Siddh Samarth

+91-7461956057 | siddhsamarth@gmail.com | LinkedIn

EDUCATION

Birla Institute of Technology, Mesra   2021 - 2025
Bachelor of Technology in Computer Science and Engineering
CGPA: **6.84**
IIT Guwahati
Cyber Security Training Programme   2024-2025
Relevant Courses: Operating System, Database Management System, Cryptography and Network Security, Object Oriented Programming, Oswap Top 10

TECHNICAL SKILLS

Programming Languages: Python, Bash, SQL, PowerShell
Libraries: TensorFlow, Pandas
IT skill: Network Analysis, Malware Analysis
Tools/Technologies: Azure-Sentinel, AndroGuard, Nmap, Wireshark, Nikto, Nessus, Hashcat, Aircrack-ng, n8n

EXPERIENCE

IIT Patna   May 2024 – July 2024
Code Vulnerability Analytic and Research Intern
- Conducted symbolic and concolic execution on Solidity smart contracts and explored emerging tools to identify and mitigate vulnerabilities.
- Utilized large language models (LLMs) and researched advanced techniques to enhance smart contract security.

Teachnook   Jan 2024 – Feb 2024
Trainee & Intern
- Gained expertise in network security and malware analysis, including identifying and mitigating potential threats.
- Learned and applied techniques for analyzing malware behavior and understanding network vulnerabilities.

SELECTED PROJECTS

Network Analysis
- Acquired hands-on experience with **Wireshark** for **network traffic analysis**, including packet capturing, filtering, and protocol analysis.
- Gained knowledge in detecting network anomalies, performing traffic visualization, and utilizing cybersecurity tools to enhance security measures. and understanding network vulnerabilities.

SIEM Investigation Using Azure Sentinel   (*GitHub*)
- Engineered end-to-end incident detection and response workflows in Microsoft Azure Sentinel, simulating a Solorigate network beacon attack, normalizing multi-source telemetry via ASIM, and crafting advanced Kusto Query Language (KQL) queries for **real-time threat hunting**.
- Designed and fine-tuned analytic rules, bookmarks, and **Threat Intelligence** integrations, aligned with **MITRE ATT&CK**, to reduce false positives, accelerate triage, and streamline forensic handover.

Certifications
- Foundations of Cyber Security
- IIT Patna Internship certificate
- Teachnook internship certificate
- Tools of trade: Linux & SQL
- POST GRADUATE PROGRAM IN CYBER SECURITY

SOCIAL SERVICE

Dristi NGO. Deoghar Chapter   Aug 2022 – Aug 2024
Documentation Head
- **Volunteered with Drishti NGO**, contributing to various initiatives during the first year.
- Promoted to **Head of Documentation**, where I managed a team and oversaw all documentation processes, ensuring accuracy and effective communication.