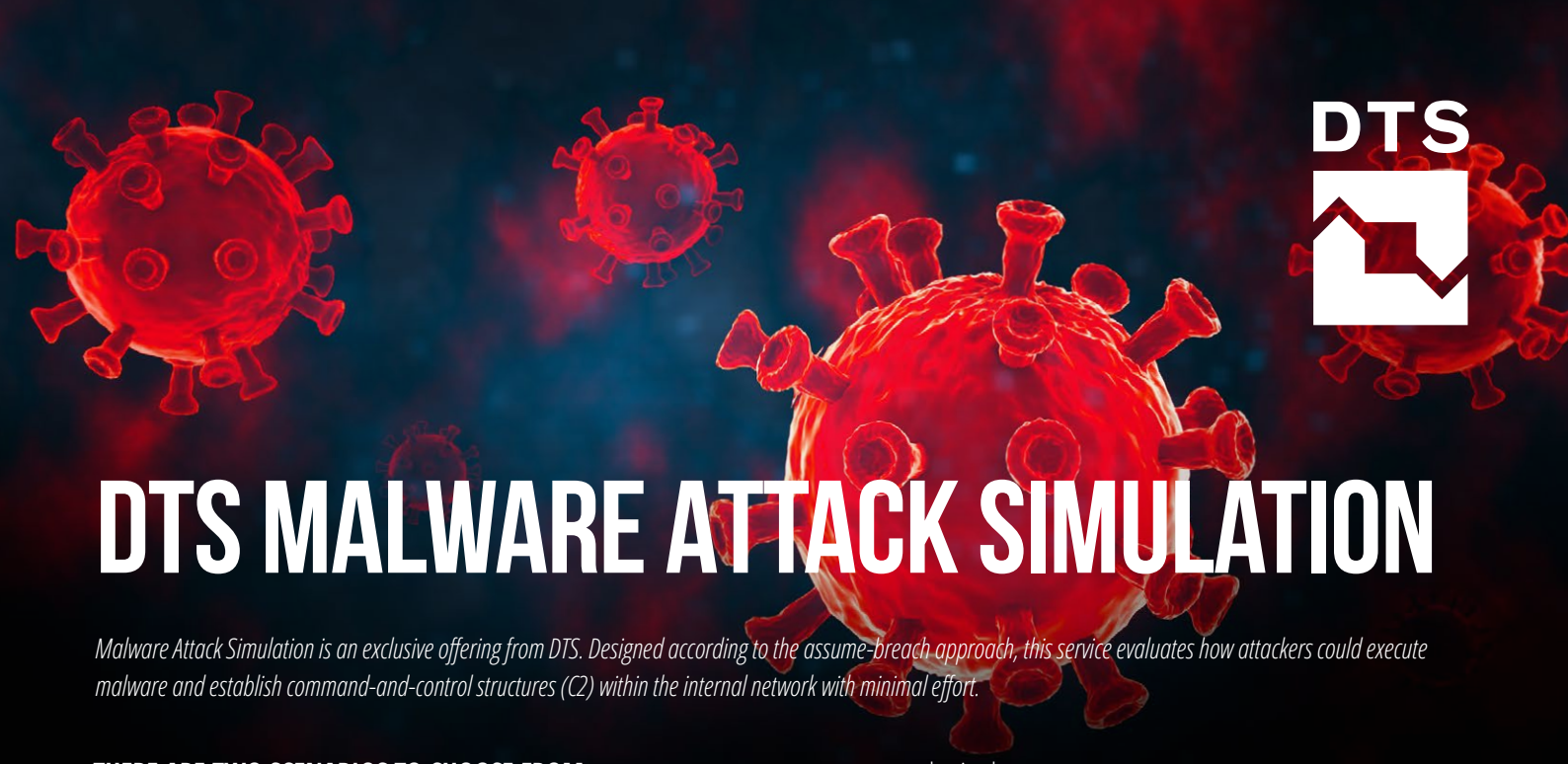

DTS MALWARE ATTACK SIMULATION

Malware Attack Simulation is an exclusive offering from DTS. Designed according to the assume-breach approach, this service evaluates how attackers could execute malware and establish command-and-control structures (C2) within the internal network with minimal effort.

THERE ARE TWO SCENARIOS TO CHOOSE FROM:

- Behavior of ransomware malware
- Behavior of industrial espionage malware

The goal of the assessment is to identify security gaps that give an attacker the opportunity to compromise systems, exfiltrate data, or disrupt critical business processes.

The focus is on the following questions:

- Ransomware scenario: How resilient is the company against attacks aimed at encryption and extortion? Can an attacker successfully establish malware, spread it within the company, and maintain control from outside?
- Industrial espionage scenario: How vulnerable is the company to the theft of sensitive data through targeted attacks? Can an attacker successfully establish malware and exfiltrate sensitive data externally via a command-and-control channel without being detected?

SERVICE COMPONENTS

1. Vulnerability analysis: This is based on an initial collection of information about available systems and services. This data reveals where attack vectors for malware exist.
2. Simulation of realistic malware attacks: DTS cyber security specialists carry out targeted simulations to check the execution of malware and the establishment of C2 structures. Common methods from the MITRE ATT&CK framework are used, e.g., from the execution, persistence, defense evasion, and command and control phases. It is assumed that initial access already exists.
3. Post-exploitation phase: After successful malware execution, an evaluation is carried out to determine how attackers could expand their presence, with a focus on:
   - Lateral movement: Attacks to spread within the network
   - Privilege escalation: Gaining administrative rights
   - Credential access: Attempting to steal access data to gain unauthorized access to systems
   - Collection: Collecting data or information from a compromised system
   - Command and control: Communication channel through which an attacker gains control over an infected system and can control it
   - Exfiltration: Attacker transfers stolen data from a compromised system to an external location

DETAILED PROCESS

- Onboarding: Devices and access data are provided, and registration on the DTS reporting platform is completed
- Kick-off meeting: Joint discussion of the technical details and objectives of the assessment
- Project work: Malware simulation and documentation of findings
- Final meeting: Presentation of results and discussion of possible countermeasures
- Optional continuation: Upon request, you can further analyze the results on the DTS reporting platform and request retests

YOUR ADVANTAGES

- Realistic simulation of malware attacks to identify potential attack paths and vulnerabilities
- Customization to the business context and security goals of the company
- Realistic insights into the effectiveness of existing security measures
- Detailed recommendations for short-term measures and long-term strategies

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de

DTS Malware Attack Simulation E 07082025