigorous tests covering tamper detection, key misuse scenarios, and signature forgery attempts, achieving full pass coverage and confirming resistance to common cryptographic attack vectors.

Research Assistant in Cybersecurity (Internship)

Jun 2025 – Dec 2025

University of West London · London, UK

- Investigated detection coverage across Linux and Windows environments by instrumenting 7 log sources in Splunk and Elastic, systematically evaluating visibility gaps across authentication, process, and network event categories.
- Conducted empirical analysis of host and network telemetry to characterise brute-force patterns, anomalous outbound connections, and persistence mechanisms, contributing to a 40% improvement in simulated incident triage speed.
- Developed Python and Bash tooling to automate log aggregation, threshold-based alerting, and SIEM ingestion pipelines, enabling reproducible experimental workflows during detection testing.

- Researched and refined SPL and Elasticsearch detection logic to reduce false positive rates by 35% while preserving ATT&CK technique coverage, applying iterative query optimisation informed by adversary behaviour models.
- Participated in structured incident response exercises, including host isolation, evidence collection, and memory capture, producing ATT&CK-mapped timelines to support forensic analysis and remediation research.

IT Support & Systems Technician

Mar 2015 – Dec 2019

Gráfica Rio LTDA · Linhares, Brazil

- Supported Windows and macOS workstations across the business, resolving hardware, software, and connectivity issues as the sole internal IT contact.
- Set up and maintained network infrastructure, including Wi-Fi, cabling, shared resources, and print system connectivity, reducing operational downtime for business-critical equipment.
- Managed user accounts, password resets, and access permissions across shared systems, improving access reliability and strengthening basic security controls.
- Standardised device configurations and documented repeat fixes, shortening resolution time for common support requests by 45%.

Manager

Feb 2010 – Nov 2014

Headmasters Ltd · London, UK

- Managed a team of 18 and improved operational efficiency by 35% through workflow redesign and structured coaching.
- Delivered health and safety training and maintained zero compliance infractions over a three-year period.
- Coached and led a team in needs-based client consultations, driving product recommendations that aligned with individual customer profiles and consistently contributed to sales targets.

KEY PROJECTS

Security Monitoring & Threat Detection

Oct 2024 – Feb 2025

Personal Lab Projects · London, UK

- Built a Linux authentication monitoring workflow in Python and Bash that parsed /var/log/auth.log, grouped failed logins by IP and username, and generated threshold-based alerts, reducing manual log review time by 65%.
- Analysed PCAP data with Zeek and Wireshark to identify SSH anomalies, scanning behaviour, and suspicious outbound traffic, producing dashboards that reduced investigation time in test scenarios by approximately 20 minutes (45%).
- Deployed Sysmon and correlated process, registry, and scheduled task events to detect persistence activity, mapping coverage across 9 MITRE ATT&CK techniques.
- Wrote and tuned Splunk and Elastic queries targeting brute-force attempts, injection activity, and scheduled task abuse, reducing false positives by 38% during validation exercises.

Final-Year Project – IoT Anomaly Detection

Sep 2023 – Jun 2024

University of West London · London, UK

- Built an IoT anomaly detection model using a convolutional autoencoder with attention mechanisms, improving separation between normal and anomalous activity across 15 test scenarios.
- Prepared and structured training and evaluation datasets, creating a repeatable workflow that shortened model testing cycles by 55%.
- Produced evaluation reports and visualisations comparing reconstruction error trends and model performance, presenting findings clearly to both technical and non-technical audiences.
- Documented methodology, results, and limitations in a final project report awarded First-Class standard within the degree programme.

EDUCATION

BSc (Hons) Cyber Security – First Class Sep 2020 – Jul 2024

University of West London · London, UK

CMI Level 3 Award in First Line Management (QCF) Sep 2013 – Dec 2013

Chartered Management Institute · London, UK

CERTIFICATIONS & TRAINING

- CompTIA Security+ — Scheduled: Sep 2026
- Microsoft SC-200 Security Operations Analyst — In progress
- Certified Ethical Hacker (CEH) — Studying

ADDITIONAL INTERESTS

Capture The Flag (CTF) challenges · AI Security research · lab write-ups · Brazilian Jiu-Jitsu