

Jamin Camp

ICS Cybersecurity Analyst

Los Angeles, California

Contact Information

prime0012@gmail.com

Skills

- **SIEM Tools:** QRadar, Splunk
- **Endpoint Protection:** CrowdStrike Falcon
- **Task Management:** Jira
- **Treat Intelligence:** Virus Total, Shodan, Talos, MITRE ATT&CK, CrowdStrike, Dragos
- **Network Analysis:** Wireshark, Zeek, Suricata, Snort
- **Programming Languages:** Python, PostgreSQL
- **Web Development:** HTML, CSS, JavaScript, PHP
- **Email Phishing Tools:** pdfid, Visual Studio Code, JOESandbox, Cyberchef Remnux
- **Malware Analysis:** Flare VM

Education

Bachelor of Science Cybersecurity and Information Assurance | Western Governors University | September 2026

Security Blue Team Level 1 | Security Blue Team | 2023

ICS515: ICS Visibility, Detection, and Response | SANS Institute of Technology | 2023

Summary

Dynamic and results-driven Cybersecurity Engineer with a strong background in web development, incident response, ICS cybersecurity and threat intelligence. Skilled in utilizing SIEM tools such as Splunk and IBM Qradar, and proficient in endpoint protection with CrowdStrike Falcon. Demonstrated success in investigating and mitigating cyber threats, managing security incidents, and developing secure web applications. Proven ability to lead teams and manage complex projects. Committed to leveraging my expertise to enhance cybersecurity measures and ensure organizational safety.

Experience

SOC Analyst

Cydeo | *Remote* | June 2024 – June 2025

- Participates in daily SOC analyst routines which includes using current threat intel from MITRE ATT&CK to discuss current and potential threats to the network.
- Utilized IBM Qradar and Splunk in conjunction with Virus Total, Shodan and Talos Reputation checker to analyze log data and identify patterns indicative of potential threats.
- Conducts static malware analysis by disassembling code with JOESandbox, Flare VM, and Remnux, successfully identifying and mitigating threats in 95% of cases.
- Investigates potentially malicious emails using pdfid, URLtoPNG, and Visual Studio Code, preventing phishing attacks in 99% of cases.
- Utilized CrowdStrike Falcon to quarantine devices and performed Digital Forensics and Incident Response (DFIR) on potentially compromised systems.

Web Developer and Pentester

Camp Massive | *Los Angeles* | April 2015 – April 2020

- Developed and secured websites for 30+ clients, implementing security controls, access management, and secure coding practices.
- Performed penetration testing and vulnerability assessments, identifying risks and recommending mitigation strategies.
- Gained functional knowledge of Python and PostgreSQL for backend development and database management, enhancing website functionality and security.

Projects

ICS SOC Lab

Created a replica of a power generation and transportation stations using ICS specific protocols and PLCs to practice and detect malicious activity. Built a functional replica of power generation and transportation systems using ICS protocols and PLCs to simulate attacks, monitor events, and practice incident response within a critical-infrastructure environment. **See the lab [here](#)**

DumpsterFire

Developed a Python tool implementing DoD 5220-22.M data erasure, encryption, and secure deletion workflows to mitigate data exposure risks. **See the GitHub repository [here](#)**

Certifications

GIAC Response and Industrial Defense (GRID)
CompTIA A+
CompTIA Network+
CompTIA Security+
CompTIA Pentest+
Linux Essentials
ITIL 4 Foundations

Re-reader (Field Supervisor)

Los Angeles Department of Water and Power | *Los Angeles*
| April 2008 – Present

- Supported critical utility operations by leading a team of 16 in field data collection and infrastructure access
- Developed and documented standard operating procedures (SOPs) to improve operational efficiency and reduce access issues by 25%.
- Communicated operational changes and risk considerations to management and field teams, supporting safe and reliable service delivery.
- Maintained strict confidentiality and compliance with utility security standards.

Volunteer Work

Cybersecurity Consultant

Sunset Congregation of Jehovah's Witnesses | *Los Angeles* |
May 2023 – Present

- Conducted security assessments, risk analysis, and vulnerability identification across multiple applications.
- Developed and enforced security policies, confidentiality requirements, and user access controls.
- Develop and enforce a privacy policy for congregation members, requiring acknowledgment before using approved applications to protect personal and sensitive information.
- Provide ongoing security training and support to congregation members, fostering a culture of cybersecurity awareness and best practices.
- Collaborate with application developers and vendors to address identified security issues and implement recommended improvements.
- Regularly update and review security protocols and policies to ensure they meet current standards and address emerging threats.
- Provided ongoing troubleshooting and system support to maintain secure and reliable operations.