Natsuki Subaru

(123) 456-7890 | Natsuki@outlook.com | Github | Blog | LinkedIn

Skills

- **SOC**: Incident Response, Detection Engineering, Log Analysis, Malware Analysis, Threat Intelligence, & Network Security
- **Tools**: Wireshark, Snort, Splunk, Wazuh, & ELK
- **Networking**: OSI Model, Subnetting, Routing/Switching, Ports & Protocols, etc
- **Programming/Scripting**: Python, Bash, Powershell & Assembly
- **OS/Virtualization**: Windows 10/11, Windows Server, Linux/Unix & VMWare

Experience

SOC Analyst - ABC Security, Nashville TN *October 2020 - Present*

- Monitoring and analyzing network traffic for suspicious activity, quickly responding to and eliminating threats in order to minimize the impact of cyber attacks on the organization.
- Performing investigations into over 40 threats and breaches by analyzing network and system logs.
- Working closely with the IT department to strengthen the network by deploying firewalls, antivirus programs, & IDS/IPS systems, ultimately lowering detected intrusions and threats by 45%.
- Create detailed and accurate documentation and reporting on over 25 security incidents from detection to eradication and recovery.

Network Administrator - Real Tech Company, Nashville TN *July 2018 - October 2020*

- Setup, configured & maintained networking hardware from Cisco like routers and switches for a network of over 450 users and 600 devices.
- Performed troubleshooting on networking equipment in order to quickly resolve issues and maintained a network uptime of 99%.
- Analyzed network performance and came up with solutions to improve the utilization, throughput and availability of the network, improving network performance by 20%.
- Created and managed backups of all device data and configurations via automated processes and made sure that the data was securely stored and easily accessible when needed.

Certifications

- CISSIP *January 2024*
- GSOM *June 2021*
- Security+ *September 2020*

Projects

SOC Homelab | Documentation *July 2023*

- Built a fully virtual SOC lab with VirtualBox using tools like Wazuh, MISP, Splunk, & ELK for detection, logging, and analysis of anomalies within the network.
- Hardened the network again threats by configuring firewalls and IDS/IPS systems.