Enterprise detection & response strategy: *How strategic interventions prevented the capability trap: results from an anonymized case study*

Dr. Sander Zeijlemaker

1. Security Operations critical to cyber risk mgt.

The Security Operations Center (SOC) is critical to the detection and response strategy for managing cyber risk. The strategy is a plan with SOC implementation choices to optimize the organization's security posture.

Figure 1. Positioning SOC within the enterprise governance structure

2. Architecture of Security Operations Center

The SOC is a centralized function employing people, processes, and technology to continuously monitor and improve an organization's security posture while detecting, analyzing, and responding to incidents.

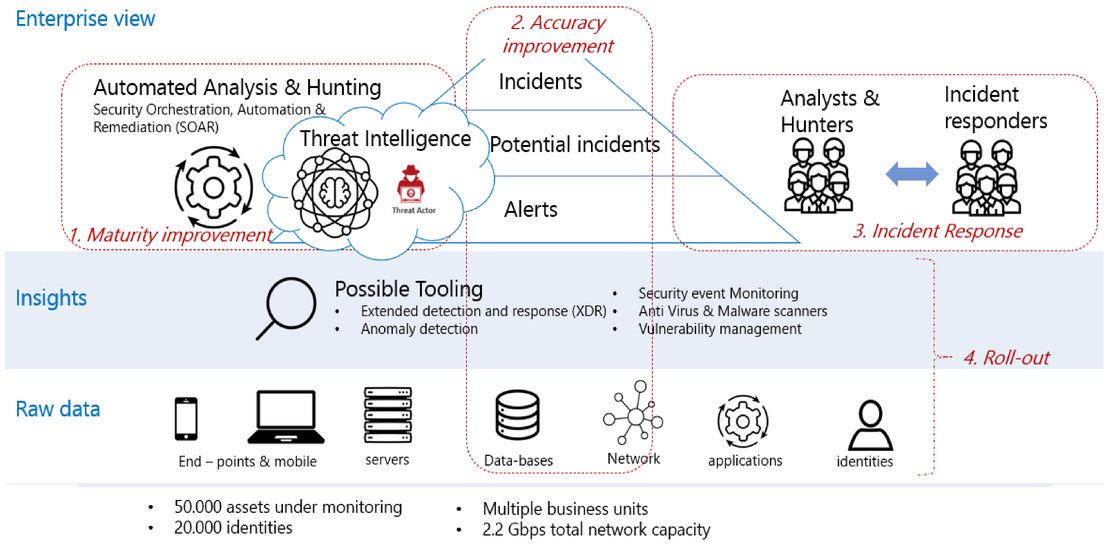

Figure 2. SOC architecture with 4 organizational priorities

3. Root cause analysis for increasing SOC costs

In recent years, the SOC forecast has been significantly overrun by its costs, affecting available funds for other essential security projects. We used a simulation-aided approach to learn why and applied a short-term focus (solving incidents) and a long-term focus (improvements) in our analysis.

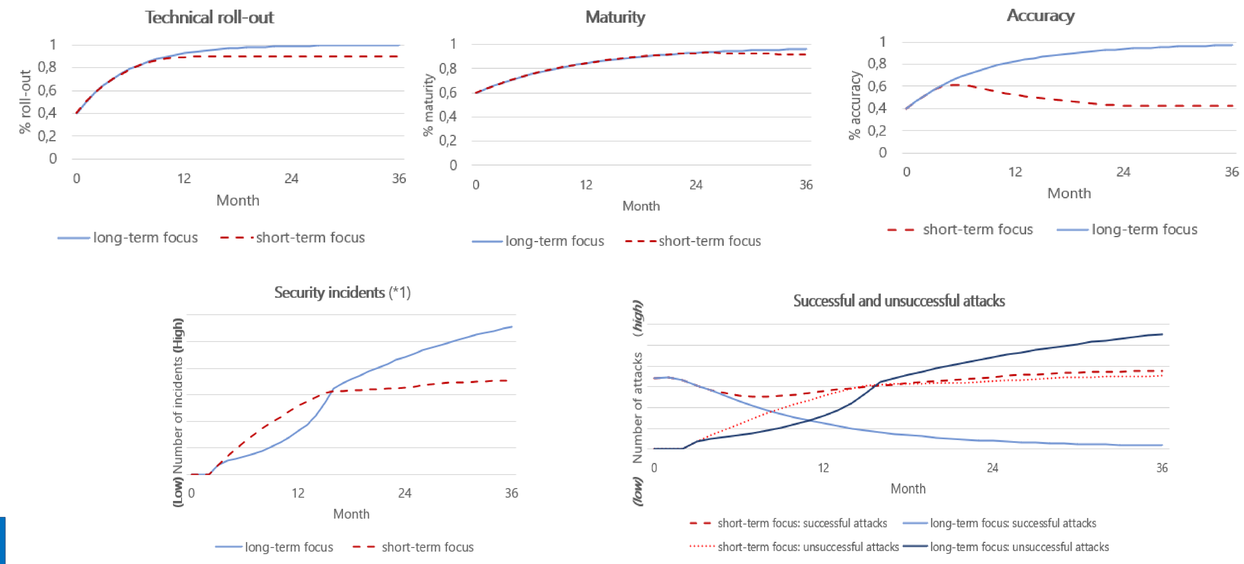

Figure 3. Simulation output on short- and long-term focus for the 4 priorities and attack behavior

4. Governance changes improve SOC performance

The SOC is susceptible to the capability trap. Short-term focus creates less and less time for improvement. Advanced attacks are detected less and less quickly, while remaining incidents take more time to analyze and resolve due to the absence of necessary ongoing improvements and roll-out.

Implemented changes to improve SOC performance (long-term focus) are:

- Change service agreements (from solution usage to response efforts).
- Create ongoing funding for improvement (mark-up) with dedicated resources (purple team).
- Create enterprise-wide projects to improve maturity (algorithm design & red teaming).
- Create continuous collaboration to improve accuracy (IT, SOC, security, and business).

Contacts: s.zeijlemaker@disem-institute.com