Shelter from the Storm

CASE STUDY

Red Team

SECURITY TESTING

INDUSTRY: FINANCIAL

CASE OVERVIEW

A major international United Kingdom-based retail banking organisation that provides a wide-range of personal, business and wealth management financial services — identified an immediate need to ensure that their physical, information and cyber security controls could withstand a "real-world attack" from current cybercriminal threat actor tools and methodologies.

The organisation required efficacy confirmation of the Information Security Management System (ISMS) deployed to protect the information assets they processed, stored and transmitted. It was imperative that the effectiveness of all the controls implemented in their business processes, staff, facilities and IT systems that prevent unauthorised access to their sensitive data be verified as "fit for purpose".

In response to this requirement, Risk Crew designed and delivered a comprehensive Red Team security test. The testing took place over 3 months and was comprised of the collection of Open-Source Intelligence (OSINT) associated with the customer, their business processes, staff and operating locations. Based upon this information, Risk Crew created and executed a series of attacks simulating the practices used by current cybercriminal organisations to exploit security vulnerabilities associated with the client's operating locations, staff and systems.

The testing resulted in identifying numerous and significant security flaws, which were easily exploited and allowed unauthorised access and data exfiltration which had not been identified in previous security audits or tests.

CASE INDUSTRY

Requirement	Confirm controls implemented to protect information assets from unauthorised access are fit for purpose
Industry	Financial
Industry Details	Large UK-based financial organisation, providing online transaction services in over 30 countries
Location	Testing was conducted against UK-based operations
Testing Period	Testing was conducted over a 3-month period

THE CLIENT

One of the top 10 UK-based retail banks with over 500+ branches, 2,000 ATMs and 8 million customers and provides the following services:

- **Online banking**
- **Transaction banking**
- **Credit and debit cards**
- **Wealth management**
- **Foreign exchange**
- **Margin trading facilities**

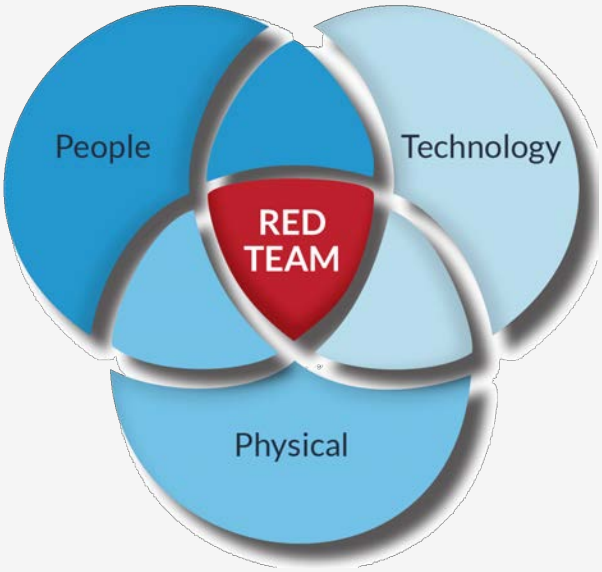
THE CHALLENGE

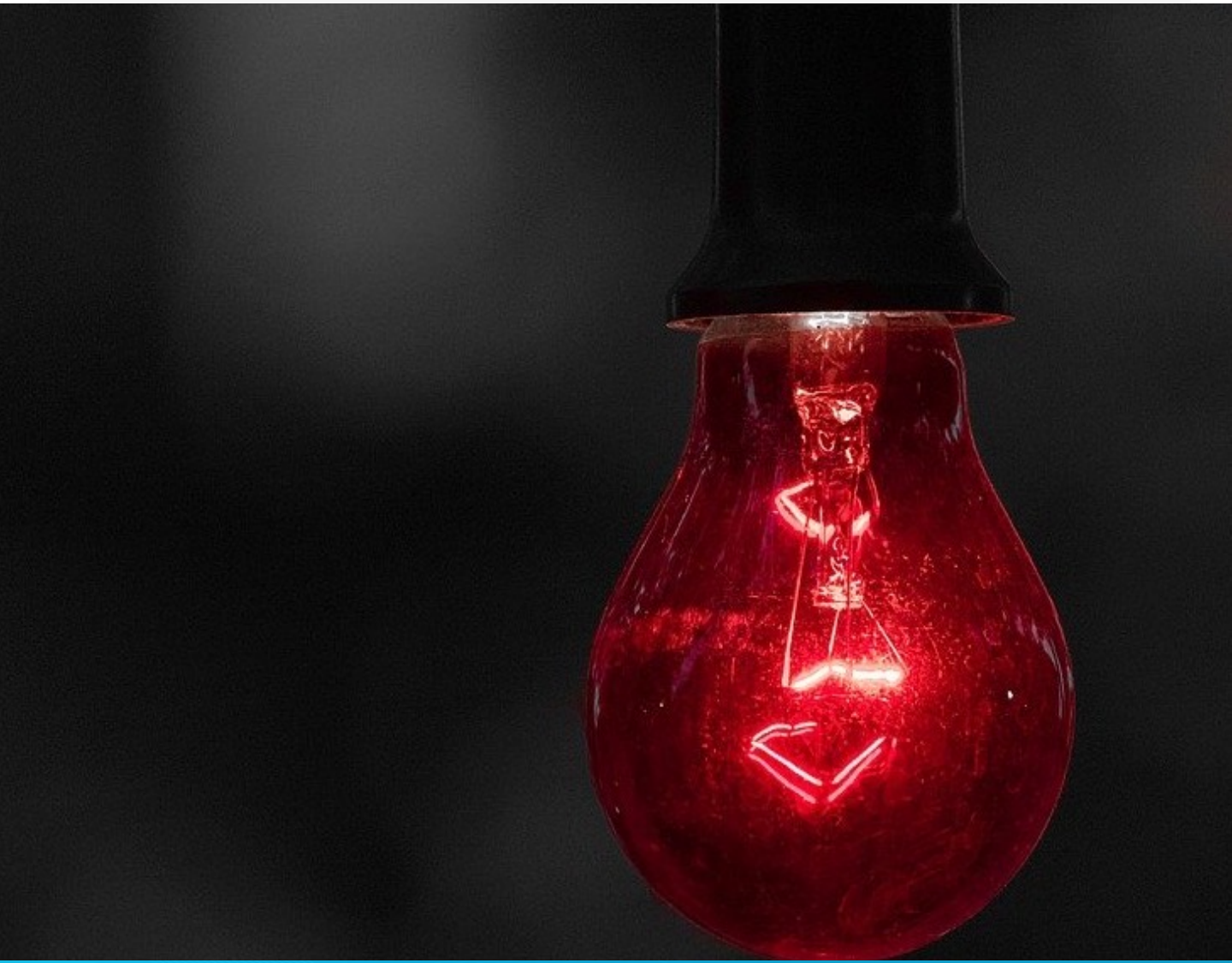
The customer objectives were threefold: First, to confirm that controls implemented to prevent unauthorised access to the information assets processed, stored and transmitted on their systems were effective. Second, to confirm if it was possible to obtain user credentials to their systems without authorisation. Finally, to verify if it was possible to bypass existing security controls, obtain unauthorised access to their systems and exfiltrate data without detection.

THE SOLUTION

Risk Crew's Red Team testing solution comprises a proven methodology for understanding how well an organisation would fare against a real-life cyber attack.

Conventional security penetration testing seeks to assess the security integrity of the information technology systems being tested. Red Team testing identifies and exploits ***any*** vulnerabilities associated with the organisation allowing access to the system – like a real-world attacker.





THE APPROACH

Engagement Confirmation

Prior to commencement, Risk Crew met with the client to discuss and confirm the **Threat Actors** to simulate in the testing, **Attack Vectors** to attempt to exploit, testing objectives, timelines and Rules of Engagement.

Cyber Threat Actors & Attack Vectors

A Threat Actor is a term used for any individual, or group of individuals, that conduct or attempt to conduct malicious cyber attacks or activities against an enterprise, whether intentionally or unintentionally.

There are five recognised Threat Actor groups that include Hacktivists, Cybercriminals, Competitors, Insiders and Nation States.

An Attack Vector is a pathway used by a Threat Actor to penetrate the target system and to achieve the attack's objective. There are three recognised Attack Vectors: employees, IT systems (technology) and operating locations.

A threat actor researches and assesses each vector to determine exploitable vulnerabilities that would allow access to the objective.

Risk Crew's Approach

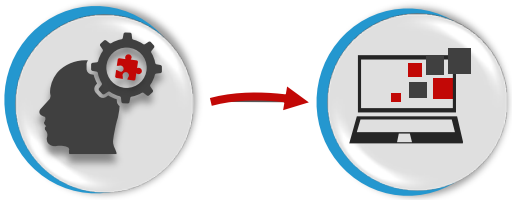
It was agreed that the Risk Crew Red Team would engage as a Cybercriminal Threat Actor and attempt to identify and exploit vulnerabilities associated with the client's information technology systems, staff and operating locations (Attack Vectors).

The testing objective was for the team to get unauthorised access to the client's system and exfiltrate data undetected. Rules of Engagement were established, and it was agreed that testing would take place over a 3-month period.

THE METHODOLOGY

Reconnaissance

In the first step, our Red Team collected all Open-Source Intelligence (OSINT) associated with the client's business, staff, and operating locations for analysis.



Collect OSINT Map & Plan Attacks

This included collecting:

- Company's House registration data
- Street addresses of operating locations (and Google Maps street views)
- Publicly available building floorplans
- Publicly available 3rd party supplier contracts
- Publicly available business utility information
- Whois lookup
- DNS records
- Exterior facing systems information and, (such as hosting providers
- Domain, subdomain names and services
- Websites URLs
- System IP addresses and services
- Firewall manufacturer
- Make and model data
- Wi-Fi access point configuration details

All publicly available personal data associated with the client's employees require analysis such as:

- Email addresses
- Employees' ID numbers
- Work telephone numbers
- Social media profiles
- Client information available on the dark web such as compromised user credentials

Risk Crew conducted some "exploratory phishing". The Red Team sent several phishing emails to entice the client's employees to click on a link that did not deliver malware but allowed the Red Team to harvest additional targeting information such as:

- Browser versions
- Operating system versions
- Usage of .NET within the organisation
- Public IP addresses of their VPNs
- Out of office email footers and whether the link was also followed by a third-party security vendor

The information was then used to identify potential attack vectors and payloads that could be used to obtain unauthorised access and exfiltrate data.

Prepared Attacks & Payloads

With the information collected in the first phase, the Red Team begin to design and prepare attacks and payloads to be executed by the Red Team. Risk Crew built a lab environment that replicated the client's technology stack identified in the reconnaissance and duplicated their antivirus, endpoint detection and response, web gateway and next-generation firewall products.

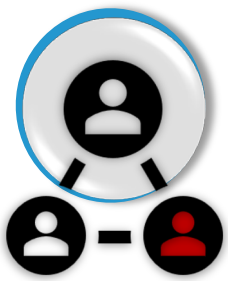
The lab was used by the Red Team to ensure their payloads bypassed (or triggered insufficient noise on) the client's systems before these are delivered in the attacks. The Red Team then configured attack servers and the appropriate forwarders (i.e. reverse proxies) and acquired domain names for waterhole and phishing attacks. The Team identified trusted domain names that had a history and were available for purchase.

Next, The Red Team created payloads that could be delivered to the client's staff via social engineering platforms. Specifically, they created Office documents with executable code (in the form of VBA macros) and tested these inside the lab environment to ensure the payloads did not execute on devices outside of the client's perimeter.

THE METHODOLOGY

Additionally, the Red Team designed multiple phishing templates with varying goals to solicit employee passwords and trick them into executing commands and downloads. External facing services that did not use two-factor authentication were identified for brute force attacks and the Red Team created wordlists containing usernames gathered in the reconnaissance phase for password spraying attacks.

Finally, the Red Team obtained burner phones for "Smishing" and "Chishing" attacks, created fake social media profiles used for "catfishing" and bogus employee ID badges to bypass physical access controls.



Executed Attacks

Once the payloads were tested and validated against a replicated lab environment, the Red Team devised step-by-step plans for their delivery. For this client engagement, the Risk Crew Red Team executed multiple successful attacks through eight vulnerable attack vectors:

Credential Harvesting:

The Red Team harvested over 230 (previously breached) client system user credentials from the internet. 55% of the provided system access.

Phishing:

The Red Team sent phishing emails to 3,000 UK client staff to deceptively solicit system user credentials. The attack resulted in obtaining 709 user credentials over 3 weeks.

Smishing:

The Red Team sent smishing texts to 100 C-Level executives to deceptively solicit their user credentials. The attack resulted in obtaining 33 user credentials over 2 weeks.

Impersonation:

The Red Team entered 8, randomly selected, client facilities by impersonating personnel and uploaded payload applications from unattended user terminals undetected. Each attack executed was successful.

THE METHODOLOGY

Road Apple:

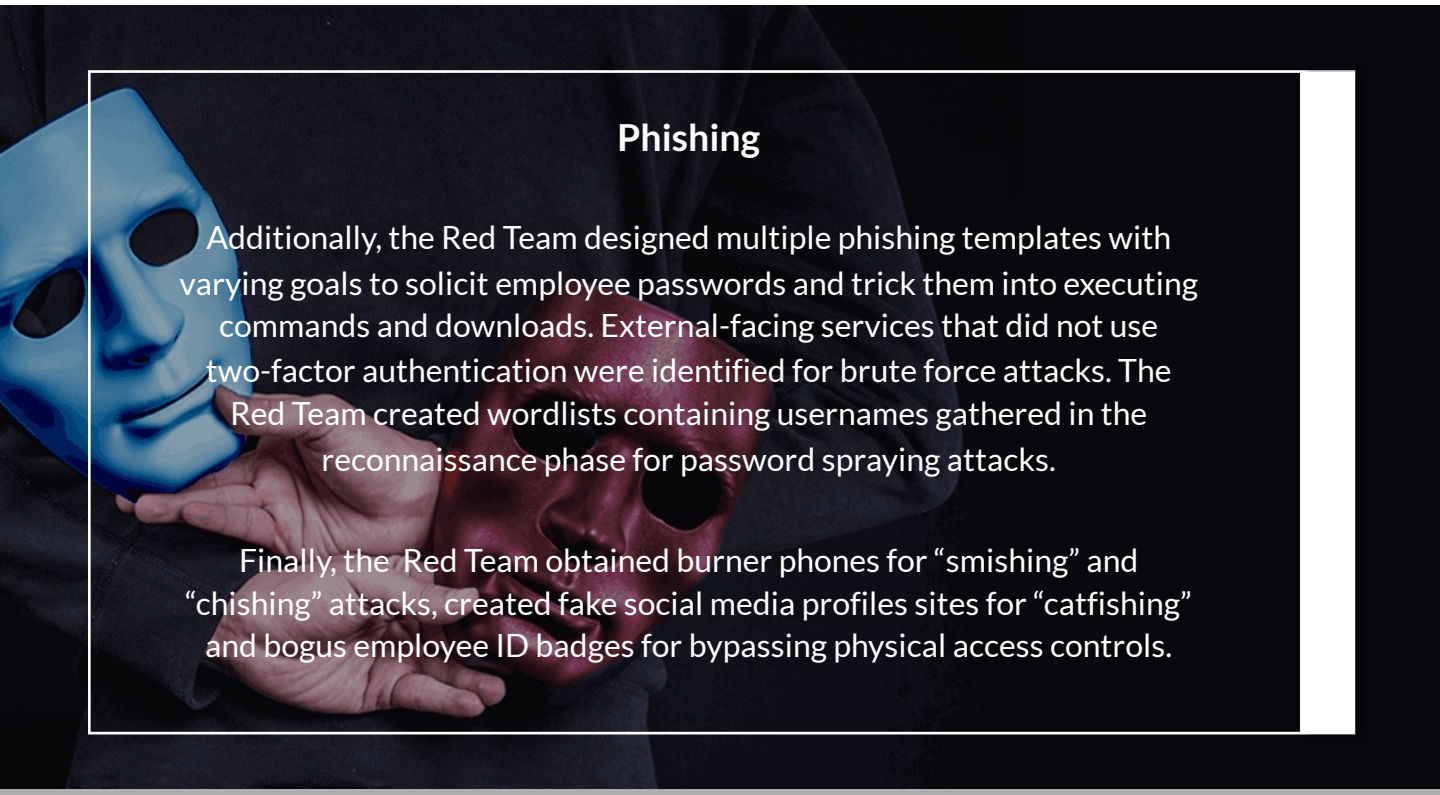
The Red Team left 200 road apples (pin drives bearing client logo containing payload applications) in client parking lots and restroom facilities. The attack resulted in applications uploaded into client systems in 42 instances.

Tailgating:

The Red Team donned bogus employee ID badges and tailgated employees into client facilities unchallenged to access IT hosting rooms and upload payload applications. Attacks were successful at 8 of 10 randomly selected client locations.

CVE Exploitation:

The Red Team exploited numerous vulnerabilities identified on exterior-facing client systems to obtain unauthorised access and upload payloads. Most notably, they exploited a memory corruption vulnerability (Pule Connect Secure version 9.1R11.4) allowing them to remotely execute arbitrary code as the root user.



Phishing

Additionally, the Red Team designed multiple phishing templates with varying goals to solicit employee passwords and trick them into executing commands and downloads. External-facing services that did not use two-factor authentication were identified for brute force attacks. The Red Team created wordlists containing usernames gathered in the reconnaissance phase for password spraying attacks.

Finally, the Red Team obtained burner phones for “smishing” and “chishing” attacks, created fake social media profiles sites for “catfishing” and bogus employee ID badges for bypassing physical access controls.

THE METHODOLOGY

Data Exfiltration & Actions on Target

Once the Red Team gained unauthorised access to client's systems — the final objective of the engagement was to attempt to exfiltrate data from systems. All attacks resulted in the Red Team's ability to remove client data from the client's systems undetected.

To increase the client's return on investment for this engagement, once breaching the systems undetected, the Red Team attempted numerous actions to assess internally deployed controls and quantify the client's detection level capability.

The Red Team conducted the following "on target" actions:

Kerberoasting:

The Red Team used this technique to target service accounts to obtain and crack system user passwords. Kerberoasting is a pervasive attack technique targeting Active Directory service account credentials.

Privilege escalation & lateral movement:

The Red Team attempted to move laterally across the systems unchallenged and compromise further infrastructure verifying if it was possible to obtain higher privileges than those assigned to the compromised credentials.

Malicious Network Activity Detection:

Using attacks such as brute force against Active Directory, the Red Team established how far they could go undetected.

Monitoring and Incident Response:

The Red Team assessed the capability and efficiency of the client's monitoring and incident response teams when reacting to an identified attack.

THE METHODOLOGY

Protection of Privileged Accounts:

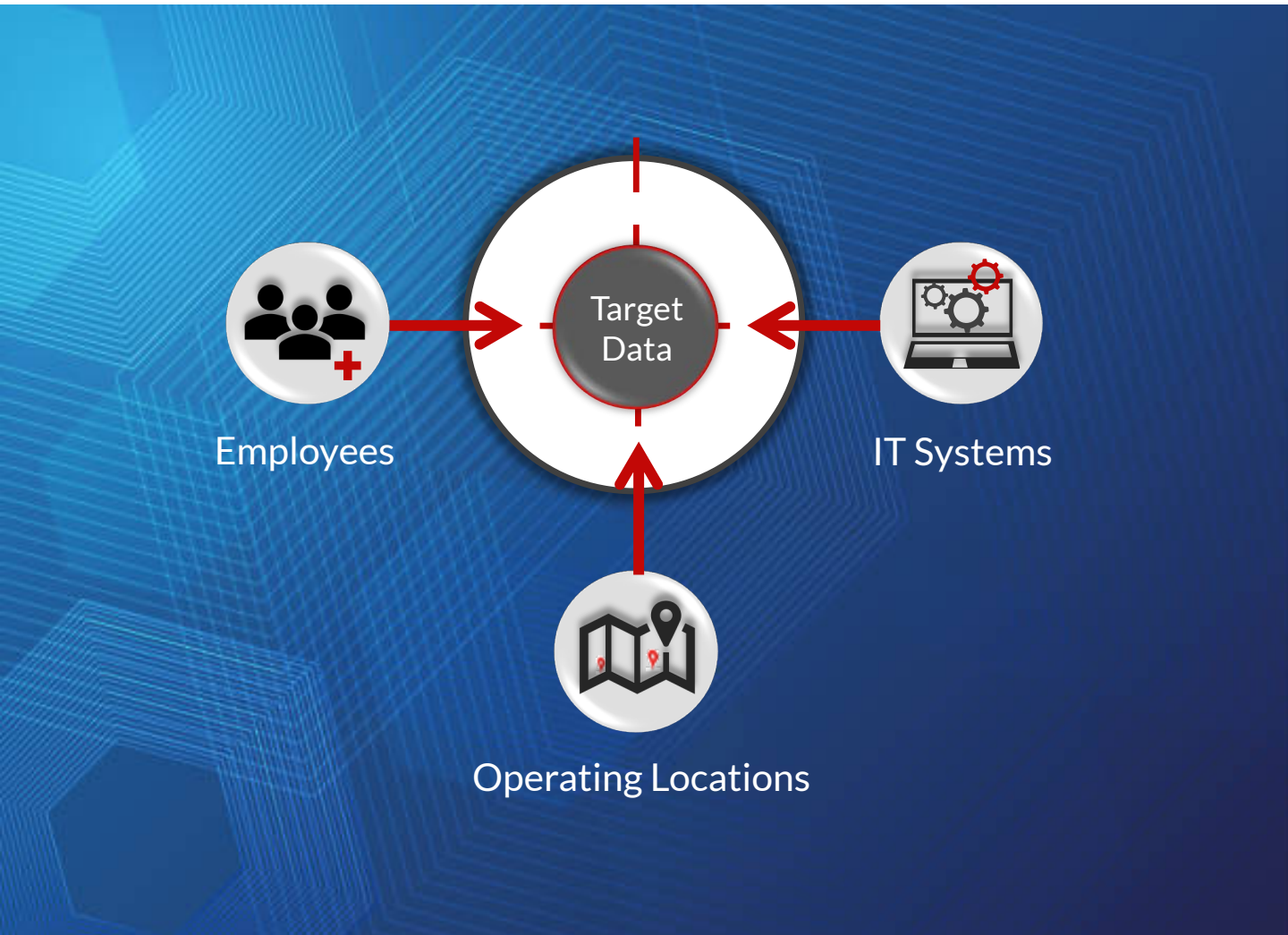
The Red Team analysed the security of the high privileged accounts used to manage hosts on the network.

Domain Security Policy:

The Red Team assessed domain security policies and noted any weaknesses identified.

Patch Management Policy:

The Red Team identify unsupported operating systems, missing patches on compromised builds to verify best practice had been enforced.



THE DELIVERABLES

Risk Crew met with the client prior and identified a specific set of deliverables that would result from the solution as all deliverables are pre-agreed with Risk Crew customers. As a result of this engagement, the client received the following:

Report of Findings & Recommendations

Upon completion of testing, Risk Crew produced a detailed report of findings and associated remedial recommendations. The report contained time and dated visual and audio evidence of each attack implemented and the associated results along with documented attack vectors used to breach client systems for record.

Executive Summary Presentation

Critical test findings and recommendations were documented in a PowerPoint presentation for Board and Senior Management. The presentation contained visual evidence of breaches along with recommended management roadmap for risk reduction.

Findings Workshop

Risk Crew additionally conducted a half-day workshop with all client stakeholders to ensure their understanding of test findings, attack methodologies, outcomes and implementation of remedial actions.

Red Team Testing was carried out by Risk Crew trained, certified & seasoned cyber security testing engineers

ABOUT THE CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

+44 (0) 20 3653 1234

riskcrew.com

info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB