Srikamakshi Mahesh

srikamam@alumni.cmu.edu | (609) 468-1696 | linkedin.com/in/srikamakshi-mahesh

EDUCATION

Carnegie Mellon University, Heinz College, Pittsburgh, PA 08/2023 – 05/2025
Master of Science in Information Security Policy & Management GPA: 3.95/4.0
Sri Sivasubramanian Nadar College of Engineering, Chennai, India 08/2016 – 09/2020
Bachelor of Engineering in Electronics & Communications

ACADEMIC PROJECTS

- **Master's Thesis – AI-Augmented Hybrid Incident Response:** Developed an integrated **NIST SP 800-61 + ISO 27001/20007 + NIST RMF** model; produced executive-level documentation translating complex technical processes into clear, decision-useful artifacts
- **IT Risk & Compliance Assessment – Tesla Case Study:** Modeled asset-level risk using SOC 1/2 and OCTAVE Allegro; synthesized findings into concise technical briefs highlighting supply-chain and cloud vulnerabilities
- **Penetration Testing & Threat Correlation:** Conducted Nmap/Wireshark/Metasploit investigations; mapped findings to CVE/CWE and produced structured summaries for leadership review
- **Automated Digital Forensics Platform:** Developed a Python-based UI integrating Sleuth Kit and Autopsy to automate evidence extraction, hash verification, and timeline reconstruction for incident investigations

EXPERIENCE

Drexel University, Philadelphia, PA 08/2025 – Present
Research Assistant

- Designing interpretable AI and anomaly-detection models for syslog and IDS datasets using Python, pandas, and Jupyter
- Reviewing research papers on security, ML, and cloud-scale detection and summarizing insights for senior researchers

Sequretek, Princeton Jn, NJ 05/2024 – 08/2024
Security Operations (SOC)/Product Development Intern

- Investigated SIEM, EDR, IAM, and firewall telemetry; identified emerging threat patterns and **mapped detections to MITRE ATT&CK**
- Contributed to SOC dashboards developments, enhancing visibility, streamlining rule tuning, and reducing incident triage time by 25%

Viasat, Chennai 10/2020 – 06/2023
DevSecOps Engineer II, Network Traffic Enforcement

- Identified monitoring blind spots in the security logging pipeline and implemented syslog forwarders with **Splunk and Kibana dashboards** and improved detection of unauthorized access and reducing false negatives
- Configured **AWS VPC, Secrets Manger, and IAM components** for a monitoring system, enabling dynamic rule tuning and anomaly-based alerting **across DNS, TCP/IP, and HTTP/HTTPS layers**
- Automated data collection and deployment workflows **using serverless CI/CD patching pipeline (Kubernetes + Jenkins + Ansible** to improve patch compliance and reduced mean time to resolution (MTTR) by 40%
- Built **Grafana-Elasticsearch-Druid** dashboards to monitor telemetry and execute **SQL-style** correlation queries for early detection of misconfigurations and security events
- **Triaged and resolved on-call incidents** involving policy violations and performance anomalies, and documented processes and post-incident remediation tracking to improve consistency across incident workflows
- Led **agile ceremonies as interim Scrum Master;** led sprint planning, retrospectives, and mentorship initiatives to strengthen secure development practices

SOFT SKILLS

- **Teaching Assistant at CMU**: **Communicated complex security concepts** and guided students in hands-on labs
- **CMU ISPM Ambassador**: Engaged the university community in cybersecurity initiatives. continuously refining outreach strategies based on feedback and lessons learned
- **Mentorship at Viasat**: Supported an intern in network monitoring and issue resolution
- **Rotaract Club Leadership**: Collaborated and facilitated cross-cultural projects between Indian and Sri Lankan club

CERTIFICATIONS & PUBLICATIONS

- **Scrum Master** by the Scrum Alliance
- Conducted a performance analysis of the Yugam-128 cipher and presented the results at the ICIDCA 2019 Conference, published in the Lecture Notes on Data Engineering and Communications Technologies (Vol. 46, Springer)