# R Mohamed Junaid

Chennai, Tamil Nadu • +91-8056160184 • Mohamedjunaid1234@gmail.com • linkedin.com/in/mj-07

**Information Security Engineer**

A skilled Senior Security Operations professional with over 7 years of experience leading SOC operations, incident response, and security engineering. Currently building an internal SOC from the ground up, transitioning from an MSSP, covering over 15,500 endpoints, 70+ AWS accounts, 10+ Azure Subscriptions, with extended visibility into Azure and GCP. Skilled in RCA, SIEM tuning, security tooling, and real-time threat detection. Known for setting up strong security processes, training teams, and supporting audits and compliance. A hands-on problem solver who drives improvements through collaboration, documentation, and sound decision-making.

## WORK EXPERIENCE

**NextGen Healthcare India** **11/2024 - Present**

**Senior Information Security Engineer** • **Full-time** **India**

- **Set up an internal Security Operations Center (SOC)**, orchestrating the transition from MSSP and providing internal **monitoring, threat detection, and incident response** for more than **2,500 endpoints** and **70+ AWS accounts**, along with increasing visibility into **Azure** and **GCP workloads**.
- **Set the foundation for SOC processes and documentation** to facilitate future growth through core **workflows**, **incident management**, **escalation processes**, **SOPs**, **playbooks**, and **knowledge bases**.
- **Provided L2/L3 incident resolution** via triaging alerts (e.g., threats), performing forensics, and doing **root cause analysis (RCA)** to comprehend and solve problems with lasting solutions.
- Identified by management for **finding root causes**, transforming investigations into **strategic lessons**, and creating **RCA reports** that enhanced detection and avoided incidents.
- **Managed the SOC mailbox**, responding promptly and in a timely fashion to **security issues** and **phishing complaints**. Assisted in rolling out **24x7 emergency paging** for high-priority incidents.
- Functioned as **Incident Commander** for high-impact **security incidents**—managed teams, timelines, and communications to stakeholders, ensuring timely resolution and documentation for review.
- Signed off and approved **EDR tool implementations** or policy changes for compliance with internal security policies before deployment at an enterprise level, including environments hosted on **Azure** and **GCP**.
- Enabled **security tool evaluation and procurements** through **POCs**, operational testing, and suitability assessments, providing **comparative reports** to support leadership decisions.
- Led an **industry-leading ZTNA deployment**, moving access control from traditional VPNs to **context-aware policy control**, enhancing security and user experience across **hybrid cloud** environments.
- Guided **SIEM tuning** and **use case development**, defined detection rules, reduced noise, and synchronized with internal **threat models** and **threat intelligence feeds** (including **Azure Sentinel** and GCP-native logs).
- **Hired and trained over 12 analysts and service desk members**, improving organizational response by guiding them through real incidents and **compliance awareness**.
- Partnered with **Product Security**, **GRC**, and **IT/DevOps** to assist in **audits**, **threat modeling**, **vulnerability scanning**, and **compliance reporting**, promoting a **security-aware culture**.
- Enabled **SOC2**, **HIPAA**, and **customer audits** by developing documentation, logs, and **RCA reports**, and maintaining **audit readiness** and **risk mitigation**.
- Facilitated **tabletop exercises and simulations** to train the organization against threats such as **phishing**, **credential compromise**, **ransomware**, and **insider threats**.
- Developed **concise, actionable incident and vulnerability reports** to management, highlighting **technical issues** in **business-oriented risk narratives**.

**Cisco Systems Inc.** **01/2022 - 11/2024**
**Information Security Engineer** **Bangalore**

- To forestall and **mitigate security incidents**, an extensive **threat analysis was performed and threat intelligence strategies were utilized** into practice using a variety of log sources like EDR, Firewalls, NIDS, HIDS, Sys Logs etc. With employing various standards and frameworks in **Cryptography, Incident Response, and regulatory compliance.**
- Management of **AWS, Azure, and GCP cloud security**, deploying and debugging SOC tools to maintain oversight over and safeguard cloud resources.
- **Developed high-impact security use cases** and crafted detailed playbooks, significantly **bolstering incident detection and response capabilities.** Improved the efficiency of incident resolution by overseeing the **development and upkeep of Security Operations Center (SOC) Runbooks, incident response documentation, and related standard operating procedures (SOPs).**
- Worked on permissions, access levels, and configuration-related aspects of **Container Kubernetes security** (AKS,EKS). It generated a couple of playbooks for monitoring K8 notifications from Defender, Guardduty, and other sources.
- Organized and led 24/7 security monitoring in SOC environments using **Splunk and Microsoft Defender for Cloud**, including incident escalation, analysis, developing Dashboards if needed and troubleshooting.
- In an effort to improve incident detection rates for pertinent Use cases, I **Developed Splunk queries for effective threat detection and log analysis**. I also constructed dashboards for targeted monitoring. **Worked similarly in KQL and Sumologic configurations**
- **Established ownership in vulnerability managemen**t, took charge of their identification, and liaised with relevant parties until the **remedy started in effect and resources were dealt with**. Oversaw the organization's risk management and Linux typical vulnerabilities and exposures (CVE) program, including **identifying and assisting stakeholders and application/Infra owners in managing risks and resolving vulnerabilities.**
- Assisted in the **automation of incident response** investigation steps using **Python scripting** for better analysis.
- **Assisted with and participated in tabletop exercises to refresh the team's process and technical skills,** primarily in the areas of **incident response, threat intelligence, and forensics (where necessary).**

**Aspect Technology** **09/2019 - 01/2022**
**SSOC Sysadmin - Analyst** **Bangalore**

- Monitoring Logs and Triggered alerts 24/7 with proper escalation of non-complaint and anomalies.
- Raising ticket for Valid incidents, Real-time investigation and Analysis of alerts in the SSOC from multiple sources and sensors.
- Serve as Watchdog to **identify, protect, detect, respond and recover IT infra and assets.**
- Expedite in acting for **Incident response of Malware alerts and incidents**, by investigating and alerting as per the regular Runbooks and reference documents.
- Administer and maintain end user accounts, VPN access, permissions and access rights for MFA and Access regulations.
- Conduct trainings and guiding employees, colleagues on compliance and policy.
- Scheduling **Vulnerability scans and conducting PCI Audits per quarter.**
- **Participate in patching/upgrading** and administer requirements with various tools and Infrastructure facilities.
- Process and study logs if needed from **Linux, Windows servers, VMware virtual machines,** and logs from AWS CloudTrail.
- Monitor, protect Cloud and On-premises system in local data centers.

**Amazon** **10/2017 - 11/2018**
**Associate (Alexa Security, ML)** **Chennai**

- **Monitor transcriptions, annotation data flow and hunt anomalies.**
- Ensuring that advanced methods are employed in working with the built of the IoT device.

- Comparing with competitors' devices and upfront erection of security qualities for outstanding performance.
- Profanity filtering and checking certs for logged-in instances.
- Conducting compliance training on how to implement and regulate IoT usage for better and safer daily usage.
- Mostly **monitoring and escalating DDoS alerts and other bad actor works with help of AWS integrated dashboard**.

## EDUCATION

**Master's degree in Business Administration in Process Control and Professional Ethics**
Annamalai University — Chennai

**Bachelor of Engineering in Electronics and Communication Engineering**
Anna University — Chennai

## CERTIFICATIONS

**RHSCA and RHCE**
RedHat Linux

**CCNA**
Cisco

**Splunk Fundamentals**
Splunk

**Cisco Cybersecurity Fundamentals**
Cisco

**Network Security Engineer**
Fortinet

**Cloud Security Specialty**
Cisco

**Trained in Security+**
CompTIA

**Trained in SAA C02**
AWS

**Trained in AWS Security Speciality SCS-C02**
AWS

## SKILLS

**ZTNA:** Zscaler

**SIEM:** Splunk, Next-Gen SIEM Crowstrike, Sentinel

**Cloud Security:** AWS, Azure, GCP, Kubernetes

**EDR/XDR:** Crowdstrike, Cisco Secure Endpoint, Microsoft Defender, McAfee Endpoint Security

**CSPM:** CSP: Wiz.io, Crowdstrike

**Data Serialization and Scripting:** Python, YAML, JSON

**Framework and knowledge bases:** Framework: NIST Incident Response, Cyber Kill Chain methodology, Cryptography and MITRE ATT&CK Tactics