ROBERT CHRISTOPHERSON

Signal: cyberrob.07 | fruit.alpaca659@eagereverest.com | linkedin.com/in/thecyberrob | https://cyberrob.tech

Professional Summary

A passionate InfoSec specialist with 2 years of experience, combining self-education and formal training, I excel in integrating, operating, maintaining, governing and advancing blue-team initiatives. My expertise encompasses a range of industry specific defensive and offensive skills as well as in-depth fundamental troubleshooting abilities. My capabilities remain focused towards bolstering the security posture of organizations and ensuring the continuing support and accessibility to critical infrastructure for end users while maintaining relevancy in today's Information Security landscape.

Education and Certifications

Active DoD Secret Clearance
Cybersecurity Certificate | Coding Dojo, Part of Colorado Technical University | January 2023
CompTIA Security+ | Expires June 2029
CompTIA CySA+ | Expires June 2029
EC-Council Certified SOC Analyst | Expires May 2028

Technical Skills

- **Defensive Security:** PaloAlto Firewall | TCP/IP | Ivanti MDM | Vulnerability scanning and remediation | Active Directory | MITRE ATT&CK | PKI | SIEM (Wazuh) | XSOAR (Cortex) | Automation/Playbooks with Python | Proofpoint (Mail filtering, Threat Intelligence) | MFA/IAM solutions | Global Protect | CrowdStrike | Malware Analysis Techniques | Incident Response
- **Offensive Security:** Kali Linux | Metasploit | Wireshark | Nmap | OSINT
- **Additional Skills:** Virtual machines | Citrix | Containerization | Knowledge management | ITSM | OSI Model | Software/Hardware/Network troubleshooting | Scripting | Document Management Systems | M365/Exchange

Technical Projects

SIEM Deployment | Proof of concept deployment of an open source SIEM/XDR into my home network.

- Deployed a single cluster Wazuh instance to Ubuntu Server including the indexer, server and dashboard.
- Installed agents on all Windows/Mac/Linux endpoints and configured log forwarding from my router.
- Set up VirusTotal API integration and python scripts on endpoints to wipe malicious file downloads.
- Configured read-only accounts for non-privileged access to the service.

Cloudflare Tunnel | Securely exposed services on my internal network using Zero Trust Tunnels.

- Installed and configured the Cloudflared agent on my server running in a Docker container managed via Portainer.
- Configured Cloudflare to be the DNS resolver for my domain then I used this to self-host my website from my server.
- Set up Public Hostnames to access internal services running on my server such as the Wazuh dashboard.

Malware Analysis Exercise | Air-gapped virtual machine running Remnux within a simulated network.

- Performed static analysis against a suspicious .doc file using Pestudio, and open-source python scripts resourced from GitHub to de-obfuscate and analyze malicious macros.
- Performed dynamic analysis using InetSIM, Wireshark, Procmon and Fiddler to observe the macros within the file.
- Implemented eradication and remediation techniques such as machine reimaging, DNS sink holes, blacklisting IP's, updating rulesets in IDS/IPS/Firewalls, and disabling the use of macros by default on an enterprise scale.

Black Box Pentest | Attack a Windows 7 VM using Kali Linux to gain root access and obtain flags.

- Utilized a suite of industry standard tools and services including Nmap, Stegcracker, Hydra, Metasploit, MSFVenom, CyberChef, SCP, SSH, FTP, Telnet to capture various flags.
- Demonstrated network enumeration, password cracking, privilege escalation and exploitation.
- Authored a detailed writeup encompassing the landscape and methodologies used to capture the flags.

Professional History

Service Desk Support Technician | *Perkins Coie* | November 2023 – Present | Full-Time

- Triaged phishing investigations and other network security events using Cortex XSOAR
- Participated in remediation efforts and provided best practice training to end users.
- Assisted T2, T3 teams and management to streamline ITSM workflows with documented processes and procedures.
- Joined multiple pilot test groups to provide valuable testing and feedback to development teams.
- Simultaneously maintained above average metrics in ticket creation, handling, and first call resolution.
- Obtained elevated Service Desk Admin rights for various tools and services used in the organization.
- Joined the KBAT team and assisted in Knowledge Base administration and KB article authoring.
- Received multiple recognitions and awards for outstanding customer service and rapid break-fix resolution.

Systems Administrator | *Wash Worx LLC* | May 2023 – March 2024 | Freelance

- Single-handedly researched, architected, and implemented Microsoft cloud solutions to enable accessibility, scalability, and data integrity.
- Provided remote and onsite support with required troubleshooting until resolution.
- Collaborated with upper management to ensure organizational policies and procedures align with business objectives.
- Elevated organizational security posture with password managers, MFA, IAM/user account lifecycle management, industry best practices and patch management.
- Developed processes for onboarding and offboarding employees.

SMIT Help Desk Tier 1 | *Leidos* | March 2023 – October 2023 | Full-Time

- Upheld SLAs via proper ticket documentation, approved escalation paths, first call resolutions, low handle times, and proper reporting of outages and incidents.
- Enforced security policies and zero-trust relationships, managed user accounts and permissions, ensured asset health and compliance with Navy standards.
- Provided end users with exceptional customer service and communication while assisting in troubleshooting extensive software/hardware/network break/fix scenarios and performing service requests.
- Collaborated with SOC, NOC, NNWC Cloud Operations and other teams to ensure availability and security on the network.