SATYA NALLAM

HYDERABAD • +91 9581821622 • nallamsatyasai@gmail.com • linkedin.com/in/satya-nallam • github.com/Satya-Nallam

Security Engineer | DevSecOps Engineer

Security engineer with 6.5+ years of professional experience across security operations and DevSecOps. Currently the DevSecOps owner at a managed security services provider, where I secure GitLab CI/CD pipelines, run vulnerability management across the organization, and drive SOC 2 and ISO 27001 compliance work. Before this, I worked in 24x7 SOC operations across Microsoft Sentinel, Google SecOps, Splunk, CrowdStrike and SentinelOne. I build security into engineering pipelines instead of adding it at the end.

SKILLS

SIEM, SOC & Detection Engineering

- SIEM
- SOC Monitoring
- Incident Response
- Logging & Monitoring
- Microsoft Sentinel
- Google SecOps
- Splunk
- M365 Defender
- KQL
- Detection Engineering
- MITRE ATT&CK

DevSecOps & CI/CD Security

- DevSecOps
- GitLab CI/CD
- CI/CD Security
- SAST
- SCA
- Secret Scanning
- Dependency Scanning
- Container Security
- ArgoCD
- GitOps
- Kubernetes

Cloud, Infrastructure & Endpoint Security

- Cloud Security
- Azure Security
- Google Cloud Security
- IAM
- Infrastructure Security
- System Hardening
- Zscaler
- Endpoint Security
- EDR/XDR
- CrowdStrike
- SentinelOne

Vulnerability, Compliance & Automation

- Vulnerability Management
- Compliance Remediation
- Data Protection
- Risk Assessment
- Security Documentation
- SOC 2
- ISO 27001
- Security Runbooks
- Python
- Bash
- Security Automation

WORK EXPERIENCE

Human Managed **04/2025 - Present**
CyberOps Analyst | DevSecOps Engineer **Chennai(Remote)**

- Own DevSecOps for the organization following a senior engineer's exit - GitLab CI/CD pipelines, ArgoCD GitOps deployments, container registries and pipeline security scanning across 8+ product repositories.
- Run GitLab security scanning (SAST, secret detection, dependency/SCA and container scanning); triaged a backlog of ~1,870 findings, cleared every critical SLA breach, and built an SLA-tracked vulnerability management process using the GitLab API with Slack escalation to remediation owners.
- Administer GitLab security controls: access reviews and offboarding, group and project permissions, CODEOWNERS, protected branches, MR approval rules and CI token rotation.
- Operate ArgoCD GitOps workflows for Kubernetes CD deployments; managed Harbor container registry including supply-chain risk reviews and image scanning.
- Drive security compliance remediation in Vanta across SOC 2, ISO 27001 and ISO 42001 -closing control gaps in access management, change control and monitoring evidence.
- Conduct vulnerability assessments and CVE triage across client environments, prioritizing critical findings using CVSS scoring and CISA KEV cross-reference.
- Deploy and manage EDR (CrowdStrike, SentinelOne) and zero-trust access (Zscaler) across endpoints; enforced device compliance and disk encryption policies.
- Analyze 100+ daily security alerts across Microsoft Sentinel, Google SecOps, Splunk, CrowdStrike, SentinelOne and Trellix for multiple customer environments; run end-to-end triage, containment and remediation for high-severity incidents.
- Develop and tune SIEM detection rules mapped to MITRE ATT&CK, reducing false positives by 35%; built AI-assisted triage artifacts that cut investigation time by 40% and MTTD by 45%.
- Automate incident response and customer reporting workflows using Python and platform APIs, cutting manual effort by 60% and report turnaround from hours to minutes.
- Author 10+ incident response runbooks, threat intelligence reports, and vendor risk assessments for enterprise clients.

Tata Consultancy Services **03/2022 - 03/2025**
SOC Analyst **Hyderabad**

- Monitored 500K+ daily security events using Microsoft Sentinel, M365 Defender, SentinelOne, and SIEM platforms for real-time threat detection.
- Investigated and resolved 150+ security incidents, including malware infections, credential compromise, unauthorized access attempts, and data breach investigations.
- Enhanced detection efficiency by 25% through KQL query development, threat intelligence analysis, and CVE triage.
- Reduced false positives by 30% through alert correlation, tuning, and behavioral analysis.
- Mentored 4 junior SOC analysts on incident response processes, investigation techniques, and threat intelligence methodologies.

Grama Ward Sachivalayam **11/2019 - 02/2022**
Panchayat Secretary Grade VI – Digital Assistant **Kothapeta**

- Managed digital governance platforms and maintained confidential records for 3,000+ citizens, implementing foundational cybersecurity controls to protect sensitive government data.

PROJECTS

AI-Assisted CI/CD Security Scanning Pipeline - GitLab CI, Semgrep (SAST)

- Built an automated security scanning pipeline in GitLab CI using Semgrep (SAST) with AI-assisted triage of findings
- Embedded security guardrails into the development workflow - scans run on every merge request, with AI-generated remediation guidance for developers

AI SOC Analyst Agent - Azure AI Foundry

- Designed and deployed an AI SOC analyst agent on Azure AI Foundry to assist with alert triage and investigation workflows
- Automated enrichment and first-pass analysis of security alerts, accelerating investigations and standardizing triage quality
- Documented the build and delivered a knowledge-sharing workshop to the security team

CERTIFICATIONS

Microsoft Certified: Security Operations Analyst Associate 09/2025 - 09/2026
Microsoft

Google Cloud Certified Professional Security Operations Engineer 10/2025 - 10/2027
Google

Certified Cybersecurity Educator Professional (CCEP) 11/2025 - 08/2026
RED TEAM LEADERS

Proofpoint Certified AI Email Security Specialist 09/2025 - 09/2027
Proofpoint

EDUCATION

B.Tech – Electrical & Electronics Engineering
Aditya University - JNTUK Surampalem • 06/2016 - 05/2019

Diploma – Electrical & Electronics Engineering
Aditya Polytechnic Colleges Surampalem • 06/2013 - 05/2016

AWARDS & SCHOLARSHIPS

5/5 Performance Rating 01/2023
TCS

On-the-Spot Team Award – Critical Incident Management
TCS