BRADLEY FREEMAN

Senior Cybersecurity & Infrastructure Security Engineer
Batavia / Cincinnati, OH • (513) 720-2005 • bradleyjfreeman@gmail.com • bradleyfreeman.com • linkedin.com/in/bradleyfreeman

PROFESSIONAL SUMMARY

Senior Cybersecurity Engineer & Systems Architect with 20+ years of experience spanning defensive operations, vulnerability management, malware analysis, and high-throughput security event pipelines. Proven background conducting deep vulnerability assessments (TP/FP verification), dissecting malicious payloads, and managing offensive security workflows alongside 3M+ EPS ingestion infrastructure and SOAR automation.

TECHNICAL EXPERTISE

Threat & Malware Analysis	Malware Dissection & Payload Analysis, Behavioral Tracking, Reverse Engineering, Wireshark, IOC Extraction
Vulnerability & Offensive Sec	Vulnerability Assessments & TP/FP Triage, Attack Surface Testing, Remediation Roadmaps, System Hardening
SIEM & Telemetry Ingestion	Splunk, High-Throughput Ingestion Pipelines (3M+ EPS), Kafka, Syslog Normalization, Custom Parsers & Correlation
Security Automation & IR	Incident Response Playbooks, SOAR (Swimlane Turbine), EDR/XDR Integration, Python, REST APIs, Ansible, Bash
Infrastructure & Network	Firewall Telemetry, IPTables, Linux/Windows Hardening, Directory Services/RBAC, Virtualization (VMware/Xen)

PROFESSIONAL EXPERIENCE

Technical AI Trainer & Security Evaluator **2025 – Present**

- Evaluate and benchmark advanced LLMs and autonomous agents on cybersecurity engineering, exploit triage, vulnerability discovery, and script automation workflows.

Swimlane Turbine Certified SOAR Developer • DeepSeas **Jan 2024 – July 2025**

- Architected automated security orchestration workflows using Swimlane Turbine, significantly reducing manual response times across enterprise multi-system infrastructures.
- Developed modular Python-based integrations for incident response, automating alert enrichment, IOC validation, and cross-tool containment actions.

SOAR Engineer • AHEAD **June 2022 – Oct 2023**

- Engineered custom SOAR playbooks and REST API connectors linking SIEM detection alerts to automated remediation pipelines for enterprise-level clients.
- Partnered with enterprise IT and network teams to conduct attack surface audits, validate firewall configurations, and automate vulnerability mitigations.

Senior Infrastructure & Security Applications Engineer (Lead) • Nuspire Networks **March 2009 – Sep 2021**

- **Vulnerability Management & Triage:** Conducted enterprise vulnerability assessments, performing manual deep-dive verification to accurately classify True Positives vs. False Positives and author actionable remediation guidance.
- **Malware Analysis & Threat Dissection:** Dissected suspicious binaries and obfuscated payloads using packet capture (Wireshark) and behavioral analysis to uncover hidden malicious actions and extract actionable IOCs.
- **Offensive Security Management:** Managed offensive security operations and internal attack surface testing in corporate environments to proactively identify and remediate exploitable vectors.
- **Private Cloud & Distributed Pipelines:** Architected and maintained a petabyte-scale private cloud Hadoop ecosystem (HDFS, Kafka, Impala) on bare-metal hardware, scaling log ingestion past 3,000,000 events/sec with 99.999% uptime.
- **Protocol Engineering:** Intercepted and reverse-engineered proprietary Fortigate network security protocols via Wireshark, building high-throughput parsing engines to normalize byte streams into structured key-value pairs for SIEM correlation.

Linux Systems Administrator / Web Developer • ByteHosting Internet Services **Feb 2007 – Dec 2008**

- Maintained multi-tenant Linux server environments and built secure web applications, focusing on performance tuning, access control, and fundamental server hardening.

CERTIFICATIONS & CORE SECURITY TOOLKIT

• **Certifications:** Swimlane Turbine Certified Developer • CompTIA Security+ • CompTIA Network+ • CompTIA Linux+ • CompTIA A+
• **Core Security Toolkit:** Wireshark, Splunk, Python, REST APIs, IPTables, Kafka, Linux/Unix Internals, VMware, Docker, Git