CAITLIN ALLEN

SECURITY INCIDENT RESPONSE ANALYST

CONTACT

Walnut Creek, CA

(908) 268-0441

caitlinallen6199@gmail.com

caitlinmallen.com

SKILLS

Log Analysis

Security Incident Response

AWS

Azure

Threat Hunting

SentinelOne EDR

Google Chronicle SIEM

Tines

Splunk

macOS

Linux

Windows

CERTIFICATIONS

Nov 2025
Microsoft Certified: Azure Fundamentals

Nov 2024
Offensive Security Defense Analyst (OSDA)

Jan 2024
AWS Certified Cloud Practitioner

Sept 2023
ATT&CK® Purple Teaming Methodology Certification

June 2023
ATT&CK® Cyber Threat Intelligence Certification

June 2020 – June 2023
Splunk Core Certified Power User

WORK HISTORY

Stripe

Security Incident Response Analyst — Remote Nov 2021 - Nov 2025

- Performed initial triage and containment for security incidents including malware infections, phishing attacks, and insider threat investigations.
- Monitored and triaged SIEM alerts to identify potential security threats.
- Assisted with conducting root cause analysis into security incidents.
- Analyzed process logs, network traffic, and telemetry from EDR tooling to investigate security alerts, security incidents, and insider threats.
- Worked cross-functionally with security teams to identify improvements in security detection rules to reduce false positives.

NuHarbor Security

Threat Analyst - Colchester, VT Jun 2021 - Nov 2021

- Performed threat hunting, intelligence analysis, scoping for incident response, and acted as an escalation point for CTAC (Cyber Threat Analysis Center) clients.
- Assisted SOC team with additional responsibilities, tasks, and provided input to improve the SOC's performance and daily operation.
- Authored client specific weekly threat reports and bi-weekly threat trends.

NuHarbor Security

Managed Services Intern - Colchester, VT May 2020 - May 2021

- 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 in threat hunting.
- Mapped IOCs to MITRE ATT&CK tactics and techniques for intelligence program.

Kivu Consulting

Digital Forensics Intern, Burlington, VT Jan 2020 - May 2020

- Developed Linux Forensics and Incident Response training program, database, and automating key artifact extraction in Powershell to expedite the investigation process of Linux hosts.

Leahy Center for Digital Forensics & Cybersecurity

Tier 1 Cybersecurity Analyst, Burlington, VT Aug 2018 - Dec 2018

- 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.

Leahy Center for Digital Forensics & Cybersecurity

Technical Intern, Burlington, VT Aug 2017 - Dec 2017

- Researcher for the *HackRF One Project*

EDUCATION

Bachelor of Science Computer Networking & Cybersecurity

Champlain College - Burlington, VT May 2021

- Extracurricular Activities: Communications Lead for Womxn in Technology, Northeastern Cyber Defense Competition Team (NECCDC) Linux Alternative 2019 and 2020, Digital Forensics Association (DFA), Cyber Security Club (CCSC)
- Study Abroad Semester in Dublin, Ireland at Champlain College Dublin Fall ‘19