

CHAITANYA INGALE

SOC ANALYST

CONTACT

+91-9370702635

chaitanyaingale28@gmail.com

pune

EDUCATION

2020 - 2023

SAVITRIBAI PHULE PUNE
UNIVERSITY

Bachelors of Engineering

SKILLS

- SIEM – Splunk/ Microsoft Sentinel
- EDR - CrowdStrike
- Firewall - Palo Alto
- Email Gateway- Proofpoint
- Web Proxy - Zscaler
- Web Application Firewall - Imperva
- Anti-Malware - McAfee
- IDS/IPS – McAfee

CERTIFICATIONS

- Incident Response Lifecycle
- Executive Vulnerability Management

PROFILE SUMMARY

I have 2.5 years of experience as a SOC Analyst, specializing in monitoring and responding to security incidents. I am skilled in using tools like SIEM, IDS/IPS, Firewalls, AV/EDR, and Email Gateways to detect and address cyber threats. I have experience investigating security issues, improving security measures, and working with teams to strengthen defenses. I stay up-to-date with the latest security trends and am eager to apply my skills in a new cybersecurity role.

WORK EXPERIENCE

AARNA Technologies Pvt. Ltd.

JAN 2023 - MAR 2025

| SOC Analyst

- Conduct proactive monitoring and efficient triage of security events.
- Monitored and identified critical web applications requiring enhanced protection through continuous security event analysis.
- Monitor diverse security events and logs (Proxy, IPS/IDS, Firewall, Email, AV, EDR, and WAF).
- Look into suspicious emails, classify them, and give recommendations to users.
- Investigates malware infections, ransomware attacks, phishing attempts, and advanced persistent threats (APTs).
- Update incident response plans to stay prepared for security events.
- Investigated and responded to historical and potential threats targeting web applications, including OWASP Top 10 vulnerabilities

AlifCloud IT Consulting Pvt. Ltd.

APR 2025 - PRESENT

| SOC Analyst

- Conducted 24/7 monitoring of security events and alerts in Microsoft Sentinel, ensuring timely detection and acknowledgment of potential threats.
- Monitored security alerts and incidents in Microsoft Sentinel and responded to threats in real-time.
- Performed initial investigation of alerts using KQL queries, user activity logs, and correlated data across integrated sources like Azure AD, Office 365, Defender for Endpoint, and firewalls.
- Maintained updated knowledge of MITRE ATT&CK framework mappings in Sentinel alerts to understand attacker TTPs.