PETER VAN ROSSUM

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

EXPERIENCE

Company: Log(N) Pacific May 2025 - Present

Title: Cyber Security Support Analyst (Vulnerability Management & SecOps Intern)

Vulnerability Management:

- Conducted vulnerability scans, provided detailed reports, and implemented PowerShell-based remediations, contributing to a 100% reduction in critical, 89% in high, and 76% in medium vulnerabilities for the server team.
- 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: Senior Technical Writer

- Liaison between technical teams and non-technical stakeholders, translating complex concepts into actionable business and policy documents.
- Developed data-informed marketing and policy documents tailored to diverse stakeholder audiences, translating complex information into clear, compelling narratives.
- 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

Vulnerability Management and Threat Hunting Projects
Source: https://github.com/SecOpsPete
Platforms / Technology Used: Tenable.io, SIEM (Microsoft Sentinel), EDR (Defender for Endpoint), Azure VMs, KQL

DISA STIG Compliance Labs
Source: https://github.com/SecOpsPete/disa-stig-compliance-labs
Platforms / Technology Used: Tenable.io, Azure, PowerShell, Windows Registry, DISA STIG Repository

Incident Response with Microsoft Sentinel
Source: https://github.com/SecOpsPete/incident-response-sentinel
Platforms / Technology Used: Sentinel, Defender for Endpoint (MDE), Azure Log Analytics Workspaces, KQL

Professional-Grade Home Lab for Cybersecurity Research & Network Hardening
Source: https://github.com/SecOpsPete/secure-soho-network
Platforms / Technology Used: Elastic Stack (ELK), UFW, Raspberry Pi Syslog Server

SOC Tools and Training
Source: https://tryhackme.com/p/SecOpsPete
Hands-on cybersecurity training via TryHackMe (110+ labs, SOC Level 1 Analyst path, top 3%)
Platforms / Technology Used: Splunk, Snort, Wireshark, Elastic Stack (ELK), Sysmon, PhishTool, Wazuh, etc.

CERTIFICATIONS

CompTIA CySA+ – 2025
CompTIA Security+ – 2025
(CompTIA Security Analytics Professional- CSAP stack)
CompTIA Network+ – 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

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, Networking, ELK, Syslog, Sysmon, Technical Writing, Solution Demonstrations, Product Demos, Stakeholder Communication, C-Suite Engagement, Business Needs Analysis, Network Security, Compliance Frameworks (NIST, DISA STIG, PCI-DSS, HIPAA), Cloud Security (Azure), Sales Enablement, Client Retention, Policy and Report Writing, Problem-Solving, Communication Skills.