

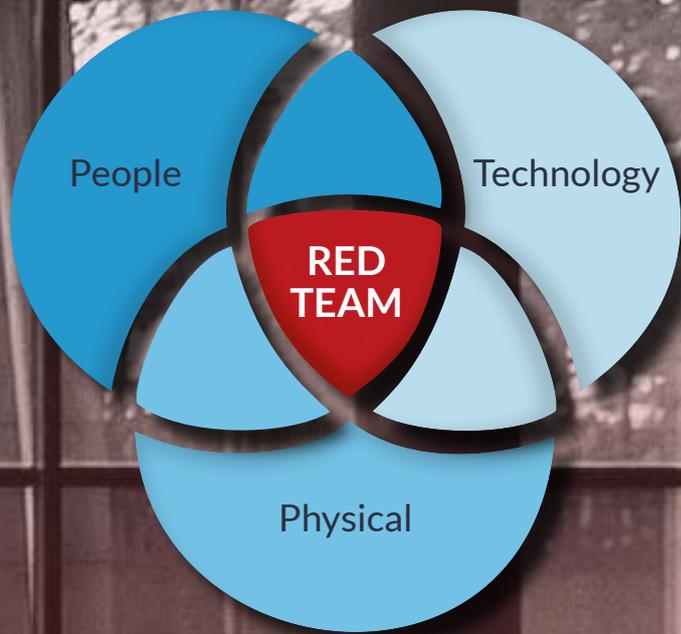


Shelter from the Storm

RED TEAM SECURITY TESTING

Knowing Your Weaknesses is More Important than Knowing Your Strengths

www.riskcrew.com/security-testing



RED TEAM TESTING

A Red Team test is a valuable method for assessing how well your organisation would defend itself against an actual (real-life) cyber-attack.

A Red Team's objective is to discover and exploit any vulnerabilities they can find to obtain unauthorised access to the sensitive data you process store and transmit on your systems. Just like an attacker would. It's best to test the effectiveness of all the controls you have put in place to prevent a breach of your data.



Unlike conventional security penetration testing, which just seeks to assess the security integrity of the technology that hosts and protects your sensitive data, Red Team Testing also seeks to test the controls you have implemented in your staff and operating locations – that if exploited – could provide access to an attacker.

A Red Team deploys authentic (Threat Actor) methodology to discover and exploit weaknesses they find in any (Attack Vector) associated with your organisation.

»»» Threat Actors

A Cyber-Threat Actor is a term used for any individual or group of individuals that could conduct a malicious cyber attack or activity against your organisation: **There are five recognised groups.**

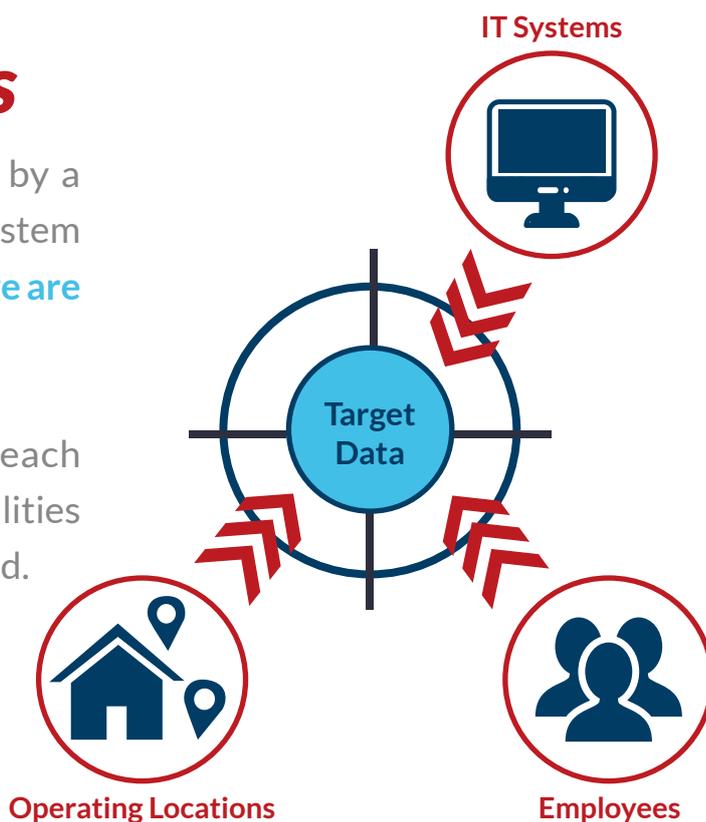


Each of these Threat Actors has different motivations, skills sets and deploy unique attack methodologies through particular “Attack Vectors” to achieve their goals.

»»» Attack Vectors

An Attack Vector is a pathway used by a Threat Actor to penetrate the target system and achieve the attack’s objective. **There are 3 recognised Attack Vectors.**

Threat Actors research and assess each Vector to identify exploitable vulnerabilities that would provide the access they need.



Red Team Testing entails the comprehensive researching and assessment of all the potential Attack Vectors associated with the target organisation and then designing and launching a series of attacks typically used by a Threat Actor over a duration of time to breach – to breach that organisations security controls.

TESTING METHODOLOGY

Risk Crew deploys a six step methodology for conducting Red Team Testing.



Set Rules of Engagement



Collect & Analyse OSINT



Plan & Map Attacks



Execute Attacks



Document Findings



Conduct Workshop

First, Risk Crew will discuss and agree on the rules of engagement for the testing with you confirming; the Threat Actors to simulate, the target objective(s), any barred tools or prohibited attacks, the testing duration, and specific Incident Response control triggers or Blue Team engagement objectives.

1

Next, we will collect all Open-Source Intelligence (OSINT) associated with the attack vectors selected for your organisation. Our Red Team will assemble all publicly available information associated with your business' operating locations, staff and information technology systems.

2

Once all OSINT information has been collected, the Red Team will then assess the data to identify potential weaknesses in security controls in each of the Attack Vectors (IT systems, operating locations and employees). The Team shall then plan specific attacks conducive to bypassing existing security controls undetected to gain unauthorised access to the target data on your systems.

3

At this stage, select targeted attacks that have been designed and mapped out by the Red Team are executed. Typical attacks may range from spear phishing, telephone pretexting, credential stealing, encryption cracking, tail-gaiting, bypassing card access systems, deploying road apples, gaining a foothold, escalating privileges, lateral movement to data exfiltration.

4

Upon completion and clean-up of attacks attempted, The Red Team shall document their findings and remedial recommendations. Documentation shall include visual evidence (screenshots) of any breaches achieved. In addition, the Team shall submit video and audio recordings of attacks where applicable.

5

The goal is to produce a document which becomes an effective tool for improving your overall information security controls and increase your organisation's resilience to real cyber-attacks. Documentation includes an Executive Report, Detailed Findings & Remedial Recommendations, Attack Vector Maps, and a Recommended Risk Mitigation Roadmap and Key Risk Indicators (KRIs) to monitor.

Following the submittal of the report of findings and recommendations, Risk Crew will conduct a workshop meeting with your organisations stakeholders to ensure their understanding of test findings and recommendations.

6

WHY CHOOSE RISK CREW

When you choose Risk Crew, you're electing to work with qualified experts.

Our skilled and experienced security engineers implement proven Red Team Testing using proprietary and open-source tools ensure they effectively assess your businesses capabilities to detect & mitigate cyber-attacks. We don't assume, we verify.

We follow Intelligence-led, multi-attack vector approach methodology that mimics the tactics, techniques and procedures of real-life threat actors and meets the TIBER-EU framework.

Our deliverables produce metrics that you can use to monitor and manage real-world cyber risks.

- + Best Practices**
Risk Crew follows best practices including ISO 27001 and NIST
- + Accredited**
Engineers carry CREST, C|EH and GIAC credentials
- + Certified**
Engineers hold ISACA CISSP, CISM and CRISC certifications
- + Subject Matter Experts**
Risk Crew engineers are SMEs with published articles in industry journals & magazines



OUR TEAM'S ACCREDITATIONS



“WHAT OUR CUSTOMERS SAY”

“The Red Team exercise was perfectly designed and we got a real value from it. We didn't know what to expect and were very impressed”

“Compared to other Information Security consultancies; Risk Crew understand both (ALL) threats and governance from a top down perspective and plugging in the necessary resources to achieve the task. It was a pleasure to have worked with Risk Crew both in the UK and Asia.”

“They were exceptionally easy to work with from contract negotiation to final deliverable and close out. Every interaction was professional and full of expertise from the Project Manager to the Security Engineer. If you are in need of solid cybersecurity expertise that you can trust, I highly recommend Risk Crew.”

“We have worked with the Risk Crew on two such projects and I was extremely pleased with the work they did for us. They worked hard to understand the nature and needs of our business, put together an innovative testing strategy and carried out that testing very effectively.”

We don't sell product — we sell results. Get some.

Let our expert security testing engineers help you stay ahead of security threats.

Contact a Red Team Expert Today

ABOUT RISK 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
United Kingdom



Shelter from the Storm