Sunil Kumar W | Cloud Security Analyst

Chennai-India | +91 97916 36292 | Nirmalsunil0112@gmail.com | linkedin.com/in/sunil-kumar-0112/

PROFESSIONAL SUMMARY

Professional Experience with 5+ years in cybersecurity and team leading. Expertise in SIEM monitoring, endpoint security, and threat intelligence. Proven skills in incident handling, team leadership, and Client Handling. Proficient in Sandboxes (Hybrid Analysis, AnyRun), Threat Intel Sites (Cisco Talos, IBM X-Force), Firewalls (Cisco Firepower, Sophos), IDS/IPS (ELK, Snort), SIEM (Sumo Logic, Snort), and EDR (TrendMicro, Sophos, Defender) ., **Currently preparing for CEH-Master**

AREAS OF EXPERTISE

- SIEM Monitoring
- Incident Handling
- Endpoint Security
- Presentation
- Project Management
- Team Management
- Threat Intelligence
- Ticket Handling
- Communication
- Client Handling

PROFESSIONAL DEVELOPMENT (Seminars / Workshops)

- One Day Workshop in Cyber Security **– TJS Polytechnic College** — Sep 2024
- Innovative Cybersecurity Navigator: Empowering Through Career Guidance, Awareness, and Investigation Training – **RMK College of Engineering & Technology** — March 2024
- Stress Management – **BharatFIH** — June 2023
- Network Security Introduction Webinar – **BharatFIH** — July 2023
- Phishing Email Awareness Campaign – **Ganesan CA Association** — Aug 2023

WORK EXPERIENCE

Cloud Security Engineer — May 2024 - Present

TCS(Deputation), Hyderabad, Telangana

- Monitoring the firewall logs on 24x7 basis in SIEM Tool and investigating the logs
- Led threat hunting exercises on SIEM and EDR platforms, utilizing the results to increase in the identification of potential threats.
- Preparation of SOPs and technical documentation on the new implementation of tools
- Responded to client requests, concerns, and suggestions, achieving an increase in client satisfaction. Conducted regular meetings and presentations.
- Ticket handling via ServiceNow and closely monitoring with the end user for closing before SLA.
- Implementation of SIEM Tools and modified the queries based on requirement
- Troubleshooting VPN issues and 2FA authentication
- Email Analysis on open-source threat intel tools and sandbox.
- Investigating logs of SIEM and cross verify with Firewall.
- Conducting cyber security Awareness Campaign
- Malware analysis on Endpoint with the help of Sandbox and open threat Intel tools
- Managing client meeting and preparation of client for the monthly meeting.
- Planning Shift based on resources availability
- Taking Seminars/workshops in open forum.
- Leading team of 30 members from various process at designation of Team Lead in Non-IT
- Handling P1/P2 Call based on the priority and Creating RCA,

- Supporting on Any Rule Modification and Creating Artefacts
- Working and Creating Change Request (CR) and Follow-up for Approval
- Rule Implementation and troubleshooting the issue based on Client Request
- Creating Dashboards on Sentinel and Workbooks
- Preparing Health Check report and Sharing with Client

Network Engineer March 2023 - Aug 2023

BharatFIH, *Tada, AP*

- Designed and implemented robust network architectures, optimizing flow for 50% increased efficiency and minimizing downtime by 10 %
- Managed network operations, including call logging, monitoring, and proactive troubleshooting to ensure seamless connectivity and performance.
- Executed Identity and Access Management (IAM) protocols, enhancing Windows OS security through user authentication and access control configuration.
- Led network setup and troubleshooting initiatives, resolving connectivity issues promptly and ensuring optimal network functionality.
- Championed Cyber Security Training and Implementation, providing essential education and implementing measures to fortify network security against potential threats.

SOC Analyst Aug 2021 - March 2023

HTC Global Services, *Chennai, TN*

- Orchestrated incident response coordination with customers, resulting in a 25% reduction in time to identify, assess, and mitigate security incidents.
- Validated security incidents with precision, achieving a improvement in the accuracy of incident validation, ensuring only genuine threats were addressed.
- Collaborated with SOC Manager to improve incident detection and closure processes, resulting to reduction in mean time to detect and mean time to respond.
- Conducted thorough audits of logging and correlation processes, improving efficiency and ensuring the accuracy of security event correlation.
- Developed, documented, and tuned threat detection use cases, leading to increase in SOC's detection capabilities and a more proactive approach to emerging threats.
- Executed risk hunting activities, resulting in the identification and mitigation of potential threats, contributing to reduction in the overall risk landscape.
- Responded to client requests, concerns, and suggestions, achieving a increase in client satisfaction. Conducted regular meetings and presentations, fostering transparent communication with clients.
- Led threat hunting exercises on SIEM and EDR platforms, utilizing a robust methodology that resulted to increase in the identification of potential threats.
- Set up monthly meetings to review reports with clients, improving the reporting process, ensuring timely and relevant information exchange.

Production Supervisor (Team Lead) June 2019 - Aug 2021

Zen Lenin International Pvt Ltd, Tada, AP

- Lead and managed a production team, providing guidance, coaching, and support to ensure effective performance and achievement of 100% production target
- Develop and implement production plans, considering factors such as resource availability, equipment capacity, and customer demand to maximize efficiency
- Plan and execute production projects, overseeing the entire project lifecycle to ensure timely delivery, quality standards, and adherence to project specification

TECHNICAL SKILLS

- **Sandboxes -** Hybrid Analysis | App AnyRun | Virus Total | MX ToolBox |
- **Threat Intel Sites** - Cisco Talos | IBM X-Force | Virus Total | IPvoid | AbuseIPDB | TrendMicro | IP2Location|
- **Firewall -** Cisco Firepower | Fortinet | Sophos | Checkpoint
- **IDS/IPS -** ELK | Kibana Snort | Ossec |
- **SIEM -** Sumo Logic | Aikido | Snort | Sentinel |
- **Ticketing Tool -** Services Focus | Remedy | Service Now
- **Phishing Tools -** Gophish|Knowbe4| Phishing Campaign| Email Analysis| Zphisher
- **Endpoint Security -** TrendMicro | Sophos | Defender
- **Vulnerability Management -** Nessus |
- **Management Skills -** Incident Management| Project Management| IT - Infrastructure Management | Team Management| Infrastructure management| Client Handling| Shift Handling| Ticket Management
- **Reporting Tool** - TheHive Project.

LICENSES & CERTIFICATIONS

CEH - Master, EC-Council – Preparing

Project Management, Loyola Institute of Business Administrator – May 2024.

PROJECT

Investigation in Data Extraction - Internal Project in Cyber Security

- Extracting captured data by using Wireshark and investigating the packet and finding hidden message on the attachment with the using of Steghide.

Home Lab - Implementation SOC Lab and Firewall Configuration in Virtual machine.
SIEM - Sumologic - Collector installation and Log Forwarding to Central SIEM,
- Correlation, Parsing, Query Modification and Dashboard Creation

EDUCATION

BBA-Business Administration, Annamalai University – 2021 – 2023

PDCIL-Professional Diploma in Cyber Investigation and Law, Hindustan University – 2019 – 2020

DME-Diploma in Mechanical Engineering, TJS Polytechnic College – 2016 – 2019