Peter Van Rossum

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

Professional Summary

IT Support Specialist and security-minded Support Engineer with 2+ years in service desk operations, endpoint troubleshooting, and SaaS administration. Skilled in ticket workflows, documentation, and cross-team collaboration. Strong grounding in access control and data protection, supported by 10+ years of customer-facing communication with executives and non-technical users.

Experience

Log(N)Pacific – Support Engineer
May 2025 – Present

AI Threat-Hunting Agent Model Improvement

- Enhanced an open-source AI threat-hunting agent with guardrails for time-window enforcement, PCI/HIPAA-compliant redaction, anomaly scoring, and structured JSON logging, improving 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

- Conducted 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 MDE and Sentinel detection rules using KQL to automate host isolation and suspicious process investigations, improving alert fidelity.

Zimmerman Communications – IT Support Technician/Senior Technical Writer
July 2024 – Present

- Executed 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.

PVR Equine Therapeutics – Independent Consultant/Owner
May 2013 – July 2024

- 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 and a 30% customer referral rate upon selling the business in 2024.

KW Real Estate/Prudential California Realty – KW Team Leader/Sales Lead at Prudential
Jan 2002 – May 2013

- 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.
- Improved agent productivity and pipeline visibility by ~20% through structured coaching and technology adoption.

Projects

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, increasing detection coverage for attack techniques by 50%.

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 incident-response workflows for host isolation, credential reset procedures, and log scoping across Azure Log Analytics workspaces, reducing incident triage time by an estimated 25%.

Certifications and Training

CompTIA CySA+ – 2025
CompTIA Security+ – 2024
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 (250+ labs, Top 0.5% ranking) – 2025

Education

B.A. Business Communication – Washington State University

Additional Skills and Technologies

Windows/Linux administration, hardware and software diagnostics, ticketing systems, Active Directory and Group Policy, TCP/IP, DNS, DHCP, patch management, system hardening, firewall and IDS configuration, Wireshark, PowerShell, Python, SIEM (Sentinel, Splunk), KQL, vulnerability assessment (Tenable, Nessus), Sysmon, Microsoft Defender for Endpoint, ELK Stack, Docker, Azure/AWS security fundamentals, PCI-DSS, HIPAA, GDPR, NIST 800-53 and 800-61, log analysis and normalization, VPN configuration, VLAN segmentation.