Jawad Charafeddine

(832)-217-5259 • contact@jawad.ch • github.com/jawadchar • linkedin.com/in/jawadchar

EXPERIENCE

LogN Pacific Dec. 2025 – present

Cybersecurity Support Analyst (Vulnerability Management & SecOps – Contract)

Vulnerability Management:

- Conducted vulnerability scans, provided detailed reports, and implemented PowerShell-based remediations, contributing to a 100% reduction in critical, 90% in high, and 76% in medium vulnerabilities for the server team.
- Performed vulnerability assessments and risk prioritization using Tenable across Windows and Linux environments.
- Executed secure configurations and compliance audits (DISA STIG) with Tenable to meet industry standards.
- Automated remediation processes and STIG implementations using PowerShell to address critical vulnerabilities.
- Deep understanding of the "soft" side of Vulnerability Management: rapport, trust, transparency, and business need.

Security Operations:

- Performed threat hunting with EDR, detecting IoCs from brute force attacks, data exfiltration, and ransomware.
- Designed, tested, and published advanced threat hunting scenarios for incident response tabletop exercises
- Developed custom detection rules in Microsoft Defender for Endpoint to automate isolation and investigation of compromised systems.
- Reduced brute force incidents by 100% by implementing inbound NSG/firewall rules to limit Internet exposure.
- Created Microsoft Sentinel dashboards to monitor logon failures and malicious traffic using threat intelligence.
- Experienced with KQL (similar to SQL/SPL); used to query logs within the SIEM and EDR platform.

G&E Impressions, Inc. May 2025 – Dec. 2025

IT Support Specialist

- Supported Windows endpoints by diagnosing hardware, software, and configuration issues affecting system availability.
- Resolved network connectivity issues (Wi-Fi, DNS, basic TCP/IP) to maintain reliable access to business systems.
- Applied baseline security practices, including OS patching, credential hygiene, backup procedures, and basic access controls to reduce operational and security risk.
- Documented incidents, resolutions, and process improvements to standardize troubleshooting workflows.
- Provided on-call support by triaging issues and prioritizing remediation based on impact and urgency.

Self-directed Home Lab May 2025 – present

Cybersecurity Analyst

- Built and maintained a SOC-focused home lab (Kali + Windows) to simulate alert triage, host-based investigations, and network traffic analysis using repeatable investigation workflows.
- Analyzed DNS and network traffic in Wireshark to identify suspicious resolution patterns, command-and-control indicators, and visibility trade-offs related to DNS over HTTPS (DoH).
- Executed controlled exploitation scenarios in isolated lab environments and investigated post-compromise behavior by analyzing process execution, command-line activity, and outbound network connections.
- Correlated host and network artifacts to assess potential impact, persistence mechanisms, and attacker objectives during simulated security incidents.
- Documented investigation steps, findings, and remediation recommendations, aligning technical observations with vulnerability management and security hardening processes.

EDUCATION

University of Houston

Bachelor of Science in Psychology with Biology minor

CERTIFICATIONS

CompTIA Security+ ; CompTIA CySA+; THM Cyber Security 101

ADDITIONAL SKILLS AND TECHNOLOGIES

Sentinel, KQL, IAM, EDR, ELK stack, Syslog, MITRE ATT&CK Mapping, CVE/CWE Management, CVSS Scoring, OWASP Top 10, Risk Prioritization, Vulnerability Remediation, PowerShell/BASH Scripting, Firewall/NSG Configuration, NIST 800-37: Risk Management Framework, NIST 800-53: Security and Privacy Controls, NIST 800-61: Computer Security Incident Handling Guide, NIST 800-40: Guide to Enterprise Patch Management Planning, NIST Cybersecurity Framework, PCI-DSS, GDPR, HIPAA, ISO 27001, SOC 2 Compliance Support, Audit Documentation, OS Hardening, Imaging and Deployment, Account Provisioning, IaaS/PaaS/SaaS