TYLER DROXLER *droxler4@gmail.com*

Ridley Park | PA | 19078 | 610.957.2178 [Project Portfolio](#) | [LinkedIn](#)

CERTIFICATIONS & SKILLS:

- CERTIFICATIONS: CompTIA Security+, Network+, A+, (ISC)² CC, ITIL 4, LPI Linux Essentials
- TOOLS: Microsoft Azure, Defender for Endpoint, Tenable/Nessus
- LANGUAGES: Python (Scripting), Powershell
- FRAMEWORKS: NIST 800-37: Risk Management Framework, NIST 800-53: Security and Privacy Controls, NIST 800-61: Computer Security Incident Handling Guide, NIST CSF, MITRE ATT&CK

LABS & PROJECTS:

THREAT HUNT INVESTIGATION [Link] November 2025

- DESCRIPTION: Led a threat hunt investigation using Microsoft Defender for Endpoint and Log Analytics Workspace to trace file activity, process execution, and external network connections through KQL queries. Compiled an evidence backed timeline and concise incident report for management, translating raw EDR and SIEM telemetry into prioritized findings and recommended next steps.
- TOOLS USED: Microsoft Azure, Defender for Endpoint, Log Analytics Workspace, KQL

VULNERABILITY REMEDIATION PROGRAM [Link] September 2025

- DESCRIPTION: Scanned Azure VMs and services with Nessus/Tenable, prioritized high-severity risks, applied targeted fixes and automated PowerShell/Bash remediations, then validated improvements with follow-up scans to strengthen overall security posture.
- TOOLS USED: Tenable/Nessus, Microsoft Azure VMs, PowerShell

PHISHING ANALYZER TOOL [Link] August 2025

- DESCRIPTION: Built a Python tool to parse and score .eml files, extracting headers, body, links, and attachments for phishing indicators. Combined rule based keyword and URL analysis with heuristics (display name/reply-to mismatches, typosquat detection, suspicious file attachment extensions) to produce a phishing score. Implemented weighted scoring with thresholds to mitigate false positives. Integrated the program with VirusTotal to scan for known malicious domains.
- TOOLS USED: Python, VirusTotal API

EDUCATION:

Bachelor’s of Science: Cybersecurity and Information Assurance — *Expected Graduation: May 2026*

Western Governors University: College of Science & Technology

EXPERIENCE:

FIDERI NEWS NETWORK, Media, PA

Information Security Consultant October 2025 - *present*

- Designed and deployed an internal SMTP-enabled GoPhish server to run company-wide simulated phishing campaigns for on-going security awareness training. Configured email infrastructure, campaign tracking, and reporting dashboards to measure user interaction metrics including click-through and credential submission rates.
- Implemented server hardening and access controls to secure the phishing simulation infrastructure and prevent external abuse.

LOG(N) PACIFIC, Remote

Cyber Security Support Analyst *(Intern)* June 2025 - *present*

- Conducted Tenable scans and DISA STIG audits across Windows and Linux VMs, prioritized risk, and delivered remediation guidance. eliminated 100% of critical, 90% of high, and 68% of medium vulnerabilities for the server team through PowerShell scripts.
- Conducted EDR threat hunts with KQL to find IoCs (brute-force, exfiltration, ransomware); created Defender detection rules to automate containment. Built Sentinel dashboards for SOC visibility, and blocked Internet-facing vectors with NSG/firewall rules to eliminate brute-force incidents.