CHOLLANGI MANOJ KUMAR

+91 9154689407 chollangimanojkumar@gmail.com linkedin.com/in/manoj-kumar-chollangi/

Professional Summary

Cybersecurity professional with 3+ years of SOC experience, specializing in incident response, threat analysis, and vulnerability management. Proficient in SIEM tools like LogRhythm, Cortex XDR, Qualys VM. Skilled in optimizing security defenses and mitigating cyber threats through proactive risk management.

Work Experience

Cognizant Technology Solutions
Jul 2021 – Present

Lead Cybersecurity Engineer *Hyderabad, India*

Security Operations, Administration and Monitoring

- Managing LogRhythm SIEM, Cortex XDR/XSIAM, Microsoft ATP, Phish-ER, Darktrace, and Delinea Privilege Manager, along with Qualys VM.
- Conducting technical log analysis and initial incident response, including analyzing malicious scripts using sandboxes to extract Indicators of Compromise (IoCs) and supporting threat intelligence.
- Creating and managing exclusions, exceptions, and rule tuning to reduce false positives in SIEM solutions. Optimizing Cortex XSIAM rule configurations,which has reduced false positives by 16% in 2024.
- Privilege Identity Management support through Delinea Privilege Manager.
- Identifying and assessing vulnerable devices by correlating security advisories, recommending optimal remediation strategies to asset owners.
- Collaborating with stakeholders, clients, and users to provide security recommendations and enhance security posture.
- Developing and presenting security assessment reports.

Education

GITAM University
Jul 2017 - Jun 2021

Bachelor of Technology in Computer Science and Engineering (CGPA of 8.15) *Visakhapatnam, India*

Certifications

- **AZ-900 Microsoft Certified: Azure Fundamentals**
- **SC-900 Microsoft Certified: Security, Compliance and Identity Fundamentals**
- **Zscaler Zero Trust Certified Associate**
- **Google Cloud Digital Leader Certification**
- **Cortex XSOAR - Automation and Orchestration (EDU-380)**
- **RedHat Certified Server Administrator (RHCSA)**
- **TryHackMe**

Technical Skills

SIEM:Logrhythm SIEM, Cortex XSIAM
EDR/XDR: Cortex XDR
Email Security: Microsoft ATP/Defender for M365, Phish-ER
Network Security: DarkTrace Network Threat Visualizer, Cisco Umbrella, Cisco Prime, Infoblox, PaloAlto Panorama Firewall
Vulnerability Assessment: Qualys VMDR, Nessus
Identity Management: Delinea Privileged Access Management and Identity Security
Programming Languages: C, C++, Java, Python, C.#
Web Technologies: HTML, CSS, PHP, JavaScript
Databases: Oracle SQL Developer, MySQL
Operating Systems: Windows, Linux (Red Hat Enterprise, Kali, and Ubuntu)
Tools & IDEs: Burp Suite, XAMPP, Unity 3D, Nmap, Hydra, Metasploit Framework

Profile Links

- GitHub
- LinkedIn