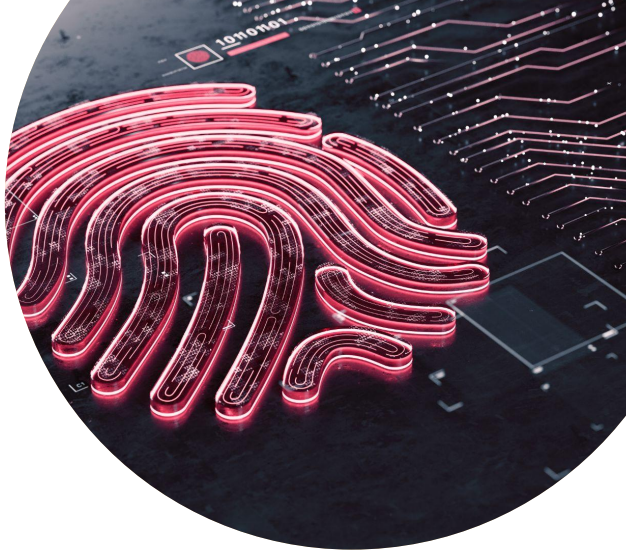
devoteam
Cyber Trust



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. Its aim was to identify weaknesses in their systems and processes.

The Solution

We provided a Red Team service covering different tactics, techniques, and procedures (TTPs) emulating targeted attacks and ransomware. During the exercise, our team carried out various activities to gather information on the client's exposed attack surface.

Intrusion actions were triggered from the outside using social engineering and technical exploitation of vulnerabilities, culminating the exercise with data persistence and exfiltration.

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, the weaknesses in the technological infrastructure and the processes that support it. Because the exercise was carried out without the general knowledge of the organisation, the client had the opportunity to realistically assess the performance of its SOC and implement measures that led to improved resilience to cyberattacks, considerably reducing the risk to the organisation.

Related Services

- Red Teaming

Making your tech journey more secure.

For more information, please visit
www.integrity.pt