Zhiyuan He

SOC Analyst

CONTACT

415-608-3052

Gig Harbor, WA

zhiyuanfw@gmail.com

linkedin.com/in/zhiyuanhe

horzhiyuan.com

CERTIFICATION

- CompTIA Security+
- CompTIA A+
- Sophos Certified Architect
- Sophos Certified Engineer
- SOC Core Skills w/ John Strand

SKILLS & TOOLS

Cybersecurity

- Sophos Endpoint/Security Onion/NodeZero
- Elastic Stack
- Wireshark/Velociraptor/AC-Hunter/RITA/OWASP ZAP
- PowerShell/Bash
- Windows/macOS/Linux

Web Development

- JavaScript/TypeScript/Python
- HTML/CSS/SASS
- React.js/Vue.js
- Next.js/Vite.js/Redux/Zustand
- Mocha/Chai/Karma

Control System

- Modules installation/removal on Rockwell Studio 5000

EDUCATION

UNIVERSITY OF CALIFORNIA RIVERSIDE - 2019

- Bachelor of Science
- Computational Mathematics

Work Experience

Cyber Defense Analyst
Intuitus Corp **04/2024 - Present**

- Collaborated on detecting and responding to security incidents, maintaining alerting procedures, and participating in investigations.
- Provided 24/7 SOC monitoring and alert processing to prevent malware intrusion, conduct directory analysis, and perform memory forensics.
- Utilized Sophos Security and Security Onion to provide security baseline, threat mitigation, and network monitoring to PSAP, power grid, and midsized organizations.
- Conducted triage of real-world malicious alerts and PCAPs, wrote security reports, and presented findings to the team, enhancing threat detection response capabilities.
- Facilitated Incident Response Refresher Training, reinforcing the Incident Response lifecycle and improving the team's analysis and decision-making skills.
- Implemented a Cybersecurity price schema on the company's website, enabling customers to visualize cost savings associated with purchasing our SOC-as-a-Service.
- Developed report generation capabilities for Sophos Security.
- Built a firewall for remote monitoring and management of client nodes using Sophos XG Firewall.

Frontend Engineer
Enable Data **01/2021 - 10/2023**

- Implemented the frontend for a cloud-based SaaS healthcare product, contributing to a $2M funding round and reducing prior authorization costs and response times by over 50%.
  - Designed and implemented a user interface for the Criteria review section supporting up to 20k criteria using React.js, Easy-Peasy, and SASS.
  - Revamped the Policy panel interface, boosting user satisfaction by 35% through improved view and edit capabilities for policy, criteria, and associations.
- Led the development of a headless e-commerce platform for farm products, increasing customer engagement by 25%. Improved team productivity by 20% through effective coordination and reduced coding errors by 10% with regular code reviews.