Brindha Sivakumar

947-275-0417 brin2595@gmail.com linkedin.com/in/brindha-sivakumar brindha-sivakumar.github.io/portfolio

Summary — Graduate student in Artificial Intelligence with 7 years of cybersecurity and infrastructure security experience. Specializes in the implementation of robust security measures and the automation of workflows to effectively mitigate risks. Currently pursuing applied research on AI threat landscape with a focus on securing the AI lifecycle, focusing on adversarial robustness against model extraction and training data poisoning within cloud-native infrastructures.

Education

University of Michigan-Dearborn **[Expected Graduation: May 2027]**
Master of Science in Artificial Intelligence

University of Limerick **[GPA: 3.54/4]**
Master of Engineering in Information and Network Security

Anna University **[GPA: 7.38/10]**
Bachelor of Engineering in Computer Science

Academic Projects & Research

- Explainable AI for Network Intrusion Detection (*Research Paper*) - Applying Causal Inference and XAI to improve alert prioritization and classification in Network Intrusion Detection Systems (NIDS).
- Politeness Detection in Text (*Project*) - Developed and compared ML approaches (SVM, LSTM, BERT) for automated politeness classification, achieving 69.2% accuracy with an ensemble system.

Professional Experience

Workday **Jan 2023 – Oct 2024**
Cybersecurity Engineer

- Designed and developed policies that act as guardrails for best practices and security standards for Kubernetes platforms using Gatekeeper with Open Policy Agent.
- Performed security reviews of changes in application code using IaC and CI / CD pipelines.
- Developed a solution to identify and remediate unused IAM roles in a large-scale organization

Smarttech247 **Jun 2020 – Dec 2022**
Security Engineer- Technical Lead

- Managed and trained new teammates over a 6-month period and offered mentorship on duties and best practices.
- Developed SOAR playbooks, streamlining incident response and reducing resolution time by 50%.
- Identified and ingested high value assets' logs in SIEM, enhancing detection coverage and reducing false positives.

Security Engineer

- Spearheaded deployment, maintenance, and upgrade of security toolsets – SIEM, SOAR, UEBA
- Managed threat intelligence and IoC management with STIX TAXII compatible platforms.
- Developed automations, policies, and procedures as part of continuous improvement and provided concise technical documentation for internal use.

Tata Consultancy Services **Nov 2016 – Aug 2019**
Systems Engineer

- Administered network and security policies in NextGen firewalls and automated system hardening for Windows and Linux servers using CIS benchmarks.
- Implemented antivirus and vulnerability assessment solutions, configuring policy catalogs in the central management server.

Skills

Programming
Python, Bash, Go, Rego, Terraform, AWS Policy

AI/ML Frameworks
PyTorch, TensorFlow, scikit-learn, Pandas, NumPy

Security Operations
SIEM, SOAR, UEBA, EDR

Infrastructure Security
Kubernetes Security, Cloud Security, DevSecOps

Certifications

GIAC Cloud Security Automation (GCSA)
AWS Certified Security – Specialty
Certified Kubernetes Administrator (CKA)
Certified Kubernetes Security Specialist (CKS)