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
Martinez, CA 94553

Phone
(908) 268-0441

E-mail
caitlinallen6199@gmail.com

Twitter
twitter.com/CaitlinMAllenn

LinkedIn
linkedin.com/in/caitlinallenn

Skills

SQL

Threat Hunting

Splunk

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 the root cause and coordinate with cross-functional stakeholders.
- Created easy to follow runbooks for Security Operations processes and detections that include screenshots and internal resources.
- Developed a Slack channel for vendor agents to ping the security team to ask questions or report suspicious activity and developing revamping a tracker for these security inquiries across both vendors and Stripe employees.

2021-06 - Current

Threat Analyst

NuHarbor Security, Colchester, VT

- Performed threat hunting, intelligence analysis, scoping for incident response, and acting as an escalation point for CTAC clients.
- Assisted SOC team with additional responsibilities, tasks, and provides input to improve the SOC's performance and daily operation.
- Authored 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 will reset after 24 hours of use.

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 - 2018-12

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