Michael Maldonado

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

Professional Summary

Experienced Cyber Security professional, with a passion for learning new things. Hands on experience remediating different types of cyber incidents ranging from email account compromises to ransomware. Able to solve problems efficiently and effectively. Homelab and Linux Enthusiast.

Education

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

Professional Development

CISA 301V/301L - ICS Cybersecurity
SANS SEC503 - Network Monitoring And Threat Detection (In Progress)

Skills

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

Work History

Union Pacific Railroad - Omaha, NE — 05/2022 - Present

Senior Cyber Security Engineer, 05/2023 - Present

- 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

- IT vulnerability management via Tenable (reporting, creating scans, deploying new scanners, etc)
- Security administration and troubleshooting for 14000 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

Marco Technologies - Omaha, NE 07/2020 - 05/2022

Cyber Security Specialist, 10/2020 - 05/2022

- 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

- Served as a first line of defense for our T1 helpdesk, dispatching tickets and calls.

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

IT Support Specialist

- 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.

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

Technology Intern

- 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.
- Actively contributed to the overall IT infrastructure by implementing solutions that improved system performance and user productivity.

Personal Project - Homelab

I have been building a homelab for a few years now. The lab includes used enterprise server and networking equipment. This homelab is dual use it is partially "production" and "development". The production side includes the NAS, media server, network wide ad-blocking, and a few other "critical" services that my family in multiple states rely on. The "development" side is where I am able to do testing with new technologies without fear of losing production uptime. I also have dozens of IoT devices deployed, everything from power monitoring to smart bulbs to cameras - all managed via Home Assistant.
Technologies used:

- Docker
- FastAPI
- Kubernetes (k8s/k3s)
- TrueNAS
- Ansible
- Terraform
- Cisco Networking
- VMware (ESXi/vCenter) and ProxMox VE
- Linux (Ubuntu, RHEL 9, CentOS 8, OpenSUSE, FreeBSD)