CHOLLANGI MANOJ KUMAR

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

PROFESSIONAL SUMMARY

Cybersecurity professional (CEH) with 4 years of hands-on experience in incident response, threat analysis, and vulnerability management. Expert in utilizing SIEM tools such as LogRhythm, Cortex XSIAM, and Qualys VM to detect and respond to complex threats. Proven ability to optimize security operations by deploying advanced detection systems and proactively reducing organizational risk. Seeking to contribute advanced technical expertise and comprehensive threat management skills to an innovative organization committed to cybersecurity excellence.

WORK EXPERIENCE

Cognizant Technology Solutions   **Jul 2021 – Present**
Lead Cybersecurity Engineer   *Hyderabad, India*
Security Operations, Administration and Monitoring
  - Lead a team in Cortex XSIAM, Microsoft ATP, Phish-ER, Darktrace, Delinea Privilege Manager and Qualys VM.
  - Conduct technical log analysis and initial incident response, including analyzing malicious scripts using sandboxes to extract Indicators of Compromise (IoCs).
  - Created and managed exclusions, exceptions, and rule tuning in SIEM; optimized Cortex XSIAM rules to reduce false positives by 16% in 2024.
  - Provided support for Privileged Identity Management via Delinea Privilege Manager.
  - Correlated security advisories to identify vulnerable devices and recommend remediation strategies.
  - Collaborated with stakeholders and users to enhance security posture and provide recommendations.
  - Developed and delivered comprehensive security assessment reports.

EDUCATION

GITAM University   **Jul 2017 - Jun 2021**
B.Tech in Computer Science and Engineering (CGPA: 8.15)   *Visakhapatnam, India*

CERTIFICATIONS

- Zscaler ZDTA (2025)
- CEH (2025)
- Cortex XSOAR - Automation and Orchestration (EDU-380) 2025
- AZ-900: Azure Fundamentals
- SC-900: Security, Compliance and Identity Fundamentals
- Zscaler Zero Trust Certified Associate
- Google Cloud Digital Leader Certification
- TryHackMe

TECHNICAL SKILLS

- **SIEM:** LogRhythm SIEM, Cortex XSIAM
- **XDR:** Cortex XDR
- **Email Security:** Microsoft ATP/Defender for M365, Phish-ER
- **Network Security:** Darktrace, Cisco Umbrella, Cisco Prime, Infoblox, Palo Alto Panorama Firewall
- **Vulnerability Management:** Qualys VMDR, Nessus
- **Identity & Privilege Management:** Delinea PAM Identity Security
- **Programming Languages:** C, C++, Java, Python, C#
- **Web Technologies:** HTML, CSS, PHP, JavaScript
- **Databases:** Oracle SQL Developer, MySQL
- **Operating Systems:** Windows, Linux (RHEL, Kali, Ubuntu)
- **Tools & IDEs:** Burp Suite, XAMPP, Unity 3D, Nmap, Hydra, Metasploit Framework

PROFILE LINKS

- GitHub
- LinkedIn