FUJITSU

Red Team Exercise

Simulate. Expose. Strengthen

To truly understand your security posture, you need to challenge it with the tactics of real-world adversaries.

A Red Team Exercise is a controlled, intelligence-led simulation of real-world cyber attacks. It tests your organisation's ability to detect, respond to, and recover from sophisticated threat actor tactics, without prior warning to your defenders. This is not a checklist audit, it's a full-spectrum adversarial emulation.

Real-world threat simulation

Emulates advanced persistent threats (APTs) using MITRE ATT&CK-aligned tactics, techniques, and procedures (TTPs).

End-to-end security validation

Tests people, processes, and technology across cyber and physical domains.

Actionable risk insights

Delivers technical findings mapped to business risk, with clear remediation guidance.

Blue team uplift

Post-exercise purple teaming sessions help your defenders learn from real attack scenarios and improve detection and response.

The risks it uncovers

- Gaps in endpoint and network detection.
- Weaknesses in identity and access controls.
- Susceptibility to phishing and social engineering.
- Physical security vulnerabilities.
- Inadequate incident response coordination.
- Data exfiltration pathways and DLP gaps.

Discover how your security stands up to real-world threats

Our approach

Our Red Team methodology is modular and tailored to your environment, risk appetite, and objectives. Key components include:

Phishing and social engineering

We run phishing campaigns in waves to test resilience. Spear-phishing uses LinkedIn and social media intel. Vishing and smishing are simulated. USB bait like “Payslips” is dropped on-site.

Initial compromise simulation

We simulate an initial breach to assess how an attacker could operate inside the environment. Custom payloads are crafted in an attempt to bypass AVs.

Internal reconnaissance

We map systems and Active Directory. Critical assets like code and finance systems are identified. Misconfigs like LLMNR and NTLM relay are exposed.

Physical intrusion testing

We test access via tailgating or lockpicking. Rogue devices are planted. Badges are cloned.

Persistence and exfiltration

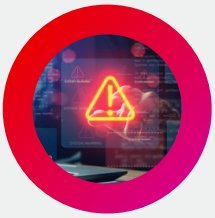
We create persistence with tasks or registry keys. Data is exfiltrated via HTTP(S), DNS, or rogue devices. DLP and EDR responses are tested.

Detection and response evaluation

We test how well your SOC detects and responds. IOCs, evasion methods, and timelines are shared to help identify and remediate security gaps.

Modern attackers don’t follow the rules ...

They exploit human behaviour, misconfigurations, and overlooked entry points. Red Teaming reveals how your organisation would fare against a determined adversary, highlighting blind spots in detection, response, and resilience that traditional testing often misses.



Comprehensive report: Technical findings with MITRE ATT&CK mapping and business risk context.

Remediation guidance: Prioritised recommendations with walkthroughs.

Executive summary: Clear, non-technical insights for leadership.

Contact us today

Schedule your Red Team Exercise and uncover the gaps before attackers do.