

ChandraPrakashreddy Kusam

Security Analyst

✉ Prakashsoc45@gmail.com

☎ +91-6300872203

Diligent and meticulous cybersecurity analyst with over 3 years of experience, actively seeking a role in a reputable organization that offers opportunities for professional growth, job satisfaction, and challenging work. Committed to making valuable contributions to the success of the organization.

Experience

APPLITECH SOLUTIONS

Security Analyst - Jun 2023 to present

- 24/7 SOC operations, overseeing real-time event monitoring, incident identification, tracking, and analysis, along with comprehensive reporting.
- Performed real-time security monitoring, incident management, analysis, and escalation of threats from various log sources.
- Handled and escalated SIEM alerts, ensuring alignment with organizational security policies and prompt resolution.
- Led investigation and remediation efforts for cyberattacks, conducting root cause analysis and advising stakeholders on preventive measures.
- Analyzed suspicious activity to determine the validity of incidents (true or false positives) using advanced tools, improving accuracy in threat detection.
- Supported vulnerability management by monitoring infrastructure risks, coordinating timely remediation efforts, and implementing IP whitelisting/blacklisting strategies.
- Assisted customers during high-priority incidents, providing real-time guidance on attack containment and recovery to minimize impact.
- Created knowledge base documentation, including detailed playbooks and incident response procedures, to streamline team operations.
- Performed threat hunting activities, proactively searching for potential vulnerabilities and anomalous behavior across networks and endpoints.
- Trained junior analysts in security tools and incident response techniques, enhancing overall team effectiveness and skill sets.

Atos syntel

Associate Consultant - Jan 2022-May 2023

- Monitored and analyzed real-time security alerts across multiple sources, including IPS, firewalls, proxy logs, and system logs, ensuring prompt detection and escalation of incidents within SLA.
- Conducted detailed malware analysis using sandbox environments to understand behavior and develop actionable mitigation strategies.
- Investigated phishing, BEC, malware, and SPAM emails, leading to successful identification and resolution of multiple high-risk incidents.
- Collaborated with cross-functional teams to maintain a proactive approach toward evolving threats by fine-tuning detection mechanisms and rules.
- Developed concise and actionable incident reports to enhance management decision-making processes and optimize security policies.

Education:

- **KSRM College of Engineering**

- Bachelor of Engineering in Electrical and Electronics - 2021

Skills:

- Incident Response
- Microsoft Azure
- ES Splunk
- Email & Malware Analysis
- Threat Hunting
- CIS Benchmark, NIST
- Problem-solving
- Creativity

Personal Details:

DOB: 10-07-1999

Languages Known: English, Telugu.

Address: Tadipatri, Anantapur dist-515411

Declaration:

I hereby declare that the information provided above is true and correct to the best of my knowledge and belief. I take full responsibility for the accuracy of the information contained in this resume.

ChandraPrakashreddy