Sambhu Rajendran

sambhurajendran10@gmail.com |519-949-7297 |Ontario, Canada |linkedin.com/in/sambhurajendran

Work Experience

Network Support Specialist, Auvik Networks – Ontario May 2021 – Present

- Configured firewalls, switches, and routers, and designed monitoring policies to ensure seamless integration with Auvik's network monitoring tools, improving visibility and performance management
- Configured and optimized firewalls from vendors like Fortinet, Palo Alto, Cisco, and implemented security policies.
- Analyzed NetFlows and packet captures to identify network anomalies, diagnose performance issues, and implement effective resolutions to network bottlenecks
- Monitored and analyzed EDR activity to detect and respond to advanced threats, strengthening incident response effectiveness by reducing downtime of endpoint devices
- Analyzed network and security performance data to identify trends, detect anomalies, and potential security risks
- Used SQL queries to analyze backend data, identify discrepancies, and resolve customer issues efficiently, reducing repeat support queries by 25%. Documented solutions to improve troubleshooting efficiency
- Analyzed large volumes of network and security data to identify performance trends, detect anomalies, and assess potential security risks
- Trained new team members on technical concepts and operational processes, ensuring quicker onboarding and enabling them to contribute to ticket resolution sooner, thereby improving overall team efficiency
- Set benchmark SLA targets by consistently achieving above 85%, prompting managers to adopt this performance as the standard for the team
- Authored technical articles to improve knowledge sharing and technical proficiency

Security Analyst (Part-time Rotation), Auvik Networks – Ontario June 2024 – Nov 2024

- Mitigated high-risk SAST findings by working with development teams to implement security fixes
- Executed vulnerability scans on corporate and product environments, ensuring systems and applications remained up-to-date
- Resolved critical vulnerabilities reported through bug bounty programs within, working with ethical hackers and DevOps teams
- Used Carbon Black to monitor endpoint activity and security incidents, mitigating potential damage
- Configured custom alerts and notifications in Amazon GuardDuty to improve incident response times and proactively mitigate security threats

Server Administrator Tier 2, Hashroot Technologies – Kerala, India Oct 2018 – July 2019

- Hardened servers by implementing and maintaining security best practices, including regular patching, software updates, and access control measures
- Implemented security tools, including antivirus solutions and vulnerability scanners, to improve threat detection and prevention capabilities
- Migrated on-premises servers to cloud, improving system reliability and scalability, and increasing uptime by 99%.
- Implemented system health monitoring solutions using Nagios and Icinga to identify and resolve issues proactively
- Automated Routine Tasks with scripting languages (e.g., PowerShell, Bash, Python) to improve efficiency and reduce human error
- Provided real-time troubleshooting support via screen share, resolving customer issues live, reducing resolution time by 50%, and improving satisfaction
- Directed a team of Tier 1 Server Administrators, overseeing daily operations and implementing strategies to enhance server management, support, and security

Network Engineer, Amrita Center for Cyber Security Systems and Networks – Kerala, India Mar 2016 – Sept 2018

- Configured network hardware, including routers, switches, firewalls, and wireless access points, to optimize connectivity and security
- Implemented security measures, including firewalls, access controls, and intrusion detection systems, to strengthen network defenses
- Resolved network connectivity issues for users and devices, restoring functionality and minimizing downtime by 30%
- Partnered with IT support, server administrators, and cybersecurity staff to maintain uninterrupted network operations and reduce downtime

Skills

Cloud & Infrastructure: Amazon Web Services, Azure
Log and Network Analysis: Syslogs, Wireshark, Netflow, Datadog
Vulnerability Management: Nessus, Snyk (SAST/DAST)
Scripting: Python, Bash
Security Governance: Tugboat
Endpoint Detection and Response (EDR): Carbon Black
IDS/IPS: Snort, Suricata

Certifications

Certified Information Systems Security Professional (CISSP) Feb 2025
CompTIA Security+ Feb 2024
Certified in Cybersecurity by ISC2 Mar 2024
Amazon Web Services Solutions Architect Associate Dec 2019
Cisco Certified Network Associate (CCNA R&S) Jan 2016

Education

Pondicherry University – Bachelor's in Electrical and Electronics Engineering Nov 2014

Accomplishments

Guinness Book of World Records for Rubik Cube event Jan 2023
Asia and India Book of Records for Rubik Cube event Feb 2022