Sunny Kumar

Cyber Security Analyst |LinkedIn profile-www.linkedin.com/in/sunnyk992
Phone: +91 8802054992 | Email: sk.dln8@gmail.com | Location: New Delhi, India

---

Objective

Experienced Cyber Security Analyst with a good background in checkpoint firewall management, network monitoring, and SIEM incident response. Seeking to apply expertise in advanced SIEM Splunk tool, Checkpoint firewall management, and detailed log analysis to strengthen an organization's security posture. Committed to delivering proactive security solutions that ensure the integrity, confidentiality, and availability of critical data in fast-paced, high-stakes environments.

Key Skills & Competencies

- **Network Security**: Firewall Configuration & Management, Intrusion Detection & Prevention, VPN, Security Event Monitoring
- **SIEM Tools**: Splunk Enterprise and Enterprise Security, Log Management, Security Incident Response
- **Endpoint Detection & Response**- CrowdStrike (Training in progress)
- **Firewalls**: Checkpoint Firewalls, Configuration, and Troubleshooting
- **Security Monitoring**: Log Analysis, Event Correlation, Incident Management
- **Networking Protocols**: TCP/IP, DNS, DHCP, OSI Model, Routing, Switching
- **Troubleshooting**: Wireshark, Fault Diagnosis, Root Cause Analysis
- **Ticketing Tools**: ServiceNow, Freshdesk
- **Certifications**: CCNA, Checkpoint Security, Splunk Enterprise Security
- **Operating Systems:** Linux, Windows 10, Windows 11
- **Network Security Devices:** Checkpoint Firewalls, IDS/IPS, Proxy Servers.
- **Networking Protocols:** TCP/IP, DNS, DHCP, HTTP, SSL/TLS, VPN

Professional Experience

Hitachi System India Pvt. Ltd. – New Delhi, India

Cyber Security Analyst || July 2024 – Present

➢ Working in a 24x7 Security Operations Centre
➢ Monitoring the customer network using Splunk SIEM.
➢ Good knowledge of Splunk Distributed cluster Architecture.
➢ Installing Splunk apps and Addon on the Splunk.
➢ Act as first level support for all Security Issues

➢ Analysing Realtime security incidents and checking whether its true positive or false positive
➢ Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
➢ Collaborate with other teams, such as network operations, system administrators, and application developers, to gather information and coordinate incident response efforts.
➢ Raising true positive incidents to the respective team for further action
➢ Creating tickets on service now and assigning it to the respective team and taking the follow-up until closer
➢ Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.
➢ Investigate malicious phishing emails, domains, and IPs using Open-Source tools and recommend proper blocking based on analysis.

QOS Technology – New Delhi, India

Security Analyst
June 2022 – March 2024

➢ Working as a CCSP Partner for Checkpoint Firewall.
➢ Constantly monitor security devices and applications for performance problems and provide troubleshooting support for clients. When issues arise, they must analyse the root cause and resolve them promptly or else escalate them to another department while updating clients all throughout.
➢ Troubleshooting, Diagnosing and resolving hardware, software, and other network problems related to Check Point technical assistance centre.
➢ Provide accurate and creative solutions to end-user problems to ensure their satisfaction.
➢ Daily monitoring the log and analysing and create the logs report.
➢ Good knowledge of Splunk Distributed cluster Architecture
➢ Detail knowledge of the working functionality of various components of Splunk such as Indexer, Search head, Heavy forwarder, deployment server etc.
➢ Experience in onboarding of data sources with Splunk such as Windows, Linux, Chekpoint Firewall etc.
➢ Installing Splunk apps and Addon on the Splunk.
➢ Doing the troubleshooting in case any device is not reporting to the Splunk.
➢ Knowledge of Creating dashboard, Reports in Splunk.
➢ Blacklisting the Ip’s as per customer needs.
➢ Whitelisting the IP as per need of the customer.
➢ Provide accurate and creative solutions to end-user problems to ensure their satisfaction.
➢ To recognize the importance of customer focus and/or of serving the needs of the end-user.
➢ Research, understand, and analyse different cloud environments.
➢ Monitor and adjust detections based on their performance impact, input from customers.
➢ Daily monitoring the log and analysing and create the logs report.
➢ Daily monitoring the and creating the health report.

Gramin Vikas Sansthan (GVS) – Huawei Project – New Delhi, India

Optical Fiber Trainer (OFT)
October 2020 – June 2021

➢ Conducted fibre optic installation and splicing training, teaching professionals to maintain fibre networks.
➢ Led teams in the cabling of underground and underwater fibre optic lines, ensuring proper installation practices.
➢ Designed training programs to enhance fibre optic troubleshooting and network setup skills.

Indian Telephone Industries (ITI) Limited – Bangalore, India

Network Field Engineer
October 2018 – June 2020

➢ Installed and configured OLT (Optical Line Terminal) and ONT (Optical Network Terminal) devices for client networks.

➢ Performed fault management using NOFN-NMS and GPON-EMS applications, identifying and resolving network issues.

➢ Provided L1 and L2 support for troubleshooting and network performance enhancement.

➢ Managed fibre splicing, preventive maintenance, and subscriber management for GPON systems.

Education

Bachelor of Technology (B.Tech.)
Electronics & Communication Engineering
AKTU University, 2017

Higher Secondary Certificate (HSC)
UP Board, 2013

Certifications & Training

- **CCNA** (Cisco Certified Network Associate)
- **Checkpoint Firewall**
- **Splunk Enterprise and Enterprise Security**

Personal Information

- **Date of Birth:** September 10, 1995
- **Marital Status:** Single

- **Nationality:** Indian
- **Gender:** Male
- **Passport:** Yes

Declaration

I hereby declare that the information provided is true and correct to the best of my knowledge.

Date:
Place: New Delhi, India

Signature:
Sunny Kumar