# RUPOJI RAO

## Cyber Security Analyst

+91 97018 14605

rupoji75@gmail.com

https://www.linkedin.com/in/rupoji-rao-a26225268/

---

## PROFILE

I have overall 4 Years of experience as a SOC Analyst and good experience in security operations including Incident management, Endpoint security and logs analysis through SIEM. Experience on working in 24x7 operations of SOC team, offering log monitoring, and security information management.

---

## WORK EXPERIENCE

### HCL technologies - Bangalore

**JAN 2023 - TILL DATE**

**INFORMATION SECURITY ANALYST**

**ROLES & RESPONSIBILITIES:**

- Working in Information Security on security operations, incident management, intrusion detection, and security event analysis using SIEM tool like IBM Q-Radar, ArcSight &
- Sentinel. Working in Offshore SOC team. Monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Proactively work with vendors on P1 issues and finding the Root cause also excel in taking Remediation's in the client Environment.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks.
- Co-ordinate extensively with networking teams to maintain and establish communication to Remote HP Arcsight Collectors/Processors.
- Demonstrated experience in Blacklisting the required countries and IOC in the firewalls, Email Security, EDR, etc.,
- Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
- Determine the scope of security incident and its potential impact to Client network recommend steps to handle the security incident with all information and supporting evidence of security events.

  Mostly worked on Broken authentication, Sensitive data exposure, Broken access control, XSS, Using components with known vulnerabilities, Insufficient logging and monitoring.

- Creation of reports and dashboards and rules and Maintain document the application support strategy.
- Take immediate remediation on the Bad Threat Intel IOC's includes IP'S, URLs, etc.,
- Utilized and managed SentinelOne and Falcon CrowdStrike for endpoint detection andresponse (EDR).
- Monitored firewalls, including Palo Alto and Zscaler, to protect network perimeters.
- Managed email security solutions like Proofpoint and O365 to prevent phishing and malware attacks. Deployed TrendMicro and McAfee antivirus solutions to ensure endpoint protection.
- Utilized Proofpoint and O365 as email gateways to filter and analyze incoming emails. Used ticketing tools such as ServiceNow and Jira to track and manage security incidents.
- Monitored additional security tools like IDS, IPS, DLP, and Cisco Umbrella.
- Conducted phishing and email analysis using Proofpoint and O365 to identify and mitigate threats.
- Ensured endpoint protection through Microsoft Defender for Endpoint.
- Maintaining relationships with external intelligence communities, ensuring the organization stays informed on the latest threat trends and IOCs.

**Centific Tech - Hyderabad** **NOV 2021 - DEC 2022**
**SECURITY ANALYST**

**ROLES & RESPONSIBILITIES:**

- Monitored and analyzed cybersecurity events using Splunk and QRadar SIEM tools.
- Examined logs, events, and alerts from multiple platforms for anomalous activity to monitor internal and external threats.
- Developed and executed SOC (Security Operations Center) procedures and standard operating procedures.
- Triaged security events and incidents, detected anomalies, and directed remediation actions.
- Collected evidence of security incidents and other error conditions that could breach security or degrade system/data integrity and confidentiality.
- Integrated and collaborated threat information to enhance incident detection capabilities.
- Generated reports from security solutions and prepared them for management or leadership review.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP etc.
- Escalating the security incidents based on the client & SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.
- Good understanding of security solutions like Firewalls, DLP, Anti-virus, IPS, Email Security etc.

## EDUCATION

**Aacharya Nagarjuna University - 2017**
Bachelor's of Technology
Computer Science and Engineering

## CERTIFICATIONS

- Pursuing CEH

## SKILLS

- **SIEM**: IBM QRadar, Splunk -
- **EDR**: SentinelOne, Falcon CrowdStrike
- **Firewalls**: Palo Alto, Zscaler
- **Email Security**: Proofpoint, O365
- **Anti-Virus**: TrendMicro, McAfee
- **Email Gateway**: Proofpoint, O365
- **Ticketing Tools**: ServiceNow, Jira
- **Other Security Tools**: IDS, IPS, DLP, Cisco Umbrella
- **Phishing & Email Analysis**: Proofpoint, O365
- **Endpoint Protection**: Microsoft Defender for Endpoint

## DECLARATION

I hereby declare that the information provided in this resume is true and accurate to the best of my knowledge and belief.

**RUPOJI**