Bryan Miller

Los Angeles, CA | 714-916-1412 | bryan.p.miller7@gmail.com
linkedin.com/in/bryan-p-miller | bryanpmiller.com | github.com/bryanpmiller

PROFESSIONAL SUMMARY

Security+ certified cybersecurity analyst with hands-on experience spanning vulnerability management, security operations, threat hunting, detection development, system hardening, and security automation across Windows, Linux, and Azure environments. Experienced with Tenable/Nessus, Microsoft Defender for Endpoint, Microsoft Sentinel, KQL, and PowerShell to identify risk, investigate threats, automate remediation, and strengthen security controls. U.S. Marine and summa cum laude cybersecurity graduate with a 3.99 GPA.

CYBERSECURITY EXPERIENCE

Cybersecurity Support Analyst Intern Jan 2026 - Present

Vulnerability Management & Security Operations | Log(N) Pacific

- Supported vulnerability scanning, risk prioritization, and remediation across Windows and Linux systems, contributing to server-team reductions of 100% in critical findings (2 to 0), 92% in high findings (12 to 1), and 88% in medium findings (17 to 2).
- Performed secure-configuration and DISA STIG reviews with Tenable/Nessus and developed PowerShell remediation and hardening workflows to reduce manual effort and accelerate finding closure.
- Investigated EDR/SIEM telemetry with Microsoft Defender for Endpoint, Microsoft Sentinel, KQL, and Azure Log Analytics for brute-force activity, data exfiltration, and ransomware indicators; built custom detection rules and dashboards to improve investigative visibility.
- Configured Azure NSGs and virtual-machine host firewalls to restrict inbound exposure, contributing to a 100% reduction in observed brute-force incidents during the measured period.

SELECTED CYBERSECURITY PROJECTS

- **Password Spray Threat Hunt:** Used Microsoft Defender for Endpoint Advanced Hunting and KQL within a Microsoft Sentinel workflow to trace an RDP compromise through execution, persistence, evasion, C2, and attempted exfiltration; mapped evidence to MITRE ATT&CK and identified detection opportunities.
- **Akira Ransomware Threat Hunt:** Analyzed MDE telemetry with KQL to scope affected hosts and reconstruct remote access, staging, lateral movement, defense evasion, data staging, and impact; documented IOC timing, ATT&CK mappings, evidence gaps, and detection opportunities.
- **Vulnerability Management & DISA STIG:** Reduced Tenable findings from 32 to 4 through authenticated scanning and remediation; scripted and validated selected Windows 11 STIG controls with PowerShell.

ADDITIONAL EXPERIENCE

Warehouse & Facilities Manager | UTB Ventures | Los Angeles, CA | Mar 2015 - Jan 2026

- Managed daily facility operations while installing, maintaining, and troubleshooting the network and IP security-camera system, including connectivity and device-access issues.

Field Artillery Fire Control Man, Fire Direction Control | United States Marine Corps | Sep 2009 - Dec 2012

- Led teams of 3-8 Marines as an NCO while operating, maintaining, and troubleshooting mission-critical communications and targeting systems under time-sensitive conditions.

EDUCATION & CERTIFICATIONS

Norwich University: B.S. Cybersecurity, Computer Forensics & Vulnerability Management | Mar 2025
GPA: 3.99 | Summa Cum Laude
Cypress College: A.S. Business Administration | May 2021 | Graduated with Honors
Certifications: CompTIA Security+ | May 2026 • Google AI Professional | Jul 2026

TECHNICAL SKILLS

Vulnerability Management & Hardening: Tenable/Nessus, Authenticated Scanning, CVE/CWE Review, CVSS Scoring, Risk Prioritization, Remediation Tracking, DISA STIG, Windows/Linux Hardening
Security Operations & Detection: Microsoft Defender for Endpoint, Microsoft Sentinel, KQL, SIEM/EDR Analysis, Threat Hunting, Incident Triage, MITRE ATT&CK Mapping, Detection Rules, Azure Log Analytics
Automation & Systems: PowerShell, Bash, Python, SQL, Active Directory, Windows, Linux
Network & Cloud Security: Azure NSGs, Firewalls, pfSense, Wireshark, VLANs, SSH, RDP