Jeremy Tarkington

Lake Charles, LA 1-337-515-8618 jtarkington.dev@gmail.com https://jtarkington-portfolio.netlify.app

Profiles

jtarkington77

Jeremy Tarkington

Summary

Systems/Security Engineer (MSP + regulated). Ran a solo 4-day CMMC Level-2 initial assessment and delivered a 72-page POA&M plus leadership next-steps memo. Built a Linux PXE + PowerShell zero-touch Windows imaging platform; operate a Wazuh-backed SIEM/EDR lab on OPNsense with Cloudflare. Shipped safe admin automations (Win11 upgrade workflow, AI “preflight” checker) and ViperKit, a portable, offline-first Windows incident response toolkit that walks Tier-1/2 techs from “I think this box is compromised” through hunt, persistence checks, temporal sweeps, cleanup, hardening, and PDF case reports.

Labs + tooling portfolio: https://jtarkington-portfolio.netlify.app

Projects

ViperKit — **June 2025 - Present**

Portable Incident Response Toolkit for Windows

https://github.com/jtarkington77/ViperKit

Portable, offline-first incident response toolkit for Windows built for MSP and IT teams without dedicated security staff. Guides Tier-1/2 techs through a full workflow — IOC hunting, persistence discovery (including PowerShell history analysis), temporal artifact sweeps, reversible cleanup, security hardening profiles, and exportable PDF case reports.

Incident Response, Windows Security, Threat Hunting, Malware Triage, Persistence Discovery, Digital Forensics, Security Hardening, PowerShell, DFIR, Endpoint Security, Security Automation, Case Reporting

Home Security Network

Segmented **Home LAN** and **isolated Detonation Lab** for safe malware testing using **OPNsense firewall**; separate routing/egress; DNS/logging tuned for analysis.

Network Segmentation, Home Lab, Detonation Lab, OPNsense, Firewall configuration, DNS Logging, Traffic Analysis, Malware Analysis Lab, Intrusion Detection, Packet Capture, WireShark

HomeLab — **2025**

Active Directory + Wazuh 4.7.5 SIEM on an isolated virtual network

- Built and secured a multi-OS cyber lab simulating enterprise endpoint + SIEM architecture on a fully isolated virtual network
- Deployed Samba-based AD and joined Windows 11 and Ubuntu 24.04 endpoints; created baseline user/computer objects and GPOs
- Stood up Wazuh manager stack and onboarded agents with auth keys
- Enabled core modules per host: Syscollector, Vulnerability Detector, SCA, and FIM

Wazuh, SIEM, SCA, CIS Benchmarks, File Integrity Monitoring, Syscollector, Windows 11, Ubuntu Server, Ubuntu Desktop, Samba AD, Hardening, Detection Engineering, Vulnerability Detection

Wazuh SIEM + OpenEDR

Deployed across Home vs. Detonation; baseline dashboards/rules; endpoint onboarding; alert tuning/noise reduction.

SIEM, EDR, Endpoint Detection, Security Monitoring, Log Collection, Correlation Rules, Alert Tuning, Noise Reduction, Detection Engineering, Linux, Threat Detection

Container Networking at Scale

Resolved Docker **address-pool exhaustion** by designing **custom bridge networks**; reorganized Compose stacks; standardized env/backup runbooks.

Docker, Docker Compose, Container Networking, Bridge Networks, Custom Subnets, CIDR Planning, Linux, Infrastructure as Code, Network Design

Cloudflare Zero-Trust Front Door

Placed **all self-hosted services** behind **Cloudflare Tunnels/Access** (reverse proxy); strong auth; *no* public ports.

Cloudflare, Zero Trust, Cloudflare Tunnels, Cloudflare Access, Reverse Proxy, Identity Aware Proxy, SSO, Application Security, Secure Remote Access, DNS, Web Application Protection, Networking

AI “Preflight” Script Checker (Linux)

Gatekeeper scans Bash for **risky/destructive patterns** and runs an **AI review**; quarantines flagged scripts; emits timestamped **pass/fail** codes.

Bash, Linux, Static Analysis, Script Security, AI Safety, Guardrails, Automation, DevSecOps, Code Review, CLI Tools, Risk Detection, Large Language Models

Experience

National Networks — **05/2025 - Present**

Systems Engineer III — Lake Charles, LA

- Initial CMMC L2 assessment delivered solo in 4 days (14 domains/110 controls) with evidence capture; authored a 72-page POA&M and leadership next-steps memo in the same window.
- Malware remediation incl. RAT/persistence hunting & removal; post-incident hardening on endpoints/servers.
- Microsoft 365/Entra & AD admin, Exchange/Entra config, permissions/shares, printer/scan routing.
- WatchGuard policy/VPN updates; EDR/MDR agent deployment & alert triage (Huntress).
- RMM/Automation: Windows 11 compatibility checker; scoped safe in-place upgrade workflow (setup flags, reboot handling, CW asset tagging).
- Delivered security-awareness micro-sessions for client staff; published one-page SOP handouts.

Golden Nugget Casino — **10/2019 - 05/2025**

Senior IT Support Specialist — Lake Charles, LA

- Designed, built & maintained a Linux-based PXE Windows deployment server (golden image + selectable app bundles) with PowerShell post-install automation and secure auto-sign-out/lockdown.
- Supported compliance audits in a regulated environment; prepared evidence packages & documentation.
- Resolved complex server/network/user issues; coordinated vendors; wrote SOPs and repeatable fix docs.

Braun Intertec — **2015 - 2019**

Engineering Tech/Project Manager — Beaumont, TX

Tolunay-Wong Engineers — **2005 - 2015**

Engineering Tech — Sulphur, LA

Education

Western Governors University — **08/2025 - Present**

Cybersecurity & Information Assurance

Delta Tech — A.A.S

Information Technology

Skills

Incident remediation & hardening

persistence & creds cleanup; controls; malware removal

●●●●○

persistence cleanup, autoruns, scheduled tasks, WMI event filters, services/drivers, startup folders, LSA/credential theft artifacts, malicious GPO/logon scripts, PowerShell history, registry run keys, DLL hijack traces, firewall policy, EDR re-enrollment, browser extensions

Detection engineering (SIEM/EDR)

Design detections, tune noise, investigate alerts, and drive containment across SIEM/EDR stacks.

●●●●○

SIEM, EDR, detection rules, alert triage, containment, tuning, Wazuh, OpenEDR, Huntress, Defender, telemetry baselines, noise reduction

Identity & tenant administration (M365 / Entra / AD / Exchange)

Operate and secure Microsoft tenants: identity lifecycle, CA/MFA, GPO/permissions, and mail-flow policy.

●●●●○

Microsoft 365, Entra ID, Azure AD, Active Directory, GPO, Conditional Access, MFA, SSPR, licensing, SMB permissions, DNS/DHCP, Exchange Online, transport rules, routing, Networks

Network edge & zero-trust

Build segmented edge with VPN and zero-trust access; publish services safely without public ports.

●●●○○

OPNsense, WatchGuard, Cisco, firewall policy, VPN, segmentation, IDS/IPS, Cloudflare Tunnels, Cloudflare Access, zero trust, reverse proxy

Imaging & endpoint lifecycle

Deliver zero-touch builds and upgrades using PXE/WinPE with RMM-driven post-install automation.

●●●●○

PXE, WinPE, imaging, golden image, app bundles, post-install automation, ConnectWise RMM, asset tagging, upgrade workflow, Linux, custom server

Automation & Scripting

Ship safe admin tooling and repeatable ops automation that reduces toil and error

●●●●○

PowerShell, Bash, Python, scripting, automation, policy gates, preflight checks, CLI tools

Containers & platform ops

Run containerized services reliably with proper networking, IPAM, backups, and updates.

●●●○○

Docker, Docker compose, bridge networks, IPAM, service discovery, backups, standardization

Certifications

CompTIA A+
CompTIA
04/2023
https://comptia.org

Google IT Support Professional
Google
2023

CompTIA Network +
CompTIA
In Progress

CompTIA Security +
CompTIA
In Progress