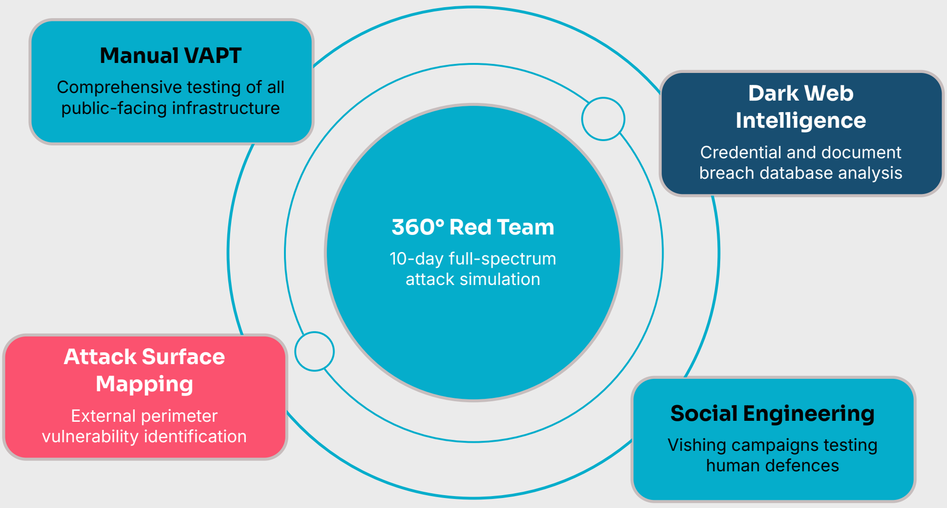
360° Red Team Assessment for Industrial Manufacturing

A leading European construction materials manufacturer sought independent validation of their security posture against sophisticated threat actors. Despite investing in robust defensive measures, executive leadership recognised the critical need to verify their organisation's true resilience across digital infrastructure, network perimeters, and human elements. This comprehensive assessment would reveal whether their substantial security investments could withstand real-world adversary tactics employed by modern cybercriminals and nation-state actors targeting industrial operations.

The Engagement Approach



What We Found

Our assessment uncovered multiple high-severity security gaps that exposed the organisation to immediate compromise. Each vulnerability represented a viable attack path that sophisticated threat actors could exploit to gain unauthorised access, exfiltrate sensitive data, or disrupt operations.

Attack Vector	Critical Vulnerability	Business Impact
Web Infrastructure	Remote Code Execution on main website	Complete server takeover capability
Dark Web	C-level documents and active credentials in breach databases	Immediate account compromise risk
Human Layer	VPN access obtained via single vishing call	Perimeter bypass without technical exploit
Email Security	Corporate emails on 40+ personal accounts; domain spoofing possible	Perfect phishing campaign feasibility
Exposed Services	Internal systems accessible via forgotten endpoints	Direct internal network access

Key Findings and Business Impact

01

Technical Defences Insufficient

Whilst network security controls were implemented, the organisation's defences could be entirely circumvented through non-technical attack vectors. A single social engineering telephone call successfully obtained VPN credentials, demonstrating that technology alone cannot secure modern enterprises.

02

Critical Web Vulnerability

Remote code execution capabilities on the primary website presented an immediate threat. Attackers could achieve full server compromise, potentially pivoting to internal networks, exfiltrating intellectual property, or deploying ransomware across production systems.

03

Exposed Credential Risk

Discovery of C-level credentials and confidential documents in dark web breach databases created immediate compromise risk. These credentials provided attackers with potential access to privileged systems without requiring sophisticated exploitation techniques.

Outcome and Remediation

We demonstrated that technical defenses alone were insufficient - the VPN could be bypassed with a phone call, and the website could be fully compromised. The client received a prioritized remediation roadmap addressing all critical gaps before real attackers could exploit them.

10

Assessment Days

Complete security evaluation

48

Hours to Report

Actionable remediation plan

Book a Meeting