

- +91 7010455613
- chockoct20@gmail.com
- Hyderabad, 500032

CHOCKALIINGAM SUBRAMANAIM

Sr. Analyst

Objective

Skilled and dedicated Security Analyst with more than 3 years of experience in cybersecurity field, seeking to leverage extensive expertise in threat detection, incident response, and security management to strengthen the information security posture of a forward-thinking organization. Adept in using industry leading SIEM and EDR tools. Committed to continuous learning and contributing to a robust security framework that supports the organizational needs, goals and compliance requirements.

Education

- Bachelor of Technology** (2017-2021) from SASTRA Deemed University, Thanjavur, Tamil Nadu. - GPA: 7.3
- Senior Secondary - CBSE Board** (2015-2017) from Royal International school, Namakkal, Tamil Nadu. Percentage: 93

Soft Skills

- Analytical thinker
- Communicator
- Collaborator
- Problem solver
- Time Management
- Team-oriented

Profile Summary

- Certified Senior SOC Analyst with three years of cybersecurity experience, specializing in the development and optimization of SIEM use cases.
- Expertise in leading tools including Azure Sentinel, ArcSight, Qradar, CrowdStrike, and SentinelOne for effective monitoring and incident response.
- Worked on creation and optimization of use cases and reports customized to client needs.
- Proficient in incident reporting and collaborating with stakeholders for incident resolution using ticketing tools such as servicenow.
- Demonstrated leadership in managing customer relationships and committed to enhancing organizational security posture while advancing professional capabilities in threat detection and response.

Certifications

- Microsoft Certified: Security Operations Analyst Associate (SC-200)
- CompTIA Security Plus SY0-701, <http://verify.CompTIA.org> - MN84BMC55EB4QC3G
- SC-900 - Microsoft Certified: Security, Compliance, and Identity Fundamentals
- AZ-900 - Microsoft Certified: Azure Fundamentals
- Google Cloud Profile: https://partner.cloudskillsboost.google/public_profiles/cd3102f0-3690-4d2e-ada1-e8b5d5c0964c

Core competencies & Tools

- Azure Sentinel
- ArcSight
- Qradar
- CrowdStrike
- SentinelOne
- ServiceNow
- SIEM & SOAR
- EDR & XDR
- Incident Response
- Use case creation and fine-tuning
- Vulnerability Assessment

Awards and Achievements

- Received CRS high flyer and Team contributor awards within Wipro.
- Managed multiple key roles simultaneously during interim SOC Establishment.
- Received appreciation from customers for ensuring Quality of service and Reliability.
- Received multiple monetary rewards for completing multiple courses and certifications in a short time.

Organizational Projects

- Security Monitoring - Shared Platform (7 clients)
 - Used ArcSight for security monitoring and ServiceNow for incident reporting and management. Monitored client environments for suspicious network and audit related activities.
- GSOC - Dedicated client (Telecom)
 - Worked on numerous OPCOs spread across multiple countries.
 - Used Azure Sentinel, ArcSight SIEM & SOAR for security monitoring and worked on tools such as Crowd strike, Sentinel One and Microsoft Defender XDR.

Work Experience

Wipro Technologies: July 2021- Present

- **Senior Analyst: April 2024 - Present**

- Working as a senior analyst for a dedicated customer. Providing Security monitoring and reporting services along with Threat hunting and Vulnerability reporting.
- Key Responsibilities:
 - Overseeing L1 analysts and investigating incidents escalated by them.
 - Working on alerts from MDCA, MDI, MDE through Defender XDR and ArcSight SIEM.
 - Providing custom in-house threat intel and vulnerability reporting.
 - Preparing Daily health check reports, Weekly incident report and Monthly SOC efficiency report.
 - Reporting high priority incidents and coordinating with stakeholders for incident response and preparing RCA (Root cause analysis) reports.
 - Creating custom use cases and dashboards along with SOPs as per customer requirements
 - Fine Tuning use cases to reduce false positive count and whitelist benign positive alerts.
 - Incident follow-up and management along with mapping to MITRE TTPs.
 - Creating APT rules covering all TTPs used by threat actors.
 - Creating rules for suspicious activity monitoring: Linux, Windows, Firewalls, WAF, Proxy and VPN.
 - Adept in filters, query and report configuration.
 - Preparing Root cause Analysis, Governance and SOC efficiency reports and presenting reports in periodic calls and ensuring customer satisfaction.

- **Analyst: July 2021 - March 2024**

- Worked as an L1 analyst in shared SIEM platform for 7 customers, monitoring and reporting security incidents through ServiceNow ticketing tool. Assumed the role of incident manager by assigning and taking follow ups on incidents. Prepared and presented monthly SOC reports to customers.
- Key Responsibilities:
 - Monitoring for suspicious activities in client environment.
 - Raising incidents based on log analysis and OSINT for threat Intel
 - Weekly report generation for audit activities.