Michael Maldonado, GCIA

7409 S. 177th St, NE 68136
605-760-7918
michael@maldonado.tech —— linkedin.com/in/michaelcmaldonado —— github.com/punchy98

Professional Summary

Results-driven Cyber Security professional with extensive experience in managing and remediating diverse cyber incidents, ranging from email account compromises to ransomware. Proficient in Windows and Linux administration, IT vulnerability management, and Network Analysis. Demonstrates strong problem-solving skills, effective and efficient performance under pressure, and a quick learning ability. Skilled in multiple scripting languages to automate tasks and enhance security operations. Adept in using DevOps tools like Ansible and Chef, and experienced in managing Microsoft O365/Azure environments. Passionate about continuous learning and leveraging homelab projects for professional growth.

Education

Bachelor of Science: Cyber Operations
Dakota State University - Madison, SD

Professional Development

GIAC Certified Intrusion Analyst (GCIA)

- SANS SEC503 - Network Monitoring And Threat Detection

CISA ICS Cybersecurity Training

- ICS Cybersecurity & RED-BLUE Exercise (301) - 4 day, live, hands-on course at Idaho National Laboratory ending in a 7 hour Red team engagement
- ICS Cybersecurity (300) - Online course, building up ICS security skills and fundementals

Skills

- Problem Solving and Extreme Googling
- Quick learner
- Languages: PowerShell, Python, Bash, Perl
- Windows and Linux administration/troubleshooting
- Effective and efficient performance under pressure
- Network Analysis
- Microsoft O365/Azure
- DevOps (Ansible, Chef, etc.)

Work History

Senior Cyber Security Engineer, 05/2023 - Present
Union Pacific Railroad - Omaha, NE

- Lead the OT vulnerability management program to meet TSA directives for Class I Railroads
- Coordinated Proof of Concepts with OT security vendors and created success criteria
- Coordinated other teams to identify OT patching processes
- Facilitated access management reviews
- Acted as a mentor to new team members
- Continued all functions from previous role

Cyber Security Engineer, 05/2022 - 05/2023
Union Pacific Railroad - Omaha, NE

- IT vulnerability management via Tenable (reporting, creating scans, deploying new scanners, etc)
- Security administration and troubleshooting for 14,000 Linux servers
- Scripted automated access management reporting in Python

- Created process documentation
- Acted as a mentor to new team members, helping with whatever they needed
- Lead our team's script conversion process going from Perl 5 to Python 3.9

Cyber Security Specialist, 10/2020 - 05/2022
Marco Techologies - Omaha, NE

- Responded to and handled different types of incidents ranging from Office 365 account compromises to ransomware.
- Monitored logs in an ELK-based SIEM.
- Active threat hunting looking for indicators of attack that SIEM/EDR did not detect.
- Assisted clients with ongoing 3rd party audits and remediating the findings.
- Performed security assessments for clients aligned to the NIST Cyber Security Framework.
- Performed vulnerability scans, created remediation plans, and assisted with the remediation.
- Wrote scripts to automate various tasks, including O365 management.
- Served as a Cyber Security SME to clients.

Rapid Resolution Technician, 07/2020 - 10/2020
Marco Techologies - Omaha, NE

- Served as a first line of defense for our tier 1 helpdesk, dispatching tickets and calls.

IT Support Specialist, 04/2020 - 07/2020
First Dakota National Bank - Sioux Falls, SD

- Provided exceptional support by promptly addressing and resolving user queries through support calls and help desk tickets, ensuring a seamless user experience.
- Installed and configured various equipment, ensuring seamless functionality and optimal performance.
- Automated routine tasks by developing PowerShell scripts, enhancing efficiency and reducing manual workload.

Technology Intern, 05/2019 - 04/2020
Fishback Financial Corporation - Brookings, SD

- Provided exceptional support by promptly addressing and resolving user queries through support calls and help desk tickets, ensuring a seamless user experience.
- Demonstrated technical proficiency by efficiently installing equipment and managing the decommissioning process for virtual desktops, contributing to streamlined and optimized IT operations.
- Played a key role in the successful transition to Windows 10, providing valuable assistance in the conversion process and ensuring a smooth migration for end-users.
- Leveraged expertise in automation by creating and implementing time-saving PowerShell scripts, enhancing operational efficiency and reducing manual workload.

Personal Projects - Homelab

I have been building a homelab for 5+ years. It has gone through many iterations over the years, as of Spring 2024, it consists of a NAS, media server, network wide ad-blocking, and a few other "critical" services that my family in multiple states rely on. The lab also consists of a "dev" side is where I am able to do rapid testing with of new technologies without fear of taking down the "critical" services.
Technologies used:

- Docker
- FastAPI
- Kubernetes (k8s/k3s)
- TrueNAS
- Ansible
- Terraform
- Cisco Networking
- Virtualization (VMwware vSuite, ProxMox VE, KVM)
- Linux (Ubuntu, RHEL 9, CentOS 8, OpenSUSE, FreeBSD)
- Security Onion (Snort, Zeek, ELK)