

DURGAM KIRAN

SOC ANALYST

PHONE | (+91) 8465859774
EMAIL | durgamkiran426@gmail.com
LOCATION | Hyderabad, INDIA
EXPERIENCE | 4 Years 2 Months

Key Skills

- SIEM Tools: Splunk Enterprise Security, Microsoft Azure Sentinel, Threat Intelligence Platforms: Recorded Future, ThreatConnect, IDS/IPS: Endpoint Protection: Carbon Black, CrowdStrike, Falcon
- Vulnerability Scanners: Nessus
- Qualys SOAR Tools: Palo Alto Cortex, XSOAR, Splunk Phantom
- Networking Tools: Wireshark, Nmap
- Cybersecurity Frameworks: MITRE ATT&CK, NIST Cybersecurity Framework

Languages

- English
- Hindi
- Telugu

Profile Summary

Experienced SOC Analyst with over 4 years of expertise in cybersecurity monitoring, threat detection, and incident response. Skilled in analyzing and responding to real-time security events, performing in-depth investigations, and mitigating risks across enterprise environments. Proficient with industry-leading SIEM tools such as Splunk, Azure Sentinel and knowledgeable in handling advanced cyber threats, malware analysis, and vulnerability management. Adept at log correlation, threat hunting using the MITRE ATT&CK framework, and collaborating with cross-functional teams to protect critical systems from cyberattacks. Strong problem-solving skills and a passion for maintaining and improving the security posture of organizations.

Work Experience

SOC Analyst

ISG Novasoft Technologies

08/2020 - Present

The SOC Analyst is responsible for monitoring and protecting the organization's network and systems from cyber threats. The analyst works within the Security Operations Center to detect, analyze, and respond to security incidents using various security tools and technologies. The role involves investigating security breaches, documenting incidents, and collaborating with IT and security teams to improve the overall security posture.

Education

B.Tech - Electronics and communication engineering

2014

Projects

Security Log Monitoring and Analysis for Threat Detection

5 Months

The main goal of this project is to monitor, analyze, and correlate security logs from various sources (e.g., firewalls, servers, applications, network devices) to detect abnormal behavior or potential security incidents and respond to them in a timely manner.