JEEVANA MUNINARAYANA

Jersey City, NJ — Open to Remote / Relocate (US)
+1 (551) 344-7268 | mjeevana00@gmail.com | LinkedIn | GitHub

IT Security Analyst (Senior/Specialist) | Agency-Wide Security Program Management | Vulnerability Management | Threat Management | SIEM: Microsoft Sentinel | Governance, Risk, & Compliance (GRC) | COOP/DR Planning | Incident Response Leadership

Summary

Senior **IT Security Analyst (Senior/Specialist)** with 4+ years serving as technical authority for agency-wide **Vulnerability Management**, threat detection, & security governance programs across cloud & enterprise environments—managing **strategic planning / roadmap development** & measurable risk reduction initiatives impacting statewide operations. Deep hands-on expertise with **Microsoft Sentinel**, BlueVoyant (MDR), Microsoft Defender for Endpoint (MDE), Securin ASM, & vulnerability risk platforms, leading proactive **threat hunting**, **behavioral analysis**, **automated alerting**, **security telemetry correlation**, & senior-level incident response to rapidly contain threats & minimize operational impact. Proven ability to serve as highest-level technical authority for IT security, data privacy, Continuity of Operations (COOP), & Disaster Recovery (DR)—developing cybersecurity policies/procedures aligned to **CJIS + NIST Framework + Washington State Security Policies (regulatory frameworks)** & delivering executive-ready risk analyses & audit-traceable documentation to support statewide regulatory missions.

Experience

EVONAIRE INC. — Remote, US
Lead Security & Privacy Engineer (Technical Security Authority) Oct 2025 – Present

- Served as technical authority & strategic lead for enterprise **Vulnerability Management** program across 8 production applications & 30+ data-processing workflows; drove **strategic planning / roadmap development** & **vulnerability remediation / risk mitigation** priorities that achieved 85% remediation closure within 60 days.
- Conducted **vulnerability assessments (enterprise apps, hardware, network, cloud)** across enterprise applications, hardware, network infrastructure, & cloud services (AWS/Azure) to support regulatory alignment.
- Led agency-wide **GRC** initiatives to strengthen cybersecurity oversight, accountability, & risk management practices across the organization.
- Drove development & refinement of cybersecurity policies, procedures, & standards aligned to **CJIS + NIST Framework + Washington State Security Policies (regulatory frameworks)** & evolving threat landscapes.
- Conducted internal **security risk assessments** & **quantitative & qualitative risk analysis** (impact/likelihood/mitigations) to enable data-driven decisions by executive leadership & prioritize investments.
- Led formal **Security Design Reviews** with architects, development teams, & operations to validate secure design principles & ensure new systems/infrastructure changes met documented security standards throughout planning & implementation.

COMMUNITY DREAMS FOUNDATION (Healthcare SaaS) — Remote, US
Security Software Engineer (Threat Detection & Response Lead) Nov 2024 – Sep 2025

- Led **Threat Management** operations by correlating **security telemetry correlation** from **Microsoft Sentinel**, cloud audit logs (AWS CloudTrail, Azure Monitor), Microsoft Defender for Endpoint (MDE) telemetry, & **threat intelligence** feeds to identify emerging attack patterns & prioritize response actions.
- Detected & responded to advanced threats through **real-time monitoring**, **behavioral analysis**, & **automated alerting** within **Microsoft Sentinel**; rapidly contained incidents to minimize operational impact.
- Conducted **threat hunting** & in-depth **log analysis** using **Microsoft Sentinel**, Defender for Endpoint, & cloud-native tools to identify **Indicators of Compromise (IOCs)**, anomalous behavior, **lateral movement detection** attempts, & privilege escalation patterns prior to escalation.
- Served as **senior incident responder** for high-severity incidents; performed **forensic investigation**, **evidence preservation**, **root cause analysis**, comprehensive documentation, & cross-functional remediation coordination.

PACE UNIVERSITY — New York, NY
Graduate Research Assistant (Security Analytics & Detection) Sep 2023 – Jun 2024

- Built evaluation criteria & decision frameworks to improve detection outcomes, investigation consistency, & threat hunting effectiveness; documented repeatable procedures to support operations quality & auditability.
- Authored a 40+ page research paper on cloud exploitation TTPs & detection frameworks, mapping attacks to MITRE ATT&CK Cloud Matrix & proposing behavior-based detection strategies.

INFOSYS LTD — Bangalore / Mysore, India
Senior Systems Engineer Nov 2021 – Jul 2022

- Improved incident triage, escalation, & cross-functional coordination by refining severity criteria & routing logic; reduced containment time by 25% through structured response procedures & stakeholder communication protocols.
- Built security analytics dashboards & KPI reporting across 90+ enterprise environments to support governance, risk visibility, & remediation prioritization for leadership.

Systems Engineer Nov 2019 – Oct 2021

- Automated SIEM enrichment & workflow routing using Python/Bash; improved SOC efficiency & reduced false positives by 20% through enhanced correlation, context enrichment, & alert tuning.
- Authored runbooks/SOPs covering threat investigation steps, escalation criteria, evidence collection, & incident documentation to strengthen auditability, repeatability, & compliance readiness.

Selected Projects (Security Program Innovation)

OpenSecOps AI — Advanced Threat Simulation & Detection Validation - Developed behavior-based threat simulations aligned to attacker TTPs (MITRE ATT&CK); improved alert fidelity by 40% & published reusable hunting playbooks, tuning guidance, & detection logic for security operations teams.

Compliance Remediator — Automated Remediation Tracking & Validation - Built automated remediation tracking & validation pipeline integrating vulnerability findings with Infrastructure-as-Code changes; closed audit control gaps by 60% with repeatable, audit-ready evidence workflows supporting agency-wide compliance initiatives.

IAM Governance Tracker — Identity Security & Privilege Monitoring - Implemented detections for privilege escalation & suspicious access patterns; strengthened identity logging, forensic readiness, & reduced unauthorized access risk by 35% across federated identity environments.

Education

M.S., Cybersecurity — Pace University, New York, NY May 2024
B.E., Computer Science — Visvesvaraya Technological University, Bangalore, India Jun 2019

Certifications

Google Cloud Professional Cloud Security Engineer May 2025
AWS Certified Solutions Architect – Associate Scheduled: Oct 2026
Security Certifications (In Progress): CISSP, CISM, CEH, GIAC, CompTIA Security+ (target: Q2 2026)