HENRIQUE CARVALHO

Porto • henrique1781@gmail.com • linkedin.com/in/henrique-carvalho-849450156 •
https://github.com/henryu1781

Cybersecurity Specialist & Systems Architect

Emerging Cybersecurity Professional with a specialized focus on Security Operations (SOC) and Defensive Architecture. I combine a rigorous analytical mindset with a structured approach to incident triage and risk mitigation. Adept at operating Linux ecosystems, I execute deep network traffic inspection, security event monitoring, and forensic log analysis to detect and neutralize threats. Driven by continuous learning and built for high-pressure environments, I am equipped to audit, protect, and harden critical infrastructures.

WORK EXPERIENCE

Hospitality Sector
High-Pressure Operations Management (Night Shift) — Porto

- Executed operational control in high-stress, time-critical environments, maintaining absolute accuracy and focus under pressure.
- Forged advanced situational awareness, rapid decision-making, and concurrent task management skills.
- Maintained strict operational discipline and seamless team collaboration during critical peak periods. (Note: These soft skills directly mirror the psychological requirements of an Incident Response / SOC environment).

EDUCATION

Higher Technical Professional Course (CTeSP) in Cybersecurity
ISTEC Porto — Porto

Core Focus: System and Network Security, Cryptography, Threat Modeling, Hardening, Networks and Protocols, Incident Response.

PROJECTS

Secure App Architecture & Refactoring

- Engineered the refactoring of a legacy PHP incident reporting application into a secure, modern Flutter/Dart environment.
- Implemented rigorous secure coding standards, applying Argon2id password hashing concepts, AES-256 encryption principles, and JWT-based secure session handling.
- Drafted comprehensive technical documentation targeting incident management, traceability, and strict security compliance.
- Aligned the complete project lifecycle with defensive security principles.

SOC Operations & Network Forensics Labs

- Executed deep network traffic analysis utilizing Wireshark to isolate abnormal patterns and identify malicious behavioral signatures.
- Performed forensic log analysis across Linux systems to pinpoint failed authentication vectors and potential brute-force intrusions.
- Mapped identified threat behaviors directly to the MITRE ATT&CK framework, producing structured, actionable intelligence reporting.
- Deployed foundational system hardening protocols, focusing on strict SSH configurations and access control policies.

Enterprise Network Routing & Security Design

- Architected and provisioned highly segmented network topologies leveraging VLANs and dynamic routing protocols (OSPF, EIGRP, RIP) in simulated environments.
- Integrated centralized DHCP, precise authentication measures, and access control mechanisms.
- Optimized infrastructure design to maximize network visibility and continuous security monitoring, specifically tailored for SOC readiness.

Threat Modeling & Wargaming Operations

- Applied Cyber Kill Chain, Unified Kill Chain, and MITRE ATT&CK methodologies to dissect and analyze complex attack scenarios.
- Co-developed TechVoyer, a custom threat-modeling framework emphasizing aggressive reconnaissance and defensive countermeasures.
- Formulated structured architectural diagrams and intelligence reports mapping attacker TTPs to specific defensive controls.

SKILLS

Defensive Operations (SOC): Alert Triage, Basic Incident Analysis & Response, Security Event Monitoring

Infrastructure & Hardening: Docker, Linux Environments (Arch Linux, Ubuntu Server), System Hardening, User & Permission Management

Network Intelligence: Deep Packet Inspection, DHCP, DNS, Network Segmentation, TCP/IP, Traffic Analysis (Wireshark)

Security Tooling: Caido (Traffic & Request Analysis), Git/GitHub, Nmap (Reconnaissance)

Operational Mindset: Highly Analytical Thinking, Precision under Stress, Rapid Problem-Solving, Team Collaboration