

Aniket Sinha

Entry-Level Cybersecurity Analyst | SOC & DevSecOps Enthusiast | Threat Intelligence | Log Analysis | AI in Cybersecurity | TryHackMe | CyberDefenders | PortSwigger | WAPT |

Email: aksinha6572@gmail.com

Phone: +91 9780208759

LinkedIn: www.linkedin.com/in/anikets207

GitHub: <https://github.com/AniketS207>

SUMMARY:

Entry-Level Cybersecurity Analyst & Aspiring DevSecOps Engineer with hands-on experience in threat intelligence, log analysis, and AI-driven detection using Python and Streamlit. Familiar with SDLC, CI/CD principles, DevOps fundamentals and secure development methodologies. Practical knowledge of Sysmon monitoring, MITRE ATT&CK mapping, gained through hands on projects. Completed multiple labs on TryHackMe, PortSwigger & CyberDefenders to enhance skills. Strong in teamwork, communication, and problem-solving, with a keen interest in contributing to SOC operations, securing development pipelines and compliance initiatives.

TECHNICAL SKILLS:

- **Programming:** Python, C/C++, Java, JavaScript, SQL
- **Cybersecurity:** Threat Intelligence, SOC Monitoring, Incident Response, Log Analysis, Malware Detection & Mitigation, Risk Classification, OSINT, Vulnerability Scanning, WAPT, OWASP, Network Security, Active Directory, Reverse Engineering.
- **Tools, Technologies, Frameworks, Compliance:** Wireshark, Nmap, Burp Suite, Streamlit, Scikit-learn, Pandas, Plotly, SQLite, dotenv, SMTP, REST APIs, MITRE ATT&CK, Git, GitHub, Docker, Kubernetes, ISO(basic), NIST(basic), PCI-DSS(basic).
- **DevSecOps & Engineering:** SDLC, Secure Coding, CI/CD Fundamentals, DevOps Tools (Basic), UML Modeling (Basic).
- **Platforms & Environments:** Linux, Windows, Docker, Cisco Packet Tracer, AWS (EC2, S3), Firewalls (Configuration & Types), OS.

SOFT SKILLS:

Analytical Thinking, Problem Solving, Communication, Leadership, Collaboration, Time Management, Work Ethics, Speaking Skills, Documentation Skills (Word, Excel, PDF, Spreadsheets).

PROJECTS:

AI-Powered Real-Time Threat Intelligence Dashboard

[\[GitHub Link\]](#)

Tech Stack: Python, Streamlit, scikit-learn, Plotly, SQLite, SMTP, APIs

- Built an AI-driven dashboard to analyze and classify threat intelligence from multiple live sources, enabling real-time monitoring of suspicious IP activity.
- Integrated a machine learning based risk scoring system using Random Forest, triggering automated email alerts for high-risk threats via SMTP.
- Designed a robust logging and reporting system via SQ Lite with exportable CSV report and interactive country-wise threat visualizations to support security analysis using Plotly.
- Enabled secure integration for API key management using Dotenv and reusable Python components for scalable data processing.

AI-Augmented Real-Time Incident Response Simulator

[\[GitHub Link\]](#)

Tech Stack: Python, Streamlit, Sysmon, SQLite, scikit-learn, MITRE ATT&CK, Pandas, Matplotlib, SMTP

- Simulated real-time SOC operations by processing live Sysmon event logs into an interactive Streamlit dashboard for threat visibility and event correlation.
- Built a machine learning pipeline to classify security events by severity (Low, Medium, High), enabling automated risk-based triage.
- Integrated MITRE ATT&CK mappings to contextualize detection events and support threat attribution workflows.
- Automated email alerting and generated structured PDF reports with severity breakdowns, timelines, and mapped tactics to aid incident response.

EDUCATION:

Chitkara University – Rajpura, Punjab (2022-26)

B.E CSE - 7.4 CGPA

ST Peter's Sec School – Chandigarh (CBSE 2021)

12th | 86 %

AKSIPS 41 – Chandigarh (CBSE 2018)

10th | 87.2 %

CERTIFICATIONS:

CCNA TRAINING: CISCO, Issued May 2025

[\[Link to Certificate\]](#)

Introduction to Cybersecurity Tools &

[\[Link to Certificate\]](#)

Cyberattacks : IBM, Issued January 2025

Computer Networks and Network Security:

[\[Link to Certificate\]](#)

IBM, Issued February 2025

Cybersecurity Compliance Framework,

[\[Link to Certificate\]](#)

Standards & Regulations: IBM, Issued January 2025

ROLES OF RESPONSIBILITY: Open Source Chandigarh, CyberSecurity Team — Team Member

[\[Link to Letter Head\]](#)

Contributed to Cyber Team by organizing workshops, group learning sessions, and completing TryHackMe's Advent of Cyber 2023.