Daniel Cooper

Hudson, MA | 978-460-5303 | daniel.s.cooper.dev@gmail.com |Linkedin| www.daniel-cooper.dev/

Cybersecurity Analyst with 8+ years experience in Software Development and currently completing Google Cybersecurity Professional Certificate. Experienced in cybersecurity practices, risk identification, Python, Linux, and SQL, with expertise in Splunk, WireShark, Tcpdump, and Suricata. Seeking a cybersecurity role with opportunities for continuous learning and collaboration within a dynamic team.

RELEVANT SKILLS & EXPERTISE

Tools/Languages: Linux, Windows, SQL, BigQuery, MySQL, PostgreSQL, Splunk, WireShark, Tcpdump, Suricata, Python, Java, ChatGPT, Node.js, C#, HTML
Security Practices: Information Security, Network Security, Vulnerability Assessment, Threat Analysis, Log Analysis, Security Frameworks and Controls
Software Platforms: Google Workspace, Slack, Microsoft Teams, Jira, Bamboo, Github
Strengths: Critical Thinking, Collaboration, Problem-Solving, Attention to Detail, Leadership, Calmness Under Pressure

CYBERSECURITY PROJECTS

TryHackMe Rooms: Utilized interactive, gamified virtual environment to enhance practical knowledge and hands-on skills:

- **Linux Fundamentals** (1, 2, & 3) and **Linux Strength Training** - Navigated directories and files, adjusted permissions, analyzed logs, explored common utilities
- **Intro to Logs** and **Log Analysis** - Identified log types, located logs, employed regular expressions (RegEx), and utilized command line and CyberChef for effective log analysis
- **Wireshark Basics** and **Wireshark 101** - Gained proficiency in packet dissection, navigation, and filtering techniques; analyzed ARP, ICMP, TCP, DNS, HTTP, and HTTPS traffic for network troubleshooting and security analysis
- **Windows Fundamentals** (1, 2, & 3) and **Windows Forensics** (1 & 2) - Acquired fundamental understanding of Windows, including file systems, user account control (UAC), control panel, system configuration, security, firewall, registry, and FAT/NTFS file systems; developed skills in accessing hives, utilizing registry explorer, and recovering files
- **Splunk Basics**, **Incident Handling with Splunk**, and **Splunk** (2 & 3) - Developed skills in navigating Splunk; conducting incident handling using Splunk; participated in the Boss of the SOC investigation for security analysis

PROFESSIONAL EXPERIENCE

Technical Support Specialist • *Law Office of Mark D. Cooper, Boston, MA* **10/2022 - 06/2025**

- Migrated physical case files over to the Cerenade digital system.
- Added 400+ clients to the database, linking families of clients for easy form population.
- Assigned variables to make managing new cases and filling out new forms with existing clients less time-consuming.

Software Engineer • *Liberty Mutual Insurance Group, Dover, NH* **01/2021 - 01/2023**

- Used agile principles, working with enterprise-level development tools, including Jira and Bamboo, building 8 Full-stack employee management applications, each deployed globally with AWS.
- Utilized React, Typescript, Node.js, AWS, and PostgreSQL, adopting team code standards and general team norms.
- Leveraged Python and Google Apigee and AWS S3 Buckets to deploy an application allowing the secure transfer of files.
- Recognized for good work, elevated to a mentorship role and worked with vendor contractors.

Web Development TA • *Stack Education, Framingham, MA* **10/2020 - 11/2021**

- Assisted 50+ students through their web development bootcamp, tracking their progress and giving special instruction.
- Designed courses to teach data structures, code cleanliness, and relational databases.
- Taught the fundamentals of Javascript, CSS, HTML, SQL, React, and MongoDB.

EDUCATION, CERTIFICATES, & CERTIFICATIONS

Google Cybersecurity Professional Certificate • *Merit America, Virtual* **09/2025**

- Cultivated holistic understanding of cybersecurity's critical role in organizational security, privacy, and success, including how to systematically identify and mitigate risks, threats, and vulnerabilities
- Gained practical experience with **Linux**, **SQL**, **Python** and utilized **SIEM tools**, **IDS**, and **network protocol analyzers** for proactive threat management
- Applied knowledge to real-world scenarios, developing skills in proactive **threat detection** and **response** through completion of dynamic hands-on projects, including: conducting a simulated **security audit**, responding to a **cyber incident**, analyzing **vulnerable systems**, and completing an **incident handler's journal**

Web Development • *Stack Education* **01/2020**
Advanced Software Construction in Java • *MITx* **05/2017**

B.S Psychology • *Northeastern University*, *Boston, MA*