INSIYAH BHATIA

Mumbai, India | +91 7021841172 | insiyahmbhatia@gmail.com | linkedin.com/in/insiyahbhatia | github.com/InsiyahBhatia

EDUCATION

K. J. Somaiya Institute of Technology 2023 – 2027

B.Tech, Artificial Intelligence & Data Science | Honors Specialization: Cybersecurity

EXPERIENCE

Cybersecurity Intern, Claidroid Technologies Pvt. Ltd. Jun 2025 – Jul 2025

- Built a data pipeline merging **747,000+ records** from three raw datasets into a single, clean schema. Engineered 151 features and used SMOTETomek resampling to fix severe class imbalance.
- Trained and validated a model on the processed data, reaching **95% accuracy**, and deployed it through a REST API with batch and health check routes.

LEADERSHIP

Joint Public Relations Officer, Society for Data Science (S4DS), KJSIT Jan 2025 – Present

- Organized KnowCode 3.0, a 36-hour hackathon with 100+ participants, coordinating logistics, communications, and cross-team scheduling.

PROJECTS

Detection Engineering & Threat Hunting Lab

Splunk · Sigma · YARA · Snort · Zeek · MITRE ATT&CK · AWS

- Investigated two real attacks in Splunk's BOTS v3 dataset (~2M events): AWS credential theft escalating to **576 attempted EC2 launches** across 15 regions, and an S3 misconfiguration serving a cryptominer to company employees.
- Authored detection rules across Sigma, YARA, Snort, and Zeek, CI-validated for schema correctness on every commit; mapped findings to **16 MITRE ATT&CK techniques** and tuned the Splunk dashboard against normal AWS background traffic.

AI Detection Engineering Assistant

n8n · Google Gemini · GitHub API · JavaScript · Sigma/SPL/KQL/Elastic DSL

- Built an automated n8n workflow that turns a plain-language detection use case into a complete detection package - MITRE ATT&CK mapping, Sigma rule, Splunk SPL, Microsoft Sentinel KQL, and Elastic Query DSL - via a Gemini-based AI agent.
- Added a second AI reviewer for quality assurance and a JavaScript validation layer that rejects incomplete or placeholder output before auto-publishing versioned Markdown/JSON reports to GitHub.

Threat Intel Agent - IOC Enrichment & ML Scoring Platform

Python · FastAPI · XGBoost · LightGBM · React · SHAP

- Built a platform that queries 4 OSINT sources (VirusTotal, Shodan, AbuseIPDB, OTX) in parallel and scores risk using an XGBoost + LightGBM ensemble, achieving **F1-macro ≈ 0.96** on a temporal split.
- Added SHAP explainability for every verdict and a Chrome extension for in-browser IOC lookup.

Active Directory Attack Lab - Privilege Escalation via RBCD

Active Directory · Kerberos · Impacket · Splunk · Kali Linux

- Simulated a full AD attack path - chaining Kerberoasting, credential reuse, and Kerberos delegation abuse - to escalate from a standard domain user to Domain Admin in a home lab environment.
- Mapped each step to MITRE ATT&CK and wrote Splunk SPL queries against the Windows Event IDs that flag this attack chain.

TECHNICAL SKILLS

- **SIEM & Detection:** Splunk, SPL, Sigma Rules, YARA Rules, Snort Rules, Zeek Scripts, Sysmon, Windows Event Logs
- **Automation & AI:** n8n, Google Gemini API, Prompt Engineering, GitHub API, JSON Schema Validation
- **Offensive Security:** Kali Linux, Nmap, Metasploit, Burp Suite, NetExec, Impacket, Ettercap
- **ML & AI Security:** XGBoost, LightGBM, scikit-learn, SHAP, Flask/FastAPI
- **Frameworks:** MITRE ATT&CK, MITRE ATLAS, OWASP Top 10, Active Directory, Kerberos
- **Languages:** Python, Bash, SQL, JavaScript, PowerShell, C/C++

CERTIFICATIONS

- TryHackMe - AI Security Level 1 Path · SOC Apprentice · Top 20%
- Developing Ethical Hacking Tools with Python - LinkedIn Learning
- Career Essentials in Cybersecurity - Microsoft & LinkedIn · Introduction to Cybersecurity - Infosys Springboard