Caitlin M. Allen

Security Operations Analyst

Security Operations Analyst with a passion for protecting companies against both internal and external threats. Talented at threat hunting and recommending preventive measures to mitigate security flaws. Has an educational background in forensics and security engineering that enhances threat hunting and mitigation capabilities.

Contact

Address
Burlington, VT

Phone
(908) 268-0441

E-mail
caitlinallen6199@gmail.com

Twitter
twitter.com/CaitlinMAllenn

LinkedIn
linkedin.com/in/caitlinallenn

Website
caitlinmallen.com

Skills

Splunk

Threat Hunting

Cyber Threat Intelligence

ThreatConnect

Malware Analysis

Linux Forensics

Windows Forensics

Security Engineering

System Administration

Work History

2021-11 – Current

Security Operations Analyst

Stripe, South San Francisco, CA

- Part of a front-line response team for investigating and triaging security threats to reveal root cause and coordinate with cross-functional stakeholders
- Developing a Slack channel for vendors to ping the security team to report suspicious activities or files
- Integration of bot to track metrics for security team pings, time to resolution, etc. to provide information needed for team performance improvement and education of users on security policies, topics, etc.

2021-06 – 2021-11

Threat Analyst

NuHarbor Security, Colchester, VT

- Performing threat hunting, intelligence analysis, scoping for incident response, and acting as an escalation point for CTAC clients.
- Assists SOC team with additional responsibilities, tasks, and provides input to improve the SOC's performance and daily operation.
- Authoring client specific weekly threat reports and bi-weekly threat trends.

2020-05 - 2021-05

Managed Services Intern

NuHarbor Security, Colchester, VT

- Developed a ThreatConnect Playbook that automates IOC enrichment using open-source intelligence sources through API calls upon indicator upload.
- Created a lab environment for analysts to train themselves to threat hunt in that resets after 24 hours of use.
- Data mapping IOCs to MITRE ATT&CK tactics and techniques for intelligence program.

2020-01 - 2020-05

Digital Forensics Intern

Kivu Consulting, Burlington, VT

- Developed Linux Forensics and Incident Response training program, database, and automating key artifact extraction in Powershell to expedite the investigation process of Linux hosts.
- Aided junior and senior analysts during forensics investigations.

2018-08 - 2018-12

Cybersecurity & Digital Forensics Analyst (Tier 1)

Leahy Center For Digital Investigation, Burlington, VT

- Performed an entry-level managed services role through monitoring network logs, threat hunting, and continuing to improve the ELK Stack SIEM solution with development endeavors.
- Fulfilled incident response duties such as imaging, investigating, and remediation.

2017-08 - 2018-02

Technical Intern

Leahy Center for Digital Investigation, Burlington, VT

- Researcher for the *HackRF One Project.*
- Preparing students for the spring semester during LCDI Spring Orientation by answering questions for incoming interns and providing guidance in their new role.

Education

2017-08 - 2021-05

Bachelor of Science: Computer Networking & Cybersecurity

Champlain College - Burlington, VT

- Communications Lead for Womxn in Technology
- Member of Digital Forensics Association (DFA)
- Member of Cyber Security Club (CCSC)
- Northeastern Cyber Defense Competition Team (NECCDC) Linux Alternative 2019 and 2020
- Study Abroad Semester in Dublin, Ireland at Champlain College Dublin Fall 2019

Certifications

2023-06 Splunk Core Certified Power User