

GOGULAMANDA ROHITH

+91 6300507355 | gogulamandarohith@gmail.com

SUMMARY

Associate IT Security Analyst with 2+ years' cybersecurity experience in incident management, endpoint security, and SIEM log analysis. Skilled in 24x7 SOC operations, threat escalation, and detailed incident documentation. Proven ability to support vulnerability scans and patch management while maintaining rigorous security protocols and effective communication.

TECHNICAL SKILLS

- **Firewall & Network:** Cisco Firewall, Palo Alto, Wireshark
- **SIEM Tools:** Microsoft Sentinel, Splunk IBM QRadar
- **Endpoint Protection:** O365 Defender for Endpoint, Proofpoint, CrowdStrike, Carbon Black, Sentinel One
- **Cloud Services:** Entra ID production, Azure Services
- **Additional Security Tools:** SOAR, O365 ATP, Any Run, Virus Total, URL Scan, browser-ling, OSINTS, Vulnerability Assessment (VA), OWASP, Incident documentation
- **Ticketing & Productivity:** ServiceNow, Zira, Excel, Word

WORK EXPERIENCE

Happiest Minds

Aug 2022 - Dec 2024

Security Monitoring and Operations

- Analyzed triggered alerts using SIEM tools (Splunk, Microsoft Sentinel) and SOAR platforms to identify genuine incidents.
- Reviewed and acknowledged alerts, closed false positives, and raised tickets using ServiceNow and Zira for validated incidents.
- Collaborated with incident response teams by following playbooks, documenting investigations, and coordinating remediation efforts.
- Participated in weekly SOC meetings to review incident trends and update incident documentation and SLAs.
- Utilized security solutions such as antivirus, Cisco Firewall, Palo Alto, IPS, Email Gateway, and Proxy to monitor and secure endpoints.
- Applied knowledge of malware analysis, threat hunting, and vulnerability assessment (VA) to support proactive defense measures.
- Leveraged industry frameworks such as MITRE ATT&CK, NIST, SANS, and OWASP to guide analysis and compliance efforts.
- Monitored and documented SOC processes including alert monitoring, tiered escalation, and incident resolution.
- Investigated and reported on security incidents, performing root cause analyses and preparing detailed security incident reports.
- Configured centralized detection/prevention policies and dashboards using Splunk, IBM QRadar, and Microsoft Sentinel to improve monitoring accuracy.
- Assisted in vulnerability scans and supported patch management efforts to mitigate critical and high threat alerts.
- Managed endpoint security tasks including deployment of Falcon sensor, troubleshooting host sensor issues, and executing regular Trend Micro scans.
- Developed advanced correlations and queries with Kusto Query Language (KQL) for Azure Sentinel, enhancing detection of adversary actions.
- Conducted incident response activities such as host triage, malware analysis, remote system analysis, and end-user interviews to support swift remediation efforts.

EDUCATION

D.N.R pg. college

2025

M.Sc., Computer science

•GPA: 68.8%

Himalayan University

2020

BSC, Computer science

•GPA: 70.8%