PETER VAN ROSSUM

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

EXPERIENCE

Company: Log(N) Pacific May 2025 - Present

Title: Support Engineer

AI Threat Hunting Agent Model Improvement

- Enhanced an open-source AI threat hunting agent by implementing guardrails for time-window enforcement, PCI/HIPAA-compliant redaction, anomaly scoring, and structured JSON logging to improve SOC readiness.
- Applied OWASP LLM Top 10 and MITRE ATLAS controls to harden the model against adversarial ML threats.

Vulnerability Management:

- Performed vulnerability assessments using Tenable.io, prioritizing Windows/Linux findings through CVSS, CWE/CVE mapping, and environmental risk scoring to guide remediation strategies and strengthen risk posture.
- Demonstrated strong interpersonal skills in vulnerability management, building rapport and trust while balancing transparency, business priorities, and cross-department workflows to ensure coordinated remediation outcomes.

Security Operations:

- Performed threat hunting with Microsoft Defender for Endpoint (MDE), detecting IoCs from brute force attacks, data exfiltration, and ransomware while correlating telemetry across hosts, services, and network events.
- Developed custom detection rules in Microsoft Defender for Endpoint and Sentinel analytic rules, automating host isolation and suspicious process investigations using KQL (similar to SQL/SPL) to improve alert fidelity.

Company: Zimmerman Communications July 2024 - Present

Title: IT Support Technician & Senior Technical Writer

- Performed endpoint troubleshooting using Windows Event Viewer, Group Policy, remote administration tools, and basic network diagnostics (ipconfig, nslookup, traceroute).
- Managed user accounts, permissions, and workstation deployments, improving reliability across Windows 10/11.
- Facilitated communication between technical teams and non-technical stakeholders, translating complex concepts into clear policy documents.
- Consistently exceeded all submission deadlines for client and partner deliverables.

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

Title: Owner/Operator

- Built and managed long-term executive relationships, serving as the primary point of contact for strategic accounts.
- Delivered product demos and technical walkthroughs as part of sales enablement efforts.
- Presented as a subject matter expert to large groups at nationally accredited continuing education events.
- Achieved over 90% client retention rate; customer referral rate 30% upon selling the business in 2024.

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

Title: KW Team Leader, Sales Lead at Prudential

- Led a team of 100+ agents as office manager and integrated a cloud-based CRM solution to streamline operations.
- Spearheaded sales team that set a $32 million one-day sales record, led high-touch client sales efforts.
- Achieved Chairman's Circle status, ranking in the top 3% of agents nationwide over multiple years.

PROJECTS

Secure Network Lab Architecture

Designed, deployed, and hardened a segmented SOHO network with VLAN-separated trusted/IoT/guest subnets, static IP governance, and firewall hardening (DNSSEC, DNS-over-TLS). Built a centralized logging pipeline using a Raspberry Pi (rsyslog, UFW, Fail2Ban) forwarding router and system logs into a Dockerized ELK stack with Logstash JSON pipelines.

Active Directory Detection Lab

Built and configured Windows Server AD domain with workstation joins to simulate threats (brute-force, unauthorized privilege escalation). Implemented Sysmon with a custom XML configuration, mapped events to MITRE ATT&CK, and built SIEM correlation rules for anomalous logon behavior, service creation, registry tampering, and lateral movement indicators.

Incident Response with Microsoft Sentinel

Built Sentinel analytic rules and KQL hunting queries to detect token theft, suspicious PowerShell execution, and remote service abuse. Investigated incidents using MDE alerts, entity timelines, and process trees; validated IR workflows for host isolation, credential reset procedures, and log scoping across Azure Log Analytics workspaces.

Vulnerability Management & Threat Hunting

Ingested Tenable.io scan data to identify privilege issues, outdated services, and insecure configurations on Azure Windows hosts. Wrote KQL queries to flag unpatched CVEs, missing ASR rules, unsigned binaries, persistence artifacts (Run keys, scheduled tasks), and abnormal network destinations, strengthening the lab's detection coverage against common TTPs.

CERTIFICATIONS AND TRAINING

CompTIA CySA+ – 2025
CompTIA Security+ – 2025
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 (200+ labs, Top 1% ranking) – 2025

EDUCATION

B.A. Business Communication — Washington State University

ADDITIONAL SKILLS AND TECHNOLOGIES

Windows/Linux administration, endpoint troubleshooting, hardware/software diagnostics, ticketing systems, Active Directory (users, groups, GPOs), network troubleshooting (TCP/IP, DNS, DHCP), patch management, system hardening, firewall/IDS configuration, Wireshark, PowerShell, Python, SIEM (Microsoft Sentinel, Splunk), KQL, vulnerability assessment (Tenable.io, Nessus), Sysmon, Microsoft Defender for Endpoint, ELK Stack, rsyslog, Docker, Azure/AWS security fundamentals, PCI-DSS, HIPAA, GDPR, NIST 800-53 & 800-61, Group Policy (GPO) management, Windows Event Viewer log analysis, Azure Log Analytics Workspace, Logstash pipeline configuration, syslog forwarding and log normalization, EDR telemetry analysis (MDE), VPN configuration (NordVPN, IPSec/OpenVPN), VLAN segmentation.