Adeen Ellicott

Buffalo, New York | bardificer.com | adeen@bardificer.com | linkedin.com/in/sean-manly | github.com/bardificer

Education

University at Buffalo, SUNY **B.S. Information Technology and Management** | GPA : 3.33 *August 2019 – May 2023*
Minor | Cybersecurity

Experience

Risk and Information Security Analyst | *SitusAMC* *May 2023 –Present*

- Review and investigate alerts, incidents, and requests corroborating evidence from tools including CarbonBlack, Ivanti, Varonis, Proofpoint, Tenable, and Microsoft Azure AD.
- Create scripts for high-importance clients reliant on efficiency and security using Python to control 400,000+ individual data points and multiple API endpoints.
- Drive and oversee implementation of new security tooling within company infrastructure, expanding security functions past previous capabilities.
- Serve as on-call DFIR specialist for the company, and direct incident-related TTXs and recovery efforts.

Cybersecurity Analyst | *GlobalSecurityIQ* *March 2021 – May 2023*

- Engaged in Cybersecurity Risk Assessments with 10+ clients focusing on continuing essential security functions and growing alerting capabilities.
- Managed consulting services and conducted incident response as part of a third-party security team while learning tools selected for each client uniquely.
- Lead a small team to perform Digital Forensics investigations and Incident Response functions leveraging industry-standard and custom developed software.

Network Security Instructor | *University at Buffalo* *August 2020 – May 2023*

- Planned, wrote, and taught the UBNetDef Network Security course, working with network virtualization, security software, packet capture analysis, and security report writing.
- Develop solutions to classwork errors revolving around Vagrant, VirtualBox, Snort, Suricata, Zeek, and Wireshark.

Cybersecurity Analyst Intern | *Calspan* *May 2021 – August 2021*

- Created a security awareness training course to satisfy NIST 800-171/CMMC requirements.
- Monitored and maintained security stance of company with following tools: WSUS, TrendMicro, Darktrace, Barracuda, Cisco Firepower, Lansweeper, Sophos Central, Nessus.

Technical Skills

Specialities : Digital Forensics, Incident Response, Cyber Research, Malware Analysis, SIEM Configuration, Linux, Windows
Programming Languages : Rust, Python, Nim, Ruby, Bash, Powershell, SQL, C/C++
System Administration : Virtualization, Database Management, Data Analytics, AWS, OCI, Azure, Network Configuration, CI/CD
Offensive Security : Burpsuite, Metasploit, OSINT, Kali Linux, API Exploitation, Web Vulnerabilities, Penetration Testing
In Progress : ISFCE CCE Certification, SANS FOR608 Work-study, GREM Certification

Awards and Certifications

Top 2% User | *TryHackMe*	*2023*
Peak Rank #432 | *HackTheBox*	*2022*
CompTIA CySA+ | *CompTIA*	*February 2021*

Projects

Self-Managed Research Laboratory | *Proxmox, FlareVM, REMnux, PfSense, RDP, Wireguard, Wazuh, Elastic, TheHive* *Ongoing*

- A built-out home lab for security research. Configured with a simulated network for capturing malware IoCs and artifacts.
- Used as a host for all other training projects currently managing 18 virtual machines and custom security configurations for each, up to CIS standards.

TCM Security PMAT Course | *Proxmox, FlareVM, REMnux, Wireshark, Ghidra, Cutter, INetSim* *2023*

- The training course for the Practical Junior Malware Researcher certification. Focuses on hands-on analysis of malware samples and malicious code.
- Certification exam yet to be taken.

HackTheBox Bug Bounty Hunter Job Path | *Burpsuite, cURL, Nikto, HTTP* *Spring 2023*

- The training course for HackTheBox's Bug Bounty Hunter certification, practicing web vulnerability analysis and exploitation for both common and novel exploits.