Rama Ramana Sharma Parnandi

Columbus, Ohio | parnandi.2@osu.edu
linkedin.com/in/ramaparnandi | github.com/ramz-021002

Education

The Ohio State University Columbus, OH
Master of Science in Computer Science and Engineering *Expected May 2026*

- Relevant Coursework: Software Security, Malware Analysis, Network Security, Software Engineering for AI

VIT-AP University India
Bachelor of Technology in CSE (Specialization in Networking and Security) *July 2024*

- Relevant Coursework: Cybersecurity, Digital Forensics, Secure Coding, Data Structures & Algorithms

Technical Skills

Security Tools: Suricata, Zeek, Snort, Wazuh, Ghidra, Volatility, Cowrie, Nmap, Wireshark, Burp Suite, angr, Qiling, Ghidra
Infrastructure: AWS, ELK Stack (Elasticsearch, Logstash, Kibana), OpenSearch, Docker, Kafka
Languages: Python, Java, SQL, C, Bash Scripting
Compliance & GRC: NIST Framework, ISO 27001, Threat Modeling, Risk Assessment

Experience

ICDT (Institute for Cybersecurity & Digital Trust) Columbus, OH
Student Data Specialist *Feb 2025 – Present*

- Engineered the migration of the internal data from Flask/MySQL architecture to Django, leveraging Django ORM to optimize database performance and security.
- Designed automated Python scripts to sanitize and process sensitive financial datasets, reducing manual data handling risks and ensuring 99.9% reporting accuracy.
- Implemented Role-Based Access Control (RBAC) within the new Django architecture to strictly limit data exposure to authorized personnel.

CyberToolGuardian Remote
Security Researcher & Technical Content Lead *Sep 2023 – Present*

- Architected and documented full-stack security monitoring pipelines, integrating Zeek and Suricata logs into ELK Stack (Elasticsearch, Logstash, Kibana) for real-time threat analysis.
- Demonstrated advanced threat detection workflows, such as configuring Wazuh with Yara signatures (Valhalla) to identify and block polymorphic malware families.
- Published comprehensive technical guides on configuring OpenSearch and X-Pack security features, serving as a practical resource for security practitioners.

DigitalFortress Private Limited Amaravati, India
AI Security Intern *Dec 2023 – Jun 2024*

- Conducted threat modeling on AI/ML pipelines to identify vulnerabilities such as model inversion and data poisoning attacks.
- Researched and documented emerging Artificial Intelligence security risks to update the organization's internal security posture and defense strategies.

CyRAACS™ Bengaluru, India
GRC Intern *Nov 2023 – Feb 2024*

- Assisted in conducting organizational risk assessments aligned with NIST and ISO 27001 standards to identify compliance gaps.
- Executed Data Localization audits and RBI-mandated compliance checks, ensuring regulatory adherence for financial data sovereignty.

Projects

Automated Network Forensics & Visualization Tool | *Python, PcapXray, Zeek*

- Developed Pcap Xray v2, a network forensic automation tool that parses PCAP files to generate interactive topology graphs of network traffic.
- Integrated ISP geolocation and threat intelligence feeds to automatically flag malicious actors and visualize attack vectors within the traffic map.

Automated Threat Detection & IPS Engine | *Python, Suricata, AbuseIPDB*

- Engineered a Python-based automation tool that queries threat intelligence APIs to identify malicious IPs and dynamically updates Suricata blocking rules.
- Deployed as an active Intrusion Prevention System (IPS) to block emerging network threats in real-time.

Enterprise SIEM Deployment | *HELK, Kafka, Docker, Winlogbeat*

- Deployed a Hybrid ELK (HELK) stack to simulate an enterprise SOC; configured ElastAlert to detect Active Directory attacks (e.g., Zerologon) via log correlation.