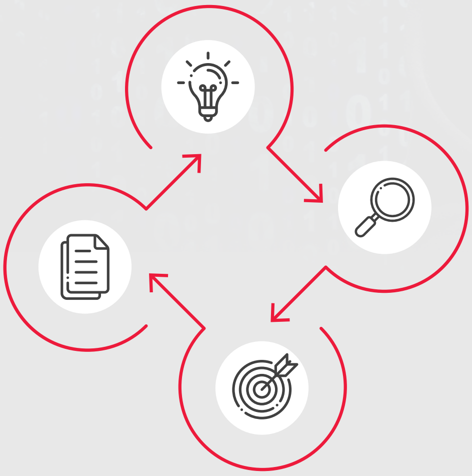
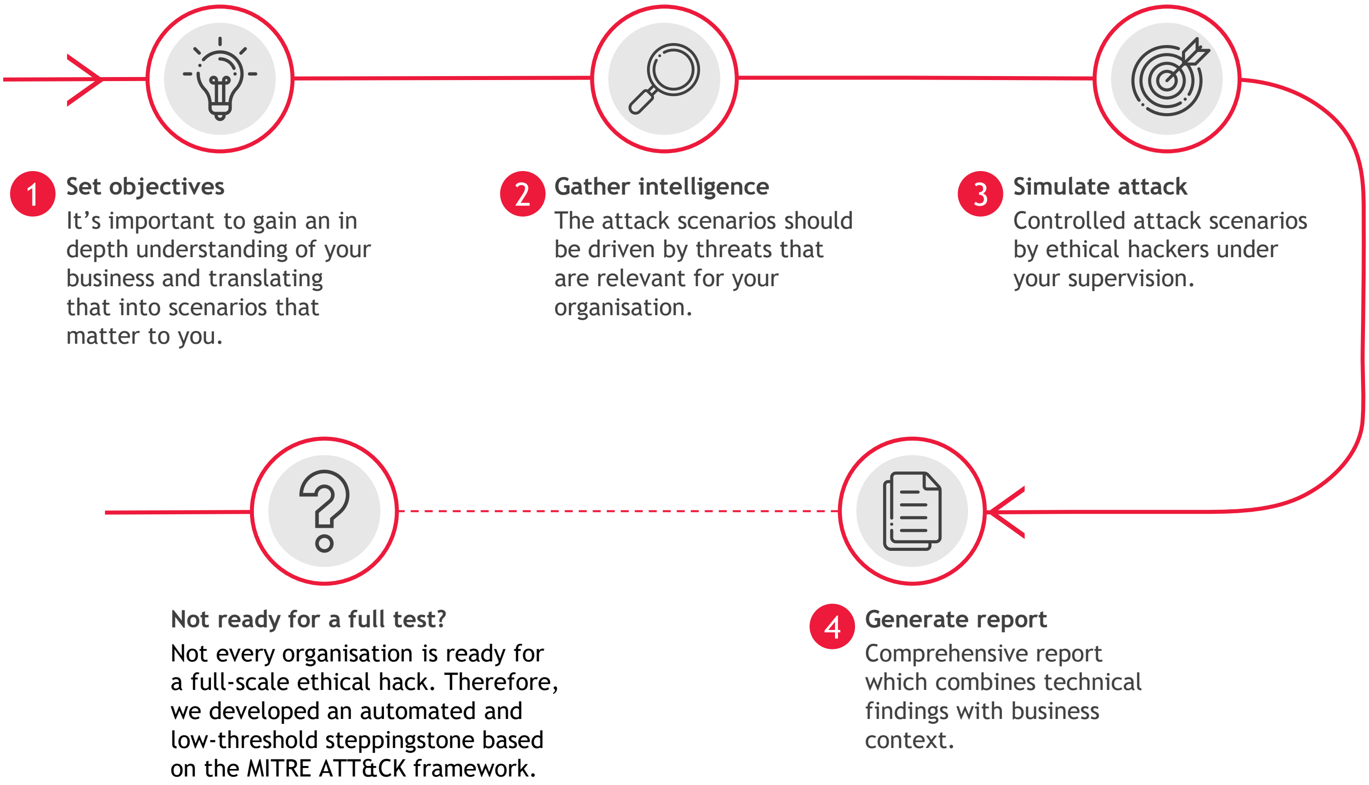
# BDO RISK ADVISORY SERVICES
# OFFENSIVE SECURITY



## To beat hackers, you must think like them

In an increasingly digital and connected world, cyber threats are growing in complexity and scale. As traditional security concepts and compliance based controls no longer provide sufficient protection against hackers, organisations face market and regulatory pressure to take their cyber resilience to a higher level. This results in an increased demand for red team testing to actively simulate multi-layered attacks used by real life hackers.



1 **Set objectives**
It’s important to gain an in depth understanding of your business and translating that into scenarios that matter to you.

2 **Gather intelligence**
The attack scenarios should be driven by threats that are relevant for your organisation.

3 **Simulate attack**
Controlled attack scenarios by ethical hackers under your supervision.

4 **Generate report**
Comprehensive report which combines technical findings with business context.

**Not ready for a full test?**
Not every organisation is ready for a full-scale ethical hack. Therefore, we developed an automated and low-threshold steppingstone based on the MITRE ATT&CK framework.

## Example objectives

Steal
10 Mn EUR

Shutdown
manufacturing
line

Steal research
information

Access
CFO office

## Some facts & figures*

There is a hacker attack every **39 seconds**

On average, it takes **6 months** for a company to detect a breach

**3,9 Mn EUR** is the average cost of a breach

*Cybersecurity Statistics and Trends for 2021: Varonis

## Our ethical hackers focus on 3 key elements:

**Physical:** Office building, data center, warehouse

**Human:** Employees, customers but also third parties or contractors

**Technology:** Network, applications, switches, firewall, endpoints etc.

## Direct benefits of red teaming:

- ✓ You can **experience a real company wide attack**, without the negative consequences
- ✓ Your internal security team will **gain essential knowledge on how to defend against the next attack** on your organisation
- ✓ Potential findings are **translated to business value**, it’s not just a technical report
- ✓ **Increases the overall cyber resilience** of your organsation and provides input for your security roadmap

Cyber Security has become the top priority on European Regulators agenda as organisations face increased pressure to comply with the evolving regulatory requirements. Recent regulatory initiatives include Cyber Resilience Oversight Expectations (CROE), Threat Intelligence Based Red teaming (TIBER), Directive on security of Network & Information Systems (NIS) & the Digital Operational Resilience act (DORA).

Euro Cyber Resilience Board for pan-European FMIs (ECRB - **2018**)

Cyber Resilience Oversight Expectations (CROE) **(2019)**

TIBER-BE v1.2 & TIBER-NL v3.0 **(2020)**

Digital Operational Resilience Act (2021)

## Interested? Get in touch with:

**STEVEN CAUWENBERGHS**
Partner Risk Advisory Services
E-mail: steven.cauwenberghs@bdo.be
Tel.: +32 (0)497 05 12 23

**FRANCIS OOSTVOGELS**
Manager Risk Advisory Services
E-mail: francis.oostvogels@bdo.be
Tel.: +32 (0)474 92 08 00

**THOMAS CORNELIS**
Senior Risk Advisory Services
E-mail: thomas.cornelis@bdo.be
Tel.: +32 (0)493 64 49 01

Follow us

www.bdo.be

BDO Risk & Assurance CVBA/SCRL, a company under Belgian law in the form of a cooperative company with limited liability, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.