MOHAMMED ASLAM

Cyber Threat Intelligence Analyst

mhdaslmnzr@gmail.com | +91 95393 33732 | 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. Awarded 3 times in a row 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, Cyber Kill Chain, Cyber Risk and Threat Identification, Investigative Mindset, APTs, Zero days, and best practices.
- Managed a team of analysts in conducting a comprehensive Third-party Vendor Risk assessment for a client with 650 vendors.

Threat Intelligence & Analysis:

- Spearheaded the delivery of TIP, TIM, and Research reports through OSINT and Deep/Dark web surveillance.
- Led OSINT investigations by effective analysis of Social Media, Darknet Marketplace, and Ransomware sites.
- Proactively monitor 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 Web Scrapers for Automation of data collection and visualization.
- Developed and implemented an OSINT lab in Kali Linux, automating nearly 50% of investigative tasks, using self-developed scripts for domain/IP investigation.
- Curated scripts for automated IOC extraction from URLs, and contributed to 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.
- Drafted SOPs for Threat Research Reports, Use Case development, and Case Studies for RFPs following RFIs.
- Pioneered the successful migration of the Threat Intelligence Platform (TIP) between vendors, conducting proofs-of-concept for new solutions while managing threat intelligence tools, product contracts, and vendor 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.
- Drafted custom curated intelligence solutions for diverse sectors, enabling intelligence-driven decision-making.

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 / Supply Chain Security Risk Assessment | Malware Analysis | Investigative Research, Identification, Analysis, Documentation, & Reporting
- **Sectors:** Banking, Financial Services, Insurance | Energy, Oil & Gas, Power Plants, Nuclear, Electricity, Critical Infrastructure | Aviation | Healthcare | Biotech & Pharma | Retail | Conglomerate | Food & Beverages | Agriculture | Telecommunication
- **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 | Bash | Powershell
- **Languages:** English | Malayalam | Hindi | Tamil | Arabic (Basic) | German(Basic)

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*