AARON FILLMORE

CYBERSECURITY PROFESSIONAL

w33t.io | me@w33t.io | United States

w33t.io/linkedin | w33t.io/htb | w33t.io/thm

ABOUT ME

I am a dedicated and passionate cybersecurity professional. My unique background in business ownership and working in the MSP/MSSP field gives me unparalleled experience when considering business aspects, as well as technical, making me a fantastic asset to your organization.

WORK EXPERIENCE

Information Security Engineer II 2022 - Present

Electric Power Research Institute, United Sates

- Consult with end users regarding their secure computing needs, making recommendations for new products and solutions
- Identify and mitigate vulnerabilities and attacks within the EPRI computing environment
- Research new threats, attacks, and vulnerabilities that may affect the EPRI computing environment to learn how to identify and react to them
- Drive development of critical security projects to achieve organizational goals
- Co-ordinate EPRI's endpoint protection and participate in any required incident response

Security Analyst III 2022 - 2022

Deepwatch, United Sates

- Participate in training plan development to shape the onboarding process of analysts
- Interface with customers as an SME on the topic of cybersecurity
- Mentor Tier 1 and Tier 2 analysts in proper analysis procedures
- Provide a point of escalation within the squad for more complex incidents
- Expertly triage and handle various alerts from clients, including Fortune 500 companies
- Maintain knowledge of current industry trends and attacks to better mentor and analyze incidents
- Identify opportunities to tune alert logic to reduce alert fatigue within the squad

SOC Analyst II 2021 - 2022

Green Cloud Defense, United States

- Train new Tier 1 and Tier 2 SOC Analysts
- Perform host-based analysis, artifact analysis, network packet analysis and malware analysis in support of security investigations and incident response
- Created SOPs related to daily operation and provide feedback on current processes to maximize efficiency
- Identify, collect, and analyze threat intelligence from internal and external sources
- Investigate, document, and report on information security issues and emerging trends

WORK EXPERIENCE

NOC Technician

2019 - 2020

Imprezzio, United States

- Monitored LogRhythm SIEM and responded to alerts
- Handled creation and termination of Active Directory accounts
- Provided systems support for various building tenants
- Monitored company applications for availability
- Created centralized monitoring stack utilizing Grafana, Prometheus and several available plugins with Docker on CentOS 8
- Automated alerting using Power Automate and Opsgenie
- Interfaced with client IT support to maintain availability of Imprezzio's applications

Chief Executive Officer

2019 - 2023

Digital Edge LLC, United States

- Manage IT infrastructure for several local companies
- Configure and maintain cloud deployments of client applications
- Analyze current infrastructure and recommend solutions to clients
- Create security SOPs around business needs and risks
- Perform security posture assessments and report findings with remediation suggestions

EDUCATION

Bachelors in Cybersecurity

Western Governors University, 2019 - 2023

Network and Systems Administrator Cert

New Horizons CLC, 2018 - 2018

CERTIFICATIONS

CompTIA

- A+
- Network+
- Security+
- PenTest+
- CySA+
- CASP+

Miscellaneous

- LE-1 Linux Essentials
- ISC2 CC
- Google IT Support Specialization
- FEMA ICS-100

SKILLS

- Vulnerability Management
- Systems Engineering
- Network Security
- Penetration Testing
- Incident Handling
- Risk Management
- Working Python Knowledge
- TTX Coordination
- OSINT
- Reconnaissance
- Physical Penetration Testing
- Social Engineering

SOFTWARE

- FortiEDR, FortiSIEM, FortiOS, FortiDeceptor
- Swimlane SOAR
- Metasploit
- Burp Suite
- LogRhythm SIEM
- SentinelOne EDR/XDR
- NMAP
- Wireshark
- Qualys VM
- Exabeam
- Mythic C2
- Sliver C2