Danielle Vivolo

Email: danielle.vivolo@gmail.com | LinkedIn: linkedin.com/in/daniellevivolo | GitHub: github.com/dvivolo

Professional Summary

Cybersecurity Analyst with 6+ years of combined experience in security operations, incident response, and threat detection. Strong background in DFIR, SOC processes, and documentation of detection workflows. Currently expanding expertise in DevSecOps, Terraform, and cloud security (AZ-500 in progress). Adept at bridging detection engineering logic with analyst actionability through clear documentation, playbooks, and process improvements.

Key Skills

- Incident Response (DFIR, triage, containment, recovery)
- SOC Operations & Detection Engineering
- Microsoft Sentinel, Defender for Endpoint, Arkime, Splunk
- Network packet analysis, threat hunting, SIEM tuning
- Playbook and runbook documentation
- Terraform & Infrastructure-as-Code (learning)
- Cloud Security (Azure) – AZ-500 in progress
- PowerShell scripting, automation basics

Professional Experience

Applied Research Laboratories – Security Analyst
Feb 2025 – Present | Austin, TX

- Perform network packet analysis using Arkime, Wireshark, and Splunk to identify and investigate security events.
- Support CMMC compliance efforts, documenting detection workflows and early-stage SOC processes.
- Collaborate with engineers to improve detection logic and analyst actionability despite limited automation.
- Develop playbooks and triage guides to streamline incident response.

Texas Legislative Council – Security Analyst
Nov 2018 – Feb 2025 | Austin, TX

- Monitored SIEM alerts (Microsoft Sentinel, Fidelis) for malicious activity across state networks.
- Led triage and containment efforts for endpoint and network-based incidents.

• Authored SOC triage guides and detection workflow documentation to reduce alert fatigue.
• Collaborated with IT teams on response actions, incident reports, and compliance audits.

Education

Master of Science in Cybersecurity – Western Governors University (2025)
Bachelor of Science in Web and Multimedia – Westwood College

Certifications

• CompTIA SecurityX (in progress, test date Nov 7, 2025)
• AZ-500 Microsoft Certified: Azure Security Engineer (in progress)

Projects & Learning

• Terraform IaC Labs – Building secure Azure environments via Terraform modules.
• DFIR Playbooks – Authored investigation workflows for SOC teams, bridging detection logic with analyst response.
• DevSecOps Roadmap – 12-week hybrid learning plan integrating SecurityX prep with cloud security and IaC.