

MOHAMMED ASLAM

Cyber Threat Intelligence Analyst || Full Stack Developer

✉ mhdaslmnzs@gmail.com ☎ +91 95393 33732 💻 mhdaslmnzs 📧 mhdaslmnzs 📍 INDIA

Profile

Cyber threat intelligence analyst and full stack developer offering 1+ years of experience providing **customized threat intelligence solutions**. Instrumental to the **establishment and growth of the CTI team from scratch** - contributed to the Threat Intel Platforms, monitoring threat intel and processes independently developed the CTI dashboard, and contributed to investigative research reports. Built internal web apps to improve team efficiency by **60%**, mentoring 12+ junior analysts, and delivering **100+** high-impact threat landscape assessment reports. Passionate about leading threat intelligence teams and building comprehensive cyber defense strategies through both strategic analysis and technical solutions. Eager to take on leadership roles, expand capabilities, and help secure critical systems at forward-thinking organizations.

Professional Experience

Cyber Threat Intelligence Analyst, EY Global Delivery Services

Oct 2022 - present | Kochi, India

- Expanded client base by **500% (12+ new clients)** via successful execution of 30+ high-profile security risk assessments, proofs-of-concept, and RFPs/RFIs for international organizations like reserve banks, international summits, conglomerates, energy leaders, stock exchanges, and aviation companies.
- Developed & implemented innovative solutions to streamline CTI operations, **boosting team efficiency by 60%**:
 - **Independently designed & developed internal CTI web dashboard** (NextJS/Python), monthly threat analysis tool, and threat scoring Power BI application.
 - Built various web crawlers (Python) to automate data collection from open sources, Telegram, and deep/dark web.
 - Created innovative scripts for comprehensive OSINT and darknet analysis during a **650+ vendor assessment**.
- Enriched threat intelligence gathering & reporting:
 - Spearheaded **continuous asset & brand monitoring, tailored one-time assessments**, and third-party vendor/tool assessments across APAC, the Americas, and the Middle East.
 - Enriched IOCs from diverse sources through automation, generating malware assessments for **targeted threat intelligence & red teaming reports**.
- **Mentored 12+** analysts on threat intelligence & MITRE best practices, ensuring high-quality client delivery and solutions.

Data Analysis Consultant Intern, KPMG Corporate Finance LLC

Jun 2020 - Jul 2020 | Virtual

- Completed virtual task modules in data quality assessments data insights and presentation
- Solved virtual data tasks in data insights

Skills

- **Cyber Threat Intelligence:** Open Source Intelligence | MITRE ATT&CK | Dorking | Automation | Continuous Asset Monitoring | IOC Collection and Management | POC and evaluation | Documentation and Reporting | Threat, Vulnerability and Risk Assessment, Analysis and Mitigation | Darkweb Crawling | Security Assessments and Audits | Third Party Vendor Security Audit | Investigative research and Analysis
- **Tools:** ThreatQ | Digital Shadows | SpiderfootHx | Shodan | MISP | Threat Miner | Censys | Penetration testing Burp Suite | Microsoft Excel PowerPoint | Kali Linux and tools | Maltego | Cyble | Virustotal | AlienVault
- **Development:** Python Scripting and Automation | MySQL | MERN Stack + NextJS | Flask | Django | Digital Ocean | AWS | Azure | ML | Powerbi | Docker | CosmosDB
- **Soft skills:** Leadership | Collaboration | Communication | Adaptability | Problem-solving | Analytical skills | Critical Thinking |
- **Languages:** English | Malayalam | Hindi | Tamil | Arabic | German

Education

Bachelor of Technology, Computer Science and Engineering,

Jul 2018 - May 2022 | Kochi, Kerala, India

COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

- **CGPA: 8.07**
- Organiser Spaceup CUSAT 2022 | Reboot Kerala Hackathon, State-level participant 2020

Achievements & Awards

EY Appreciate Spot Award, EY

May 2023

EY Appreciate Pursuing Innovation Award, EY

Oct 2023

Certificates

Foundations of Operationalizing MITRE ATT&CK (AttackIQ) | Network Security Associate 1 (Fortinet)

Foundation Level Threat Intelligence Analyst (arcX)