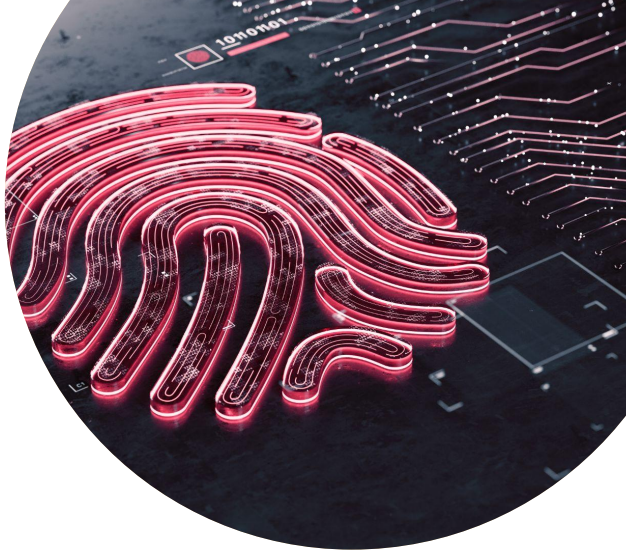
devoteam
Cyber Trust



Case Study

Red Team Service

The Client

Banking
Dimension: 20.000
Global presence

The Challenge

The client sought to improve its security posture and response protocols to better defend against cyber threats, such as targeted attacks or ransomware. They aimed to identify weaknesses in their systems and processes.

The Solution

We provided a Red Team service covering different tactics, techniques, and procedures (TTPs) mimicking targeted attacks and ransomware. During the engagement, our team performed multiple activities in order to gather intelligence on the client's exposed attack surface, attempt to breach the network from the outside, and persist inside the network.

For the engagement, we defined together with the client the different vectors to be performed and techniques to be used, which included social engineering, phishing emails, USB drops, lateral movement and C2 communication.

After the execution of the exercise, we provided a detailed description of the actions performed, attack paths used, and vulnerabilities exploited in order for the client to analyse and improve the overall posture, including detection and response processes.

During the process, we worked with the client's SOC/Blue Team to help identify blind spots, and help assess the improvements implemented after the exercise

Impact

The client now has a better understanding of the exposed attack surface, weaknesses in systems and processes, and has improved the overall resilience to attacks and detection and response mechanisms and processes, effectively reducing considerably the risk to the organisation.

Related Services

- Red Teaming

Making your tech journey more secure.

For more information, please visit
www.integrity.pt