

Evan Lutz

Network Security and Python Software Engineer

A determined leader, cybersecurity engineer and Certified Ethical Hacker; a passion for problem solving, application development, network security, Linux, learning, data analytics, efficiency, and automating tasks with Python.

GITHUB: <https://github.com/evanlutz725>

LINKEDIN: <https://www.linkedin.com/cyber-evan>

EXPERIENCE

Cybersecurity Engineer: Logan, UT — Rent Dynamics LLC

November 2021 - June 2023

- Brought the organization to SOC compliance for the first time in company history in under 12 months with a completely undisputed opinion.
- Led the cybersecurity efforts for the entire organization as the sole dedicated cybersecurity resource.
- Created and administered custom cybersecurity awareness trainings for the organization, both for compliance and for proper edification.
- Conducted and led technical trainings to the development team on topics including Docker, company data flows, and Kubernetes.
- Facilitated audits, risk assessments, and orchestrated remediations to ensure compliance.
- Use of exploitation frameworks to search and designate vulnerabilities in systems based on operating systems, version numbers, open ports, traffic filtering, etc.
- Undertook in house penetration testing for both internal and external networks on an annual basis.
- Worked alongside developers to determine secure coding implementations for new projects and features.

Network Security Engineer: Fort Myers, FL — Cigent Technology, inc.

June 2019 - November 2021

- Creation and Deployment of the SOC Alerting infrastructure, automated monthly report writing software that computed aggregated data and presented it in a way that was understandable to a non-technical person, and Beacon Detection and Alerting Software.
- Creating and maintaining XDR systems, including alert rule creation, and configuring security device servers.
- In depth SOC analyses of customer data for the purpose of ensuring customer network integrity.
- Creation of an IP Reputation server that aggregated over 500 million malicious IP Addresses whose results were pushed to all production sensors on an hourly basis.
- Security Hardware installation and sales of security devices.
- Malware analysis on live machines, including first and second stage viruses, ransomware, droppers, and Trojan Horses, for the purpose of creating rules that indicate this infection on the network.
- Incident response and forensic drive analysis.
- Public speaking on behalf of the company for local news and events

Southwest Florida
(601)-376-9840
cyberevan11@gmail.com

PROFICIENT KNOWLEDGE & SKILLS

SOC/SIEM Creation ◦ Python ◦ ELK Stack ◦ Automation ◦ Suricata ◦ Agile ◦ Scrum ◦ Application Security ◦ Ethical Hacking ◦ Traffic Analysis ◦ Network Detection And Response ◦ Automating Technical Report Writing ◦ Incident Response ◦ Forensic Drive Analysis ◦ Server Administration ◦ AWS ◦ Beacon Analysis ◦ Virtualbox ◦ CA Deployment ◦ Centralized Cloud Management ◦ Git ◦ Bash ◦ CI/CD ◦ SOC Compliance ◦ Compliance Automation ◦ Phishing Training ◦ Education

CERTIFICATIONS

EC-COUNCIL CERTIFIED ETHICAL HACKER (C|EH)
March 2019 (exp 2023 - planning to renew)

COMPTIA NETWORK+
February 2019

ISC2 CISSP
Anticipated September 2023

EDUCATION

SOUTHERN NEW HAMPSHIRE UNIVERSITY, Hooksett, NH: 2019-2022 —
Master's degree in Cybersecurity with Honors

SOUTHERN NEW HAMPSHIRE UNIVERSITY, Hooksett, NH: 2016-2018 —
Bachelor's degree in Mathematics with Honors