RED TEAMING IN IT/OT SYSTEMS

Secura

Secura delivers world-class security services. One of our most sophisticated services, and the service with the highest value to the overall security of our customers, is Red Teaming. Red Teaming in the Operational Technology (OT) domain tests the resilience of your operations against advanced persistent threats in addition to the detection and response capabilities of the network defenders.

IN CONTROL WITH SECURA

Secura is your independent, trusted security partner. We help organizations by providing valuable insight into their digital security from a people, process and technology perspective.

Secura offers audit, test & certification services in the world of IT, IoT and OT. We link our audit and test work to international norms, standards and metrics.

Red Teaming

Security in the Operational Technology (OT) domain is a wide, wild landscape. With a large number of risks that belong to the category of 'unknown unknowns' and pushed by sophisticated cybercriminals and nation state threat actors, companies and states are combatting an ongoing flood of attacks. Dealing with such events requires more than a dedicated Security Operations Center (SOC); it requires hands-on training and learning by doing. An increasingly popular way of testing and training in a controlled way is 'Red Teaming'.

Originating in the military arena, Red Teaming is a security discipline that is gaining popularity in all sectors of critical infrastructure, highly secured private companies and governments. **By simulating full-spectrum cyber attacks, defenders get to practice their detection and response capabilities against high impact, low frequency events.**

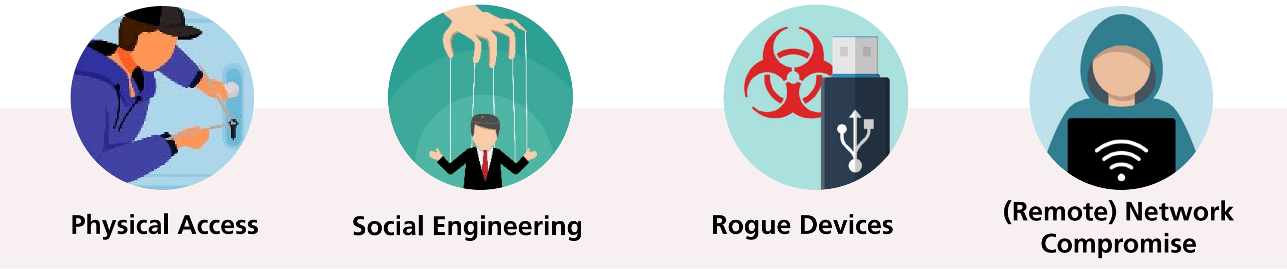


Figure 1. Full spectrum of offensive operations used within Red Teaming for OT

Safety of Red Teaming in OT Environments

Red Teaming in the OT domain is significantly different from traditional Red Teaming against traditional enterprises. Therefore the level of Red Teaming will change significantly depending on the scenario and the target infrastructure for that scenario. For example, initial access to the IT-domain can be obtained with traditional Red Teaming techniques, but once access to the OT-domain has been realized, the focus shifts away from a real attack simulation.

In this second phase, tests will be performed on lab setups, or on real devices under supervision of specialized personnel of our customers. **Ensuring the continued operation and safety of our customers infrastructure is of paramount importance during the Red Teaming assessment.**

Secura's Offering

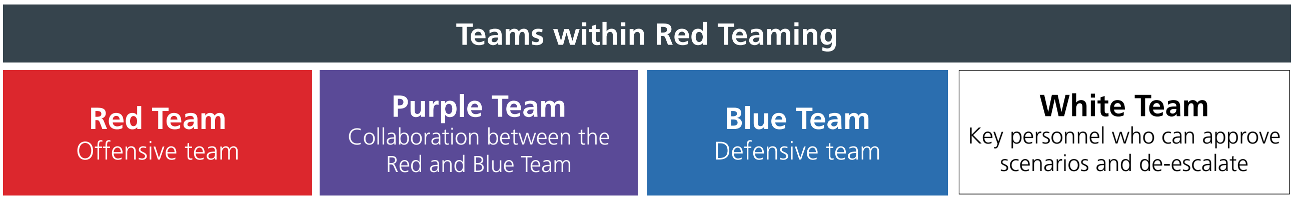
The goal of this Red Teaming assessment is to **obtain clear insight into the degree of resilience of our customers to targeted (cyber) attacks of adversaries within its threat landscape.** The final objective of this assessment is the **exploitation of critical elements of our target's OT infrastructure.**

The so-called 'crown jewels' for Red Teaming assessment in OT are linked to high impact events in the OT domain. The main focus for an attacker will be the ability to degrade or destroy the critical mission of the organization at a moment of their own choosing. These can include: the (simulated) ability to spoil chemical batches, produce under- or overpressure in critical components, de-energize powerlines or even cause long-term system failures.

To gain access to these crown jewels, Secura adheres to high ethical and quality standards to ensure you have optimal learning from the Red Teaming at minimal risk with realistic scenarios.

The actors that perform a real life attack will alter their modus operandi based on the situation they find themselves in. For this reason, instead of creating a fixed scenario chain, **Secura will keep scenarios flexible, to allow the chain to be altered if the situation requires it.**

Other important factors are attribution and operations security (OPSEC). Concerning attribution, it is key to provide fast and clear insight on whether the Red Teaming party is responsible for reported incidents or an actual attack is taking place. It is highly likely that real attacks are performed by actual cybercriminals during the exercise. The White Team must be able to contact the Red Team 24/7 to find out if it was actually Secura that performed a detected attack. Additionally, our own OPSEC always has our attention: we are dealing with sensitive files and privileged access to our customers' infrastructure, applications and data. Managing our own security is therefore a generic critical success factor and therefore we set up dedicated infrastructure for each Red Teaming assignment.



Teams within Red Teaming

Red Team
Offensive team

Purple Team
Collaboration between the Red and Blue Team

Blue Team
Defensive team

White Team
Key personnel who can approve scenarios and de-escalate

Figure 2. Different types of teams within Red Teaming

Threat Landscape

Attacks against OT networks are becoming more and more common in the real world. Where previously these attacks have been mostly attributed to nation states, cyber criminals now have discovered OT networks as lucrative targets as well. See figure 3 for a timeline of OT cyber attacks.

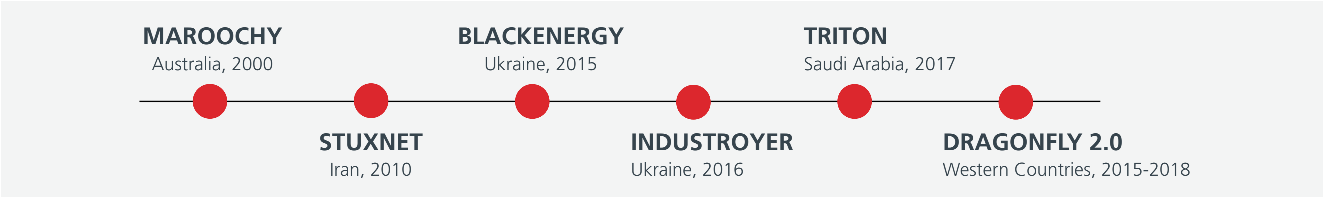


Figure 3. The timeline of publicly known cyber physical attacks against OT networks and systems.

Emulating Real World Attackers

In order to emulate real world attackers Secura uses **Tools, Techniques and Procedures (TTP)s** during the Red Teaming campaign that are based on, but not limited to TTPs used by the simulated threat actors. TTPs for these threat actors are collected by **MITRE in their ATT&CK framework** and their recently released ATT&CK for Industrial Control Systems (ICS) (for an excerpt see figure 5).

Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control
Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State
Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading

Figure 4. Excerpt of the ICS ATT&CK Matrix by MITRE

Phases of a Red Teaming Assessment in OT

Secura follows a methodology that is similar to what real life threat actors use. These phases are defined as follows:

Directed Collection Operations

Directed collection operations focus on gathering information for the later exploitation phases. The initial target for this phase will usually be the IT network in addition to the OT network as is commonly observed during cyber-physical attacks. The IT landscape often contains useful information to proceed with the attack.

Strategic Access Operations

Strategic access operations focus on obtaining persistent access to target networks and strategic systems in the environment. It is also referred to as 'preparing the battlefield'. Strategic access is sought for both the IT and the OT networks, as information and systems from both environments can be useful for performing the actual attacks in the third phase.

Non-Kinetic CNA Operations

The goal for non-kinetic CNA operations is the possibility for an attacker to perform sabotage to (temporarily) degrade or destroy the target infrastructure. Effectively creating a 'kill-switch'.

Secura's Phased Approach

Red Teaming assignments are considerable projects with substantial budgets. Secura therefore offers a **phased approach** to start small and allow your organization to grow into a (multiyear) Red Teaming program to continuously enhance its cyber resilience. The first step in our approach are workshops with stakeholders in the organization. In these workshops we jointly determine threat actors, their modus operandi and the organizations' crown jewels. Based on this we can determine high-level attack scenarios based on the MITRE ATT&CK framework, budget these scenarios and develop a Red Teaming plan. Our phased approach offers multiple go/no-go moments. The plan makes your Red Teaming ideas for the organization tangible for involved stakeholders.

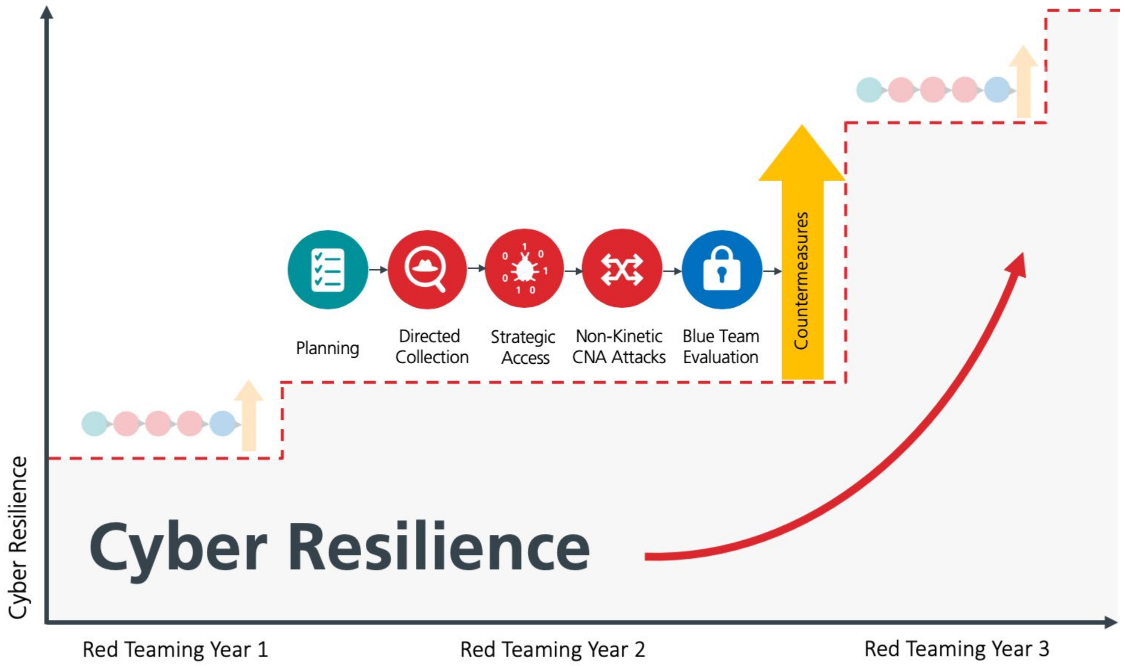


Figure 5. Build cyber resilience with Secura's phased Red Teaming approach

Success

When is a Red Teaming exercise a success? Some would say "when the crown jewels or flags have been reached without being detected by the Blue Team". However, this definition also implies that the Blue Team will have learned little. On the other hand, it means that a plausible and realistic attack path has been exposed, that can now be closed or mitigated. We consider it a success when the Red Team has had a proper challenge, yet identified many new attack paths or unknown vulnerabilities requiring solutions. The Blue Team will have gained interesting insights and detections and response can be adapted accordingly. **In the end, you will know your systemic cyber risks, and be prepared and capable to mitigate these unknown unknowns. This is the ultimate goal of Red Teaming.**

Secura's experience in red teaming, combined with our capabilities, passion and sector-specific experience, provides our customers with the best possible basis for the clean, solid execution and management of Red Teaming engagements.

Our Related Services

- **OT Risk Assessment**
  The OT risk assessment is specifically designed to identify sitelevel risks as opposed to organizational level risks.
- **NIS (Wbni) Compliance Assessment**
  The goal of the NIS directive is to improve the cyber-resilience of critical infrastructure within the EU, thereby ensuring the safety of operations.
- **SOC/SIEM Testing**
  Secura provides a test service to (continuously) test and verify the functioning of the SIEM and provides assurance that threats will not go unnoticed.
- **IEC 62443 Testing & Certification**
  IEC 6244 validates the security of individual ICS systems or the way in which they are deployed inside the company's network.

Interested?

Would you like to learn more about our services? Contact us today:

Follow us:

☎ +31 88 888 31 00

✉ info@secura.com

secura.com