Danielle Vivolo

danielle.vivolo@gmail.com | linkedin.com/in/daniellevivolo

PROFESSIONAL SUMMARY

Cybersecurity Analyst III and cyber threat intelligence professional with a Master's in Cybersecurity and Information Assurance and certifications including CompTIA CySA+, PenTest+, Security+, and ISC2 Certified in Cybersecurity. Experience spanning SOC operations, threat intelligence, incident response, vulnerability research, threat hunting, security automation, network analysis, and executive reporting. Skilled at translating complex technical findings into actionable intelligence for technical teams and leadership.

CORE SKILLS

Cyber Threat Intelligence (CTI) • SOC Operations • Incident Response • Threat Hunting • CVE & Vulnerability Research • Threat Actor & Campaign Analysis • SIEM & Log Analysis • Network / NetFlow Analysis • IOC Enrichment & Correlation • Executive & Technical Reporting • Security Automation • KQL • Splunk • Microsoft Sentinel • Defender for Endpoint • SentinelOne • CrowdStrike • RSA NetWitness • Corelight • Google Threat Intelligence / VirusTotal • Recorded Future • Intel 471 • GreyNoise • Censys • CTIX • ThreatMon • PowerShell • Logic Apps • Palo Alto

PROFESSIONAL EXPERIENCE

Texas Department of Information Resources / Texas Cyber Command Oct 2025 - Present
Cybersecurity Analyst III - Cyber Threat Intelligence | Austin, TX

- Conduct cyber threat intelligence research and analysis on vulnerabilities, threat actors, campaigns, and cyber incidents affecting Texas government and public-sector organizations.
- Research and assess CVEs for exploitability, active exploitation, exposure, and operational impact; translate technical findings into actionable intelligence and risk-focused reporting.
- Support high-priority cyber incidents through threat research, infrastructure analysis, IOC enrichment, log and network-data correlation, and investigative NetFlow analysis.
- Produce intelligence reports, incident assessments, risk and exposure findings, weekly intelligence products, and executive-level briefings for technical teams and leadership.
- Conduct threat hunting and investigative analysis using SentinelOne and CrowdStrike EDR, correlating endpoint telemetry with network data, threat intelligence, and other security sources to identify and assess suspicious activity.
- Collaborate across threat intelligence, SOC, intrusion analysis, incident response, and partner teams to develop and communicate actionable findings during active investigations.
- Develop and maintain SOPs, intelligence workflows, reporting templates, and operational documentation to standardize CTI processes and improve consistency across investigations and intelligence production.

Applied Research Laboratories, The University of Texas at Austin Feb 2025 - Oct 2025
Cyber Security Analyst | Austin, TX

- Investigated and triaged security alerts in Fidelis and ServiceDesk to identify potential breaches, phishing, and malicious activity.
- Used Splunk and threat intelligence sources including VirusTotal, AbuseIPDB, ANY.RUN, and urlscan.io for forensic analysis, enrichment, and correlation.
- Authored CMMC documentation and aligned gap assessments with corrective actions; updated incident-response workflows and playbook documentation.
- Managed and closed more than 514 Fidelis alerts and 481 ServiceDesk tickets in under four months.

Texas Legislative Council Dec 2021 - Jan 2025
Cybersecurity Support Specialist | Austin, TX

- Led SOC alert triage and incident response across Microsoft Sentinel and Defender for Endpoint, handling approximately 50 Sentinel alerts and 10 phishing investigations daily.
- Developed custom Microsoft Sentinel Logic Apps and API-integrated workflows to automate categorization, escalation, and response processes.
- Performed threat hunting and investigative analysis using Microsoft security tooling and endpoint platforms; enriched investigations with VirusTotal, urlscan.io, ANY.RUN, IP geolocation, and Palo Alto sandboxing.
- Maintained Palo Alto firewall/Prisma blocklists and executed tenant-level blocks in Exchange to contain malicious infrastructure and activity.
- Created a SharePoint knowledge base of policies, procedures, and playbooks and produced data-driven reporting on incident trends for risk and operational decision-making.

Texas Legislative Council Nov 2021 - Dec 2022
System Administrator I | Austin, TX

- Provisioned and administered Windows Server virtual machines using Hyper-V and Virtual Machine Manager; managed DNS, patching, backups, disaster recovery, and Active Directory/Azure AD support.
- Built a GUI-driven PowerShell backup and restore solution to replace an internal tool and improve operational efficiency.
- Monitored infrastructure health with PRTG and performed backup and recovery operations using Veeam Backup & Replication.

Texas Legislative Council Nov 2018 - Nov 2021
Infrastructure Specialist Lead | Austin, TX

- Delivered Tier II hardware, software, networking, and TCP/IP support across a multi-building legislative campus; supported LAN/WAN infrastructure and workstation lifecycle projects.
- Mentored junior technicians, coordinated technical rollouts, and developed internal documentation to improve consistency and team knowledge.

Bar-Z Mobile Development Feb 2018 - Sep 2018
Technical Project and Client Success Manager | Austin, TX

- Managed technical projects and relationships for 300+ clients, coordinating application deployment, backend configuration, QA, escalations, and cross-functional delivery.
- Improved CRM and Agile workflows through logic-based automation and developed internal documentation and training materials.

Nortek Control / Numera Jun 2015 - Feb 2018
Technical Services Supervisor / Technical Support Specialist | Seattle, WA / Carlsbad, CA

- Supervised technical support staff and partnered with engineering through Agile scrums to resolve Tier 3 issues, product defects, and recurring field failures.
- Performed root-cause analysis that eliminated approximately $31K in unnecessary device returns; developed technical documentation, training, and support workflows.
- Provided B2B support for connected security and medical-alert devices, troubleshooting networking, firmware, hardware, and remote configuration issues.

EDUCATION & CERTIFICATIONS

Western Governors University — M.S., Cybersecurity and Information Assurance, 2025

Westwood College — B.S., Web and Multimedia Design, GPA 3.95, 2012

Certifications: CompTIA CySA+ • CompTIA PenTest+ • CompTIA Security+ • ISC2 Certified in Cybersecurity