Matthew Velez

631–974-1988 | matthewvelez25@gmail.com | Newark, NJ
LinkedIn: https://bit.ly/3A69Ads | HackTheBox: https://bit.ly/3npIUwG | TryhackMe: https://bit.ly/3RScRlO

Objective

Innovative cybersecurity professional with strong leadership and problem-solving abilities possessing a passion for cloud security, malware and vulnerability management. Hard-working, energetic, personable, and technically minded leader with strong analytical and problem-solving abilities. Possesses strong customer obsession along with robust communication skills and the ability to work independently in a fast-paced environment.

CERTIFICATIONS

CompTIA Security+ Certification
Validation Code: B5TQE9MQKBB4QH3F

AWS Certified Cloud Practitioner
Validation Code: ZG39HX9KS24QQ45S

SKILLS

- **Python**
- **Bash**
- **Burp Suite**
- **Penetration Testing**
- **Endpoint Security**
- **Phishing Training**
- **Java**
- **JavaScript**
- **Metasploit**
- **Cloud Formation**
- **Wireshark**
- **Vulnerability Management**
- **Windows Administration**
- **Splunk**
- **Malware Analysis**
- **Network Security**
- **Digital Forensics**
- **Linux**
- **AWS EC2**
- **Secrets Manager**
- **Incident Response**
- **Firewall Configurations**
- **Autopsy**
- **Active Directory**
- **Group Policy**
- **Windows**
- **Mac OS**
- **Security Groups**
- **Service Roles**

PROFESSIONAL EXPERIENCE

Essex County Vocational Technical Schools., Newark, NJ Aug 2017 - Present
Systems Network Security Administrator

- Modernized key security policies, procedures and practices to address the emergence of cloud and microservice architectures and to address gaps in legacy security standards.
- Developed and implemented a comprehensive vulnerability management program program based upon preventive, detective and responsive controls to mitigate vulnerabilities and threat vectors.
- Provided technical leadership to the team that addressed all cyber security risks and concerns throughout a multi-building school campus.
- Implemented the district's virtual architecture and infrastructure to facilitate remote teaching and learning during COVID.
- Established an Identity Access Management (IAM) recertification framework that crosses both cloud and legacy environments to ensure every user has the appropriate permissions.
- Managed a team of network engineers to automate the onboarding process for 7000 staff and students.
- Performed weekly assessments on all computer systems, network devices and endpoints with the district’s infrastructure.
- Leveraged Barracuda Networks and its use of AI/ML to scan for phishing attacks within the school email ecosystem.
- Managed the process to establish alerts and monitoring recipes for telemetry gathered from Splunk.
- Trained district staff on all aspects of the district’s security policies, procedures and practices.

Education

Associates in Cybersecurity
Essex County Community College

ADDITIONAL SECURITY TRAINING & EXPERIENCE

Active Directory Home Lab

- Home lab using ESXi with VMware on all of my virtual machines for when I am conducting penetration testing and for when I participate in CTF events. The VMs that I maintain on my Server are Windows, Ubuntu, and Kali Linux.
- I created an AWS EC2 instance for my CTF teammates to have an environment to be able to work on CTFs and continue their studies.

- I created the AWS EC2 instance because I constantly have teammates that run into machine issue on their personal devices so the home lab actually gives them access through a VPN and they get their own environment to run CTFs in and continue their studies without fear of hardware failure or data loss.

Security Events & Affiliations

- Active participant in Hack The Box, TryHackMe, and multiple similar Platforms