JEEVANA MUNINARAYANA

394 Baldwin Ave, Apt 2, Jersey City, NJ 07306 | mjeevana00@gmail.com | 551-344-7268 | LinkedIn

TECHNICAL SKILLS

AWS (IAM, Security Hub, GuardDuty), Azure (Sentinel, Defender, Azure AD), Google Cloud Platform (GCP) Security, Cloud Access Security Broker (CASB) Solutions, Okta, Identity & Access Management (IAM), Multi-Factor Authentication (MFA), Single Sign-On (SSO), Privileged Access Management (PAM), Firewalls, VPNs (Site-to-Site, Remote Access), VLANs, STP, OSPF, BGP, EIGRP, Network Access Control (NAC), Software-Defined Networking, Zero Trust Network Architecture, Nessus, Splunk, Wireshark, tcpdump, Burp Suite, OWASP ZAP, Endpoint Detection & Response(CrowdStrike), PowerShell, Python, Bash, Java, Ansible, Terraform, Docker & Kubernetes, NIST Cybersecurity Framework, CIS Controls, ISO 27001, SOC 2, GDPR, HIPAA, PCI DSS, Cloud Native Security (Containers, Microservices), Security Awareness Training, MITRE ATT&CK

PROFESSIONAL EXPERIENCE

Software Engineer | Community Dreams Foundation

Jersey City, NJ ***[Nov 2024 – Present]***

- Established **secure access policies** for **cloud environments**, ensuring **100% NIST and CIS benchmark compliance** for **50+ team members.**
- Streamlined **security reporting with Python scripts**, cutting manual effort by 50% and reducing report generation time from 2 hours to 30 minutes.
- Facilitated **vulnerability assessments for 50+ systems**, facilitating **remediation of 85% of critical vulnerabilities** within 30 days.
- Implemented **role-based access controls (RBAC)**, decreasing unauthorized access incidents by 40%.

Senior Systems Engineer | Infosys

Bangalore, India ***[Nov 2021 – Jul 2022]***

- Spearheaded **security hardening for Microsoft Azure and AWS**, minimizing attack surfaces by 40% across 200+ cloud resources.
- Architected **Zero Trust IAM policies**, safeguarding access for 5,000+ users and reducing unapproved attempts by 60%.
- Optimized **vulnerability scanning and patching via PowerShell**, boosting remediation efficiency by 60% and decreasing unpatched vulnerabilities by 45%.
- Engineered **Splunk SIEM correlation rules**, accelerating **threat response time by 35%** and minimizing false positives by 20%.
- Performed **50+ network security assessments**, enhancing network security by 30% through **firewall configuration optimization.**
- Integrated **IAM best practices into 100+ CI/CD pipelines**, elevating compliance by 25%.

Systems Engineer | Infosys

Mysore, India ***[Nov 2019 – Oct 2021]***

- Administered **user access controls for 10,000+ users across AWS IAM, Okta, and Azure AD**, reducing access-related incidents by 40%.
- Maintained **firewalls, VPNs, and network security policies for 500+ endpoints**, thwarting unpermitted access attempts by 30%.
- Pioneered **vulnerability assessments and patch management**, achieving 98% compliance with NIST and CIS benchmarks.
- Fine-tuned **SIEM solutions**, improving **security event detection accuracy by 40%** and expediting **incident investigation time by 35%.**
- Crafted **20+ PowerShell automation scripts for security compliance checks**, slashing manual efforts by 50%.
- Co-ordinated with **incident response teams**, analyzing and mitigating **200+ security threats over 2 years.**
- Developed and enforced security best practices, leading to a 25% reduction in phishing incidents.
- Held security awareness training sessions for employees, increasing company-wide security compliance by 30%.

EDUCATION

Pace University | New York, NY *M.S. in Cybersecurity [May 2024]*
Visvesvaraya Technological University | Bangalore, India *B.E. in Computer Science and Engineering [Jun 2019]*

PROJECTS

Vulnerability Management Framework

- Designed a **Python-based vulnerability tracking system** to automate risk scoring for 500+ assets, reducing manual effort by 60%.
- Enhanced incident response workflows by integrating **real-time security analytics dashboards using Splunk and Power BI**, improving efficiency by 30%.
- Developed an **automated ticketing system** that shortened vulnerability remediation time from 10 days to 3 days.
- Simplified compliance audits by embedding **security reports into CI/CD pipelines**, reducing verification time by 40%.
- Formulated custom **risk-prioritization algorithms** to streamline remediation workflows, decreasing exploitable vulnerabilities by 45%.

Cloud Security Automation

- Mechanized **cloud security monitoring for AWS and Azure environments**, achieving **95% compliance with GRC** policies across 250+ cloud resources.
- Implemented **log correlation techniques using AWS CloudTrail, Azure Monitor, and ELK Stack** to improve threat detection accuracy by 50%.
- Deployed **IAM policy audits** to enforce least privilege access principles, reducing excessive permissions by 70%.
- Configured **serverless security automation using AWS Lambda and Azure Functions** to eliminate manual cloud security checks by 90%.
- Incorporated **security automation scripts into DevSecOps pipelines** to reduce misconfigurations in cloud deployments by 35%.

Threat Intelligence Dashboard

- Built a **real-time security dashboard integrating threat feeds from MITRE ATT&CK, AlienVault OTX, and VirusTotal** to increase threat visibility by 60%.
- Accelerated security incident response time by implementing pr**edictive analytics and systematized alerts via Splunk and Grafana**.
- Constructed **threat correlation algorithms** that identified 80% of high-risk threats before escalation while minimizing false positives by 35%.
- Activated **SOAR workflows** to automate playbooks and reduce incident resolution time from 2 hours to 30 minutes.
- Facilitated **centralized threat intelligence sharing** across security teams to improve collaboration and reduce data breach response time by 50%.

Establishing Secure LAN Internet Using SoftEther

- Deployed **SoftEther VPN to establish a secure virtual LAN** across **geographically distributed locations**, improving data encryption reliability by 40%.
- Implemented **SSL-VPN and X.509 authentication** mechanisms to enhance user authentication security and reduce unauthorized access attempts by 50%.
- Configured **firewall rules** and conducted performance tests to reduce network latency by 30%, ensuring seamless multiplayer gaming and remote access.
- Drafted **custom VPN encryption policies** to increase data transmission security while maintaining a network uptime of 99.9%.
- Analyzed network traffic using **Wireshark and TCPDump** to identify and mitigate anomalies, improving overall network reliability by 35%.

ACHIEVEMENTS

- Improved enterprise security posture by automating IAM policies, reducing unauthorized access incidents by 50%.
- Enhanced network security by implementing SD-WAN solutions, improving traffic efficiency and security.
- Recognized for optimizing vulnerability remediation workflows, reducing resolution time from 7 days to 48 hours.