PETER VAN ROSSUM

peter@petervanrossum.com
github.com/SecOpsPete
linkedin.com/in/vanr

EXPERIENCE

Company: Log(N) Pacific May 2025 - Present

Title: Support Engineer

Vulnerability Management:

- Conducted vulnerability scans, provided detailed reports, and implemented PowerShell-based remediations.
- Performed vulnerability assessments and risk prioritization using Tenable across Windows and Linux environments.
- Automated remediation processes and STIG implementations using PowerShell to address critical vulnerabilities.
- Demonstrated deep understanding of the "soft" side of Vulnerability Management: rapport, trust, transparency, and business need.

Security Operations:

- Performed threat hunting with EDR, detecting IoCs from brute force attacks, data exfiltration, and ransomware.
- Developed custom detection rules in Microsoft Defender for Endpoint to automate isolation and investigation of compromised systems.
- Created Microsoft Sentinel dashboards to monitor log on failures and malicious traffic using threat intelligence.
- Experienced with KQL (similar to SQL/SPL) used to query logs within the SIEM and EDR platform.

Company: Zimmerman Communications July 2024 - Present

Title: IT Support Technician & Senior Technical Writer

- Resolved technical issues, optimized network configurations, and managed user accounts to ensure uninterrupted business operations.
- Liaison between technical teams and non-technical stakeholders, translating complex concepts into actionable business and policy documents.
- Consistently exceeded all submission deadlines for client and partner deliverables.

Company: Peter Van Rossum, APF May 2013 – July 2024

Title: Owner/Operator

- Delivered product demos and technical walkthroughs as part of sales enablement efforts.
- Increased annual profitability seven consecutive years with continuous client growth.
- Subject matter expert and presenter at nationally accredited continuing education events.
- Achieved over 90% client retention rate; sold business in 2024.

Company: KW Real Estate & Prudential California Realty Jan.2002 – May 2013

Title: KW Team Leader, Sales Lead at Prudential

- Team leader and office manager - trained and supported 100+ agents.
- Spearheaded sales team that set $32 million one-day sales record.
- Chairman's circle award, ranking in the top 3% of company agents nationwide

PROJECTS

Active Directory Detection Lab

GitHub: github.com/SecOpsPete/active-directory-labs/tree/main/active-directory-detection-lab
Deployed an **Active Directory** environment with domain controllers and workstations to simulate attacks. Built **detection rules in SIEM/Sysmon**, correlated **event logs**, and **response actions** to improve detection in enterprise-like conditions.

Incident Response with Microsoft Sentinel

GitHub: github.com/SecOpsPete/incident-response-sentinel
Designed and tested IR workflows with **Microsoft Sentinel**, **Defender for Endpoint**, and **Azure Log Analytics**. Created **custom detection rules** and **hunting queries** to investigate simulated credential theft, lateral movement, and persistence.

Vulnerability Management & Threat Hunting

GitHub: github.com/SecOpsPete
Built threat-hunting workflows to strengthen detection using **Tenable.io**, **Microsoft Sentinel (SIEM)**, and **Defender for Endpoint** on **Azure VMs**. Developed **KQL detection queries** to identify misconfigurations and attacker TTPs.

DISA STIG Compliance Labs

GitHub: github.com/SecOpsPete/disa-stig-compliance-labs
Automated **Windows 10/Server hardening** with **PowerShell** to remediate Tenable findings against DISA STIG benchmarks. Leveraged **Windows Registry modifications** and STIG XML baselines to enforce security policies.

CERTIFICATIONS AND TRAINING

CompTIA CySA+ – 2025
CompTIA Security+ – 2025
(CompTIA Security Analytics Professional- CSAP stack)
CompTIA Network+ – 2025
CompTIA A+ – 2025
Cisco Certified Support Technician – (CCST) Networking & Cybersecurity – 2025
Registered DoD RMF Practitioner (RDRP) – 2025
Salesforce Certified Associate – 2024
Certified Customer Success Management Professional (CCSMP) – 2024
TryHackMe – SOC Level 2 Training Path (170+ labs, Top 2% ranking) – 2025

EDUCATION

B.A. Business Communication — Washington State University

ADDITIONAL SKILLS AND TECHNOLOGIES

Vulnerability Management, Risk Assessment, Incident Response, Threat Hunting, Security Operations, EDR (Microsoft Defender for Endpoint), SIEM (Microsoft Sentinel, Splunk), KQL, PowerShell Scripting, Python, Linux, Basic Cisco IOS, Networking, ELK, Wireshark, Snort, Autopsy, Syslog, Sysmon, Technical Writing, Solution Demonstrations, Product Demos, Stakeholder Communication, C-Suite Engagement, Active Directory (AD), Network Security, Compliance Frameworks (NIST 800-53, DISA STIG, PCI-DSS, HIPAA), eMASS, MITRE ATT&CK, OWASP Top 10, EDR, Cloud Security (Azure), Sales Enablement, Client Retention, Policy and Report Writing, Problem