

KRISHNARJUN PESALAL SARAVANA

Security Engineer

College Park, MD — Phone: +1 734 596 6429 — krishnarjuns119@gmail.com — LinkedIn

Cybersecurity Engineer with 5+ years of cybersecurity experience across security operations, cloud security, and application security. Skilled in SIEM/EDR, threat detection, incident response, vulnerability management, IAM, and Zero Trust architecture, with a focus on emerging technologies, AI security, and security automation.

Professional Experience

Cybersecurity Engineer

Fusion Global LLC, Texas

Jul 2025 – Present

- Correlated endpoint, network, and cloud alerts to investigate suspicious activity, improving incident triage and response.
- Supported monitoring of Terraform-managed AWS/Kubernetes environments with Zero Trust and least-privilege controls.
- Validated security controls by reviewing firewall rules, access policies, and vulnerability scan results.
- Analyzed SIEM alerts using Splunk and Wazuh, improving detection of scripting attacks and privilege escalation by 30%.

Cybersecurity Engineer

Frizb Inc, San Francisco, CA

May 2024 – Jun 2025

- Developed and validated AWS security detections by correlating authentication events, network telemetry, and suspicious activity.
- Deployed EDR, IDS/IPS, and honeypots across Edge AI nodes to improve endpoint and network threat visibility.
- Implemented network microsegmentation and least-privilege controls to restrict lateral movement across containerized workloads.

Cybersecurity Analyst

Levo Inc, San Francisco, CA

Jun 2023 – Sep 2023

- Performed vulnerability assessments using Burp Suite and Semgrep, reducing application and cloud security exposure by 35%.
- Applied ASPM and Zero Trust controls across containerized environments, strengthening security posture by 40%.
- Implemented Okta IAM/RBAC and MFA-aligned access controls, reducing privilege escalation risk by 40%.
- Tuned Snort and Security Onion IDS/IPS, reducing false positives by 30% and improving detection of suspicious traffic.

Cybersecurity Analyst

Cycatz, India

Dec 2020 – Aug 2021

- Partnered with the CISO on automated web app pentesting, identifying business logic vulnerabilities in cryptocurrency apps.
- Conducted secure code reviews and vulnerability assessments, reducing OWASP Top 10 security findings by 30%.
- Leveraged Axiom for distributed vulnerability scanning and automated security assessments, reducing assessment time by 45%.

Cybersecurity Researcher

Gurugram Police Cyber Cell, India

Jun 2020 – Aug 2020

- Applied digital forensics techniques, OSINT, and cybercrime analysis during practical investigative exercises.
- Examined digital evidence and network artifacts to identify indicators of compromise and support cybercrime investigations.
- Authored and presented a paper on “Car Attack Surfaces and Penetration Testing” raising awareness of automotive security.

Education

University of Maryland, College Park

Master of Engineering in Cybersecurity

May 2024

Kumaraguru College of Technology

Bachelor of Engineering in Electronics and Communication Engineering

Apr 2022

Projects

Zero Trust MCP Security Gateway & Threat Detection

Frizb Inc.

Jan 2025

- Designed and implemented a Zero Trust security gateway for MCP servers, enforcing policy-based authorization and least-privilege access to prevent unauthorized tool execution and privilege escalation. Integrated audit logging and threat detection to identify suspicious AI agent activity and insecure tool interactions.

Cloud-Native Runtime Threat Detection & Response

Frizb Inc.

Dec 2024

- Engineered a Kubernetes runtime security monitoring system using Falco and custom detection rules to identify suspicious container activity, privilege escalation attempts, and unauthorized workload execution. Integrated automated alerting and incident response workflows.

RBAC Drift Detection and Remediation System

iQube

Mar 2022

- Developed an IAM drift detection system to identify RBAC policy deviations across cloud and Kubernetes environments, enforcing access compliance and mitigating privilege escalation risks.

Skills

Programming:

Security Tools:

Technologies:

Compliance & Frameworks:

Cybersecurity Domains:

Bash, PowerShell, Python

Axiom, Wazuh, Semgrep, Snort, Snyk, Security Onion, Zeek, Okta, Burp Suite, Metasploit, Splunk, Wireshark, Elastic

AWS, Azure, Docker, Kubernetes, Terraform, Git

NIST 800-53, ISO 27001, OWASP Top 10, MITRE ATT&CK

DevSecOps, Threat Intelligence, Threat Hunting, SIEM, IDS/IPS,

Network Security, Active Directory, CI/CD Security, EDR/XDR,

Secure Code Review, Zero Trust

Certifications

• CompTIA Cybersecurity Analyst (CySA+ CS0-003)

• CompTIA Security Analytics Professional

• CompTIA Security+ SY0-701

• Certified Information System Security professional (In progress)