IAN SIMONS

https://github.com/ian-m-simons
https://www.linkedin.com/in/ian-m-simons

Professional Summary

Network and Security Analyst with hands-on experience in XDR administration, incident response, SOAR automation, and Palo Alto/Cisco network operations. Proven ability to rapidly upskill, automate workflows, and strengthen security posture through proactive remediation, endpoint visibility improvements, and cross-team collaboration.

Skills

- Network Administration - routing, switching VLANs (Cisco IOS), DHCP, firewall administration (Palo Alto)
- XDR Administration (Cortex XDR) - IoC management, report creation, custom detection development, incident response playbook development
- Security Operations - threat hunting, query logic development, incident response
- Scripting and Automation - Python and PowerShell, log parsing, integration with Cisco IOS and Cortex XDR
- Linux Administration - server hardening, system configuration, shell scripting
- Virtualization - virtual machine provisioning, configuration and troubleshooting

Certifications

- Cisco Certified Network Associate (CCNA) - June 2026
- CompTIA Security+ (SY0-701) - October 2025
- Microsoft Azure Fundamentals (AZ-900) - January 2025

Professional Experience

Network Analyst/Security Analyst

Indiana Members Credit Union - Jan 2026-present

- Extended Detection and Response (XDR) Administrator – Primary owner of Palo Alto Cortex XDR across 925 endpoints in a previously minimally monitored environment, establishing alert triage and response workflows
- Alert Triage and Incident Response – Investigate, escalate, and remediate approximately 10-15 alerts per month that are not handled by the Managed Detection and Response (MDR) provider, including anomalous behavior below alert threshold
- Detection and Threat Intelligence – integrated IoCs based on threat intelligence and author basic XQL detections
- Security Orchestration and Response (SOAR) Playbook Development – Built 9 incident response playbooks within Cortex XDR to standardize handling of recurring security events and improve response consistency and speed
- Security Posture Improvements – Identify and remediate issues such as poor secrets management practices and MFA fail-open, reducing organizational risk and improving authentication integrity
- Reporting and Visibility – Produced daily reports using XDR metrics to provide leadership with visibility into endpoint health, alert trends, and emerging risks
- Firewall and Network Administration – Review and approve/deny web-filtering exceptions, open/close ports, clear port-security violations, and support general network operations on Cisco switches and Palo Alto firewalls
- Additional Security Tasks – Evaluated potentially malicious USB drives, performed Linux server hardening (CIS Level 2), and any other tasks directed by management

Operations Support Specialist

Indiana Members Credit Union - Jan 2025-Jan 2026

- Help desk Automation Tool – Developed an interactive PowerShell tool for network diagnostics, Active Directory computer management, system information retrieval and endpoint security operations via the Palo Alto Cortex XDR API, reducing manual troubleshooting time by an average of approximately 5 minutes per ticket
- Ticket Throughput – Consistently maintained the highest ticket volume among all technicians (60% above technician average) while meeting or exceeding quality and SLA expectations
- User Training – Trained users across multiple departments, age ranges, and technical skill levels on the proper use of VPN, MFA, and other technologies, improving authentication success rates and reducing repeat support requests
- New-Hire Onboarding – Trained newly hired Operations Support Specialists in core duties, troubleshooting procedures, and help desk workflows to accelerate onboarding and improve team readiness

Welder

Arizona Department of Transportation - Apr 2023-Apr 2024

Welder

Eden Down Home - Oct 2022-Apr 2023

Customer Experience Specialist
Alta Climbing and Fitness - Nov 2021-Aug 2022

Marine Security Guard
United States Marine Corps - Apr 2014-Oct 2019

- Embassy Security – Provided armed internal security for U.S. diplomatic missions overseas, safeguarding personnel, sensitive areas, and classified materials in accordance with Marine Corps Embassy Security Group and Department of State procedures
- Classified Material Protection – Conducted nightly security rounds to verify proper storage of classified materials, enforcing compliance and initiating corrective procedures when security violations were identified
- Security Training – Led training for Marines in chemical, biological, radiological, and nuclear (CBRN) response, close quarters battle (CQB), proper handling and storage of classified material, and tactical field care
- VIP Support Operations – Supported high-visibility security operations for the President of the United States, maintaining secure perimeters and enabling specialized security teams to focus on direct VIP protection

Projects

Help desk Automation
https://github.com/ian-m-simons/Computer-Search

A PowerShell-based utility that performs basic network diagnostics, retrieves system information, and queries Active Directory computer objects. Built to simplify routine troubleshooting tasks and provide a consistent way to gather endpoint details.

- Includes modular functions for AD lookups, remote system queries, and network checks
- Used internally to streamline common help desk tasks without replacing existing tooling

Hack The Box Academy – CPTS Learning Path
Ongoing hands-on practice and study through offensive security labs, following the Certified Penetration Testing Specialist learning path.

- Enumeration and Exploitation – Building practical skills in host/service enumeration, vulnerability identification, and exploitation across Windows and Linux targets.
- Privilege Escalation – Practicing real-world privilege escalation techniques (misconfigurations, kernel exploits, credential harvesting) to simulate attacker post-exploitation workflows.
- Reporting and Methodology – Developing structured penetration testing methodology, including documentation, attack path mapping and remediation focused reporting.

Education

Microsoft Software and Systems Academy
System and Cloud Administration - Sep 2024-Jan 2025

Completed 680 classroom hours of training in enterprise systems and cloud administration. Core competencies include Microsoft Azure, Microsoft 365 administration, Windows Server, Linux systems, virtualization fundamentals, and identity management.