# MANOJ KUMAR

## SOC Analyst

✉ marimganti.manoj470@gmail.com ☎ 6301747967

## PROFILE

Overall 3+ years Experienced IT industry, Cybersecurity Analyst with the focus on detection and response. Security monitoring and threat analysis. Possess proven technical background and information security experience combined with hands-on experience doing root cause analysis and post incident reviews. I have a passion and dedication for smart information security.

## ROLES AND RESPONSIBILITIES

- Incident Response, Intrusion Analysis and Network Security Monitoring.
- Experienced Information Systems Security professional dedicated to providing high quality services and positive results.
- Possess strong understanding of Security Operations and Incident Response process and practices.
- Have in-depth knowledge and understanding of the threat landscape and emerging security threats. Proven ability to leverage technology to achieve organizational objectives.
- Innovative problem solver whose areas of expertise include Security Event Monitoring, Log Analysis, Incident Management, Security Threat Analysis to protect computer systems.
- Hands on experience in SIEM Platform (Splunk, IBM Q-Radar, Azure Sentinel)
- Fine tuning the Use case based on the false positive detection.
- Endpoint Security: Trend Micro office scan - Administration and troubleshooting Nessus (VA) performing the scan activities.
- Carrying out log monitoring and incident analysis for various devices such as Firewalls, IDS, IPS, database, web servers and so forth.
- Knowledge of typical security devices such as firewalls, intrusion detection systems, Av and End point security.
- Monitoring 24x7 for Security Alerts and targeted phishing sites by using SIEM tools with help of technologies such as Abused IP DB, MX Tool kit and etc...
- Mostly worked on broken authentication, Sensitive data exposure, broken access control, Using components with known vulnerabilities, Insufficient logging and monitoring.
- Creation of reports and dashboards and rules.
- Maintain the Document the application support strategy.

**Tools:**

- **SIEM**: QRadar, Sentinal , Splunk
- **IDS & IPS**: Paloalto, Tipping Point
- **EDR**: Crowdstrike & Microsoft Defender
- **Threat Intelligence**: ThreatConnect
- **VM Tools**: Qualys
- **Firewall**: Paloalto and Checkpoint
- **SOAR**: Paloalto Xsoar
- **Malware Analysis**: Sandboxies
- **Threat Hunting Tools** : Crowdstrike

## EDUCATION

- Completed Bachelor of Technology (BTech) from JNTUK in 2020 with a 69% score

## PROFESSIONAL EXPERIENCE

**Security Analyst**
**Tata Consultancy Services(TCS)**

- Experience with SIEM (Security Information and Event Management) tools like monitoring real-time events using IBM QRadar, Sentinel.
- Preparing daily, weekly and monthly reports as per client requirements.
- Investigating and creating a case for the security threats and forwarding it to the Onsite SOC team for further investigation and action.
- Experience in performing log analysis and analyzing on crucial alerts an immediate basis through SIEM.
- Good understanding of security solutions like Anti-virus, DLP, Proxy, and Firewall filtering/monitoring, IPS, Email Security, EPO, WAF, etc.,
- Handling and analyzing suspicious executions through EDR Crowd strike.
- Monitor alerts generated in the security analytics solution including intrusion detection/prevention systems, firewalls, routers, switches, servers, databases, applications, and other devices.
- Working on SIEM tools providing operational support for preventing Cyber Attacks.
- Identifying potential information security incidents like security attacks and anomalous activities.
- Validate and confirm potential security incidents through a detailed investigation of logs.
- Create incidents for all alerts/findings and regular updates on overall analysis as per the defined SLAs.
- Hands-on experience in Threat Investigation analysis Security Monitoring and Operation.
- Having knowledge of vulnerability management.
- Exposure to Ticketing tools like Service Now.

## DECLARATION

I hereby declare that the information furnished above is true to the best of my knowledge.

Signature
Manoj Kumar