Rajesh R

Cyber security Analyst

rajistinnu45@gmail.com

7899168090

Bangalore

EDUCATION

Bachelor of Engineering
SIDDAGANGA INSTITUTE OF TECHNOLOGY
2020 | Tumkur, India

SKILLS

- SIEM- Splunk ES , IBM Qradar
- Ticketing tool-BMC Remedy , Suvidha

Next Gen Soc: UEBA, SOAR

- PIM-Arcos
- EDR-Trend Micro , Sentinel
- Email Gateway-MS 365
- IPS-SNORT
- Firewall-PaloAlto
- DLP-Zscaler
- DAM : IBM Guardium

CERTIFICATES

- IBM QRadar SIEM Practitioner advanced
- ARCON PAM Administrator
- IBM QRadar SIEM Foundation
- Network Security Associate- Fortinet

PROFILE

Computer security professional with 4 years of progressive experience in cybersecurity industry. Demonstrated skill identifying business risks and compliance issues and designing proactive solutions. Background designing and implementing layered network security approaches.

PROFESSIONAL EXPERIENCE

Deloitte Touche Tohmatsu India LLP
Consultant, Risk Advisory
05/2023 – present | Mumbai., India

- Working at India's central bank -RBI
- Working on the triggered offences using the SIEM tool IBM Qradar and ticketing tool Suvidha Portal.
- Daily activities like Reports such as Tripe wire , Inbound traffic , System Health Checklist and Weekly reports.
- Adding the IOC's that are in the form of advisories reported by the multiple threat intel Partners.
- Hand on experience PIM solution i.e. user/ server onboarding/deboarding etc.
- Hand on experience with banking application like Swift , RTGS , ATM Swift for monitoring and reporting.
- Working on alerts generated from various solution like Firewall, WAF , EDR and Other critical solution

Network Intelligence India Pvt Ltd,
Cyber security Analyst
05/2022 – 03/2023 | Mumbai, India

- Good understanding of common network services and protocols
- Good networking knowledge on DHCP, DNS,OSI Model, TCP, UDP, AAA, NAT, PAT, CIA Triad
- Working level knowledge on security solutions like Antivirus, Firewall, IPS, Email Gateway, Proxy,WAF
- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, SLAs, client meetings,report walk through, bridge calls
- Basic knowledge on Cyber kill chain
- Good knowledge on cyber attacks.

NOSTRUM IT SERVICES Pvt Ltd,
Security analyst
12/2020 – 04/2022 | Bangalore, India

- Deep dive analysis of triggered alerts using SIEM tool Splunk by following playbook
- Acknowledging and closing false positives and raising tickets for validated incidents
- Collection of necessary logs that could help in the incident containment and security investigation
- Escalate validated and confirmed incidents
- Creating reports and dashboards in Splunk

LANGUAGES

English

Hindi

Kannada

Telugu

- Analysis of phishing emails reported by internal end users
- Assist IRT team in incident remediation by providing supportive data and recommendations
- Follow-up with incident response team for remediation
- Maintain documentation of the new changes, updates and configuration changes