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 needs 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.

This document has been prepared by Deloitte Limited (as defined below) for the sole purpose of providing a proposal to the parties to whom it is addressed in order that they may evaluate the capabilities of Deloitte Limited to supply the proposed services.

The information contained in this document has been compiled by Deloitte Limited and includes material which may have been obtained from information provided by various sources and discussions with management but has not been verified or audited. This document also contains confidential material proprietary to Deloitte Limited. Except in the general context of evaluating our capabilities, no reliance may be placed for any purposes whatsoever on the contents of this document or on its completeness. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte Limited or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document or any other oral information made available and any such liability is expressly disclaimed.

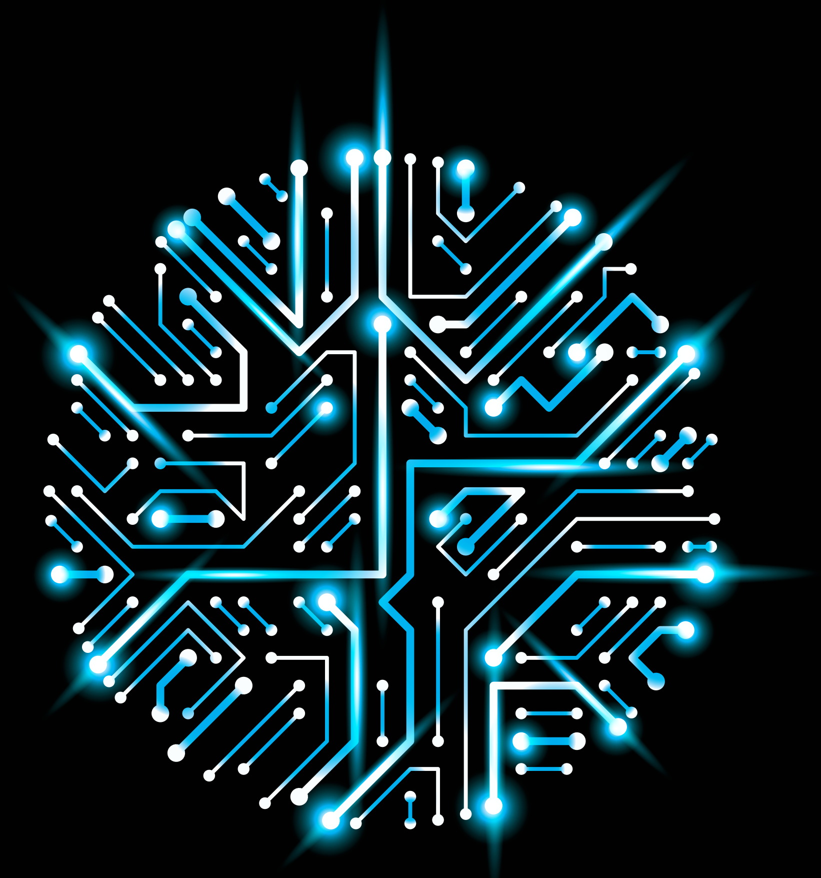
This document and its contents are confidential and may not be reproduced, redistributed or passed on, directly or indirectly, to any other person in whole or in part without our prior written consent.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

In this document references to Deloitte are references to Deloitte Limited. Deloitte Limited is the Cyprus member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see www.deloitte.com/cy/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte Limited is a private company registered in Cyprus (Reg. No. 162812). Offices: Nicosia, Limassol, Larnaca

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: Represents the buildings, the desks, the safes and the IT physical infrastructure.

Human: Represents the employees, customers, clients, third parties that bind the cyber and physical world together.

Cyber: 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
is 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
is how long we need on average to achieve a set objective after the reconnaissance phase.

Example objectives

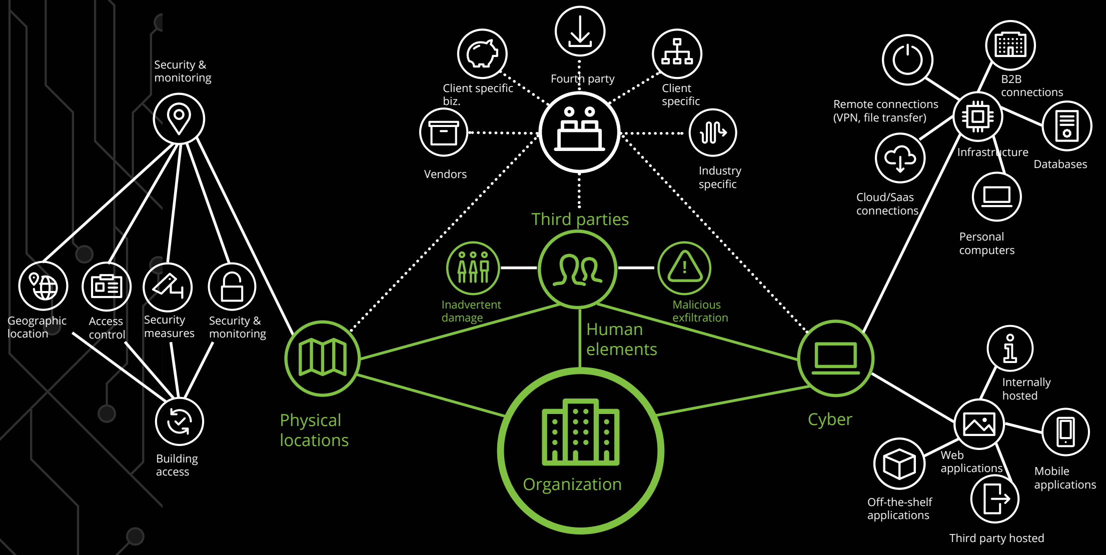
Steal 10 million Euro

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.*