SETH MALONEY

Seth.Maloney@maloneycyber.com | 517-240-9761 | Haslett, MI 48840 | Maloneycyber.com

Summary

Certified Cybersecurity Professional (CISSP,GSEC,CySA+) with over 4 years of combined IT, cybersecurity, and military experience, including 1.5+ years of hands-on Incident Response. Proven ability to detect, contain, and remediate threats across enterprise environments using industry tools (CrowdStrike), SIEMs (Splunk, LogRythm), and vulnerability management (Tenable, OpenVAS) all to improve the organization's security posture. Adept at identifying, analyzing, and mitigating threats in high-pressure environments.

Skills

- Network Security (PaloAlto,pfSense)
- Endpoint Security (CrowdStrike, Wazuh)
- IDS/IPS (Snort,Quadrant,Suricata,Pi-hole)
- SIEM (CrowdStrike SIEM,Splunk,LogRythm)
- Vulnerability Scanning (Tenable, OpenVAS)
- Operating Systems (Windows,Mac,Linux,Kali,Ubuntu)
- Threat Modeling & Hunting (SecurityOnion,YETI,MITRE ATT&CK)
- Cloud Security (AWS,Azure,O365)
- Identity & Access Management (Azure,MFA,LDAP,AD)

Experience

Incident Response Analyst | Greif – Remote | 04/2024 – Current

- Wrote programs using Python, Microsoft Power Automate, and FalconPy to improve our Security Orchestration, Automation, and Response (SOAR) workflows.
- Worked with local IT points of contact to deploy CrowdStrike EDR to over 500 devices across ten different countries, improving threat coverage by 100%.
- Deployed and managed CrowdStrike to monitor, detect, and respond to endpoint threats, ensuring Confidentiality, Integrity, and Availability across over a thousand enterprise devices.
- Worked with third-party threat hunting solutions and internal teams to reinforce and harden our network systems.
- Triaged major security incidents, working with multiple teams to ensure Recovery Time Objectives were met, all while following the NIST Incident Response lifecycle.
- Deployed and ran Tenable Vulnerability scanner across 2000 hosts, validated vulnerabilities, prioritized, and mitigated.
- Explained complex technical systems and solutions in an easy-to-understand way to help end users understand the importance of security.
- Updated multiple company federated accounts using SSO from Ping ID to Entra ID.

IT Analyst | Greif – Mason, MI | 10/2023 – 04/2024

- Oversaw Zoom transition and saved Greif over $30,000/month.
- Diagnosed and troubleshot massive plant issues that could cost Greif $5,000/day if not fixed in time.
- Worked in Linux and looked through log files daily to diagnose plant issues.
- Worked with network security team to set up and configure the Palo Alto firewall.

S6 (Communications and Technology) | United States Army National Guard - Detroit, MI | 03/2019 - Current

- Set up server closets and Network Access Points with correct levels of classification for the military.
- Served as my Platoon S6 while deployed in Syria and ensured the Base Defense Operations Center was online so the base could communicate and respond to life-threating events.
- Identified and stopped a physical network attack in Syria, preventing loss of life by initiating incident response protocol under combat conditions.
- In Syria, diagnosed and fixed network and communication issues correctly under high stress.
- Explained complex technical systems in a simple way to help foster wide understanding.
- Created an Android Team Awareness Kit Server to be used for securely locating oneself and navigating.
- Deployed Starlink and a SIPR network 20 kilometers from Russia that allowed us to communicate secret information securely.

Help Desk Technician | HBFuller – Michigan Center, MI | 12/2021 - 09/2023

- Created new accounts, reset passwords and configured access to servers and file management software for users.
- Assisted in the provisioning, review, and deprovisioning of privileged accounts in user accounts in Active Directory.
- Was the only onsite IT Technician handling the largest production plant for HBFuller.

Education and Training

Michigan State University | East Lansing, MI | August 2023-December 2024
BA Information Sciences | GPA 3.93
SANS Technology Institute | East Lansing, MI | April 2025-Present
Master of Science in Information Security Engineering

Certifications and Honors

Certified Information Systems Security Professional (CISSP) 05/2025: Credential ID 2365974
SANS GSEC 06/2025
CompTIA Cybersecurity Analyst (CySA+) 10/2024: Credential ID YJYLF4HQSMBQ1NKN
CompTIA Security+ 04/2024: Credential ID G3TD3N56BMR41651
Summa Cum Laude: For having a 3.93 Cumulative GPA at Michigan State University.