BUSINESS CASE

Maturity Model Evaluator

Understand where
your security posture
can be improved.

howest
university of applied sciences

UNIVERSITEIT GENT
CAMPUS KORTRIJK

ICIL4.0 WP3 BC

TABLE OF CONTENTS

INTRODUCTION

As part of our research, we have been looking into tools to help SMEs with a crucial pain point in their operational technology (OT) networks. Unlike servers, personal computers and other IT assets, it is rarely possible to install agents directly on industrial devices to identify weaknesses or gather telemetry. This lack of visibility makes it harder to understand risks and plan mitigations in the OT space. That is why we have been searching for an approach that allows SMEs to model their environments without intrusive agents, simulate attacks and understand where their security posture can be improved.

Tackle was developed to address this gap by enabling organizations to build a high-level overview of their industrial and office networks, see how attacks might unfold, and receive clear, actionable guidance on mitigating weaknesses.

Tackle was developed as part of an EU-funded research project by the Institute for Digitalization Aachen at FH Aachen University of Applied Sciences.

https://github.com/fhac-ida/tackle-simulator?tab=readme-ov-file

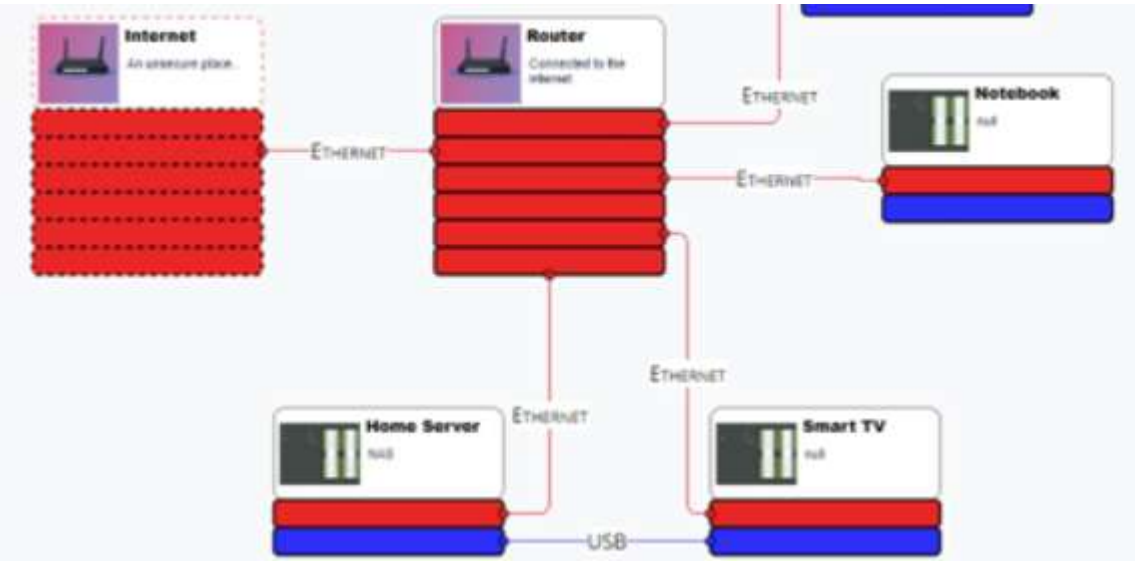
EXECUTIVE SUMMARY

Tackle is a web-based network simulator designed to help small and medium-sized enterprises (SMEs) evaluate and improve their security posture. Instead of focusing on the technology itself, it gives organizations a simple way to create a general overview of their industrial or office networks. By building a virtual version of their systems, users can identify potential weaknesses, see how different attack scenarios might unfold, and receive clear guidance on how to address these flaws.

The platform enables users to recreate their production environment using drag-and-drop maps, run simulated attack scenarios, and receive prioritized, practical mitigation advice based on their security maturity level. This business case summarizes the current product, highlights the most common weak points for SME users, and proposes concrete, prioritized measures to secure these weaknesses and to grow Tackle into a robust maturity-model evaluator product.

TACKLE

WHAT IS TACKLE?



Tackle is a web application that:

- Lets users model IT/OT networks as maps (devices as nodes, connections as edges).
- Collects organizational and personnel controls via a profile questionnaire to determine baseline maturity levels.
- Simulates attacker kill chains across mapped networks using selectable or custom attack scenarios.
- Produces visual and textual feedback per device and overall, including mitigation suggestions drawn from MITRE ATT&CK and qualitative effort metrics tailored to organizational maturity.

CORE VALUE PROPOSITION

- **Free, practical learning** for SMEs to discover realistic attack pathways.
- **Actionable remediation**: not just findings, but prioritized mitigations and didactic learning blocks that explain how to implement measures.
- **What-if analysis**: independently vary profiles and maps to quantify impact of changes such as password policy tightening or segmentation.

FEATURES & USAGE

Tackle provides three core interfaces that guide users through building a picture of their operational environment, analyzing it, and testing its resilience against cyber-attacks. Together they create a practical workflow for SMEs to understand and improve their OT security posture.

1. Profile – Establishing the Baseline

The first step for a user is to create or select a **Profile**. Instead of relying on automatic agents (which most industrial devices cannot run), Tackle uses a structured questionnaire to capture the organization's personnel and procedural security measures.

- The questionnaire can be completed in part or in full.
- Based on the answers, Tackle estimates a recommended security maturity level and applies sensible default settings for devices.
- Certain attack vectors are automatically excluded if the profile indicates that protective measures are already in place.
  All of this information is stored as a reusable profile.

2. Maps – Building the Digital Twin

After the profile is complete, users move on to creating one or more **Maps**. A map is a visual reconstruction of the actual production network: devices, connections, and configurations as they exist on the shop floor.

- Each device and connection stores the information needed to analyze which attacks would succeed.
- Maps can be combined with different profiles to see how organizational changes (for example, a new password policy) affect security outcomes.
- This separation of "map" and "profile" allows rapid what-if analysis without re-entering data.

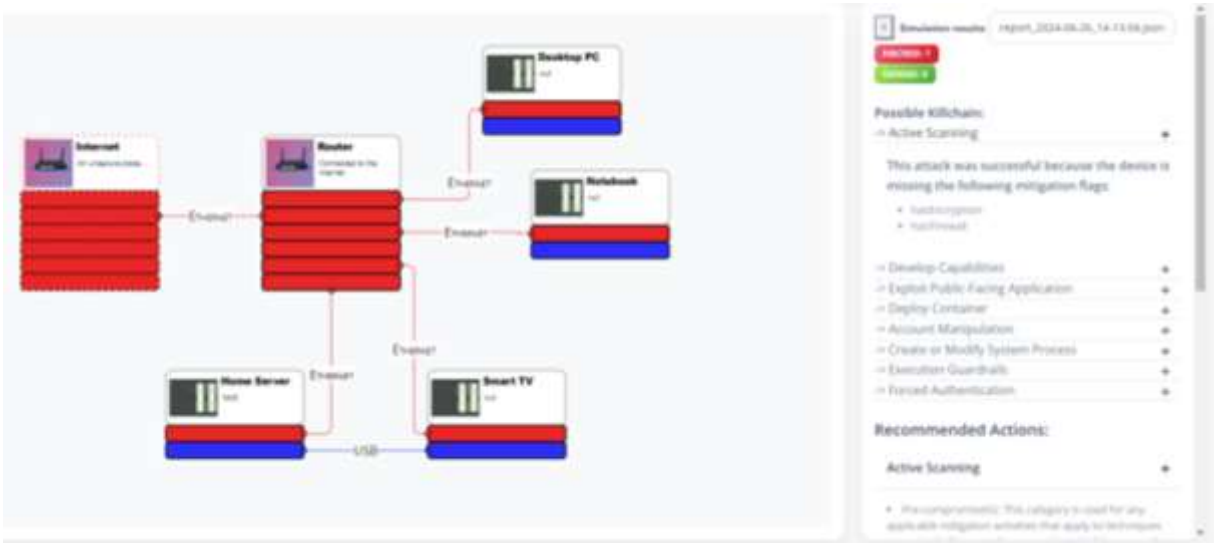
3. Attack Simulation – Testing Resilience

The **Attack Simulation** interface lets users run realistic cyber-attack scenarios against their mapped environment:

- Choose from ready-made scenarios or assemble your own from individual attack techniques.
- Select an initial access point; Tackle checks each device for the prerequisites of the chosen attacks.
- If an attacker could compromise one device, the simulation automatically tries to move laterally through connected devices.
- Detailed logs are generated for each device showing which techniques were attempted and which succeeded.

After a simulation, Tackle provides two types of feedback:

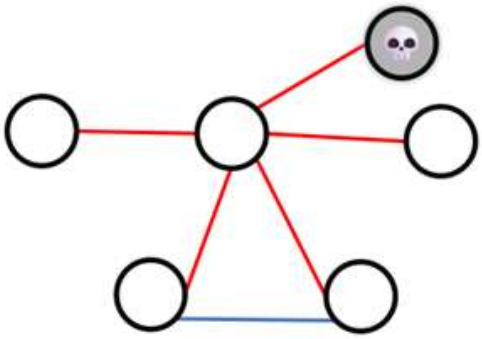
- **Graphical feedback:** affected devices are highlighted in yellow or red, and attack progression is visualised across the network.
- **Textual feedback:** clicking a device shows clear explanations of what happened, why an attack succeeded or failed, and which measures (such as changing default passwords) would prevent it.



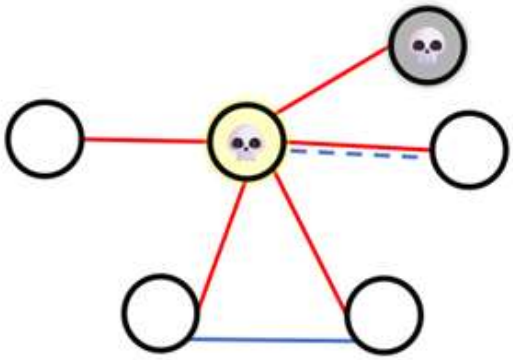
SIMULATION SEQUENCE

Behind the scenes, Tackle models the network as a graph of nodes (devices) and edges (connections):

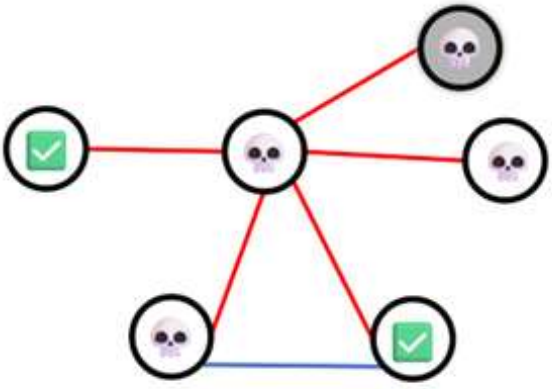
1. Mark the first compromised device (starting node).



2. For each connected node, check properties and try the selected attack techniques.



3. Compare the node's properties to the prerequisites for each technique.



4. If an attack path ("kill chain") is fully exploitable, compromise the node and continue recursively.

5. Stop when no further devices can be reached or all attack paths are blocked.

6. Present the results and recommend affordable mitigation strategies for each successful attack.

RECOMMENDED MITIGATIONS

Recommended mitigations are drawn from the MITRE ATT&CK framework but filtered by the company's maturity profile and estimated implementation effort. This ensures users see only measures that are both effective and realistically achievable for their organization.

LIMITATIONS AND CHALLENGES

While Tackle provides an innovative and accessible way for SMEs to model and test the security of their operational technology environments, it is important to recognize its current constraints:

- **High-level**
  Tackle only incorporates a limited set of predefined device types, attack techniques and mitigation factors. This makes it a useful **overview tool**, but not a complete mirror of your actual production network or a replacement for specialized penetration testing or asset discovery tools.
- **Limited scalability for very large environments**
  The current implementation is optimized for small and medium-sized enterprises. In larger or highly complex industrial networks, the manual mapping process can become cumbersome, and simulation performance may be reduced.
- **Simplified factor set**
  Because the system only considers a handful of variables per device (for example password policy, basic connectivity and a small number of organizational measures), results should be interpreted as indicative rather than definitive. Many nuanced configuration or behavioral factors are not yet modelled.
- **User-entered data quality**
  The quality of the output depends on the accuracy and completeness of the information entered by the user. Incomplete profiles or maps will naturally limit the reliability of the simulation.

These limitations mean that Tackle should be used as a **starting point for awareness and planning** rather than as a comprehensive security assurance platform.

CONCLUSION

Tackle demonstrates that even with a small set of components it is possible to give small sized enterprises a first, structured look at their operational technology security. For organizations with little or no prior experience in OT security, or those running relatively small and straightforward networks, the tool can provide clear starting points, basic maturity assessments and an accessible way to build awareness of vulnerabilities and mitigation strategies.

However, for medium-sized to large environments with complex, highly interconnected systems, Tackle remains a high-level modelling tool. Its simplified factors and limited device library mean that it cannot yet deliver deep architectural insights or replace dedicated asset discovery, monitoring or penetration testing solutions.

Despite these limitations, Tackle has already proven to be a useful research and awareness project. It offers SMEs an engaging entry point into OT security thinking, helps demystify common attack paths, and highlights where further investment in security measures may be needed. As development continues and more components are added, its value as a practical planning and training instrument will only grow.