GATTU PRATHIBA

SOC ANALYST

CONTACT

☎ +91- 7032533498

✉ gprathiba2505@gmail.com

in www.linkedin.com/in/gattu-prathiba-0156321a0

📍 Andhra Pradesh

TOOLS

- SIEM: Microsoft Azure Sentinel
- Threat intelligence – VirusTotal, Abuseipdb, MXToolBOX, IPVOID.
- Threat Analysis: Defender (MDE, MDC, MCAS, MDI), Crowdstrike Falcon.
- Email Gateway: IRONPort.
- Ticketing Tool: ServiceNow.

SKILLS

- 24/7 Monitoring and Incident response. Monitoring devices or logs (Health checks).
- Networking Concepts. SOC Processes, Log Analysis.
- Threat Hunting. KQL (Kusto Query Language).
- Malware & Phishing Analysis
- Operating System: Linux, Windows. Languages: Python & Basics of Java

CERTIFICATIONS

- Digi-Testing- AUTOMATION TESTING- Wipro.
- AZ-900: Microsoft Azure Fundamentals.
- Certificate of Cyber Security Training- SFJ Business Solutions Pvt. Ltd.

SC-200: Security Operations Analyst Associate

PROFILE

- With 2.6 years of experience as an SOC Analyst at a Managed Security Service Provider (MSSP) for multiple clients, I specialize in networking, incident response, and threat hunting, offering a strong understanding of the cybersecurity landscape. I have hands- on experience analyzing phishing and malware threats, swiftly taking action to mitigate risks. Skilled in managing multiple clients at once, I prioritize tasks based on severity and ongoing activities. I actively contribute to daily security operations, focusing on preventing data loss and system compromises by efficiently addressing security alerts.

WORK EXPERIENCE

Capgemini — 2024 | NOV- PRESENT

Security Analyst- L2

- Lead incident response, collaborating with teams to mitigate threats.
- Optimize SIEM tools for better threat detection and accuracy.
- Guide L1 analysts and document findings for reporting and compliance.
- Generated and provided daily, weekly, & monthly reports regularly.
- Proficient in using KQL queries for creating analytic rules and performing regular fine-tuning to ensure optimal rule performance.
- Skilled in implementing auto-closure based on defined criteria and conditions.
- Created and managed watchlists by adding Indicators of Compromise (IOCs) as per specific requests to enhance threat detection and monitoring.

Capgemini — 2022 | OCT

Security Analyst- L1

- Performing 24/7 (Rotational Shifts) real-time monitoring, investigation, analysis, reporting, and escalation of security alerts across various Azure Sentinel log sources.
- Serve as a managed service security analyst for multiple clients.
- Analyze phishing emails and take appropriate actions using Microsoft Defender for Office (MDO).
- Review alerts for suspicious activity and promptly organize bridge calls to address potential security concerns.
- Contact clients directly during high-priority incidents to assist with attack mitigation.
- Lead incident response activities to identify, contain, and mitigate infected systems.
- Collaborate with various teams across the organization to enhance the overall security posture.
- Conduct server health assessments to identify active and inactive servers, generating tickets for relevant teams to perform necessary restarts.
- Prepare daily shift reports and provide complete handovers, including updates and pending actions from the SOC team.

WIPRO — 10th March- 18th July 2022

Internship- Digi Testing- AUTOMATION TESTING

- Participated in live training sessions for Java and Selenium, gaining hands-on experience in automation testing. Utilized the Cucumber framework to conduct tests on various web applications, enhancing testing efficiency and accuracy.

EDUCATION

- B. Tech || SRI VENKATESA PERUMAL COLLEGE OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)- PUTTUR (ANDHRA PRADESH)
- CGPA: 9.26 / 10

2018 - 2022