M. Masoom Alam, Ph.D.

mmalam@Cytomate.net | masoom.alam@comsats.edu.pk |

Cytomate.net | YouTube

Cybersecurity Entrepreneur | Co-Founder @ Cytomate |
Tenured Professor (Cyber Security) | AI & Innovation Strategist |
Product Visionary

1 Mission Statement

As a cybersecurity entrepreneur and **Co-founder of Cytomate**, I lead the development of AI-driven solutions, including Breach & Attack Simulation, Cyber Deception, and Battle Twin simulations, to empower global enterprises and governments with resilient defenses against advanced threats. On sabbatical from a tenured academic role at COMSATS University Islamabad, I am dedicated to mentoring startups in entrepreneurship programs, fostering innovation through my expertise in ideation, AI integration, and strategic product development, aiming to bridge research and commercialization for transformative global impact.

2 Industry Experience

2.1 Chief Technology Officer and Co-Founder, Cytomate, Doha, Qatar

08/2022 – Present

As co-founder and CTO, I established Cytomate as the MENA region's first offensive cybersecurity company, headquartered in Doha, Qatar, delivering cutting-edge AI-driven solutions for threat intelligence and security posture analysis Cytomate.net. I spearheaded the creation of the Cytomate Lab, recruiting elite researchers (Red Teamers, SOC Analysts, Deception Experts, Reverse Engineers) and securing multi-million-dollar funding from Qatar Development Bank. My leadership drove high-profile showcases at Web Summit 2023 and BlackHat MEA 2023, positioning Cytomate as a regional leader. By addressing challenges in AI integration, scalability across hybrid cloud environments, and market adoption, I cultivated a transformative product ecosystem through a structured ideation process leveraging *Design Thinking, TRIZ, SCAMPER, Lean Startup, PDCA, Mind Mapping*, and *SWOT Analysis*, as highlighted in my GISPP talk (YouTube, GISPP).

- ***Ideation and Innovation in Cybersecurity***: Developed a pioneering course aligned with Cytomate's mission, teaching advanced innovation frameworks such as **Deep Impact**, which outperforms the Gartner Hype Cycle by integrating predictive analytics and risk assessment. My lecture at the *University of Doha for Science and Technology (UDST)* inspired a white paper on **Deception-as-a-Service (DaaS)**, proposing AI-driven deception to neutralize Advanced Persistent Threats (APTs) (LinkedIn). I envisioned **AI adoption across the GCC**, revolutionizing cybersecurity through scalable cloud-based solutions that eliminate the need for costly hardware, detailed in a LinkedIn white paper (LinkedIn). I founded **AlKhwarizmi Tech Labs**, a platform for *Idea-as-a-Service*, fostering collaborative ideation and accelerating cybersecurity innovation (AlKhwarizmi Tech Labs). My GISPP talk, referencing cases like Binarly Firmware Security, has empowered professionals to drive innovation, reinforcing my thought leadership.

- **Breach+ (Breach & Attack Simulation Platform)**: Conceived Breach+ to emulate MITRE ATT&CK-aligned cyberattacks, including malware, ransomware, and lateral movement, with AI-driven Tactics, Techniques, and Procedures (TTP) emulation. Achieved an 80% compliance increase for Qatar SMEs by integrating lightweight agents for hybrid environments. Overcame market skepticism through client pilots and **Revenge**, a reverse engineering brand for analyzing APT groups' malicious processes, delivering detailed threat reports (Cytomate.net, LinkedIn).
- **Sarab (Cyber Deception Platform, Launched November 2023)**: Ideated Sarab to deploy sophisticated decoy networks with fake Active Directory domains and honeypot files, reducing attack success rates by 70%. Innovated VLAN-based scalability and machine learning to minimize false positives, validated through MITRE-aligned testing. Drove adoption across financial sectors with compelling case studies (Cytomate.net).
- **NextGen-ASM (Attack Surface Management, Launched November 2023)**: Envisioned a real-time asset monitoring platform integrating dark web surveillance and phishing detection. Solved data overload with AI-driven prioritization algorithms, reducing alert fatigue by 60%. Showcased at BlackHat MEA 2023, gaining traction among GCC enterprises (Cytomate.net).
- **SnipeX (AI WAF Testing)**: Developed polymorphic payloads to bypass Web Application Firewalls, targeting vulnerabilities like SQL injection and XSS. Leveraged adversarial machine learning to enhance AI adaptability, achieving a 90% bypass rate in post-Equifax breach demonstrations (Cytomate.net).
- **Battle Twin (OT Security Simulation)**: Ideated a virtual ICS/SCADA simulation to test cyberattacks on Operational Technology systems. Overcame OT complexity through reverse engineering and digital twin technology, enabling proactive defense strategies adopted by critical infrastructure sectors (Cytomate.net).

2.2 Past Industry Roles

- **Trillium InfoSec, Pakistan** (Collaborator, 2016 – 2021): Ideated T-Eye, a honeypot-based threat intelligence platform that enhanced threat detection for Bank Al Habib and SNGPL. My contributions earned APICTA and PASHA Awards (2016) by integrating real-time analytics and deception technologies (LinkedIn).
- **Wanclouds Inc., USA** (Collaborator, 2016 – 2018): Developed Shepherd, a patented container security controller that fortified cloud-native environments against unauthorized access. My work on secure orchestration was critical to its adoption by enterprise clients (Link, LinkedIn).
- **Samsung (SISA), USA** (Collaborator, 2009 – 2011): Extended SELinux for mobile security, enhancing kernel-level protections for Android devices. My contributions resulted in a US patent (US8051459), strengthening Samsung's mobile security framework (US8051459, LinkedIn).
- **Patents Submitted**: Internet of Models (IoM) for decentralized AI systems (USPTO 18484664), Battle Twin for OT Security, and Malware Evolution frameworks, advancing proactive cybersecurity (LinkedIn).

3 Academic Experience

3.1 Tenured Professor (on Sabbatical), COMSATS University Islamabad

07/2022 – Present

Transformed the Cyber Security Lab into a leading industry-oriented research hub, securing over PKR 68 million in funding through grants and partnerships with Trillium InfoSec and Wanclouds. I led the development of T-Eye, a threat intelligence platform adopted by major banks like Bank Al Habib, by mentoring researchers and securing industry grants. My R&D frameworks and cross-functional team leadership bridged academia and industry, as showcased in my GISPP talk (YouTube, LinkedIn). My teaching inspired over 200 students to pursue cybersecurity innovation, fostering a new generation of researchers.

- **Key Projects**:
  - **T-Eye Threat Intelligence Platform** (HEC, PKR 14M, Closed in 2021): Directed AI-driven threat intelligence using honeypot analytics, enabling real-time detection of advanced threats for financial institutions (LinkedIn).
  - **Cyber Threat Intelligence Platform** (National ICT, PKR 40M, Completed): Delivered a scalable threat detection system for utilities, integrating machine learning to enhance response times by 50% (LinkedIn).
  - **Post-Quantum Cryptographic Protocol** (US Patent Granted): Led the development of a quantum-resistant protocol using lattice-based RSA, ensuring future-proof security for critical systems (US20190116035A1).
- **Courses**: Secure & Trusted Computing, Advanced Network Security, Post-Quantum Cryptography. Designed curricula that blended theoretical rigor with practical applications, preparing students for industry challenges.

3.2 Associate Professor, IMSciences Peshawar

2002 – 2013

Founded the MS Information Security program, establishing a robust curriculum that trained over 150 students in cybersecurity. Led the deployment of OpenERP (PKR 3.8M), streamlining institutional operations and enhancing data security (LinkedIn).

3.3 Supervision

- **PhD**: 1 completed (threat intelligence, focused on honeypot-based detection), 2 in progress (protocol verification for IoT security, reinforcement learning for threat prediction) (LinkedIn).
- **MS**: 20+ completed, covering topics like IOTA privacy frameworks, malware analysis, and blockchain security, with graduates securing roles in top firms (LinkedIn).

3.4 Selected Publications

- Shafeeq, S., et al. (2024). Last Line of Defense: Deception in SCADA Networks. *ResearchGate*. Proposed novel deception strategies for industrial control systems (Link).
- Saleem, A., et al. (2019). FESDA: Secure Data Aggregation in Smart Grid IoT. *IEEE Internet of Things Journal*. Enhanced IoT security with federated learning (Link).
- Shafeeq, S., et al. (2019). Privacy Aware Decentralized Access Control System. *Future Generation Computer Systems*. Developed a blockchain-based access control model (Link).
- Khan, T., et al. (2019). Proactive Cyber Threat Intelligence. *Journal of Parallel and Distributed Computing*. Advanced threat prediction using parallel computing (Link).

3.5 Awards

- APICTA Security Innovation Silver Award (2016): T-Eye Platform for innovative threat intelligence (LinkedIn).
- PASHA Security Innovation Award (2016): T-Eye Platform for industry impact (LinkedIn).
- RCCI ICT Security Innovation Award (2016): TRIAM Platform for cybersecurity advancements (LinkedIn).

- HEC Early Promotion to Associate Professor (2011): Recognized for academic excellence (LinkedIn).
- Best Ph.D. Thesis Award, ACM/IEEE MoDELS (2006): For groundbreaking work in model-driven security (LinkedIn).

4 Entrepreneurship Vision

As Cytomate's co-founder, I ideated and commercialized a transformative product ecosystem, overcoming technical and market challenges to establish a regional cybersecurity leader. My pioneering work in teaching ideation and innovation, using frameworks like **Deep Impact**, and founding **AlKhwarizmi Tech Labs**, has empowered startups to innovate. By mentoring entrepreneurs in programs across the GCC, I have guided ventures to secure funding and achieve market traction, bridging research and commercialization to drive global cybersecurity advancements.