Tylor Romine

Threat Detection | SIEM | SOC Analyst | Cybersecurity Analyst
tylor-romine.com | linkedin.com/tylor-romine| github.com/filthypotato

CYBERSECURITY EXPERIENCE

CYBERSECURITY HOMELAB ENGINEER – INDEPENDENT RESEARCH
Dec 2025 – Present – Port Orchard, WA (Remote)

- Built and maintain a cybersecurity homelab for SIEM monitoring, threat detection, and attack simulation across Windows and Linux environments
- Deployed T-Pot honeypot capturing 1,000+ attacks traffic, analyzing brute force, scanning, and exploitation attempts
- Monitored and analyzed 1000+ security events, mapping detections to MITRE ATT&CK techniques to improve visibility and coverage
- Conducted digital forensics on corrupted external drive, successfully recovering 100% of data
- Developed Grafana dashboards to visualize Wazuh SIEM data, including attack patterns, source IPs, and event trends

Active Directory Enterprise Lab (Windows Server 2025 + Windows 11)

- Built domain environment with domain controller + multiple client systems implementing DNS and Group Policy security controls
- Implemented endpoint telemetry using Sysmon + Wazuh SIEM across 5+ endpoints
- Created custom detection rules for malware behaviors (e.g. cipher.exe abuse, log wiping).
- Investigated simulated attacker activity using Windows Event logs and SIEM dashboards, analyzing 100+ or log events per scenario.

Attack & Defense Lab (Windows + Linux Targets)

- Performed incident response workflows including identification, containment, and analysis of malicious activity in lab environment
- Simulated attacker techniques such as network scanning, service exploitation and credential attacks
- Analyzed attack telemetry to validate detection capabilities within my SIEM environment

Education

Columbia College Online

A.S. Cyber Security
Jun 2026

B.S. Cyber Security
Aug 2027

Military Service

Veteran – United States Army
Honorable Discharge ARCOM Medal

TECHNICAL SKILLS

Operating Systems

Windows 10/11, Windows Server 19/25, Linux (Ubuntu, Arch), Security Distributions (Kali, Parrot), Unraid OS

Networking & Infrastructure:

TCP/IP, DNS, Network Segmentation, Samba, VPN Deployment, VLANs, DHCP, NAT, Firewall Management (pfSense)

Security Monitoring:
SIEM (Wazuh), Log Analysis, Threat Detection, Threat Hunting, Incident Response, Event Correlation, Sysmon, MITRE ATT&CK, Detection Engineering, EDR, IDS/IPS, Grafana

Cybersecurity & Offensive Tools:

WiFi Pineapple, Flipper Zero (RF testing), Vulnerability Assessment, Attack Simulation, Adversary Emulation,

Digital Forensics & Analysis:

- Documented attack techniques and mapped them to MITRE ATT&CK framework (10+ techniques tested).

PROFESSIONAL EXPERIENCE

IT FIELD TECHNICIAN TEAM LEAD 1 MONTH CONTRACT
Aug 2025 – Aug 2025 – TEKSystems @ Cox Health – Springfield, MO

- Supervised a 8-person team with the installation and configure 600+ endpoints (Tiny in One monitors, PCs, mounts, peripherals) within project timeline.
- Coordinated installation operations and resolving 20+ on-site issues to maintain deployment efficiency.
- Ensured 100% compliance with client specifications during system setup and hardware configuration.

VALIDATION AND SUPPORT TECHNICIAN L3
Jan 2024 – Sept 2024 - *Kelly Services @ Intel – Folsom, CA – Concurrent*

- Performed SSD validation with stress testing that includes S3, S4, S5 reliability across storage, power, and hardware components on 3 platforms weekly
- Diagnosed and resolved system and board level issues, including non booting conditions and hardware failures.
- Analyzed test results and system behavior to identify stability and performance issues of sleep state.

HARDWARE VALIDATION TECHNICIAN
Jan 2021 – Jan 2023 - Kelly Services @ Intel – Folsom, CA - Concurrent

- Built and deployed 500+ new systems (desktops, laptops, and NUCs), improving testing workflow efficiency, system and firmware reliability monthly
- Performed hardware level troubleshooting and boot/debug analysis, assisting in identifying dozens of firmware faults.

FTK Imager, HxD Hex Editor, Disk imaging, File system analysis (NTFS), ddrescue, Photorec

Programming & Automation:
Python (automation & Pytest), C++, Bash/Shell Scripting, SQL, HTML/CSS

Hardware & Validation:

SSD validation (S3/S4/S5), Firmware testing, BIOS configuration, System stability testing

Virtualization & Lab Environments:

VMware, VirtualBox, (KVM) Virt-Manager, Docker, Unraid, Attack Simulation Labs