RADHA PRABHAKARAN

SOC Analyst | Incident Response | Digital Forensics
Chicago, IL (open to relocation) | cybrad8@gmail.com
linkedin.com/in/radha-prabhakaran | github.com/Radha1008 | radha-prabhakaran.vercel.app

SUMMARY

SOC and digital forensics analyst with an M.A.S. in Cyber Forensics and Security. Administers Google Workspace security controls, MFA governance, and NIST-aligned compliance reporting as a Cybersecurity Automation Consultant, and runs OSINT investigations into credential fraud and AI-generated deepfake identities. Triaged over 2,000 alerts and tuned Elastic detection rules in a ten-week SOC lab cohort. Works memory captures and forensic images in Volatility, Magnet AXIOM, FTK Imager, and Autopsy, reconstructing Windows artifact timelines from registry, SRUM, prefetch, and event logs. Built Chain Reaction, a live attack-path simulator with ATT&CK-mapped chains and CI-tested Sigma rules. CompTIA Security+ expected Dec 2026.

SKILLS

- **SIEM and Detection:** Elastic SIEM (ELK Stack, Kibana), Splunk, Sigma, KQL, SPL, Zeek, Suricata, SentinelOne Singularity; alert triage, enrichment, severity classification, log correlation (Sysmon, SonicWall, Auditd, Osquery, FIM), detection rule tuning, false positive reduction
- **Incident Response and Digital Forensics:** incident response lifecycle, threat hunting, IOC analysis, MITRE ATT&CK mapping, lateral movement and credential misuse analysis, phishing and BEC investigation, containment, incident write-ups; FTK Imager, Magnet AXIOM, Autopsy, Volatility, E3, disk imaging, memory analysis, Windows artifact timelines, chain of custody
- **Identity and Access:** RBAC, MFA enforcement, least privilege, access governance, user account management, Google Workspace security administration, Active Directory
- **Networking and Traffic Analysis:** TCP/IP, OSI model, DNS, Wireshark packet analysis and filtering, Cisco networking
- **Vulnerability and Application Security:** vulnerability assessment, OWASP Top 10, WAF development, static code analysis (Bandit, CWE), SQL injection testing (SQLmap), API security
- **Governance, Risk, and Compliance:** NIST SP 800-53, NIST SP 800-171A, ISO/IEC 27001:2022, HIPAA, risk and gap analysis
- **Scripting and Platforms:** Python, Bash, SQL/MySQL, JavaScript, Git and GitHub Actions; Windows, Linux (Ubuntu, Kali), macOS, Google Workspace, Microsoft 365

PROFESSIONAL EXPERIENCE

Cybersecurity Automation Consultant, Gulf Coast Automation Group, LLC — Oct 2025 - Present
Remote: security administration, access governance, OSINT investigations, NIST-aligned compliance reporting

- Administer Google Workspace security controls across the organization, enforcing security policy and MFA governance to maintain access control and reduce attack surface
- Run open-source intelligence investigations on technical candidates, flagging credential misrepresentation and AI-generated deepfake identities before they reach client engagements
- Write and maintain internal security policy documentation and NIST-aligned compliance reporting

SOC Analyst Training Cohort (CyberPros to Success), Raices Cyber — Apr 2025 - Jul 2025
Ten-week intensive in a simulated SOC lab: Elastic SIEM, incident response, threat hunting, forensics

- Investigated and triaged over 2,000 security alerts in an Elastic SIEM environment, working each through enrichment, severity classification, and escalation
- Hunted across Sysmon, SonicWall, and Auditd/Osquery FIM logs to identify and report attacks including lateral movement, suspicious process execution, and credential misuse
- Tuned Elastic detection rule logic, thresholds, and event correlation to reduce repetitive false positives

Graduate Teaching Assistant, Illinois Institute of Technology — Feb 2025 - May 2025
Dept. of IT and Management, Introduction to Open Source Operating Systems

- Taught 48 students Linux and Windows administration, file permissions, and shell environments, and wrote the supporting course materials

Cybersecurity Intern, 247ERICPOINTCOM — Jun 2024 - Aug 2024
Remote: WAF development, requirements documentation, cross-functional collaboration

- Developed a web application firewall (WAF) prototype addressing the OWASP Top 10 and documented functional and threat-aware requirements with UML diagrams
- Led a 4-member remote team across time zones (Slack, Gather, Google Meet) and delivered project milestones on time

PROJECTS

Chain Reaction, Personal Project — Sep 2026 - Present

JavaScript, MITRE ATT&CK v20, Sigma, KQL, SPL, GitHub Actions

Live: radha1008.github.io/chain-reaction | Code: github.com/Radha1008/chain-reaction

- Built and launched a privacy-first web app showing how 24 everyday habits chain into 15 attack paths, and the cheapest link to break
- Mapped every chain step to MITRE ATT&CK v20, with a defender view of where each step could be detected
- Wrote 3 Sigma rules for Microsoft Entra ID sign-ins and Exchange Online: password-only logins from unknown devices, repeated failed passwords followed by a success, and inbox rules that hide security emails
- Built a GitHub Actions pipeline that validates each rule against SigmaHQ standards and sample logs, and converts the single-event rules to Sentinel KQL and Splunk SPL

Cyber Forensics Lab Series, ITMS 538 coursework, guided virtual labs — Aug 2023 - Dec 2023

FTK Imager, Magnet AXIOM, Volatility, DumpIt, E3, Autopsy, Wireshark

- Captured volatile memory with DumpIt and FTK Imager and analyzed it in Volatility and E3 to examine process trees, registry activity, and malicious executables; documented hidden and high-risk processes in a written report
- Reconstructed Windows user activity timelines from registry, SRUM, BAM/DAM, prefetch, and event log artifacts, and recovered deleted files from forensic disk images

Healthcare Management Database System, ITMS 528 Database Security (2-person team) — Feb 2025 - May 2025

Python, MySQL 8.0, Fernet encryption, bcrypt, TLS, RBAC, NIST SP 800-53, HIPAA

Code: github.com/Radha1008/healthcare-db-iit

- Applied NIST SP 800-53 controls in Python and MySQL: AC-2 RBAC with least privilege, AC-5 separation of duties, AC-7 account lockout, and AC-8 system use banner
- Encrypted PHI columns at rest with Fernet, hashed staff passwords with salted bcrypt, enforced TLS on all database connections, and tested with 1,000+ synthetic patient records generated with Faker

ADDITIONAL COURSEWORK PROJECTS

- **Phishing Detection OSINT App (group):** Python GUI that pulls and processes data from multiple APIs to flag phishing. github.com/Radha1008/custom-osint-application-iit
- **Source Code Analysis (group):** scanned an open source project with Bandit (static analysis) and mapped findings to CWE. github.com/Radha1008/source-code-analysis-iit

EDUCATION

Master of Applied Science, Cyber Forensics and Security — May 2025

Illinois Institute of Technology, Chicago, IL | GPA 3.90

Bachelor of Engineering, Electronics and Communication Engineering — May 2023

KCG College of Technology, Chennai, India | GPA 3.84

CERTIFICATIONS AND TRAINING

- **CompTIA Security+**, in progress — Expected Dec 2026
- **TestOut Cyber Defense Pro**, TestOut / CompTIA — Feb 2025
- **ISO/IEC 27001:2022 Lead Implementer course**, Intl. Cybersecurity and Digital Forensics Academy (ICDFA) — Feb 2026
- **ICS310: ICS Cybersecurity Foundations**, SANS OnDemand, 12 CPEs — Oct 2026
- **Script-Based Malware Analysis; AI Cyber Defense Ops**, Just Hacking Training — Aug - Oct 2026
- **Certified Ethical Hacker (CEH) course, Units 1-4**, Pearson — Sep 2026
- **SOC Core Skills**, Antisyphon Training — Apr 2025

COMPETITIONS, AWARDS, AND VOLUNTEERING

- **SentinelOne ThreatOps CTF**, WiCyS x SentinelOne, threat hunting in the Singularity Data Lake — Oct 2026
- **Sisterhood of the Traveling Packets CTF**, WiCyS x Flare x SANS, ranked 156th of the first 250 solvers — Aug 2026
- **WiCyS x Tenable CTF**, vulnerability management and web application scanning — May 2026
- **Scholarships**, SANS ICS Security Summit (SANS x Dragos, 1 of 8 awarded); WiCyS 2026 Conference — Jul 2026
- **Wireshark Workshop Winner**, IEEE WIE Global Tech Marathon; featured in IEEE WIE Magazine, Jun 2026 — Sep 2025
- **NCAE Cyber Games 2024 and 2025**, Midwest regional competitor — Mar 2025
- **Volunteer, Governance, Audit, and IAM**, Women in CyberSecurity (WiCyS) Chicago — Sep 2026 - Present
- **Treasurer and Event Planning and Coordination Lead, TEDxIllinois Tech**, Illinois Institute of Technology; event budget, vendor contracts, and sponsor coordination — Jan - May 2025