GAGAN R

Cybersecurity Analyst

CONTACT

+91 8073264322

gaganray1996@gmail.com

Bangalore,India

www.linkedin.com/in/gagan-r

TECHNICAL SKILLS

- IBM-QRADAR
- SplunkEnterprise
- MS OFFICE
- Fresher Service
- Burp Suite Tool
- Malware Analysis
- Phishing Analysis

ACADEMIC HISTORY

- Bachelor of Engineering in Gmit Institute of Technology,Davanagere

CERTIFICATIONS

- Certified Security Analyst Certification From Soc Experts
- Kali Linux Beginner Course From Udemy
- Defronix Certified Junior Security Professional Certificate From Defronix Academy (DCjSP)

PERSONAL PROFILE

Seek Challenging Opportunities where I can fully use my skills for the success of the organization.

EXPERIENCE

- **SECURITY ANALYST TRAINEE**
  Defronix Academy | May 2024-July 2024 | BANGLORE,KARNATAKA

ROLES AND RESPONSIBILITIES

- Monitoring Security For 24/7 , Deep Dive Analysis of Triggered Alerts Using SIEM.
- Acknowledging and Closing False Positive and Raising Tickets for Validate Incidents.
- Investigating Incidents, Remediations, Tracking, Follow-Up For Incidents with Concerned Teams, Stakeholders.
- Acknowledging Closures and Closing Tickets (True Positive or False Positive) as per Client Response.
- Perform Real Time Monitoring, Security Incident Handling, Analysis and Escalations of Security Events From Multiple Log Sources.
- Frequently Checking Log Source Activity and Checking EC and EP Status.
- Maintain Up-to-date Documentation, Trackers, Repositories.
- Participate In Case Review Meetings to Walk Through the Handled Incidents to Peers,SOC Manager and Stakeholders.
- Regularly Monitor Default Domain (Crtical Device Stop Sending Logs) of Respective Clients and Raise a P1 Ticket to Mssp Team Within a SLA and Inform to Stakeholders.
- Investigating Alerts Using Online Threat Intelligence Tools Such as Virus Total and Abuse IPDB.
- Frequently Sharing IOC's and Advisory's to the Client and Maintaining SLA's.
- Monitoring Important Mails and Reverting Mulitple Clients According to there Requirements.
- Responsible For Prepare Daily, Weekly and Monthly Reports.
  Drafting Shift Handover to Next Shift Person

SUMMARY

- Good Understanding of Common Network Services and Protocols.
- Good Knowledge in Security Concepts Like CIA Triad, AAA, Multi-Factor Authentication, VPN, Defense In Depth, Zeroday Malware, Hashing and Encryption.
- Working Process of Servers , DHCP, DNS, Domain-Controller, Active Directory, Web-Server, TI, WAF, Web-Gateway Etc..
- Proper Awareness of Cyber Attacks : Various Types of Malware Attacks,Network Based Attacks, Credential Based Attacks.
- Good Understanding of Various Soc Process: Monitoring Incidents, Escalations, Playbooks, Incident Documentation.
- Cyber-Kill Chain and Mitre Attack, Incident Response Life Cycle.
- Good Understanding About Event ID's. Basic Knowledge on Security Solutions like Firewall, Antivirus, IPS , Email- Gateway, Proxy Server,Web Gateway.
- Good Exposure on Basic Kali Linux Command Line.