

KAPPURAPU KARTHIK KUMAR REDDY

Hyderabad, Telangana, India

Email-id: karthikreddy0352@gmail.com

Phone NO: +91 8106195323

Profile

Worked as SOC Analyst with demonstrated history of working in the Managed Security Service Provider industry. Skilled in Security and DDOS Monitoring, Threat hunting & Malware Analysis, Phishing and Spam Analysis, Security Information and Event Management (SIEM), VAPT with manual approach and automated tools

Experience: SOC Analyst

- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from multiple log sources.
- SECURITY ANALYST (L1) in the field of cyber security operations for 24*7SOC environment using SIEM tools like (SECEON, Splunk), EDR, Firewall, and Email security
- Analyze SOC alerts that statistic and work flows to reduce false positives and properly focus engineering efforts.
- Carrying out log monitoring and incident analysis for various devices such as Firewalls, IDS, IPS, database, web servers.
- Preparing daily and weekly dashboard on the security threats. Support security incident response processes in the event of a security breach by providing incident reporting
- Analysis of SPAM and Legit emails and writing Anti-Spam, Anti-Fraud and legit rules using Regular Expressions & Hands on work experience on Email-Fishing, Malware Analysis
- Spam Analysis: Analyzing Email Headers, Call to Action Domains and other parameters to identify Spam messages and block them.
- Knowledge on Cyber Kill Chain and understanding of MITRE ATT&CK® framework Methodology.
- Performed Vulnerability Assessment and Penetration Testing on Web Applications and Network/Infrastructure.
- Hands on experience with NMAP, Nessus Professional, Metasploit Framework & Burp Suite Professional.
- Performed VAPT with manual approach and automated tools.
- Documented & reported the various vulnerabilities with proof of concepts and remediation to clients.
- Good understanding of OWASP Top10 & PTES, IDS, IPS, Threat modeling and Cyber Attacks like DOS, DDOS, MITM, SQL Injection, XSS and CSRF.
- Malware Analysis: Able to perform both basic Dynamic and static Malware analysis on enterprise sandbox environment
- Finding Reputation in different sand boxing environments like (virous Total, MX Tool, Any Run, IBM X Force, CISCO Talas, Meta defender, Abuse IP DB, URL Scan)

Tools

- VAPT Tools : Nmap, Nessus Professional, Metasploit Framework , Brup Suite PRO.
- SIEM s Threat Detection Tools : Seceon, Splunk, EDR (OPEN EDR), Alien Vault OTX.
- Malware Analysis Tools: PEid, CFF Explorer, PE Studio, Regshot, Procmon, Sysmon.
- Phishing Analysis Tools: Urlscan.io, Virus Total, MX Toolbox, Sandbox
- Operating Systems s Virtualization: Parrot OS, VirtualBox.
- Forensics Tools Forensics: Autopsy, FTK Imager, Ease US Data Recovery.

Experience& Certifications

- SOC Analyst Intern | Smart IMS India Pvt. Ltd. | Jan 2025 – July 2025
- VAPT & SOC at Hacking Trainer Institute Unit of Berry 9 It Services PVT LTD
- Preparing For CEH

Projects: Security Operations Center (SOC) Alert Monitoring & Analysis

Organization: Smart IMS India Pvt. Ltd.

Duration: Jan 2025 – July 2025

Description:

Worked as part of the SOC team to monitor, analyze, and triage real-time security alerts using the Seceon SIEM platform. Focused on enhancing alert accuracy and contributing to incident response workflows.

Key Responsibilities:

- Monitored Seceon Dashboards for environments.
- Analyzed security alerts including:
 - Suspicious login attempts
 - Brute force and credential compromise events
 - Malware and Trojan detections
 - Firewall and cloud security alerts
- Collaborated with the **NOC team** to perform in-depth analysis of critical incidents (e.g., brute force attacks).
- Maintained and updated **Excel tracker** for alert categorization, status, and follow-up actions.
- Engaged with senior analysts for insights into complex or high-severity alerts.
- Documented procedures and best practices for Seceon alert analysis and event validation.

Tools & Technologies:

- **SIEM Tool:** Seceon, Splunk
- **Documentation:** Excel-based alert tracker, SLA Sheet.
- **Security Concepts:** Threat detection, event correlation, credential misuse, malware behaviour

Education

- Rayalaseema University College of Engineering -B. Tech (ECE) 2020-2024-78 %
- Govt. Junior College Cumbum – MPC - 2018-2020-81.8%
- ZP (BOYS) HIGH SCHOOL Bestavaripeta – SSC- 2018- 93%