Michael Maldonado

7409 S. 177th St, NE 68136
605-760-7918
michael@maldonado.tech
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.

Education

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

Professional Development

CISA 301V/301L - ICS Cybersecurity

Skills

- Scripting languages: PowerShell, Python, Bash, Perl
- Windows and Linux administration/troubleshooting
- Effective and efficient performance under pressure
- VMware product suite
- Microsoft O365/Azure
- DevOps (Ansible, Chef, etc.)
- Problem solving and extreme googling
- Quick learner

Work History

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

Senior Project Engineer - Cyber Security, 05/2023 - Present

- Lead the OT vulnerability management program to meet TSA directives
- Coordinated Proof of Concepts with OT security vendors and created success criteria
- Coordinated other teams to identify OT patching processes
- Facilitated access management reviews
- Continued all functions from previous role

Project Engineer - Cyber Security, 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

- Dispatched tickets to the correct team.

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

IT Support Specialist

- Answered support calls and completed help desk tickets.
- Installed equipment
- Created PowerShell Scripts to automate tasks.

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

Technology Intern

- Answered support calls and completed help desk tickets.
- Installed equipment and decommissioned virtual desktops.
- Assisted with Windows 10 conversions
- Created PowerShell Scripts.

Personal Projects

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 relies on. The ”development” side is where I am able to do testing with new technologies without fear of losing production uptime.

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)