Raghav Rathi
Phone: (850) 284-2292 | Email: raghav_rathi@outlook.com
https://raghavrathi10.github.io/

PROFESSIONAL EXPERIENCE

Cyber Security Engineer | Florida Department of Children and Families   January 2025- Present
- Lead Incident Response activities by investigating, containing, and remediating security incidents using Microsoft Sentinel (KQL), Microsoft Defender, SentinelOne, ExtraHop, Intune, and threat intelligence from Recorded Future.
- Execute organization-wide phishing simulations and security awareness campaigns to improve user resilience.
- Perform malware triage and analysis using Recorded Future Sandbox and Kali Linux to identify root causes and attacker TTPs.
- Develop and tune analytic rules and automation playbooks in Azure Sentinel to reduce false positives and improve SOC efficiency.
- Conduct Red Team and adversary emulation activities using Atomic Red Team and Caldera against the environment defenses.
- Configure and maintain enterprise security tools, deploy new capabilities, and lead PoCs for security products.
- Assist with SSO integrations and identity-related security controls.
- Perform application security testing using Rapid7 InsightAppSec, including SAST and DAST scanning, vulnerability analysis, and remediation guidance across multiple web applications and collaborate with development teams for remediation.

Research Assistant | Department of Computer Science, Florida State University   *August 2019 – December 2024*
- **StarAngle: User Orientation sensing using Starlink Beacons ([Published])** - Engineered a custom hardware receiver for Starlink satellite signals and developed a signal processing software, achieving high-precision user orientation sensing with a median error of only 7.5 degrees. [Funded by NSF]
- **2-Pipe: Simultaneous Downlink Transmissions in LoRa ([Published])-** Designed and engineered a novel network protocols for LoRaWAN, increasing channel capacity by 166% through optimization of downlink traffic management.
- **TnB: Resolving Collisions in LoRa ([Published])-** Engineered a collision resolution protocol for LoRaWAN uplinks to mitigate network congestion, increasing system throughput and packet detection rates by 246% over existing industry standards. [Funded by NSF]
- **Intrusion Detection Using Deep Active Learning.**
- **Malware Classification and Detection using Data Mining.**

TECHNICAL SKILLS

Core Competencies

Incident Response • SOC Operations • SIEM • SOAR • Threat Hunting • Threat Intelligence • Penetration Testing • Malware Analysis • Digital Forensics • SAST • DAST • Vulnerability Management • SSO & IAM • Red Teaming • DLP • IDS/IPS

Tools & Platforms

- **Security Tools**: Microsoft Sentinel (KQL), Microsoft Defender, EntraID, SentinelOne, Palo Alto XSIAM, Palo Alto Expanse, ExtraHop, Recorded Future, Cisco ETD, Cisco WLC, Elastic (Kibana), Security Onion, Docker, Tanium, Upgaurd, ServiceNow.

- **Penetration Testing & Forensics**: Burp Suite, Nmap, Wireshark, Metasploit, John the Ripper, Hashcat, EnCase, Sleuth Kit, FTK Imager, SQLMap, Kali Linux, Commando VM, Procmon/Process Explorer

- **Web & Directory Security**: Active Directory, AD AuditPlus, Ffuf, Dirb, DirBuster, Wpscan

- **Reverse Engineering**: IDA Pro, Ghidra, radare2, GDB, Pwntools

Programming & Scripting

Python • C • C++ • MATLAB • JavaScript • Bash • PowerShell • SQL • Git

Certifications

- **CompTIA Security+**

EDUCATION

Doctor of Philosophy in Computer Science · *Florida State University*   *May 2020 – December 2024*

Master of Science in Cybersecurity · *Florida State University*   *August 2017 – December 2019*

Bachelor of Science in Computer Science · *RGPV, India*   *August 2012 – July 2016*

ACHIEVEMENTS AND INTERESTS

- Dean's Award for excellence in research and academics, 2023.
- Ted and Syauchen Baker Award for Excellence in Student Research, Fall 2023.
- Placed 1st in CyberCorps Division in 2023 JerseyCTF competition hosted by the NJIT.
- Former member of FSU Cybersecurity team (Nol3ptr).