



# KAJAL PATIL

## SOC ANALYST

 TCS-Mumbai

 +91 7821021817

 kajaltpatil2001@gmail.com

 [HTTPS://WWW.LINKEDIN.COM/IN/KAJAL-PATIL1063B833A/](https://www.linkedin.com/in/kajal-patil1063b833a/)

---

### **PROFILE:**

Result-oriented professional with experience in Information technology and proven knowledge of Information security. Aiming to leverage my skills to successfully fill the Security Analyst role at your company.

### **PROFESSIONAL SUMMARY:**

- A skilled professional with 2.9 years of experience in IT Security Operations Center.
- Experience of (24x7) working in SOC team, offering log monitoring, detecting and preventing the Intrusion attempts.
- Experience on SIEM (Security Information and Event Management) tools like Splunk and Qradar.
- Hands on experience with tools and process used in security solutions like Endpoint Security, Incident response, Security monitoring and Operations etc.
- Experience on performing Log analysis, Malware Analysis, Phishing mail analysis, Incident Response and analysing the crucial alerts at immediate basis.
- Preparing daily, weekly and monthly report as per client requirement.

### **TECHNICAL SKILLS:**

- SOC SIEM (Splunk, Qradar)
- Ticketing tools (service now)
- Malware analysis monitoring and reporting
- EDR (Crowdstrike and Microsoft Defender)
- Phishing email analysis (Microsoft Defender)
- Log and threat analysis

### **WORK EXPERIENCE:**

**[TCS SOC ANALYST] JULY 2022 TO PRESENT**

#### **SOC Analyst**

- **Incident Monitoring and Response:**

Monitoring security events and alerts generated by security tools (SIEM, IDS/IPS, etc.). Analyzing and prioritizing security incidents based on severity and potential impact. Responding to and investigating security incidents, including potential breaches, malware, and suspicious activities. Escalating complex incidents to higher-level SOC analysts or teams as necessary .

- **Threat Detection and Analysis:**

Conducting initial analysis of security alerts and events to determine their relevance and potential threat. Utilizing threat intelligence and security tools to identify indicators of compromise (IoCs) and vulnerabilities. Performing root cause analysis on security incidents and identifying patterns or trends.

- **Log and Data Analysis:**

Reviewing and analyzing logs from various sources, including firewalls, servers, and network devices. Correlating logs and data to detect unusual patterns or activities. Maintaining and updating security monitoring systems and tools as required.

- **Documentation and Reporting:**

Documenting incident details, including steps taken and resolutions in ticketing systems. Preparing and presenting incident reports and summaries to management and relevant stakeholders. Updating and maintaining SOC documentation, including runbooks and standard operating procedures (SOPs).

- **Collaboration and Communication:**

Collaborating with other IT and security teams to enhance the overall security posture. Communicating effectively with internal teams and external partners regarding security issues and incidents. Participating in regular SOC meetings and providing input on improving incident response processes.

- **Continuous Improvement:**

Staying up to date with the latest security trends, threats, and technologies. Participating in ongoing training and certification programs to enhance skills and knowledge. Contributing to the development and refinement of security policies and procedures.

## **EDUCATIONAL QUALIFICATION:**

**BACHELOR OF SCIENCE**

SHIVAJI UNIVERSITY KOLHAPUR

Dr.Ghali collage, Gadhinglaj

2022

## **DECLARATION:**

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear that responsibility for the correctness of above-mentioned particulars.