

Dinesh Alathuru

cyber security analyst

Cyber Security Professional with 3.1 Years of experience in developing and implementing security solutions in fast-paced environments. Skilled in Cyber Security, Log Analysis & Incident management, T Phishing Analysis

✉ dinesh.oct25@gmail.com

☎ 9642358827

EMPLOYMENT HISTORY

Cyber security analyst

Congnizant

Feb 2019 - Present

- **Key Result Areas:**
- Responsible for working in 24*7 in Security Operation Center (SOC) environment at Cyber Security Fusion Center.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalation of Security
- Events from Multiple log sources.
- Expertise in Monitoring/analyzing and managing the real-time events for the Creating rules and Joint rules, verify Rules with events & Fine-tuned the real time rules
- to reduce the false positives.
- Creating Active list, Updating Active List and using rules to populate an Active List.
- Monitor of the multiple network and security devices to ensure appropriate system administrative actions, investigate and report on noted irregularities.
- Monitor dashboards to keep track of security events, health of SIEM devices
- Leverages emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the
- scope of the attack.
- Sending SOC advisories to the clients regarding the current threat and patch on regular basis, Based on Symantec CVSS 2 base vulnerability score.
- Creating Incidents for different severity alerts and following up until the case is closed with proper
- RCA.
- Weekly/Monthly incident analysis report. Analyzing the events and providing solutions for the
- incidents.
- Reporting malware, web application vulnerabilities incidents and maintaining tracker. ✉ Publish weekly reports to applicable teams ✉
- Generate monthly reports on SOC activity.

EDUCATION

Marketing

Vignenan institute of technology and science, HYD

Jun 2013 - May 2015

SKILLS

splunk

SIEM

symantec

email security gateway (proofpoint)

Cisco AMP EDR

Spambox

Firewall

IDS/IPS

WAF

pathfinder ticketing tool

ServiceNow

security operations