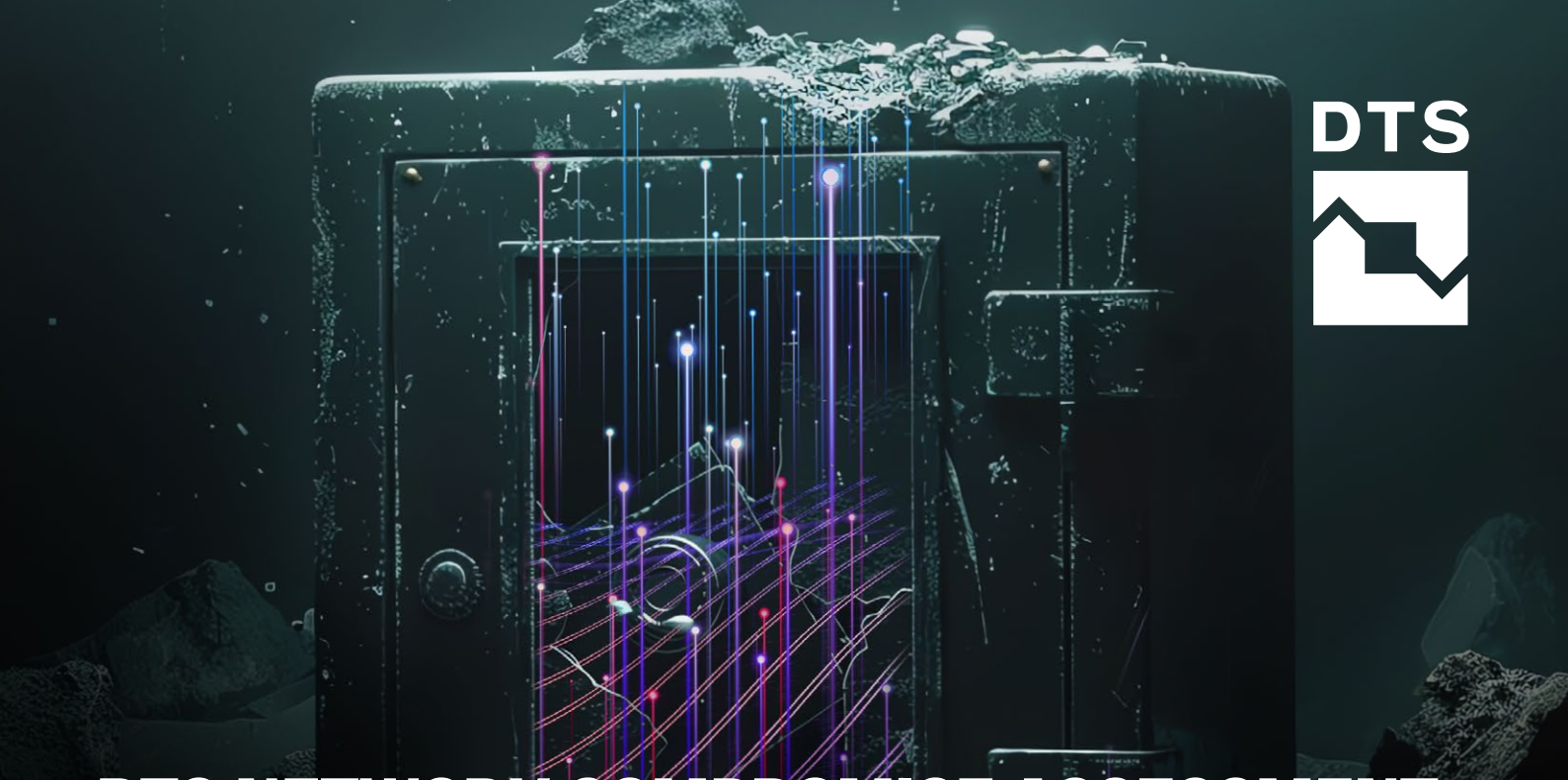

DTS NETWORK COMPROMISE ASSESSMENT

The Network Compromise Assessment is an exclusive offering from DTS. Based on the assume-breach approach, this service evaluates targeted attack vectors and vulnerabilities within a network. The focus is on how a malicious actor could compromise network resources and gain control over critical systems with minimal effort. The goal is to test the network's resilience to advanced attacks and identify potential attack paths.

FOCUS QUESTIONS

- How easy is it for an attacker to gain unauthorized access to the internal network?
- What vulnerabilities could lead to the compromise of network resources?
- How far can an attacker progress laterally within the network after gaining initial access?

SERVICE COMPONENTS

1. Vulnerability analysis: First, DTS cyber security specialists collect information about network resources, services, and, for example, the Active Directory. This analysis provides a detailed picture of the internal attack surface, shows the connections between network segments, and serves as the basis for targeted attacks.
2. Simulation of realistic attacks: Attack vectors typically used by attackers are simulated, including:
   - Attacks on network protocols (e.g., SMB, RDP, DNS)
   - Misconfigurations in firewalls and network segmentation
   - Exploits for known vulnerabilities in network devices
3. Post-exploitation phase: After successful network access, an evaluation is performed to determine how attackers could move within the network and compromise other systems, including, for example:
   - Lateral movement: Attacks to spread within the network
   - Privilege escalation: Gaining administrative rights
   - Persistence: Establishing permanent control in the network

PROCESS IN DETAIL

- Onboarding: Provision of the necessary equipment and access data, as well as registration on the DTS reporting platform
- Kick-off meeting: Joint discussion of the objectives and technical details of the assessment
- Project work: Conducting the assessment with a focus on network attacks and documenting the results
- Final meeting: Presentation of the results and discussion of measures to increase network security
- Optional continuation: Analysis of the results via the DTS reporting platform and the option of retests

YOUR ADVANTAGES

- Includes components of the assume breach assessment, which identify vulnerabilities and attack paths at the network level in a realistic and comprehensible manner:
  - Identification of vulnerabilities that could lead to the compromise of network resources
  - Recommendations for network security, for short-term measures as well as for long-term optimizations
  - Simulation of practical scenarios to demonstrate how resilient the network architecture is to modern threats
- Option for individual adaptation to the business context and network requirements of the company
- Actionable recommendations for improving network security

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de