Sai Prashanth Pulisetti

SOC Manager · Detection Engineer · Purple Teamer

Hyderabad, India | prashanth.inbox@tuta.com | prashanth.blog | linkedin.com/in/0xPrashanthSec | github.com/0xPrashanthSec

SUMMARY

Security operations leader with 7.5+ years in Security Operations Centers, managing the SOC since March 2026. Builds detection engineering programs grounded in adversary emulation: rules are written from real malware and threat-actor TTPs, validated with Atomic Red Team and CALDERA, and mapped to MITRE ATT&CK. Holds CRTE, CRTO and CRTP, with recognition from Oracle and NCIIPC for responsible disclosure.

EXPERIENCE

SOC Manager Mar 2026 – Present

Eze Castle Integration

- Manage the Security Operations Center: analysts, shift operations, escalation process and the detection program.
- Set detection engineering strategy and priorities across a multi-tenant Elastic SIEM environment.
- Designed a structured onboarding and training plan for new L1 SOC analysts.

SOC Team Lead 2025 – Feb 2026

Eze Castle Integration

- Led the SOC team through P1/P2 incident response and escalations.
- Mentored analysts and reviewed investigation quality across shifts.

SOC Specialist 2022 – 2025

Eze Castle Integration

- Authored 300+ custom Elastic detection rules from malware analysis and threat-actor TTP research, mapped to MITRE ATT&CK.
- Validated detections through adversary emulation with Atomic Red Team and CALDERA, tuning to cut false positives.
- Built IOC Hunter, an extraction pipeline that turns threat-intel reporting into Elastic hunting queries.
- Top Performer of the Year, 2022 and 2023.

SOC Engineer 2021 – 2022

Eze Castle Integration

- Threat hunting, malware analysis and detection tuning to improve signal-to-noise across EDR, SIEM, email and cloud telemetry.

SOC Analyst Jul 2019 – 2021

Eze Castle Integration

- Alert triage and investigation across SIEM, EDR and email security platforms.

SKILLS

Leadership: SOC management, shift operations, analyst training, detection program strategy

Detection: Sigma, KQL, EQL, ES|QL, YARA, SPL; MITRE ATT&CK mapping

SIEM: Elastic (ELK), Microsoft Sentinel, Splunk

EDR/XDR: CrowdStrike Falcon, SentinelOne, Microsoft Defender, CB Defense

Purple team: Atomic Red Team, CALDERA, Cobalt Strike, Active Directory attacks

Cloud & email: Microsoft 365, Entra ID, Defender for Office 365, Proofpoint, Mimecast

CERTIFICATIONS & EDUCATION

CRTE (Certified Red Team Expert) · CRTO (Certified Red Team Operator) · CRTP (Certified Red Team Professional) · CHFI (Computer Hacking Forensic Investigator) · eJPT · Elastic Security Fundamentals

M.Sc. Cyber Security, IIITMK, Kerala

RECOGNITION & OPEN SOURCE

- Oracle Hall of Fame: critical vulnerability disclosure.
- NCIIPC, Government of India: 15 acknowledged responsible disclosures.
- Bug bounty recognition from Dell, Trip Advisor and Cybrary.
- Open-source tool: IOC Hunter, turning threat-intel blogs into Elastic SIEM hunting queries.
- Contributor to Elastic's open-source detection-rules repository.