Sai Kiran Mididoddi

USA Bay Area (Open to Relocation) | saikiranmididoddi@gmail.com | +1(913)280-0952

linkedin.com/in/sai-kiran-mididoddi/

Summary

Security Intelligence and SOC engineer with 5+ years of experience and passionate about outsmarting cyber criminals. Led a team of four to build CrimeOS, an AI-driven platform that slashed investigation times by 90% and earned **Forbes India-DGEMS 2024 recognition**. At **Tesla**, disrupted **$200K+ in crypto scams** using Splunk and Python automation, while crafting Power BI and Neo4j visualizations to track threats. Skilled in OSINT, Power BI, and Azure, I turn complex data into actionable wins for safer systems.

Skills

- **Cybersecurity:** DFIR, Threat Intelligence, Phishing Analysis, SIEM, Penetration Testing, Splunk, Wireshark, Autopsy, FTK Imager, Volatility, DeepBlueCLI, Snort (IDS), Metasploit, Nmap, Netcat, URLScan, DomainTools, VMRay, Threat Hunting, Crypto Currency, Cyber Crimes, Zscaler, Authentic8 Silo, Microsoft Entra ID, Microsoft Defender, Cortex XSOAR, ELK stack, Sentinel One, HIPAA, ISO27001, GDPR, Python, Grafana, ELK Stack
- **Security-Aware Development:** OAuth 2.0, OpenID Connect, 802.1X Authentication, Threat Hunting
- **Leadership:** Team Leadership, Stakeholder Communication, Law Enforcement Coordination

Experience

Information Security Intern, Tesla, Inc. – Fremont, CA — Jan 2025 – May 2025

- Triaged and provided mitigations for **100+ phishing emails**, vendor phishing campaigns, SECaaS platform alerts, and network anomalies using EDR, Identity Management tools, Splunk, sandbox environments, and domain/IP reputation tools in coordination with the **SOC team**.
- Performed Threat Analysis on patterns and trends in spam operations, including SEO manipulation, account takeovers, and fraudulent engagement.
- Developed a Google Face-Net **machine learning model** in Python to automate spam detection, analyzing patterns in phishing emails and reducing manual triage time by 30%, improving security team efficiency.
- Led **Cyber Threat Intelligence and Threat Hunting**, identifying adversary TTPs and neutralizing **200+ impersonation domains** using OSINT, pDNS, and SIEM (Splunk), disrupting large-scale money laundering scams.
- Designed and implemented Python-based automation scripts, leveraging Splunk and OSINT to detect and dismantle over 200 cryptocurrency scam campaigns across social platforms, disrupting fraudulent transactions exceeding **$200K** and saving 50 hours of manual effort monthly.
- Developed a novel **scam detection algorithm** in Python, leveraging machine learning techniques to identify fraudulent social media activities with **75% accuracy**, enabling proactive mitigation of phishing and impersonation campaigns targeting Tesla's brand.
- Built real-time dashboards to monitor suspicious cryptocurrency wallets across BTC, ETH, DOGE, and other tokens, visualizing over $200K+ in fraudulent transactions, victim counts, and connections to known suspects. Empowered investigators to correlate wallet activity with ongoing scams, resulting in faster linkage of cybercriminal groups and improved intelligence briefings.
- Designed and deployed Grafana dashboards to monitor over 200+ fraud-related domains, tracking registrar patterns and domain creation trends. Enabled the team to proactively identify high-risk registrars and contributed to the early detection and takedown of fraudulent domains, reducing response time by 40%.
- Developed Python based automation to detect and dismantle 200+ brand impersonation campaigns running cryptocurrency scams across social platforms; leveraged SIEM to visualize threat patterns and improve detection and response capabilities.
- Performed incident response, mitigating vendor phishing attacks, and analyzing malicious URLs and files via sandbox environments, and domain reputation tools, extracting **IOCs and mapping TTPs to MITRE ATT&CK** for site takedowns.

- Contributed to the deployment of a secure web isolation platform, optimizing Python-driven automation workflows, which streamlined threat response processes and reduced incident resolution times by 20%.

Software Development Engineer, CyberEye Research Labs & Security Solutions Pvt. Ltd. – Hyd, India May 2022 – July 2023

- Led a team of four to architect **CrimeOS (crimeos.ai)**, a Python and Azure-based **AI-driven platform**, transforming cybercrime investigations by boosting case resolution efficiency by **90%**, earning **Forbes India-DGEMS 2024** recognition, and facilitating several arrests through actionable insights.
- Developed **REST APIs** and Power Automate flows to automate call log, bank statement, and linked account analysis, reducing manual **investigation time by 70%** and enabling investigators to handle 100+ cases weekly with unprecedented speed.
- Co-authored Standard Operating Procedures (SOPs) for investigating **cyber crimes**, including phishing, vishing, smishing, and bank fraud, incorporating **OSINT** to strengthen threat mitigation functionalities.
- Pioneered Neo4j graph visualizations powered by Cypher queries, mapping relationships among 100+ suspects to uncover **3 major fraud networks** with 15+ key actors, directly supporting law enforcement in dismantling 500K in fraudulent operations.
- Built Power BI dashboards with DAX and Power Query to deliver real-time fraud analytics, visualizing suspect patterns and geospatial data, cutting **reporting time by 50%** and enhancing strategic decision-making for stakeholders.
- Established **DevSecOps** practices with CI/CD pipelines in **Azure DevOps**, automating Power Platform deployments, slashing release cycles by 80%, and ensuring robust, secure production environments.

Software Development Engineer, iBuild Innovations India Pvt. Ltd. – Hyd, India July 2019 – April 2022

- Architected a Django-based **WiFi authentication** platform integrated with FreeRADIUS, implementing 802.1X authentication and role-based access control, reducing unauthorized network access by 40% and securing connectivity for **700+ users**; developed Kibana-pfSense dashboards for real-time traffic monitoring.
- Configured **SIEM** with **Suricata** and ELK Stack, normalizing logs and building a Kibana dashboard to monitor network traffic, enabling real-time detection of external and internal threats across **1,000+ endpoints**.
- Automated **AWS CloudWatch** log analysis using Python and Boto3, detecting anomalies across IoT servers and **mitigating threats by 30%**, saving 20 hours of manual analysis weekly and bolstering system reliability.
- Configured ELK Stack and Prometheus-Grafana monitoring systems to track 1,000+ endpoints, accelerating incident response times by **60%** and enabling proactive threat detection for critical infrastructure.
- Acted as POC for clients to configure Single Sign-On (SSO) in IoT Network Server using OpenID Connect and OAuth 2.0, integrating identity providers like Amazon Cognito, Google OpenID Connect, and Microsoft Entra to enable secure federated authentication.
- Guided clients in configuring secure authentication and authorization for IoT Network Server using API keys, OAuth 2.0 access tokens, and session cookies. This ensured correct rights assignment, token handling, and integration with HTTP and CLI tools for seamless API access.
- Led a 5-member **Incident Response Team** to maintain **99.99% uptime** for 100+ AWS-hosted servers, optimizing patch management and reducing operational costs by 40% through efficient resource allocation.
- Ensured **GDPR compliance** by securely managing customer data and processing data erasure requests in alignment with regulatory timelines and internal privacy protocols.
- Set up and configured Prometheus and Grafana to monitor critical production infrastructure, enabling real-time visibility into system performance and proactive anomaly detection.
- Guided clients in configuring secure authentication and authorization for IoT Network Server using API keys, OAuth 2.0 access tokens, and session cookies. This ensured correct rights assignment, token handling, and integration with HTTP and CLI tools for seamless API access.
- Authored detailed setup documentation and post-mortem reports to support incident reviews, identify root causes, and implement lessons learned, improving anomaly detection and response readiness across the team.

Founding Engineer, Viayam (no longer operational) – Hyd, India July 2018 – June 2019

- Developed Python scripts to automate log analysis and Zoho **email monitoring**, improving efficiency by 15% in a lean startup environment.
- Spearheaded the design and theoretical framework for an Android fitness app, enabling subscription-based

access to 50+ partner gyms and integrating a digital wallet for seamless transactions, driving **2,000+** user sign-ups and $10K+ in monthly transaction volume within six months.

- Collaborated with a small team to enforce secure coding practices and deliver security reports, reducing vulnerabilities by 25% as a core team member.
- Designed **security monitoring solutions** using SIEM tools (e.g., Splunk) and configured Zoho email security rules, reducing threat detection time by 20%.
- Conducted vulnerability assessments with Nessus and OpenVAS, resolving **50+ vulnerabilities** and ensuring 99.8% uptime for cloud infrastructure.

Projects

CrimeOS: AI-Driven Cyber Crimes Investigation Platform crimeos.ai

- Architected and led an AI-driven platform using Python, Neo4j, and Azure to automate cybercrime investigations, achieving a 90% efficiency gain and enabling several arrests by linking INR 500K in fraud; developed REST APIs and Power BI dashboards for real-time insights.

Cybersecurity Governance and Policy Development

- Crafted hospital-specific security policies (e.g., Acceptable Use, Asset Management, Information Disclosure) aligned with HIPAA, HITRUST, and STRIDE frameworks, mapping to NIST SP 800-53 controls to ensure compliance and mitigate threats for 5,000+ patient records.
- Conducted risk assessments using STRIDE methodology, identifying and prioritizing 20+ potential vulnerabilities in hospital data workflows, enhancing policy enforcement for regulatory compliance.
- Developed incident response procedures integrated with HIPAA requirements, reducing policy violation response time by 30% in simulated hospital breach scenarios.

Employee Wi-Fi Access Management System

- Developed an application using Django and a Radius server to automate the registration and Wi-Fi access management for 700+employees.
- Enabled administrators to easily assign, track, and monitor network traffic based on employee roles and team affiliations, streamlining network access and enhancing security oversight.

Home Network Security Setup

- Deployed Snort on Raspberry Pi for intrusion detection, writing 10+ custom alert rules to detect unauthorized access and network anomalies, achieving 95% detection accuracy for simulated attacks.
- Configured PiVPN with WireGuard for secure remote access, implementing AES-256 encryption and multi-factor authentication, reducing external breach risks by 50% for home network devices.

Education

University of Central Missouri, MS in Cybersecurity & Information Assurance Aug 2023 – May 2025

- **Coursework:** Cybersecurity Policies and Risk Management, Ethical Hacking, Computer and Network Forensics, Threat Intelligence and Incident Response, Web Applications Security, Design of Crypt Algorithms and Protocols, Introduction to Information Assurance

Rajiv Gandhi University of Knowledge Technologies, BTech in Computer Science and Engineering Aug 2016 – Oct 2020

- **Coursework:** Design and Analysis of Algorithms, Data Structures, Operating Systems, Database Management Systems, Network Analysis, Digital Logic and Design, Computer Networks, Artificial Intelligence, Compiler Design, Digital Image Processing, Applied Graph Theory, Unix and Shell Programming, Cryptography & Network Security

Certifications

- Microsoft Certified: Azure Fundamentals (AZ-900)
- CompTIA Security+ (SY0-701)
- Blue Team Level 1 (BTL1)
- CISSP (in progress)