

ASHWANTH SARAN JC

Email: ashwanthsaranjc@gmail.com | Phone: (+91) 8667020032

LinkedIn: [LinkedIn Profile](#) | Portfolio: [Portfolio Website](#) | GitHub: [GitHub Profile](#)

SUMMARY

SOC Analyst with hands-on experience in security operations, incident triage, and threat detection. Skilled in SIEM platforms (**Wazuh**) with a strong understanding of log analysis, alert correlation, network security, endpoint defense, and SOC workflows. Experienced in vulnerability analysis, CVE research, and basic threat intelligence to enhance detection and response capabilities. Proficient with EDR/XDR tools (**SentinelOne**) and firewall monitoring on **Sophos** and **Palo Alto**. Passionate about improving cybersecurity resilience through proactive monitoring, investigation, and continuous learning.

TECHNICAL SKILLS

SOC Operations: Log monitoring, alert triage, incident escalation, phishing investigation, basic incident response, and SOC ticket handling.

Security Tools: Wazuh (SIEM), SentinelOne (EDR/XDR), Palo Alto (NGFW) and Sophos (NGFW)

Threat Analysis: MITRE ATT&CK mapping, IOC identification and validation using VirusTotal and AbuseIPDB, phishing email analysis.

Networking & Protocols: Experience with Wireshark, TCP/IP, DNS, DHCP, VPN, OSI model, basic firewall concepts.

Operating Systems: Linux, Windows 10/11, Windows Server.

Scripting & Cloud (Basic): PowerShell, basic AWS (Wazuh server hosting).

Soft Skills: Incident documentation, analytical thinking, attention to detail, continuous learning.

Languages: English, Tamil, Hindi.

PROFESSIONAL EXPERIENCE

Security Operations Center (SOC) Analyst – L1 | Necurity Solutions Network Security Pvt. Ltd., Chennai

- Monitored and analyzed security alerts using Wazuh SIEM, SentinelOne EDR/XDR, Sophos and Palo Alto firewalls.
- Deployed and maintained Wazuh agents across ~800 endpoints for centralized log collection.
- Performed event correlation across endpoint, network, and server logs to identify suspicious activity.
- Conducted IOC validation using VirusTotal and AbuseIPDB to support threat investigations.
- Supported incident response by classifying alerts and escalating confirmed incidents to senior SOC analysts.
- Investigated basic network activity and logs using Wireshark for initial root cause analysis.

PROJECT

SOC IP Analyzer – Internal SOC Tool

- Built a real-time IP threat analysis tool integrating AbuseIPDB and VirusTotal for automated threat enrichment.
- Implemented a composite risk scoring system to classify IPs as Clean, Low Risk, Suspicious, or Malicious.
- Provided geolocation mapping and threat visualization using Leaflet.js and Chart.js.
- Delivered a dark-mode dashboard with caching and structured intelligence summaries to support faster SOC triage.

EDUCATION

Master of Computer Application (MCA)

B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai

Bachelor of Computer Application (BCA)

VELS Institute of Science and Technology, Chennai

CERTIFICATIONS

- **Cisco** – Security Operations Center (SOC)
- **Fortinet** – Certified Fundamentals in Cybersecurity
- **IBM** – Introduction to Cybersecurity Careers
- **Fortinet** – Introduction to the Threat Landscape 3.0
- **TryHackMe** – Pre Security
- **Planned: EC-Council** – Certified SOC Analyst (CSA)