Executive Summary

Cybersecurity Simulation and Predictive Detection Framework

Prepared by: **Alessandro Moreira – Senior Network & Cybersecurity Engineer**

Date: 2025

---

1. Objective

This project was developed as part of the MBA in Cybersecurity & Networking (defended and approved in 2025).

The primary objective is to provide a **modular and reproducible framework** for simulating cyberattacks, capturing network traffic, and applying **AI-based anomaly detection**.

The framework is designed to support:

- **Mergers & Acquisitions (M&A) due diligence** – identifying risks in legacy network assets and integration cutovers.

- **Corporate cybersecurity audits and training** – simulating real-world threats in controlled labs.

- **Critical infrastructure resilience** – providing early detection of anomalies in healthcare, logistics, and finance.

---

2. Framework Architecture

The solution integrates three modules:

- **Red Team (Attack Simulation):** Controlled execution of attacks such as IP Spoofing, SYN Flood, DNS Tunneling, and Incomplete TLS Handshake.

- **Blue Team (Traffic Analysis):** Wireshark/tshark and Scapy for automated packet capture and anomaly identification.

- **AI/ML Module:** Isolation Forest algorithm achieving >90% accuracy in distinguishing malicious vs. legitimate traffic.

---

3. Key Results

- Successfully executed multiple **Layer 3 and Layer 7 attacks** in controlled labs.

- Blue Team module flagged anomalies such as spoofed IPs, abnormal user-agents, and fragmented packets.

- Machine Learning detection reached **>90% accuracy**, confirming scalability for enterprise adoption.

- Demonstrated potential to **reduce cyber risks during M&A transitions**, ensuring network reliability and business continuity.

---

4. Impact & Applicability in the U.S.

- **M&A Projects:** Supports secure network integration and identification of unsupported (EoL/EoS) devices.

- **Corporate Use:** Enhances readiness through simulations, reports, and executive dashboards.

- **National Interest:** Applicable across U.S. sectors such as healthcare, financial services, logistics, and manufacturing.

---

5. Deliverables

- Open-source repository (MIT License): [GitHub – MBA-Cybersecurity](https://github.com/Alessandro-HCL/MBA-Cybersecurity)

- Technical documentation, screenshots, and sample anomaly reports.

- MBA validation: approved as a **capstone project** in Cybersecurity & Networking.

---

6. Conclusion

This framework demonstrates **academic merit**, **technical innovation**, and **practical impact**.

By making the code and methodology public, it provides **transparent, verifiable evidence** of capabilities that address U.S. national priorities in cybersecurity and digital resilience.

Prepared by:

Alessandro Moreira

MBA in Artificial Intelligence for Business

MBA in Cybersecurity & Networking

CCNP Enterprise | Cisco DevNet Certified | IEEE Member (2025–2026)