Kewaun Cain

Security Operations | SOC Intern (CyberTrust MA) | Security+ & CySA+ | EDR, SIEM, Risk Management

Email: kewaunscain@gmail.com

Website: kewauncain.com

LinkedIn: linkedin.com/in/kewaun-cain

Summary

Cybersecurity professional with hands-on training in threat detection, endpoint protection, and incident response. Experienced in SIEM tools, EDR, vulnerability assessments, and physical security. Proven communicator with a calm-under-pressure mindset, developed through both real-world experience and formal training.

Experience

Securitas | March 2024 - Present

- Controlled physical access at a secure site by verifying badge credentials, inspecting documentation, and escalating access anomalies to the SOC team.
- Conducted thorough interior and exterior patrols to proactively detect and deter unauthorized access, equipment tampering, and safety violations.
- Monitored and analyzed DSX access control logs daily to flag failed badge attempts, trace unusual activity, and support incident investigations.
- Responded to critical security events—including bomb threats, fire alarms, and unauthorized entry—using established emergency protocols and incident playbooks.
- Completed continuous Security Awareness Training to enhance vigilance, recognize social engineering tactics, and enforce on-site cybersecurity posture.

- Collaborated with shift supervisors, facilities teams, and security leads to maintain situational awareness and streamline emergency coordination.

CyberTrust Massachusetts | September 2024 – March 2025

- Completed immersive cybersecurity training through CyberTrust MA, focusing on real-world implementation of SIEM tools, endpoint protection, and CIS Controls-based defense strategies.
- Conducted hands-on security assessments for municipal environments, applying CIS Controls v8 to identify misconfigurations and improve endpoint protection posture.
- Monitored and triaged real-time threats using SentinelOne EDR, identifying Indicators of Compromise (IoCs) and leveraging telemetry data for root cause analysis.
- Performed vulnerability scans with Nessus and contributed to actionable remediation plans tailored to critical assets and compliance risks.
- Shadowed penetration testers from OnDefend to document hardening techniques and align findings with NIST cybersecurity best practices.
- Developed and applied a Third-Party Risk Assessment (TPRA) framework to evaluate vendor controls around identity access, MFA/2FA, and data handling.

Per Scholas | February 2024 – June 2024

- Completed a 15-week, full-time cybersecurity training program covering SIEM analysis, endpoint protection, vulnerability management, log review, and network security fundamentals.
- Configured SOHO and WAN networks using routers, switches, DHCP, port assignments, and VLANs; applied OSI model and TCP/IP principles to troubleshoot issues.
- Set up and managed virtualized lab environments using VMware, VirtualBox, and Hyper-V to simulate enterprise-level systems.
- Worked with Ubuntu Linux to explore file systems, user permissions, log analysis, and basic malware behavior.
- Practiced packet analysis with Wireshark and reviewed real-world attack scenarios, applying fundamentals like the CIA Triad and MFA/2FA authentication.

- Engaged in professional development activities, including resume workshops, mock interviews, and networking with industry professionals.

Resilient Coders | February 2022 – July 2022

- Completed a full-time, project-based coding bootcamp focused on HTML, CSS, responsive design, Git, and collaborative software development.
- Designed and deployed accessible, mobile-friendly web pages using modern layout techniques and basic JavaScript interactions.
- Used Git and GitHub daily for version control, managing branches, resolving merge conflicts, and collaborating in pull request workflows.
- Worked in agile-style teams to plan, build, and present web projects in demo day showcases.
- Participated in weekly code reviews and peer feedback sessions to improve project quality and technical communication.
- Practiced problem-solving with real-world coding challenges and emphasized career-readiness through resume workshops and mock interviews.

Certifications

- Security+ (2025)
- CompTIA CySA+ (2024)

Technical Skills

- **Cybersecurity Tools:** SentinelOne (EDR), Splunk (SIEM), Nessus, Wireshark, Active Directory, Ubuntu Linux
- **Frameworks & Concepts:** CIS Controls v8, NIST, Threat Detection, Incident Response, MFA/2FA, Network Security Fundamentals
- **Technical Skills:** Git & GitHub, HTML/CSS, JavaScript (Basic), Python (Basic), PowerShell (Basic), VS Code