JUSTIN SIEV

— Cyber and Network Security, System Administration —

Brooklyn, NY | **MOBILE:** 732-513-4798 | **EMAIL:** jsiev24@gmail.com | linkedin.com/in/justinsiev24

PROFESSIONAL SUMMARY

Analytical, detail-oriented Cybersecurity Engineer with robust background and in-depth knowledge in technical network security poised to leverage advanced knowledge in cybersecurity, risk management, vulnerability assessments, data loss prevention, & threat analysis across various industries. Currently pursuing my Azure Cybersecurity Architect Expert Certification.

- ✦ Expert at managing information security needs and cybersecurity risks in an ever-changing technology landscape.
- ✦ Proven success in fixing security vulnerabilities and risks and strengthening system security, reliability, & functionality.
- ✦ Equipped with technical expertise in current cybersecurity threats, emerging technologies, and mitigation techniques to refine existing security systems, investigate potential vulnerabilities, and deploy IT security solutions.

CORE COMPETENCIES

Cybersecurity Engineering • Network Security Engineering • IT Infrastructure Support • Technical Services Engineering • Network Defense • Policy Enforcement • Vulnerability Management • Resource & Access Administration • Risk Assessment & Mitigation • Technical Documentation • Technical End-User Support • Team Leadership & Collaboration

CERTIFICATIONS

EC-Council Certified Network Defender
EC-Council Certified Ethical Hacker
AWS Certified Cloud Practitioner
Microsoft Azure Fundamentals
Microsoft Azure Administration Associate
ISC2 Certified Information Systems Security Professional (CISSP)
CompTIA A+
CompTIA Network+
CompTIA Security+
ITIL v3 Foundations
Microsoft Azure Security Engineer Associate

EXPERIENCE & IMPACT

Vaco — **Jacksonville, FL**
Cybersecurity Engineer III — **October 2023 – Present**

Contract with EverBank working as a Cybersecurity Engineer III focusing on vulnerability management.

- Assist in managing Nexpose Vulnerability Scanner for network administration, and vulnerability scans and analysis.
- Develop and maintain asset groups, scan engines, templates, and shared credentials for authenticated scanning.
- Perform vulnerability scans on workstations, servers, and vendor appliances to detect and remediate vulnerabilities within the company environment.
- Perform weekly Twistlock base image certification by ensuring that all critical and high vulnerabilities are remediated to maintain container security for developers.
- Manage and update company's vulnerability database with latest CVEs and associated CVSS scores based on the National Vulnerability Database (NVD).

McGraw Hill Education — **Hightstown, NJ**
Cybersecurity Engineer — **March 2020 – February 2023**

- Assisted in the assessment and onboarding of potential third-party vendors in partnership with business-side teams.
- Played an instrumental role in the development of customized vendor security questionnaires via OneTrust.
- Piloted discovery and review of high-impact security risks based on vendor's scope of services and accessed data.
- Updated API access-keys through annual IAM audits and reinforced security policies such as access revoking.
- Safeguarded private accessibility of passwords, access keys or code through monthly GitHub secrets scanning.
- Supported Cover Security Operations Center and preserved positive company reputation with routine discovery, research, and elimination of typo-squatting domains through monthly SecurityTrails scanning.
- Expertly navigated Nexpose Vulnerability Scanner for network administration, and vulnerability scans and analysis.
- Developed and maintained asset groups and scan engines to perform vulnerability scans on internal hosts.
- Uncovered and remediated security vulnerabilities with application owners following Rapid7 vulnerability scans.
- Presented the importance and benefits of vulnerability management to business-side users via documentation.
- Utilized Cisco FirePower Intrusion Prevention Devices to create access control, system, and intrusion policies, including maintaining current rule sets and versions.
- Facilitated the syslog configuration efforts for data analytics by forwarding Cisco FirePower alerts to Splunk Cloud.
- Strengthened network security posture by leading Least Access Privilege Management project for 20+ vendors.

- Enabled clear visualization of vendors access with the internal network by building IPSec VPN tunnel diagram.
- Reduced potential attack surface area via disablement of unused tunnels and ports with the Networking team.
- Suppressed and investigated potential and confirmed system threats through Real Time Response.
- Drove the verification of reported hosts and access via CrowdStrike, adhering to correct policies and regulations.
- Discovered system anomalies via behavioral analytics monitoring and threat hunting using Microfocus Interset.
- Managed ZScaler Internet Access URL policies and review, approval, or denial of user requests for URL whitelisting.
- Supported the configuration and revision of exclusion policies in Symantec Endpoint Protection Manager.
- Performed multiple testing scenarios for the migration from Symantec Endpoint Protection to CrowdStrike Falcon.

Silicon East Inc. **Morganville, NJ**

Technical Services Engineer **February 2018 – November 2019**

- Consulted with and determined infrastructure requirements for client networks.
- Developed secure internal networks and VPN tunnels via configuration and deployment of SonicWALL appliances.
- Built standardized documentation for all I.T. procedures and set up and integrated new offices into client networks.
- Rendered end-to-end infrastructure support for small to mid-sized businesses as a technical services team member
- Reviewed and responded to anti-virus and intrusion detection alerts to reduce and mitigate their system impacts.
- Ensured the optimal satisfaction of clients on prompt resolution of daily technical issues in their business technology.
- Assisted in deploying and managing client servers and users, including Active Directory and Microsoft Exchange.
- Configured Aruba switches for VLANs and power-over-ethernet devices such as VoIP phones and security cameras.
- Led the configuration and deployment of customized high-performance laptops, camera systems, and Intel NUCs.

UBS AG **Weehawken, NJ**

Network Security Engineer **June 2013 – February 2018**

- Provided Level 2 Support for Intrusion Detection Systems, serving as escalation point for Level 1 incident support.
- Highly contributed to the engineering of a refresh of intrusion detection systems and packet capture & inspection.
- Formulated access control, system, and intrusion policies for Cisco Network Intrusion Detection Systems.
- Configured SNMP on FireEye packet capture and inspection devices, including tested SNMP functionality to ensure timely alert generation during occurrence of errors or malicious activities.
- Drove investigative efforts for malicious activities with automatic ticket generation for Security Operations Center.
- Documented all steps of configuration and testing for Service Delivery to implement into production environments.

OTHER EXPERIENCE

Engagement Manager | UBS AG, Weehawken, NJ

Systems Engineering Intern | UBS AG, Weehawken, NJ

EDUCATION

Bachelor of Science, *Major: Information Technology | Minor: Digital Communications in Media* May 2014
Rutgers University, New Brunswick, NJ GPA: 3.4

TECHNICAL SKILLS

SonicWALL, UNIX/Windows, Splunk, Cisco FirePower, Microsoft Office, Azure