Rahul Isola

(+1) 980 298 3828 | rahulisola@gmail.com

www.rahulisola.com | http://www.linkedin.com/in/rahulisola

PROFESSIONAL SUMMARY

Results-driven Vice President and experienced Information Security Engineer with 12+ years of enterprise experience architecting Threat Detection & Response (TDR) platforms, insider threat mitigation frameworks, Detection-as-Code pipelines, zero-touch threat mitigation engines, and Network Access Control (NAC) automation frameworks. Prolific inventor with 28+ granted patents specializing in rogue device containment, zero-day threat response, automated MAC address cloning/spoofing mitigation, and real-time rogue/unauthorized asset containment. Demonstrated expertise in engineering high-throughput SIEM analytics (Splunk) to detect behavioral anomalies and data exfiltration risks, eliminating operational toil through self-healing NAC gap remediation workflows, and building zero-trust security controls protecting global enterprise networks and DMZs.

CORE COMPETENCIES & TECHNICAL SKILLS

- **Threat Detection & Response (TDR):** Detection-as-Code, SIEM Log Analytics (Splunk), Threat Hunting (MITRE ATT&CK & TTPs), High-Fidelity Signal Generation, Root Cause Analysis, Digital Forensics & Telemetry.
- **User & Entity Behavior Analytics (UEBA):** Behavioral Anomaly Detection, Lateral Movement Analysis, Privilege Abuse Monitoring.
- **Data Protection & Exfiltration Defense:** Rogue Hardware Detection, Unauthenticated Device Isolation, Data Loss/Exfiltration Telemetry.
- **Identity, NAC & Zero-Trust Architecture:** Network Access Control (NAC), 802.1X Access Enforcement, Layer 2/3 Enforcement, Micro-segmentation, Automated NAC Gap Remediation, Rogue Device Quarantine, Non-Compliant Endpoint Controls.
- **Security Automation & Engineering:** Python, C#, .NET, Java, C++, Shell Scripting, RESTful APIs, Infrastructure-as-Code (IaC) Automation, Toil Reduction, CI/CD Security Pipelines, System Health Monitoring.
- **Edge Defense & Attack Mitigation:** Automated MAC Cloning/Spoofing Defense, Zone-Based Wireless Triangulation, Layer 7 Web Application Firewalls (F5 ASM/LTM), Bot Defense, GeoSecurity Frameworks.
- **Databases, Big Data & Infrastructure:** Splunk Big Data Analytics, MS SQL, SSIS/SSDT, MySQL, MongoDB, PostgreSQL, DB2, Cisco IOS Automation, Git, Jenkins, Linux, SNMP, TCP/IP.

PROFESSIONAL EXPERIENCE

BANK OF AMERICA | Global Information Security (GIS)

Vice President – Information Security Engineer Feb 2014 – Present

- **Behavioral Anomaly, Detection-as-Code & SIEM Telemetry Analytics:** Architected high-throughput Splunk SIEM threat hunting pipelines analyzing terabytes of log telemetry, with 100-300M+ security events and ~50–200 GB of telemetry data daily. Authored high-fidelity Detection-as-Code correlation rules aligned with MITRE ATT&CK TTPs to identify zero-day exploits, root causes, and stealth lateral movement.
- **Automated Rogue Device & Physical/Network Insider Threat Mitigation:** Engineered zero-touch automated threat containment tools that detect MAC address cloning/spoofing and rogue assets, automatically executing instant port-level isolation and quarantine to eliminate incident response lag, reducing threat isolation time from 3-4+ hours to few-seconds automated response.
- **NAC Architecture & Self-Healing Remediation:** Spearheaded enterprise Network Access Control (NAC) strategy across global networks. Designed and deployed automated NAC gap detection engines that continuously discover unmonitored endpoints and trigger self-healing remediation workflows enterprise-wide.

www.rahulisola.com

Rahul Isola

(+1) 980 298 3828 | rahulisola@gmail.com

www.rahulisola.com | http://www.linkedin.com/in/rahulisola

- **Security Automation & Engineering Toil Reduction:** Led full-stack automation for Layer-7 Web Application Firewall (F5 ASM), bot-defense profiles, and Cisco IOS / F5 LTM security policies, eliminating hundreds of hours of manual engineering toil annually and providing frictionless security integration.
- **High-Risk Insider & Endpoint Risk Monitoring & Controls:** Designed and automated the Enhanced Cyber GeoSecurity Controls platform to dynamically monitor high-risk traveler endpoints, enforcing adaptive zero-trust protections against physical asset compromise and data leakage.
- **Strategic Leadership & Cross-Functional Collaboration:** Partnered with cross-functional engineering, data science, product, and legal teams to review systemic security architecture, conduct vulnerability assessments, and drive engineering decisions across the enterprise.

UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE | Mosaic Computing Group

Technical Specialist – Application Development Aug 2012 – Dec 2013

- **Application & Infrastructure Engineering:** Designed and deployed live, scalable web applications, REST APIs, and workstation monitoring systems for the College of Engineering.
- **Secure Remote Access & System Health Automation:** Built automated SSH tunneling and secure connection solutions for researchers, timed token renewal services, system health monitoring, and campus-wide live emergency broadcast systems.

FREELANCE SOFTWARE & SECURITY CONSULTANT

Software & Systems Engineer / Technical Consultant Aug 2009 – Mar 2012

- **Full-Stack & Security Consulting:** Delivered web architectures, custom API integrations, and database performance optimizations for clients including digital agencies (Croadz Designs).

PATENTS & KEY INNOVATIONS

Enterprise Patent Leadership: Inventor of 28+ granted patents protecting enterprise security controls. Recognized among the Top 5 Inventors across Bank of America enterprise-wide (2018–2019).

Full portfolio: https://patents.google.com/?inventor=Rahul+Isola

- **Device Spoofing & MAC Cloning Detection Engine:** Automated production platform that continuously monitors network traffic to identify & prevent MAC spoofing/cloning attempts by internal bad actors / compromised devices impersonating trusted hardware to bypass 802.1X/NAC controls.
- **Automated Rogue Device Disconnection:** Instant, zero-human-touch isolation of suspicious insider assets without alerting the adversary during triage.
- **Surgical Rogue Device Isolation & Quarantine:** Deployed containment protocol allowing security teams to safely isolate and quarantine suspicious devices while enabling real-time threat investigation.
- **Zone-Based Distributed Wireless Triangulation:** Algorithms mining wireless scanning and access logs in Splunk to locate, triangulate, and track lost or rogue devices.
- **Secure Traveler GeoSecurity Framework:** Automated security framework providing dynamic data protection and endpoint surveillance for employees traveling to high-risk international regions.

EDUCATION & PRIOR RESEARCH

Master of Science (M.S.) in Computer Science | University of North Carolina at Charlotte (2013)

Bachelor of Engineering (B.E.) in Mechanical Engineering | DBIT, Mumbai University (2012)

- **Prior Research Highlights (DBIT / CSRE, IIT Bombay):** Published in IEEE Transactions on Information Technology in Biomedicine (Journal) & international conference proceedings (CBMS 2011, DeSE 2011) focusing on Neural Networks & KNN algorithms.

***Google Scholar Link**: https://scholar.google.com/citations?user=SiUKA9sAAAAJ*

www.rahulisola.com