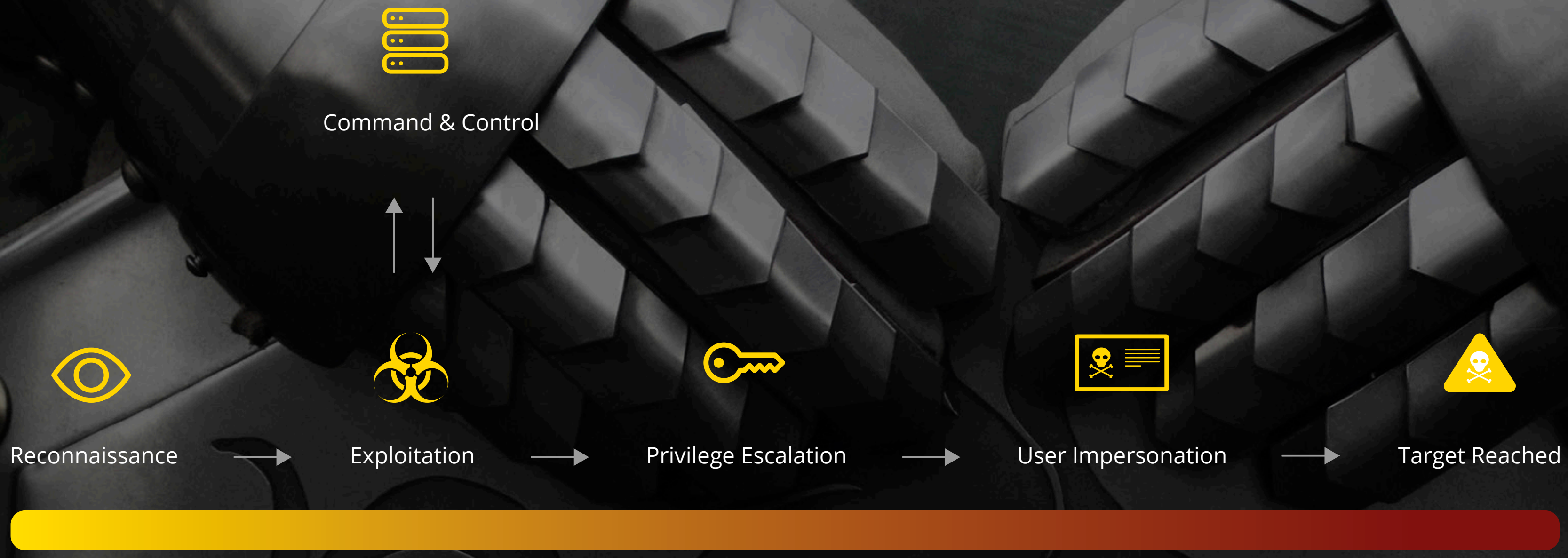
DTS

Offensive Security Services

A modern enterprise today must invest in cyber security technologies. However, technologies alone are not the only answer to the current challenges. One of the biggest problems is to gain real visibility and clarity about one's own explicit security deficits. This is the only way to verify that all security measures are intact and provide adequate protection. For the question „Is resilience purposefully and sustainably ensured in your company?“ we as DTS are absolute experts. We offer various cyber security assessments that put our experienced, certified IT experts in the role of an attacker. By simulating realistic and highly topical attacks, your company is put to the test in order to actually uncover existing security gaps.

Individual, different assessment types, e.g. vulnerability assessments, penetration tests, Red & Purple Team engagements and their highly technical results are one thing. The other thing is the combination of these procedures, the presentation of the results in meaningful reports and the subsequent derivation of recommendations for action.



Command & Control

Reconnaissance → Exploitation → Privilege Escalation → User Impersonation → Target Reached

We identify your security vulnerabilities through this combination and help you understand the damage that individual or chained vulnerabilities can cause in your business environment. Based on these security analyses, we can then develop a clear cyber security roadmap for you to significantly improve your cyber security. We build your security foundation on which data, accounts, IT systems and networks can be secured with leading defense measures and mechanisms.

Our cyber security assessments:

Internal Cyber Security Assessment

Internal security assessment by applying the assume-breach approach as well as identification of attack and spread possibilities of attacks in order to determine the possible damage potential. Vulnerabilities and misconfigurations are analyzed and security systems are put to the test.

External Cyber Security Assessment

In-depth review of externally available systems, through active penetration and collection of publicly available corporate information, and detection of vulnerabilities and misconfigurations.

Web App Assessment

Wide review of complex web applications, connected infrastructure, and application-specific permissions and role concepts.

Phishing Assessment

Analysis of your company's vulnerability to various phishing attacks.

Vulnerability Scanning

Recording the weak points of your internal IT systems, incl. prioritization, reporting, recommendations for action.

Internal Cyber Security Assessment

The question is no longer whether you will become a victim of a cyber attack, but when your own company will be affected. With the Internal Cyber Security Assessment, we offer you the ultimate cyber security kickstart. Based on predefined targets, e.g. compromising privileged accounts or exfiltrating sensitive database content, an assume-breach scenario is mapped. An attacker with access to the internal network determines the potential damage after a successful initial compromise of your organization.

An important part of this is, of course, the core: the active directory. But the entire company network, IT systems and all accounts are also audited. As a result, we provide you with vulnerabilities (e.g. authorization problems, cracked user accounts, security holes on systems and in the network), correlations of vulnerabilities and risk configurations of all kinds (to show attack paths to sensitive systems, data or user accounts) as well as long-term measures (further planning of the security infrastructure to improve it efficiently).

The identification of security gaps is one aspect. Another element is that we show you which attack possibilities actually exist and how these corresponding gaps can be exploited. Understanding how attack scenarios work and how malware spreads, for example, can make all the difference.

What are the DTS USP's? On the one hand, we act like an attacker ourselves. On the other hand, we make it possible to exploit highly technical results by combining the best effects of different methods. This makes it possible to derive both short-term and long-term, well-founded measures. In addition, it is possible to develop sustainable long-term planning for a company-specific cyber security roadmap.

- Vendor-independent analysis
- Identify & understand potential points of attack
- Improved transparency regarding critical risks
- Provision of concrete recommendations for action for corporate security
- Customer-specific prioritization of vulnerabilities
- Internal network assessment, including vulnerability assessment
- Security assessment of services in the network
- Active directory assessment, incl. password audit
- Identification of critical attack paths

In particular, you will benefit from the DTS Internal Cyber Security Assessment if...

... you are unsure of your current security level.

... you want to understand your cyber security vulnerabilities.

... you want to take appropriate and effective measures to protect the business.

... you need an action plan to strengthen your cybersecurity defenses.

... you want to maximize the ROI of your cybersecurity spending.

... you are not sure which cybersecurity projects should be undertaken and when.

External Cyber Security Assessment

Do you want to understand what techniques an attacker can use and whether your externally available systems are operated securely? The External Cyber Security Assessment is the answer to that question. DTS offensive security researchers take on the role of an external attacker and gather publicly available information about your organization, such as credentials from historical data breaches, domain, system, and user information. Available systems are scanned for vulnerabilities and misconfigurations, and attempts are made to gain access to systems or sensitive content with the goal of breaching the perimeter and digitally breaking into your organization.

- Vendor-independent analysis
- Identify & understand potential points of attack
- Improved transparency regarding critical risks
- Provision of concrete recommendations for action for corporate security
- External network penetration test
- Simulation of realistic attacks

Web App Assessment

Almost everything today is a web application or API (Application Programming Interface). Smartphone apps that exchange data via API, web stores or similar applications are publicly accessible via web-based protocols. But are they safe from unwanted access or actions?

Gartner predicts that API attacks will become the most common attack vector and cause data breaches in enterprise web applications. Many known API vulnerabilities have already impacted a wide range of organizations.

DTS cyber security researchers identify security vulnerabilities in the test scenario that is appropriate for you. Whether blackbox, greybox or whitebox test, an in-depth web app assessment is indispensable to uncover relevant vulnerabilities according to the web app penetration test (OWASP) and to put possible role concepts within the application to the test.

Access control malfunctions or code injection attacks are often the biggest gateway for attackers to gain access to the system. But users of the web application must also be adequately protected to prevent a malicious attacker from exploiting security vulnerabilities.

- OWASP
- In-depth review of a complex web application
- Review of the connected infrastructure (database, frontend server, backup)
- Review of application specific permissions & role concepts

Phishing Assessment

45 % of all users click on links in emails, even from unknown senders.

74 % of all companies worldwide fall victim to targeted phishing attacks at least 1x per year.

92 % of all cyber attacks start with a phishing email.

Emails are the biggest gateway for malware or ransomware. With our DTS Phishing Assessment, we offer you the opportunity to determine your company‘s vulnerability to various phishing attacks. As part of the targeted campaign coordinated with you, we carry out a simulated but realistic phishing attack on your company and evaluate the results together with you in order to define subsequent protective measures. In the process, we also examine the „human factor“ and its security awareness. We show how the inattention or credulity of your company‘s employees can be exploited and determine the need for further training.

- Analysis of your company‘s vulnerability to various phishing attacks
- Targeted campaign for simulated, realistic phishing attack
- Evaluation of the results & definition of protective measures
- Review of the „human factor“ or the security awareness of your employees

Vulnerability Scanning

Do you know the current patch status of your assets in the company? With the DTS Vulnerability Assessment, we offer you the opportunity to take a snapshot of the current IT hygiene. Identifying system and software vulnerabilities is one of the most basic ways to get an initial risk assessment of your deployed assets. CVEs (Common Vulnerabilities and Exposures), as well as risky configurations, are recorded in a categorized and prioritized manner and clearly prepared for you in corresponding reports. The focus here is clearly on showing you the information in an efficient and easy-to-understand manner.

Of course, we also provide you with possible recommendations for closing the vulnerabilities in combination with highly accurate prioritization through threat research (frequency and difficulty of exploitation) and other factors. In this way, we also significantly support you in effectively closing the detected vulnerabilities.

- One-time recording of the individual vulnerabilities of your internal IT systems (software vulnerabilities & risk configurations)
- Your IT hygiene in one overview
- Vulnerability analysis & prioritization
- Reporting, incl. presentation & advice as well as plan for remediation
- Execution of a network vulnerability analysis or holistic system analysis by means of authentication through provided credentials
- Collected information is processed by us & transmitted to you in the form of a report, incl. consulting & presentation of the data
- Creation, provision and presentation of reports for you