MAC CALARCO

SECURITY ANALYST • DETECTION ENGINEER • THREAT HUNTER
North Bay, ON | Open to Remote | Portfolio | Github | Linkedin | fev.dev@proton.me

PROFILE

Security analyst with a builder's mindset, specializing in detection engineering and threat-focused SIEM tuning. Built 10+ open-source security platforms across offensive and defensive disciplines, including a network forensics platform with eBPF process attribution and FFT-based C2 beacon detection (Shrike), a 49-detector phishing kill-chain extension with 1439 automated tests (Lure), and a Windows Event Log DFIR platform with 31 Sigma rules and cross-SIEM export (Vigil). Strong foundation in incident triage, log correlation, IOC enrichment, and MITRE ATT&CK mapping. Client-facing background with 10+ years translating complex technical findings into clear, actionable solutions. **ISC2: Certified in Cyber Security (CC) | TryHackMe: (SAL1) [In Progress]**

EXPERIENCE

Independent Security Researcher & Developer | Self-Employed | *2023 – Present*

- Developed and tuned SPL detection logic in Splunk covering LOTL/LOLBin abuse, credential access patterns, and lateral movement, reducing false positives and improving coverage for evasive adversary behavior.
- Assessed 5+ production applications and APIs against OWASP and API Top 10; delivered proof-of-concept exploits for XSS, CSRF, SQLi, and WAF bypass vectors mapped to CISA KEV for remediation prioritization.
- Ran full-scope attack surface assessments combining port scanning, subdomain takeover detection, default credential testing, and secret scanning across public repositories and AI infrastructure.
- Validated exploitability of JWT flaws (Algorithm Confusion, KID Injection, Null Signatures), alongside AiTM interception and OAuth abuse chains; drafted hardening guides and secure implementation patterns.

Technical Audio Engineer & Educator | Self-Employed | *2014 – Present*

- Applied structured root-cause analysis and signal processing logic to diagnose and resolve complex hardware/software failures in data-intensive production environments.
- Designed and enforced backup and recovery strategies (3-2-1 model, RAID redundancy), regularly executing validated restoration tests to ensure continuous system availability.
- Implemented least-privilege access controls and asset protection strategies across 20+ clients, ensuring the secure handling of sensitive data in multi-user infrastructure.

HOME LAB & DEFENSIVE INFRASTRUCTURE

- Built and deployed a VLAN-segmented home lab across 15+ devices (Pi 5, Synology NAS, GL.iNet, Umbrel), enforcing inter-network isolation, DNS filtering, and VPN kill-switch policies to reduce attack surface.
- Deployed a multi-endpoint Splunk SIEM environment to ingest and correlate live telemetry while validating detection logic through targeted attack simulations.
- Executed structured triage workflows, alert investigation, and IOC enrichment using VirusTotal and Shodan to simulate production SOC investigation practices.

SECURITY RESEARCH & TOOL DEVELOPMENT

Shrike: *eBPF Network Forensics & Threat Hunting Platform* (Github)

- Engineered an eBPF-based network forensics platform that maps real-time telemetry to originating PIDs and binary paths without requiring payload decryption in TLS 1.3 environments.
- Developed behavioral detection for HTTP/2 C2, WebSocket exfiltration, mTLS C2, and DNS rebinding using FFT-based beacon analysis and a custom n-gram perplexity scorer to identify LLM-generated DGA domains.
- Instrumented TLS/QUIC fingerprinting (JA3/JA4/JARM/HASSH), AD attack detection, NTLM relay, IPv6 attack patterns, and CISA KEV correlation to identify threat actor TTPs in encrypted traffic across 25+ detectors.

Lure: *Browser-Native Phishing Defence Platform & Email Analysis CLI* (Github)

- Built a multi-layered phishing defense platform comprising a Chrome MV3 extension and a Python-based email analysis CLI, featuring 49 detectors and a suite of 1439 automated tests.
- Authored a real-time behavioral scoring engine detecting AiTM proxies (Evilginx/Modlishka), OAuth abuse (Storm-2372), FIDO downgrades (Tycoon 2FA), WebSocket credential exfiltration, and canvas/CSS-based harvesting, identifying sophisticated threats that bypass traditional blacklists.

- Automated the forensic analysis of raw .eml files using YARA-X and SPF/DKIM/DMARC validation, mapping findings to MITRE ATT&CK and NIST SP 800-61r3 to accelerate incident triage and response.

`Corsair`: *HTTP Security Header Analysis & CVE Correlation* (Github)

- Built a specialized scanner to identify unkeyed header injection points (X-Forwarded-Host, X-Forwarded-Scheme) and header reflections susceptible to web cache poisoning, including HTTP/2 pseudo-header poisoning and QUIC/HTTP3 Alt-Svc injection vectors.
- Developed detection logic for sensitive contexts within CSP and Location headers to identify XSS and open-redirect vectors; implemented a non-destructive cache oracle for thorough vulnerability discovery without polluting production environments.
- 60+ header checks with compliance mapping (OWASP 2025, PCI-DSS 4.0, SOC 2), A–F posture grading, historical drift detection, live CISA KEV correlation, and SARIF output for CI/CD integration.

`Vigil`: *Windows Event Log DFIR & Detection Engineering Platform* (Github)

- Built a browser-native DFIR platform with a 12-module processing pipeline to normalize forensic data from Hayabusa, Chainsaw, and raw EVTX, enabling high-speed triage of Windows event logs without server-side infrastructure.
- Implemented automated detection for Living-off-the-Land (LOTL) techniques and credential access (DCSync/Kerberoasting) utilizing Shannon entropy scoring and auto-reassembly of fragmented EID 4104 PowerShell ScriptBlocks.
- Authored 31 custom Sigma rules mapped to MITRE ATT&CK v15 across 8 tactics and 35 techniques; automated the generation of production-ready KQL, SPL, EQL, and VQL queries.

Offensive & Supporting Tools: **`GitExpose`** (AI Infrastructure & Supply Chain Security) • **`Stiletto`** (SQLi & WAF Bypass) • **`Restless`** (OWASP API Top 10) • **`ShadowHunter`** (Threat Intel, Neo4j IOC Correlation) • **`Prizm`** (Secret Scanner) • **`Dockyard`** (Port Scanner) • **`ClaimJumper`** (JWT Toolkit) • **`Argus`** (Credential Scanner) • **`Specter`** (Subdomain Takeover)

CAPABILITIES

Security Operations & SIEM

- SIEM Deployment, Log Ingestion, & Alert Triage (Splunk, SPL)
- Detection Engineering & False Positive Reduction
- MITRE ATT&CK Mapping & Coverage Development
- Alert Triage & Escalation Workflows

Incident Response & DFIR

- Windows Event Log Analysis (EID 4624, 4688, 4104, 7045+)
- Log Correlation & Timeline Reconstruction
- IOC Enrichment (VirusTotal, Shodan, AbuseIPDB)
- YARA-X Rule Development & Malware Triage

Network Security & Traffic Analysis

- PCAP Analysis (C2 Beaconing, DNS Tunneling, FFT)
- Port Scan Detection & Network Behavior Analysis
- TLS Fingerprinting (JA3/JA4/JARM/HASSH)
- HTTP Security Header & Cache Poisoning Analysis

Detection Engineering

- LOTL Technique & LOLBin Abuse Detection
- Sigma Rule Authoring & Cross-SIEM Query Translation (SPL, KQL, EQL, VQL)
- Behavioral Correlation & Entropy-Based Detection
- PowerShell Deobfuscation & ScriptBlock Analysis (EID 4104)

Vulnerability & Threat Management

- CVE/CWE Analysis & Prioritization (CISA KEV, NIST NVD)
- OWASP Top 10 / API Top 10 Risk Identification
- System Hardening (CIS Benchmarks)
- CI/CD Security Checks & SARIF Integration

Defensive Infrastructure & Hardening

- VLAN Segmentation (15+ Devices)
- Identity & Access Controls (MFA, RBAC, SSH Keys)
- Secure Infrastructure Design (NAS, VPN, DNS Filtering)
- Backup & Recovery (3-2-1, RAID)

TECHNICAL STACK & TOOLING

Languages: Python (Automation), TypeScript/JavaScript, Bash, PowerShell, SQL.

Frameworks/Standards: Sigma, YARA, MITRE ATT&CK, NIST, OWASP, PCI-DSS.

Environments: AWS (IAM, S3), Docker, Microsoft 365, Windows, Linux, MacOS.