Mallikarjuna Patnam
Security Analyst

+91 9390606796
patnam.mallikarjuna99@gmail.com

Professional Summary

Holding 3+ years' experience as a Security Analyst with a strong foundation in security monitoring, incident response, and threat analysis. Skilled in utilizing SIEM platforms, intrusion detection/prevention systems (IDS/IPS), log analysis, and endpoint security solutions to detect and mitigate cyber threats in real-time. Passionate about proactive threat hunting, security incident handling, and continuous learning to enhance organizational security posture.

Technical Skills

- **SIEM**: Azure Sentinel, LogRhythm, Splunk
- **Email Security**: Proof point, Trend Micro, Darktrace Antigena
- **Vulnerability Assessment**: Qualys
- **EDR**: CrowdStrike falcon, Cisco AMP
- **Malware Sandbox**: Virus Total, Cisco Talos, Any.Run
- **Firewalls**: Palo Alto, McAfee NSM
- **DLP**: Symantec
- **ITSM**: ServiceNow, Jira
- **Antivirus**: McAfee, Symantec Endpoint Protection (SEP)
- **Web Proxy**: Zscaler

Professional Experience

Tata Consultancy Services **07/2021 – 01/2025**

Security Analyst

- Provides regular monitoring, triage, and incident response to automated security alerts using Security tools (like SIEM Azure Sentinel, LogRhythm, Splunk, EDR, Antivirus, and Email Security).
- Solid understanding of common network services and protocols.
- Solid understanding of OSI Layers, TCP/IP Protocol Suite, and commonly used Networking Protocols.
- Good knowledge of malware and Security attacks such as Brute force attacks, Phishing attacks, DOS/DDOS, and SQL injection.
- Knowledge of advanced capabilities like Threat Hunting and Malware Analysis.
- Responding to various security alerts for various clients and scanning for vulnerabilities using VMT tools like Nessus.
- Conduct a re-assessment after mitigating the vulnerabilities found in the assessment phase.
- Working knowledge of Security Solutions such as Proxy, Firewall.
- Good experience working/communicating with cross-functional IT infrastructure teams like network, system, database, application, and security to build and manage effective security

operations.

- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, SLAs, client meetings, report walkthroughs, bridge calls, etc.
- Ability to read and analyze suspicious activity using Splunk Enterprise.
- Capable of independently learning new technology by utilizing available documentation and vendor support resources.
- Create Alerts, Reports, and Dashboards in Splunk Enterprise.
- Escalate potential threats after prioritizing them. Good knowledge of the Incident Response process.
- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, SLAs,
- client meetings, report walkthroughs, bridge calls, etc.
- Understand the structure and meaning of logs from different log sources such as FW, AD, AV, email security, etc.
- Issue resolution with end-user following ticket raised for incident response process with various network, IT & server teams.
- Ability to read and analyze suspicious activity using Capture Client Management, N-able N-central, and Splunk Enterprise.
- Creating dashboards and generating reports on SIEM.
- Good Understanding of malware analysis.
- Provided detailed security incident reports to stakeholders.

Education & Certifications

- B.Tech - SSN Engineering College – Ongole
- Certifications: CompTIA Security+, Certified Ethical Hacker (CEH) (Pursuing)

Key Strengths

- Strong knowledge of security incident classification and triage processes.
- Understanding of OSI layers, TCP/IP, DNS, and common networking protocols.
- Hands-on experience in malware analysis and threat intelligence tools.
- Effective communication and documentation skills in security incident reporting.
- Ability to collaborate with cross-functional teams to enhance security operations.