MOSES KANAGARAJ

San Diego, CA (open for relocation) | mkanagaraj9711@sdsu.edu | (619) – 865 – 7148 | LinkedIn

EDUCATION

Masters in Cybersecurity Management | San Diego State University, San Diego, CA | GPA: 3.68/4 | 2024 - Present
Bachelor in Computer Science and Engineering | Anna University, India | GPA: 3.41/4 | 2018 - 2022

SKILLS

Technical: Python, Bash, Powershell, Linux, CI/CD, SQL, Penetration testing, Intrusion Detection & Prevention Systems
Tools: Nessus, Nmap, Wireshark, Metasploit, Burp Suite, Cloudflare Zero Trust, SIEM, IAM, Splunk, Endpoint security, Terraform
Security Practices: AWS (CloudTrail, CloudWatch), Azure (Microsoft Sentinel), Risk Assessment, Threat Intelligence, Incident Response, Vulnerability Management, Compliance, NIST, STIG, OWASP Top 10, MITRE ATT&CK and NIST Framework
AI: Copilot, Perplexity, Azure OpenAI

CERTIFICATIONS

CompTIA Security +
AWS - Cloud Security Foundations | Online – 2024

WORK EXPERIENCE

Research Assistant – SDSU | San Diego, California | 2025 – Present

- Conducted research on enhancing the security of transformer-based language models through encryption-aware fine-tuning methods.
- Developed a tokenization and embedding encryption framework also incorporated dynamic token embedding flipping at regular intervals to mitigate Man-in-the-Middle (MITM) and frequency-based inference attacks.
- Designed and integrated a Dynamic Token Embedder module within Hugging Face's fine-tuning pipeline to evaluate the trade-offs between model performance and security robustness.

KAAR TECHNOLOGIES | *Cybersecurity Analyst*, India | 2021 – 2024

- Led end-to-end SAP cybersecurity operations with primary responsibility for protecting business critical ITES environments (FI/CO, HR, SCM, CRM modules) using SecurityBridge platform.
- Conducted Security Baseline & Compliance Monitoring across multiple SAP landscapes (ERP, S/4HANA) to assess posture against SAP security guidelines and ISO 27001 controls, reducing configuration drift by 30%.
- Utilized Event Monitoring in SecurityBridge to identify anomalies such as: Unauthorized RFC destination creation, Suspicious critical role assignments, Custom ABAP code vulnerabilities resulted in proactive containment of 12+ high severity incidents, preventing potential financial and reputational damage.
- Managed Security Patch Lifecycle by continuously monitoring advisories and applying patches across S/4HANA and ECC systems; improved patch compliance from 65% to 97% within one year.
- Implemented Interface Traffic Monitoring to visualize cross system traffic, detecting lateral movement attempts and mitigating risks in SAP PI/PO and RFC communications.
- Automated Security Incident Management workflows, integrating SecurityBridge with SIEM (Splunk) reducing average incident response time by 40%.
- Collaborated with cross-functional teams (SAP BASIS, GRC, and SOC) to align SAP security with overall IT security posture, successfully passing 3 external audits with zero major findings.
- Conducted employee awareness sessions on SAP cyber risks (phishing, privilege misuse, unpatched systems), improving governance policies, compliance reporting by end-users.

PROJECTS

- **AWS Password Management Server** – Integrated AWS Secrets Manager with CloudTrail & CloudWatch for real-time monitoring, alerting, and secure key management.
- **Vulnerability Assessment Lab** – Conducted scans using Nessus and implemented remediation strategies.
- **SIEM Implementation** – Used Microsoft Azure Sentinel and custom KQL rules to enhance threat detection, incident response and locate the threat actors geographically
- **System Hardening** – Used SCAP & STIG Viewer to identify non-compliance and documented traceable remediation actions.