

CHURCHIL THARMARAJ

SOC ANALYST

Chennai, Tamil Nadu | +91 95975 82220 | churchiltharmaraj@gmail.com

SECURITY OPERATIONS / INCIDENT RESPONSE

PROFILE

Detail-oriented SOC analyst with experience in security operations, alert triage, incident investigation, endpoint protection and clear operational reporting. Comfortable working across SIEM, SOAR, EDR/XDR and service-management platforms.

SECURITY TOOLKIT

SOAR: Cortex XSOAR

SIEM & investigation: Microsoft Sentinel, Elastic

Endpoint / XDR: Microsoft Defender, Cortex XDR, Tanium, CrowdStrike

Cloud & network: Netskope, Cisco Umbrella

Email security: PhishER, Check Point Harmony

Threat monitoring: Darktrace

ITSM & collaboration: ServiceNow, Jira

EDUCATION

Madras Christian College
Bachelor of Computer Applications
2019-2022 | GPA: 78.8/100

STRENGTHS

Analytical thinking | Incident documentation | Cross-team communication | Resilience under pressure | Continuous learning

LANGUAGES

Tamil | English

PROFESSIONAL EXPERIENCE

TCS | SOC Analyst

June 2026-Present

Current security operations role using a broad stack across orchestration, detection, endpoint security and service workflows.

- **Orchestration:** Cortex XSOAR
- **Detection & search:** Microsoft Sentinel, Elastic
- **Endpoint & response:** Microsoft Defender, Cortex XDR, Tanium
- **Security & service workflows:** Netskope, ServiceNow ITSM, Jira

Deloitte | Analyst, Security Operations

February 2023-May 2026

- Monitored and investigated security events using Microsoft Sentinel to support timely detection and response.
- Used CrowdStrike and Microsoft Defender in endpoint protection and threat investigation workflows.
- Worked with Cisco Umbrella, PhishER and Check Point Harmony across network and email security.
- Supported alert tuning by reviewing event patterns and improving alert relevance.
- Prepared daily, weekly and monthly incident and threat-trend reports for operational visibility.
- Collaborated across Critical Operations Posts in a 24/7 rotational environment.

WORKING APPROACH

Evidence-led investigation, clear handovers, careful documentation and calm prioritization help turn alerts into actionable next steps.