

AKHIL BEERAM

SOC Analyst

Ph: +91 7032289339 | Gmail: akhilbeeram77@gmail.com

Professional Summary

SOC Analyst with over **3.3** years of expertise in **MSSP projects** of hands-on experience in security operations, specializing in incident management, endpoint security, log analysis, ransomware mitigation, and vulnerability management. Proficient in SIEM platforms (Splunk, Elastic, IBM QRadar), EDR/XDR solutions (Sophos, CrowdStrike), and threat intelligence tools (MISP). Skilled in 24x7 SOC operations, real-time monitoring, log analysis, and vulnerability assessment with a proven track record of SIEM optimization and incident response workflow improvements.

Work Experience

SOC Analyst | Grapple Info Solutions Pvt Ltd

MARCH-2024 – JUNE 2025

- Monitored incoming security alerts using SIEM tools such as Elasticsearch, Splunk, and IBM QRadar.
- Actively participated in the SOC team, where I monitored events and took actions to identify and prevent intrusion attempts.
- Gathered logs from diverse network devices and conducted in-depth analysis to pinpoint potential security risks and suspicious activities.
- Handled alerts from multiple security log sources such as Anti-Virus, EDR, XDR and IDS/IPS.
- Experience in Managed end-to-end cloud security for a major product-based client with a fully cloud infrastructure, overseeing comprehensive monitoring, incident investigation, and response to ensure robust protection and compliance.
- Identify potential threats, leaked data, and vulnerabilities, Proficient in assessing organizational attack surfaces, identifying potential entry points, and recommending strategies to enhance security posture and reduce exposure to attacks.
- Collaborated with the team to discuss and fine-tune false positives, creating new rules when necessary. Additionally, I developed advisories and detection rules, prioritizing remediation efforts.
- Provided comprehensive reports for clients and regularly attended weekly meetings to discuss issues related to SOC services.
- Facilitated discussions with clients, including white-listing alerts for specific users to minimize false positive alerts.
- Created dashboards for all authentication-related events, enhancing the monitoring of authentications and effectively handling issues related to failed logins from different systems.
- Hands-on experience with AWS Security Services including Guard Duty for threat detection, Inspector for vulnerability assessment, and Security Hub for centralized security posture management.
- Initiated client calls during high or critical alert triggers, providing guidance to mitigate potential security threats.

Cyber Security Analyst | Partior India Tech Private Limited

SEP-2023 – FEB-2024

- Investigated security threats and created tickets, forwarding them to the Onsite SOC team for further investigation, filled out daily SIEM health checklists and identified attacks based on their signatures.
- Conducted log monitoring and incident analysis for various devices such as firewalls, databases, and web servers.
- Prepared daily, weekly, and monthly log reports tailored to client requirements.
- Created, resolved, and managed tickets, providing recommendations for appropriate actions and Solutions for noise reduction.
- Performed in-depth malware, phishing email investigations, Ransomware attempts, and Web attacks. Demonstrated proficiency in identifying phishing emails by analyzing sender addresses, message content, and suspicious links.

- Provided prioritization recommendations to improve incident handling efficiency. Collaborated with customer personnel to continuously tune correlation rules, improve incident classification, and refine prioritization strategies.

Security Engineer | Paytm

FEB-2022 – MAY-2023

- Monitor, analyze, and respond to security alerts using SIEM tool QRadar and EDR/XDR platforms (CrowdStrike, Defender, Sentinel One).
- Perform threat detection, incident triage, containment, and recovery while documenting actions in ticketing systems like ServiceNow or Jira.
- Conduct threat hunting, malware analysis, and forensic investigations to identify advanced persistent threats and attack patterns.
- Manage and monitor security across Windows, Linux, O365, AWS, and Azure environments, including firewall, IDS/IPS, and cloud-native tools.
- Analyze phishing attacks, suspicious emails, and enforce DLP and email security controls to prevent data breaches.
- Perform vulnerability assessments, track remediation efforts, and ensure compliance with NIST, ISO 27001 and CIS controls.
- Assisted in investigating low-level security incidents like phishing and brute-force attempts.

Skills

- **SIEM:** Elastic, Splunk and IBM Qradar
- **EDR:** CrowdStrike, Sentinel One
- **Email security:** Proofpoint, Proofpoint Tap
- **UEBA platform:** Exabeam
- **Cloud security:** AWS, GCP
- **OS:** Linux, Windows
- **Ticketing tool:** Zoho, Service Now
- Proactive threat monitoring, Threat intelligence, Threat hunting.
- Incident response & Management
- Reports and dashboards creation
- **Threat Intelligence tools:** MISP, SOC Radar, Censys, Shodan, Virus total & Abuse IPDB etc.
- **Microsoft office suite:** Word, Excel, SharePoint & PowerPoint

Certifications

- Network Defense Essentials by EC-Council
- Udemy
- Try Hack Me

Education

- **Bachelor of Technology (B. Tech) in Civil Engineering-** Malla Reddy Institute of Technology and Sciences | 2019.

Declaration

I hereby declare that all the information mentioned in this resume is true and correct to the best of my knowledge and belief.

AKHIL BEERAM