Red Teaming principles

We believe...

... in the right business and technical mixture. Red teaming exercises need to combine the right amount of technical and business understanding to become useful and representative.

... in enabling your blue team and defensive capabilities, and creating joint teaming to excel, combining the expertise at both ends, to perform outstanding red teaming exercises that matter, are focused, agile and cost effective.

... that for a red teaming exercise to be successful, a thorough understanding is necessary of the actor being simulated. The objectives of this actor need to match your risks and will thus be incorporated in the defined scenarios driving the red teaming exercise.

... in tailored threat driven scenario selection and execution. We do not believe in random attacks to random objectives. We believe that the best planning comes from in depth understanding of the business, our clients, and translating that into scenarios that matter, combining risk and threat management approaches.

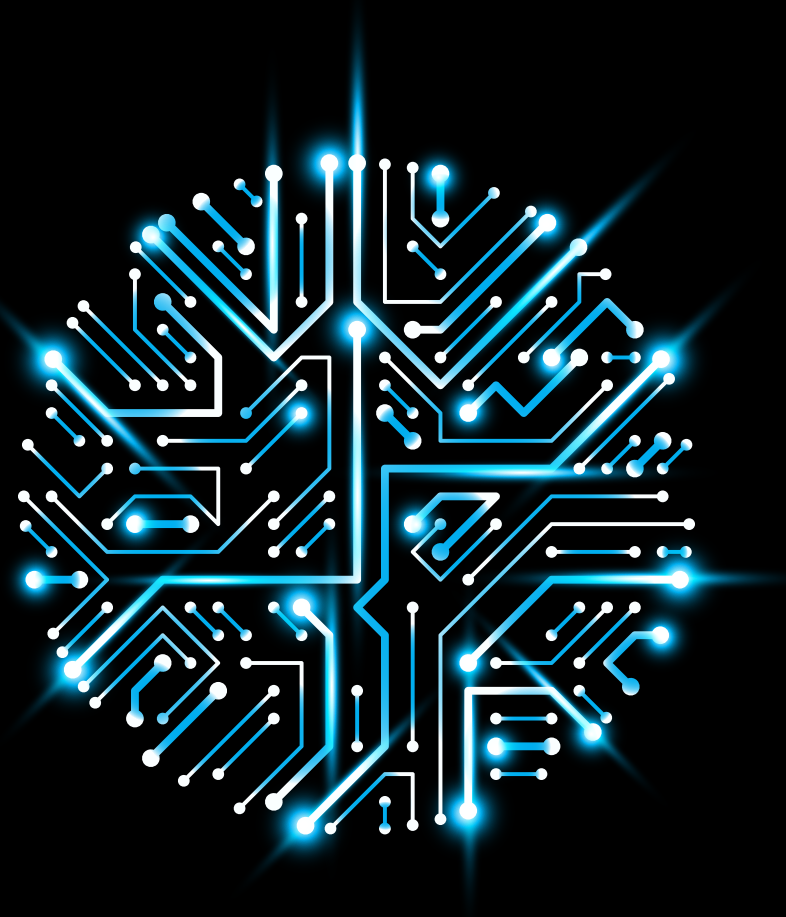
Luxembourg contacts

Stéphane Hurtaud
Partner
Information & Technology Risk
shurtaud@deloitte.lu
+352 45145 4434

Maxime Verac
Director
Information & Technology Risk
mverac@deloitte.lu
+352 45145 4258

Yasser Aboukir
Senior Manager
Information & Technology Risk
yaboukir@deloitte.lu
+352 451 45 2299

Deloitte.



Physical, human or cyber? Where are your weak links?

Red Teaming operations

Red Teaming

A realistic approach to security testing.
Security tests enables an organisation to assess their overall readiness and awareness using realistic scenario based controlled incidents.

Red teaming goes above and beyond vulnerability testing, as it takes all components within the organisation in scope and has a realistic scenario-based approach. It enhances Testing, GRC and Audit work.

Ultimately red teaming allows organisations to mature their cyber capabilities and kick start transformation programs.

Three core elements

The Information Security Trinity.

Physical: This is the buildings, the desks, the safes and the IT physical infrastructure.

Human: This represents the employees, customers, clients, third parties that binds the cyber and physical world together.

Cyber: This represents the online world, the Internet as well as corporate Intranets and all other computer networks.

Facts

94%
of our clients were successfully compromised during the red teaming engagement.

70%
of our clients had very limited capabilities in detecting or responding to the breach of their system and their crown jewels.

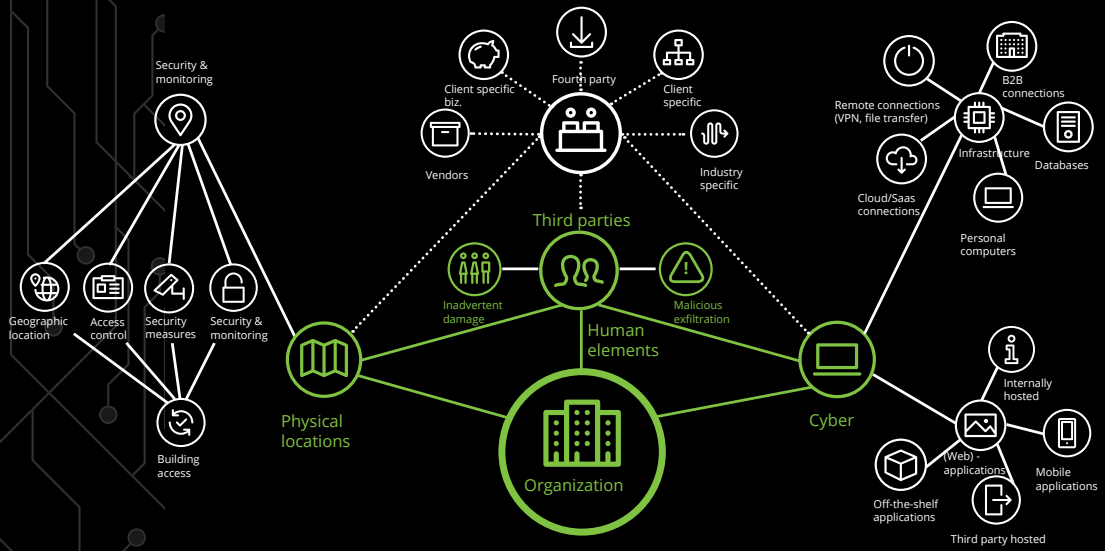
1 Day
that's how long we need on average to compromise the first device and gain initial access to the clients network after the reconnaissance phase.

6 Days
that's how long we need on average to achieve a set objective after the reconnaissance phase.

Example objectives

- Steal 10 million Euro
- Shutdown manufacturing line
- Steal research information
- Access CFO office

Attack surface



Assessing the cyber **readiness** *and* **awareness** *of your organization through scenario based controlled incidents* **tailored** *for you.*