Paul Leone

Yorktown Heights, NY | 914.441.0968 | pnleone@outlook.com | linkedin.com/in/pnleone/ | GitHub Pages: https://pnleone.github.io/Career_Projects/ | CCNA, Security+

Security Operations Analyst with 28+ years of IT infrastructure and technical operations experience, specializing in cybersecurity through advanced training, certifications, and hands-on lab development. Skilled in SIEM/EDR monitoring, alert triage, log analysis, threat detection, and incident response across enterprise environments.

SKILLS

Security Operations: SIEM/EDR Monitoring (ELK/Splunk, Wazuh), Alert Triage (theHive), Threat Detection & Hunting, Log Analysis, Detection Tuning, Vulnerability Assessment (Nessus/OpenVAS), MITRE ATT&CK Mapping

Network & System Expertise: Windows/Linux Administration, Secure Network Architecture, Firewalls, TCP/IP, DNS, VPN, Identity & Access Management (AD, OIDC/OAuth2, MFA)

Security Tooling: Suricata, Snort, Wireshark, Nmap, Sysinternals, Burp Suite, Metasploit

Automation & Scripting: Python, PowerShell, Bash, Terraform, Ansible, Git/GitHub, SQL

Platforms & Infrastructure: Docker, Proxmox, VMware, Active Directory, Kubernetes, Cloud/Hybrid Infrastructure

PROJECTS

Operational Security Lab: Enterprise Monitoring, Detection Engineering & Automation July 2025 - Present

A fully engineered, security-hardened lab simulating enterprise infrastructure to practice real-world SOC workflows, detection engineering, and incident response. Demonstrates hands-on capability across SIEM/EDR monitoring, threat hunting, vulnerability management, and secure-by-design architecture.

GitHub: https://pnleone.github.io/Career_Projects/projects/homelab/

- Investigated alerts using ELK/Splunk SIEM and Wazuh EDR; documented findings using IR procedures
- Tuned Suricata IDS/IPS rules to reduce false positives and improve ATT&CK mapped coverage
- Performed vulnerability assessments with OpenVAS and tracked remediation
- Conducted threat hunting using endpoint telemetry and network traffic analysis
- Deployed segmented, hardened infrastructure with pfSense/OPNsense and centralized logging
- Automated provisioning with Terraform and Ansible for reproducible, version-controlled builds
- Applied NIST CSF, CIS and ISO 27001 controls across lab design, monitoring, and operational processes.

Threat Intelligence Overview, Detection Strategy and SOC Workflow Recommendations October 2025

Developed a multi-platform detection strategy for Ivanti VPN exploitation campaigns, translating threat intelligence into actionable SOC workflows.

- Engineered YARA, Sigma, and Suricata rules mapped to MITRE ATT&CK techniques.
- Integrated SOC workflows into deliverables, demonstrating reproducible detection logic compatible with SIEM platforms and SOAR playbooks.
- Authored a threat intelligence brief and operational guidance tailored for healthcare SOC environments, incorporating FIM, threat intel feeds, and exploit chain correlation.

RELEVANT EXPERIENCE

Solution Architect | NWN Carousel April 2007 – November 2024

- Architected hybrid-cloud solutions that reduced operational and infrastructure costs by 20–30% by aligning enterprise requirements with scalable, secure designs.
- Led production deployments across 100+ enterprise environments, improving uptime to 99.99% through proactive monitoring and operational continuity planning. Experience that now informs my SOC approach to system reliability and risk reduction.
- Built presales automation tools that cut quoting time by 30%, standardizing workflows and improving cross team accuracy. Mirroring the structured, repeatable processes used in SOC playbooks and IR runbooks.
- Delivered complex multi-vendor solutions that drove 100%+ quota attainment, accelerating adoption of secure architectures and strengthening customer resilience.
- Provided SME guidance across cloud, virtualization, UC, and security domains, reducing engineering escalations by 25% and sharpening my ability to analyze system behavior.

EDUCATION AND CERTIFICATIONS

Bachelor of Science - Management Information Systems, Binghamton University, State University of New York

Cybersecurity Certificate | College of Staten Island, City University of New York April 2025 –October 2025

- Foundational and hands-on instruction utilizing industry-standard tools, guided projects, and real-world scenarios.

Certifications: Cisco Certified Network Associate (July 2024) | CompTIA Security+ (Feb 2025) | TryHackMe SOC Level 1 (Aug 2025) | TryHackMe Jr Penetration Tester (Oct 2025) | Fortinet Certified Fundamentals in Cybersecurity (Oct 2024).