What is Red Teaming?

Are you looking for an effective way to strengthen your organisation's cybersecurity resilience? Is your organisation well prepared for an organised (cyber)attack? Discover our Red Teaming service, based on technology, organisation and people!

Red Teaming is a method in which we create realistic scenarios to test the effectiveness of your security infrastructure. Instead of merely testing its technical aspects, Hoffmann's experts go further by considering organisational and human elements as well. Using our methodology and extensive knowledge and experience, we help your organisation act proactively and stay ahead of any threats or cyberattacks.

Modus operandi defined

The modus operandi is the cybercriminals' method of operation. They usually go big by looking for your organisation's Achilles heel to penetrate deep into its DNA. They thus look at how they can disrupt security in terms of technology, organisation *and* people. Our team of experienced cybersecurity experts do exactly the same. By thinking like the enemy and adopting their modus operandi, we can expose high-risk processes and weaknesses in your organisation. Ideally, we conduct an exploration of your organisation's potential weaknesses, both by using Open Source Intelligence (OSINT) and through on-site physical surveillance. In doing so, we employ the same tactics and techniques that a malicious actor would also employ. Based on those results, we can devise and execute an actual attack.

A real-world Red Teaming operation

Once a Hoffmann employee has gathered information over the phone, another Red Team member impersonates a supplier or vendor to conduct an initial reconnaissance of the premises. A third team member then attempts to gain access to the building and the network equipment there on the basis of the information gathered. Next, a technical expert attempts to retrieve your confidential business information from the network. Depending on the scenario, the attack may start covertly, and if desired or necessary, it may take on a rather obvious character to elicit a response. During the process, continuous contact is maintained with the client about the progress of the attack.

Are your measures strong enough to keep our Red Team out?

Like many other organisations, you likely spend a lot of money and time on cyber resilience measures. The value of these investments only proves itself when a potential attack occurs. Here, the question is not whether you will be attacked, but when you will be attacked. Professional cybercriminals will do everything they can to circumvent any and every form of security. Even if that means exploiting the vulnerability and helpfulness of your employees. (Cyber)criminals are becoming increasingly creative in this regard.

Our Red Team’s approach

Our method is not limited to testing technical aspects; organisational and human elements are also an integral part of our approach.

People

Our Red Teaming services focus on the human factor in your environment. Here, we use realistic attacks, such as phishing attempts and social engineering, to test your employees’ alertness and resilience. By creating and deploying various scenarios, we are able to observe and analyse your employees’ reactions to the threats. The outcomes form the basis for customised cyber-safe behaviour training and awareness programmes. As a result, you will know how to permanently improve your employees’ security awareness and identify and prevent potential attacks at an earlier stage.

Technology

In addition to the human factor, Hoffmann uses advanced technologies to thoroughly test the security of your IT infrastructure. Our experts conduct penetration tests to identify potential vulnerabilities in your systems, networks and applications. We use a range of methods to gain insight into those potential technical vulnerabilities. We then itemise them in a detailed report and provide you with recommendations for improvement. Our targeted approach enables you to take proactive measures to better protect the security of your data against cyberattacks.

Organisation

Besides testing the people and technology factors, Hoffmann also looks at the organisational aspects of your security measures. Using baseline measurements, we analyse your policies, procedures and governance structure. Hoffmann identifies potential areas for improvement in your processes and helps your organisation implement effective measures to strengthen them. Our aim here is to gain a comprehensive understanding of your (information) security landscape.

Implementation

Our work starts by jointly identifying your organisation’s most critical and high-risk processes. We then ask you to think about the organisation’s weaknesses. Where do these weaknesses lie? How could criminals gain entry? And how is security organised then? Hoffmann has over 60 years of knowledge and experience gained from the many investigations we have conducted. This expertise and know-how enable us to support you when it comes to people, technology and organisation. Together we determine a well-defined learning objective for the red teaming activities and then map out a realistic implementation scenario.

Next, we plan, explore and prepare, after which we execute the attack. In doing so, we adopt the enemy’s modus operandi; Hoffmann employees think and act like the enemy. Our Red Team is limited in this only by the limits of the assignment.

After the exercise, you receive a comprehensive advisory report from our Red Team, in which we name your organisation's vulnerabilities and make recommendations for improvement. In this way, you will be able to eliminate any vulnerabilities that have been identified.

A real-world Red Teaming operation

One of our clients wondered whether it was possible to launch an attack on the IT network from the inside. During the red teaming exercise, our specialists posed as printer maintenance technicians and placed a digital listening device in the network. This allowed them to remotely hack the organisation from the inside and access critical business information systems. In carrying out this exercise, our Red Team was able to expose both physical and digital security weaknesses and could share those with the client.

What does Red Teaming achieve?

After a Red Team assessment, you will know exactly where your organisation's vulnerabilities lie. This may be down to human, organisational or technical factors, or a combination of them. As a result, you can take additional measures to address those vulnerabilities. You can then periodically reassess the situation by conducting a new red teaming exercise. If you periodically conduct these, you will be as prepared as you can be for an incident or attack.

An additional effect of red team assessments is that employee security awareness and alertness increase when you share our findings with your employees from a positive perspective. Doing so can encourage them to be more alert. This is essential because in our experience, people are generally the most crucial link in security.

Would you like information on Red Teaming?

Do you have any questions? Or are you interested in a Red Teaming assessment? If so, please feel free to contact us with no further obligation on your part.

☎ +31 (0)88- 298 66 00

✉ info@hoffmann.nl

Our specialists would be happy to share their ideas on with you.