

Sai Charan Annam

Cybersecurity Analyst

(551) 277-1120 | saicharanannam13@gmail.com | [LinkedIn](#)

SUMMMARY

Cybersecurity Analyst with 3+ years of experience in Security Operations Center (SOC) environments, specializing in threat monitoring, incident response, and security investigations. Proficient in SIEM, EDR, log analysis, threat hunting, and vulnerability management. Experienced in detecting and mitigating cyber threats, performing root-cause analysis, and collaborating with cross-functional teams to strengthen security posture and ensure business continuity.

TECHNICAL SKILLS

Security Operations (SOC):	Security Monitoring, Incident Response, Alert Triage, Threat Hunting, Malware Analysis, Phishing Investigation, MITRE ATT&CK
SIEM & Log Analysis:	Splunk, IBM QRadar, Microsoft Sentinel, Log Correlation, Event Normalization, False Positive Reduction
Network & Endpoint Security:	TCP/IP, DNS, HTTP/S, Firewalls, IDS/IPS, VPN, Proxy Security, EDR, Endpoint Hardening
Vulnerability Management:	Nessus, Qualys, CVE Analysis, Risk Scoring, Patch Management, Remediation Tracking
Cloud & Application Security:	AWS Security, Azure Security Center, IAM, OWASP Top 10, WAF, Secure API Monitoring
Identity & Access Management:	RBAC, MFA, Privileged Access Management (PAM), Active Directory Security
Operating Systems & Automation:	Linux Security, Windows Security, PowerShell, Python Scripting, Bash, Security Automation
Governance & Documentation:	NIST, ISO 27001, Security Policies, Incident Reporting, RCA, Audit Support

WORK EXPERIENCE

Cybersecurity Analyst | Wells Fargo, USA | Apr 2025 – Present

- Leveraged **Security Monitoring** and **Incident Response** across IAM and Zero Trust environments, analyzing 15,000+ daily events and 250+ incidents, reducing detection and containment times.
- Utilized **Splunk** and **Log Correlation** techniques to develop 40+ detection rules and dashboards, identifying 500+ suspicious access patterns while improving alert accuracy.
- Analyzed **TCP/IP** network traffic and managed **Proxy Settings** for authentication workflows, detecting anomalous communications and reducing unauthorized network and external access risks by 30%.
- Conducted **CVE Analysis** and led **Remediation Tracking** for 120+ critical IAM vulnerabilities, achieving 65% closure rates within compliance deadlines and significantly reducing organizational risk exposure.
- Implemented **AWS Security** monitoring controls and **Secure API Monitoring** for identity services, analyzing 2 million monthly requests and reducing cloud security risks.
- Enforced **RBAC** governance policies across 5,000+ user accounts and developed **PowerShell** automation scripts, reducing excessive privileges and manual efforts.

Cybersecurity Analyst | Infosys, India | Aug 2022 - July 2024

- Performed **Alert Triage** and proactive **Threat Hunting** across cloud and SASE environments, investigating 1,500+ monthly alerts and identifying 120 previously undetected threats annually.
- Implemented **false positive reduction** strategies and led **event normalization** initiatives across multi-cloud environments, decreasing non-actionable alerts by 45% and improving threat correlation accuracy by 40%.
- Utilized **EDR solutions** and monitored **DNS traffic patterns** to investigate threats, containing 200+ incidents annually, preventing 300+ malicious external connections, and reducing malware dwell time.
- Developed **risk scoring models** and coordinated **patch management** across cloud and endpoint environments, improving vulnerability prioritization accuracy while reducing critical vulnerabilities.
- Strengthened **Windows security configurations** and enforced enterprise security policies aligned with cloud governance and SASE, reducing endpoint exposure risks, and improving compliance scores by 40%.

CERTIFICATIONS

- Certified Ethical Hacker (CEH)** - LinkedIn
- Cybersecurity with Cloud Computing** - LinkedIn
- Threat Protection with Microsoft Defender XDR** - Microsoft
- Introduction to Threat Hunting** - Security Blue Team
- Security Fundamentals (SC-900)** - By Microsoft
- Introduction to Dark Web, Anonymity and Cryptocurrency** - By EC-Council
- AWS Educate: Getting Started with Security** - Amazon Web Services
- Cybersecurity Essentials (LFC108)** - Linux Foundations
- SQL Injection Attack** - EC-Council
- Pre-Security Certificate** - TryHackMe

EDUCATION

Master's in cyber security | Sacred Heart University | 2024- 2025

Relevant Coursework: Network Security, Vulnerability management, Digital Forensics, Threat Hunting, Security, Ethical Hacking, Web and Database Security, Cyber Crime Investigation.

Bachelor's in cyber security | Swami Vivekananda Institute of Technology | 2020- 2024

Relevant Coursework: Operating Systems, Computer Networking, Data Structures, Object Oriented Programming, Computer Networks, Cryptography and network security, DBMS, Blockchain Technology, Internet of Things.