# SAI MANOJ KUMAR

Chennai, India | +91 9940389385 | manojsagadevan@gmail.com | linkedin.com/in/saimanojkumar

## PROFESSIONAL SUMMARY

Information Security Engineer with 11+ years across penetration testing, cloud security, DevSecOps, and AI/LLM security. Builds and ships production security tooling end-to-end — DLP browser extensions, MITM proxy interception, drift-detection platforms — not just audit findings. Currently focused on securing AI coding assistants and browser-based AI tools at IBM. Comfortable owning security programs independently: threat modeling, secure SDLC, SAST/DAST pipeline integration, and executive-level risk reporting.

## KEY PROJECTS — AI & PRODUCT SECURITY TOOLING

- Sentinel — Manifest V3 Chrome extension for DLP built across five phases (prompt/document inspection, data residency control, governance & managed policy, multi-site coverage, evasion resistance); shipped in three editions including a Teams edition with a Flask + SQLite manager-approval backend.
- Duskguard — Local MITM proxy + browser extension DLP tool preventing data leakage through internal AI coding assistants and browser-based AI tools; taken through a full internal innovation review.
- Drift Sentinel — Drift-detection platform (Flask, watsonx/Llama 3.3 70B, GitHub Enterprise) monitoring 70+ applications for post-approval code drift across image digest, SBOM, git SHA, and IaC checks; AI kept strictly advisory while a deterministic engine owns factual findings.
- Red-teamed an internal AI compliance assistant — identified a fabricated-reference-ID technique causing non-deterministic HIGH→LOW risk rating flips, and evaluated resistance to prompt injection and social-engineering-style authority pressure.

## EXPERIENCE

**Penetration Tester — AI & Security Innovation** | **IBM, Chennai** *Jun 2022 – Present*

- Lead AI & Innovation initiatives within IBM Consulting's security practice, designing watsonx/OpenAI and MCP-integrated tools that automate vulnerability triage, risk classification, and compliance reporting.
- Conduct black-box and grey-box penetration testing across IBM Consulting web applications and internal platforms using Burp Suite Professional.
- Run Security and Privacy by Design (SPbD) reviews and threat modeling sessions for enterprise applications.
- Reverse-engineered a custom AES-128-CBC encryption scheme end-to-end and built a Burp Suite Python extension to decrypt/re-encrypt traffic for continued testing.

**Senior Consultant — Application & Cloud Security** | **Cognizant Technology Solutions Pvt Ltd., Chennai** *Dec 2020 – Jun 2022*

- Led penetration testing and risk analytics engagements across web, mobile, and API platforms.
- Conducted AWS security assessments covering IAM governance, network controls, S3 data protection, encryption posture, and Infrastructure-as-Code reviews.

**Deputy Manager — Red Team & Security Operations** | **Axis Bank, Mumbai** *Apr 2019 – Dec 2020*

- Established and led a red-team capability, emulating real-world attacks against internet-facing services to validate defensive controls.
- Integrated SAST/DAST tooling into CI/CD pipelines and built risk & compliance dashboards for leadership reporting.

**Consultant — Application Security** | **Aujas Networks (Client: Axis Bank), Mumbai** *Nov 2017 – Mar 2019*

- Application security testing across web, mobile, thick-client, and web-services platforms, with emphasis on payment gateways and transactional flows.

**Senior Security Engineer** | **Newt Global India Pvt Ltd. (Client: Verizon), Chennai** *Nov 2016 – Nov 2017*

- Executed black-box and grey-box application security assessments; documented findings and verified fixes with engineering teams.

**Security Analyst / Junior Research Analyst** | **CSS Corp & Comodo Security Solutions, Chennai** *Apr 2014 – Oct 2016*

- Monitored security logs, analyzed vulnerabilities, and performed static malware analysis for threat research and detection signature development.

## SKILLS

**Offensive Security:** Burp Suite Pro, OWASP ZAP, penetration testing, threat modeling, red teaming

**Cloud / DevSecOps:** AWS (IAM, S3, EC2), Jenkins, GoCD, CI/CD security integration, Kubernetes, Docker, mitmproxy

**AI/LLM Security:** watsonx, OpenAI APIs, LangChain, MCP (Model Context Protocol), RAG pipelines, prompt injection testing, LLM governance, AI red-teaming

**AppSec Tooling:** Checkmarx, Veracode, Snyk, SonarQube, Nessus, Python, Flask, REST APIs

## CERTIFICATIONS

AWS Certified Cloud Practitioner | CCNA | eWPTX (Web Application Pentesting) | Multiple Bug-Bounty MVP recognitions

## EDUCATION

B.E., Computer Science & Engineering — GKM College of Engineering, Chennai (Aug 2010 – Mar 2014)