# Zach Ailor

Massachusetts, USA
Zachailor@gmail.com
https://zailor.dev

Versatile security professional with eight years of experience across a diverse array of technologies. A true jack-of-all-trades, I excel at adapting to and navigating challenges to protect businesses and create innovative solutions.

## EXPERIENCE

### **Secureworks, Remote.** - *Software Eng. - Detection Verification*

02/2024 - Present

- *Collaborate with an Agile software development team to build and maintain an automated cloud testing platform designed to test security rules, ensure comprehensive coverage, and deliver high-quality results.*
- *Developed "red team"-style automated tests by researching and executing security attacks, then automating them using PowerShell to simulate real-world threat scenarios.*
- *Designed and implemented a full-stack application using Next.js, React, and TypeScript to provide an intuitive UI to explore testing platform results, adding advanced functionality and visualizations to improve usability and insights.*
- *Created a Python-based REST API to serve as middleware to generate comprehensive telemetry reports for improved analysis and monitoring.*
- *Play a key role in enhancing the architecture and development of the testing platform, delivering a scalable, maintainable, and efficient solution.*

### **Secureworks, Remote.** - *XDR - Advanced Product Support*

08/2021 - Present

- *Designed and implemented a custom Zendesk dashboard in React to analyze support tickets using an LLM to summarize tickets, determine customer satisfaction, and ensure quality support.*
- *Designed and implemented a custom audit tool in React to reduce management time by over 60 hours a month.*
- *Provide troubleshooting support for Advanced Endpoint Threat Protection products and EDR solutions.*
- *Assist clients with integrating over 60 different 3rd party solutions to log into SecureWorks XDR, including AWS, Cisco, Microsoft, Zscaler, NGFWs, and other various cloud, endpoint, and network services.*
- *Provide advanced troubleshooting of Log Collectors leveraging K3s*
- *Collaborated with development and product management teams on shared objectives and product road maps to reach fiscal goals.*

## SKILLS

**Languages:** Python, Typescript

**Frameworks:** FastAPI, NextJS, React

**Cloud:** AWS, Azure

**Virtualization:** Docker, Kubernetes

**Automation:** Packer, Ansible, Terraform, Git CI/CD

**EDR:** Taegis Agent, Carbon Black, Crowdstrike

**IDS/IPS**: iSensor, Cisco Firepower/FTD, Mcafee ASM

**Threat Detection & Response**: SIEM, MDR, XDR

**AI/ML:** LangChain, RAG, LLMs, Prompt Engineering

## SOFT SKILLS

**Problem-Solving**: Critical thinking and effective resolution of complex challenges

**Communication**: Explaining technical concepts to non-technical stakeholders and writing clear documentation

**Adaptability**: Rapidly learning and applying new tools, technologies, and techniques

### **Secureworks, Remote.** - *XDR - Product Support*

12/2019 - 02/2021

- *Played an instrumental role in establishing and launching a new support team from the ground up.*
- *Created and implemented standardized procedures to increase overall productivity, enabling the team to process and resolve tickets efficiently.*
- *Spearheaded cross-team collaboration with leadership and engineering teams to improve existing standard operating procedures.*

### **Secureworks, Providence, RI.** - *IDS-DM Team*

08/2018 - 12/2019

- *Managed and configured IPS/IDS, WAF's, and other Linux-based security devices for a portfolio of 4000+ customers, ensuring continuous monitoring and protection of critical infrastructure from network-based threats.*
- *Deployed, maintained, and upgraded IDS appliances, including iSensor, Cisco Firepower/FTD, and Mcafee ASM to ensure high availability and optimal performance.*
- *Fine-tuned IDS signatures and policies to minimize false positives and enhance detection accuracy, tailoring to the specific needs and network architectures of different clients.*
- *Reduced downtime and improved overall network security posture by resolving issues related to IDS devices, including connectivity, configuration, and performance challenges.*

### **Infirmary Health, Mobile/Baldwin Co.** - *PC Specialist: Tier II*

03/2016 - 06/2017

- *Replaced and/or repaired network hardware, including performing diagnostic tests and troubleshooting to determine and resolve root causes.*
- *Provided various user support, including installing personal computer application software, assisting in software/hardware problem identification and resolution, and user training.*
- *Monitored and provided troubleshooting for LAN/WAN connectivity.*

## CERTIFICATIONS

Cisco CCNA: Routing & Switching

Carbon Black Defense Associate Analyst

## EDUCATION

Faulkner CC, Bay Minette, AL

AAS, Network Administration