MOHAMMED ASLAM
Cyber Threat Intelligence Analyst

✉ mhdaslmnzr@gmail.com 📞 +91 95393 33732 in mhdaslmnzr 🔗 mhdaslmnzr.space ⬡ mhdaslmnzr 📍 INDIA

Profile

Innovative Cyber Threat Intelligence Analyst and Full Stack Developer with about 2 years of experience in delivering **customized threat intelligence solutions**. Instrumental in expanding the CTI team from inception, contributing to the setup of the **Threat Intelligence Platform, Threat Intel Monitoring Platform** (continuous asset & brand monitoring), and **Threat Research Reports** (developed Standard Operating Procedures) and use case creation for CTI disciplines. Expertise in OSINT, dark web monitoring, and research report generation, collaborating with cyber teams to support effective decision-making and mitigation strategies. Thrice awarded for proactive and innovative mindset. Passionate about **leading teams**, implementing strategic analysis, and building **robust cyber defense strategies**. Dedicated to making the invisible visible by decoding threats and strengthening defenses across regions and sectors. Eager to undertake leadership roles and contribute to securing critical systems at forward-thinking organizations.

Professional Experience

Cyber Threat Intelligence Analyst, *EY Global Delivery Services*   Oct 2022 – present | Kochi, India

Leadership & Team Management:
- Led CTI team operations overseeing delivery, quality assurance, and work allocation.
- Instrumental in expanding client base by over 500% in under 2 years.
- Mentored 20+ analysts on CTI principles, OSINT, Threat Modeling in MITRE ATT&CK framework, malware campaign tracking, and Cyber Kill Chain, Cyber Risk and Threat Identification, investigative mindset, APTs, Zero days, and best practices.
- Managed a team of 5 analysts in conducting a comprehensive third-party vendor risk assessment for a client with 650 vendors.

Threat Intelligence & Analysis:
- Led the delivery of TIP, TIM, and Research reports through OSINT and Deep/Dark web surveillance.
- Led OSINT investigations creating Social Media, Darknet Marketplace, and ransomware site analyses.
- Proactively monitored internal and external landscapes for relevant events, risks, and threats.

Technical Innovations:
- Independently developed an internal CTI dashboard (NextJS/FastAPI-Python), monthly threat analysis tool, threat-scoring Power BI application, and various scrapers for automation.
- Developed and implemented an OSINT lab in Kali Linux, automating nearly 50% of investigative tasks, using self-developed scripts for domain/IP investigation.
- Developed scripts for automated IOC extraction from URLs, and supported the development of various scripts for IOC bulk update, filtering, and enrichment in the TIP.
- Led a Proof of Concept to develop a Generative AI tool for automating CTI reporting and alert classification.

Strategic Contributions:
- Spearheaded CTI operations leading to the recovery of almost 70% of investment through successful project executions across APAC (Oceania) and EMEA sectors.
- Created SOPs for threat research reports, use case development, and case studies for RFPs following RFIs.
- Contributed to effective migration of Threat Intelligence Platform (TIP) between vendors. Conducted various POCs for new vendors, owned and managed threat intelligence tools, product contracts, and relationships.
- Participated in red teaming activities, providing detailed TTPs and scenario creation collaborating with SOC, Incident Response, and threat hunting team.
- Facilitated onboarding for new clients to all CTI services and oversaw smooth delivery.

Skills

- **Cyber Threat Intelligence:** OSINT | HUMINT | MITRE ATT&CK(Threat Modelling) | Threat Intel Monitoring | IOC Collection and Management | Threat, Vulnerability, and Risk Assessment, Analysis, and Mitigation | Third-Party Vendor Security Risk Assessment | Malware Analysis | Investigative Research, Identification, Analysis, Documentation, & Reporting
- **Tools:** Kali Linux| Microsoft Excel, PowerPoint | MISP | Penetration testing - Burp Suite | Cyble | ThreatQ | Digital Shadows
- **Development:** Python | NextJs - React | Tailwindcss | NodeJs | FastAPI | Flask | Django | Digital Ocean | AWS | Azure | Machine Learning | Artificial Intelligence | Generative AI | Powerbi | Docker | CosmosDB | MySQL
- **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

Certificates

Azure Fundamentals ⬀ — *Microsoft* | **Foundation Level Threat Intelligence Analyst** ⬀ — *arcX* |
Foundations of Operationalizing MITRE ATT&CK ⬀ — *AttackIQ* | **Generative AI Overview for Project Managers** ⬀ — *Project Management Institute* | **Certified Sales Associate, Certified Solutions Engineer** ⬀ — *Cyble* | **Network Security Associate 1** ⬀ — *Fortinet* | **Developing Ethical Hacking Tools with Python** ⬀ — *Cybrary*