# Mohit Sharma

Punjab, India
+91 8847680164
makkuritz@gmail.com
linkedin.com/in/rinz0x0cruz • github.com/rinz0x0cruz • rinz0x0cruz.github.io

## Professional Experience

**Microsoft** — Hyderabad, India
**Security Researcher** | Microsoft Defender Vulnerability Management — June 2025 - Present

- Authored 9 of 10 ingestion and normalization specifications across 10+ products; resolved 100+ false-positive incidents and **reduced false-positive volume by 47%**.
- Triaged 100+ high-severity incidents and CVEs for exploitability and exposure; reproduced scenarios, debugged root causes, reviewed code, and closed detection-coverage gaps across Copy Fail (CVE-2026-31431), Dirty Frag / Fragnesia (CVE-2026-43600), and Shai-Hulud supply-chain activity.
- Designed and shipped a Remote Registry Security Configuration Assessment to General Availability across Windows 7-11 and Server 2016+, mapping MITRE ATT&CK and CIS controls and validating enterprise dependencies.
- Produced a hunt report and KQL queries for STORM-2230 during a five-day public-sector ransomware intrusion, correlating endpoint and identity evidence from credential theft through remote access, staging, and execution to support proactive containment.
- Built a machine learning-assisted CVE triage agent using a large language model, Model Context Protocol plugins, and Kusto integrations to generate standardized reports, tickets, and ready-to-merge fixes.

**Hacker4Justice** — Remote
**Volunteer OSINT Investigator** — June 2025 - June 2026

- Correlated aliases, personas, and cross-source evidence across 4,800+ suspect credentials, achieving a 23% positive-identification rate and producing law-enforcement referral packages under operational-security controls.

**Microsoft** — Hyderabad, India
**Security Researcher Intern** — May 2024 - July 2024

- Unpacked, debugged, and analyzed eight malware families through static and dynamic workflows using IDA Pro, Procmon and other Sysinternals tools, Wireshark, and an anonymized Model Context Protocol-enabled environment.
- Produced analysis artifacts and tuned YARA and behavioral detections, increasing coverage by 8-11% against the prior 30-day baseline, reaching a 3% final aggregate false-positive rate, and yielding 50K+ detections; automated VirusTotal feed analysis from about two hours to near real time.

## Projects & Research

**ExploitRank**
Go, vulnerability and threat intelligence | Momentum: fixed 5% review policy | GitHub | Live console
Engineered a dynamic, CI-refreshed console unifying KEV, NVD, EPSS, OSV, and GitHub across 1,000+ actors, 4,000+ malware/tools, 700+ ATT&CK techniques, 18,000+ relationships, and software supply-chain activity; developed Momentum to preserve a fixed analyst-review budget.

**Home Malware Analysis & SIEM Lab**
Security Onion, Windows, REMnux | Analysis and detection lab | Malscope
Built an air-gapped lab for static and dynamic malware analysis, SIEM telemetry, and detection engineering; developed Malscope to correlate IOCs and ATT&CK behavior and generate YARA and Sigma detections.

## Technical Skills

**Security Research & Exposure:** CVE triage, exploitability validation, root-cause analysis, proof-of-concept development, vulnerability management, patch and version analysis.
**Detection & Response:** KQL/Kusto, SIEM, EDR, XDR, Microsoft Defender XDR, YARA, Sigma, MITRE ATT&CK, incident response, threat hunting.
**Malware Analysis:** IDA Pro, Ghidra, x64dbg, Procmon, Sysinternals, Wireshark, REMnux, static/dynamic analysis, unpacking, debugging, fuzzing.
**Engineering & Automation:** Python, Go, C++, PowerShell, Model Context Protocol, CI/CD, Azure, AWS, Docker, Kubernetes.

## Education

**Chitkara University, Punjab** — 2021 - 2025
Bachelor of Technology (B.Tech), Computer Science & Engineering | CGPA: 9.25/10

## Certifications

ISC2 Certified in Cybersecurity (CC) | Microsoft Certified: Azure Cosmos DB Developer Specialty (DP-420)

## Languages

Professional English | Hindi | Japanese (JLPT N4)