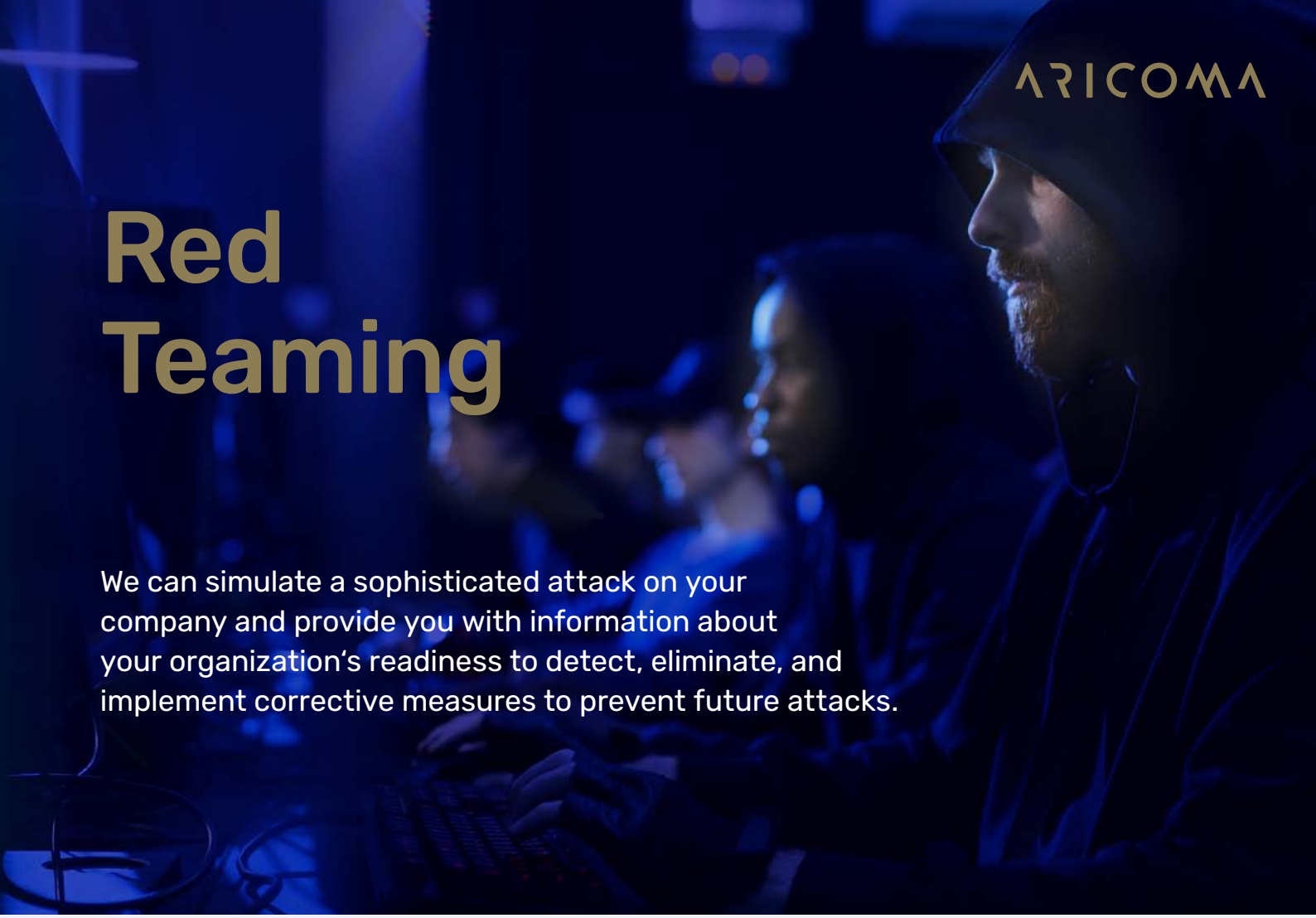


Red Teaming

We can simulate a sophisticated attack on your company and provide you with information about your organization's readiness to detect, eliminate, and implement corrective measures to prevent future attacks.

Definition of roles

RED TEAM
Our specialists who simulate the tactics, techniques and procedures of the attackers.

WHITE TEAM
A select team comprising members of the company's management to oversee the ongoing exercise.

BLUE TEAM
A team made up of the company's internal security specialists who detect an attack and take the necessary countermeasures. .

How does Red Teaming work?

The Red Team is a team of our ethical hackers who will conduct a **simulated attack on your organization** to test its security and communications. We will keep the exercise secret from employees and only share information about it with your company's senior management. We will use sophisticated modern tools, evaluate how well protected your systems are, and provide your employees with training in a secure environment. The aim of the practical test is always to **detect risk points** and prepare you for future cyber threats.

Do I need Red Teaming for penetration tests?

Pentesting and vulnerability scanning are an integral part of security, and these activities must be maintained, adhered to and developed. However, a methodological approach like this is unable to test real preparedness and thus counter cyber threats. Red Teaming, as a simulation of a real attack, will actually test your readiness, response and subsequent recovery capabilities.

Penetration Tests

- Last for a short time (1-3 weeks)
- The application administrators and owners are aware of the ongoing tests
- They aim to find vulnerabilities in a given application or infrastructure
- Strictly defined limited scope
- Additional protection layers (WAF, IPS, etc.) can be deactivated for testing purposes
- Often implemented in non-production environments

Red Teaming

- Last for longer (1-3 months on average)
- The process is classified; only White Team members know about it
- Unlimited testing of all layers of your security as a whole (technology, people, processes, physical security)
- Impacts on the production environment

We divide the tests into four groups:

Technology
Internal infrastructure, cloud, applications (web, mobile), servers, endpoint devices, etc.

People
Internal and external personnel (employees, contractors, suppliers, business partners, etc.).

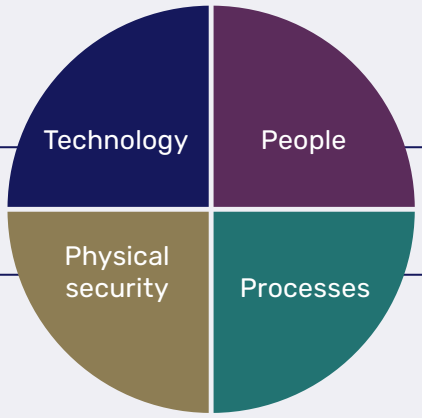
Processes
Internal processes (existence, formality, consistency and compliance), communication between defense team members.

Physical security
Testing the physical security of buildings, warehouses, data centers, manufacturing plants, etc..

Red Teaming

The Red Team tests the technology not only for potential vulnerabilities, but also in terms of the effectiveness of the defensive tools deployed.

It tests people's ability to respond in the event of a real attack to management decisions made in a crisis situation.



Tests your organization's physical security.

Tests the process setup within your company.