STEVEN J. VIK

Cybersecurity Analyst | Security Operations | Incident Response

Renton, WA

253-315-0162

steven@stevenjvik.tech

linkedin.com/in/stevenjvik

stevenjvik.tech

KEY SKILLS

• Incident Response

• Security Operations

• Threat Detection

• Vulnerability Assessment / Penetration Testing

• SIEM (Splunk, LogRhythm)

• Scripting (Python, PowerShell, Bash)

• Linux Administration

• Asset Inventory / Endpoint Security

• Digital Forensics / Malware Analysis

• Auditing / Compliance Management

• Regulatory (NIST, HIPAA, CJIS)

• Risk Analysis / Disaster Recovery

• Cloud Security

• Collaboration / Communication / Analytical Thinking / Problem Solving

CERTIFICATIONS

‣ CompTIA Security+

‣ CompTIA Network+

‣ CompTIA A+

‣ ITIL Foundation

‣ Linux Essentials (LPI 010-160)

‣ CJIS Level 4

‣ Google Cybersecurity Certificate

PROFESSIONAL SUMMARY

Cybersecurity analyst with 5+ years of hands-on experience in SOC monitoring, incident response, and threat detection. Drove a 40% reduction in incident response times by automating alert validation and standardizing IR workflows in enterprise environments. Developed strengths in SIEM tools (Splunk, LogRhythm), Python scripting, ITIL and NIST frameworks, and collaborated across technical teams for sustained compliance and uptime.

EXPERIENCE

IT Operations Center Analyst

Sound Transit, Seattle, WA (Contract via Infojini Inc.)
Mar 2024 – Mar 2025

Empowered Sound Transit's security landscape by streamlining, innovating, and coordinating enterprise SOC workflows in a dynamic, 24/7 environment.

- Streamlined log correlation and innovated alert validation with Python, driving a 40% reduction in incident response times and enabling NIST 800-53 compliance.
- Facilitated threat detection across 3,000+ endpoints and empowered resolution of 150+ SOC incidents/month using Splunk, SolarWinds, and Blackrock3— earning consistent 99.9% uptime.
- Overhauled ServiceNow workflows and developed SOPs/playbooks, empowering onboarding of new analysts 25% faster and strengthening documentation reliability.
- Partnered in cross-departmental IR reviews, empowering escalation standardization and reducing repeat incident rates.
- Enabled junior analyst growth by facilitating HIPAA, CJIS, and log analysis development sessions.

Enterprise Technology Auditor

TES USA Inc. (Amazon Campus), Tukwila, WA (Contract via Smart Source Inc.)
Jul 2023 – Jan 2024

Facilitated AV infrastructure and inventory audits for Amazon campuses, partnering and collaborating with teams to empower accurate, agile technology setups.

- Coordinated and facilitated detailed audits for 20+ Amazon buildings, empowering readiness of AV, Cisco, mic board, and projector infrastructure.
- Partnered with teams to verify and streamline asset inventory, overhauling documentation and supporting agile workspace upgrades.
- Developed improved asset tracking processes, earning a shortened audit cycle and boosting equipment accuracy.
- Collaborated on cross-functional walkthroughs and recommendations to restructure infrastructure and enhance usability.

EDUCATION

B.S. Cybersecurity & Information Assurance
Western Governors University (Expected Dec 2025)

A.A. Cybersecurity & Forensics
Highline Community College

Family Caregiver (State-Sponsored)

WA State DSHS, Renton, WA
Jan 2021 – Jun 2023

Coordinated regulated in-home care responsibilities while developing continual IT and cybersecurity expertise, empowering ongoing professional growth.

- Coordinated regulated care duties, empowered certified standards, and developed continual IT/cybersecurity expertise through self-directed innovation.

IT Consultant

Seattle University & City of Medina Police Department, Seattle, WA (Contract via Robert Half & TIG)
Mar 2020 – Mar 2021

Enabled secure hybrid operations for academic and law enforcement teams, innovating and streamlining remote access and incident response continuity.

- Facilitated secure remote access and empowered CJIS endpoint security for 200+ users, innovating continuity solutions during COVID-19.
- Overhauled incident protocols and streamlined SolarWinds data flows, innovating a 20% increase in SOC efficiency.
- Designed and developed IR playbooks, enabling knowledge transfer and onboarding in a hybrid environment.

IT Security Specialist

Joint Base Lewis-McChord, Tacoma, WA (Contract via TEKsystems)
Mar 2017 – Mar 2018

Developed and overhauled DoD security environments, restructuring compliance and empowering teams to maintain advanced audit readiness.

- Restructured risk management and overhauled patching for DISA STIG-compliant Windows 10 deployment, empowering 500+ DoD users and earning a 25% reduction in unauthorized access.
- Developed Splunk SIEM threat hunting protocols and vulnerability management strategies, enabling a 35% stronger security posture.
- Streamlined audit procedures and empowered specialists through compliance sessions, earning improved audit outcomes.

KEY PROJECTS

SOC Process Optimization
Developed escalation/IR workflows (MTTR -40%).

Automation Dashboards
Built Python-based log correlation tools (+40% efficiency).

Proxmox Lab Deployment
Created SOC lab with Grafana/Python for analyst training.