Combat Future AI-Powered Cyber Threats Using Digital Twin Simulations

Dr. Sander Zeijlemaker, Dr. Michael Siegel, Michiru Ishikawa, Dr. Abhishta Abhishta*, Yasir Hak*, Annet Chau

* = Technical University Twente (Netherlands)

1. Digital Twin (DT) Simulation Approach

Digital Twin technology allows to make a virtual replica of your organization and helps to explore for effective strategies through simulation (see Fig 1).

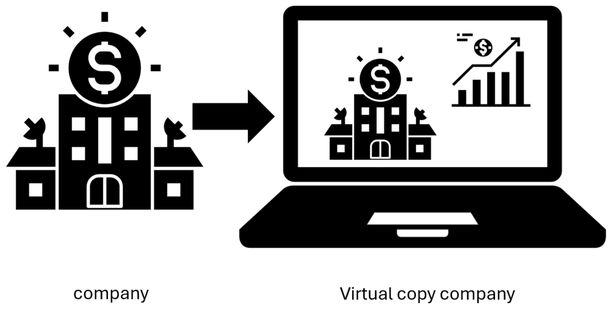

Figure 1. Concept of Digital Twin Technology

We repurposed proven simulation technology *(Jalali, et al., 2019)* and allowed security leaders to combat the ransomware threat with it.

2. Unlock Hidden Management Challenges

Security leaders digital twin simulation result (see Fig 2) :

- 50% struggle to find effective long-term strategies against ransomware.
- 50% required on average three full simulation attempts to find this strategy.

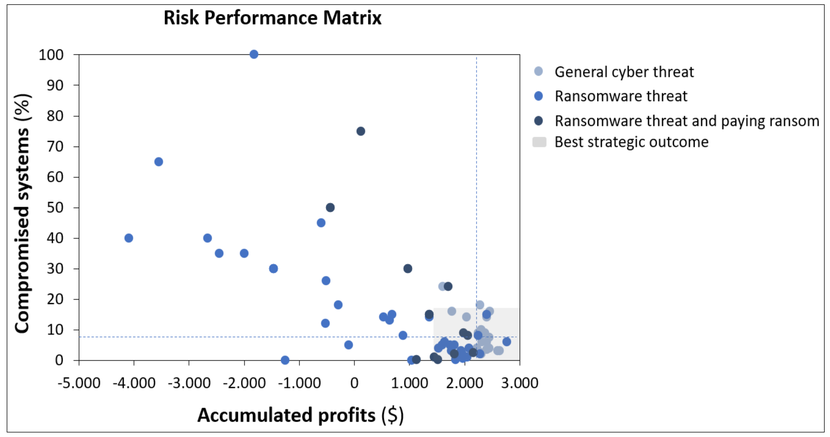

Figure 2. Simulation Results (after 5 years) by Security Executives.

3. AI-Powered Attacks Reshape The Threat Landscape

AI-powered attacks are on the rise and reshaping the threat landscape by e.g.:

- Misleading detection (e.g. Black Mamba).
- Adopting or blend in target system (e.g. Mylobot, Deeplocker).
- Exploiting vulnerabilities automatically and moving across the technology stack (e.g., Mimikatz, Stuxnet).

Evolving adversary tactics significantly increase the challenge to combat cyber threats.

4. Digital Twin Can Help to Anticipate this Difficulty

A DT simulation approach allows to replicate past and simulate future performance of a wide range of performance indicators relevant to cyber risk management

In future we want to tailor this machinery to get a detailed understanding about how to combat AI powered threats.

To play our ransomware *Simulation* scan the QR code

Use Google Chrome

SCAN ME

5. Malicious Software Repository Boost our DT

We have 650K+ malicious software samples scan results over 2006 – 2024 to boost adversarial behavior in our DT engine and we are still counting.

Jalali, M.S., Siegel, M., & Madnick, S., (2019). Decision-making and biases in cyber-security capability development : Evidence from a simulation game experiment. *The Journal of Strategic Information Systems, Volume 28*, Issue 1, March 2019, Pages 66-82.

6. Join our Project for a Tailored DT Case Study

Inquiries: msiegel@mit.edu, s.zeijlemaker@mit.edu