Red Team Provider Profile

Copyright

Notice

Any methodology and information contained herein is confidential to Risk Crew and is submitted to the recipient on the basis that it shall not be disclosed to any other party, either in whole or in part without the prior written consent of Risk Crew. Risk Crew is a trading name of Risk Factory Ltd.

Document Control

Document Title	Red Team Provider Profile
Author	Andrew Wilson

Document History

Version	Date Modified	Name	Remarks
0.1	05/04/2022	A. Wilson	DRAFT
1.0	02/05/2022	A. Wilson	FINAL

Table of Contents

1. Document Target Audience

Risk Crew is a Red Team (RT) testing service provider. A Red Team test is a methodology for assessing how well an organisation would defend itself against a “real life” cyber attack.

A Red Team seeks to identify and exploit *any* vulnerabilities associated with an organisation to obtain access to a specified target. The Team duplicates the tactics, techniques, and procedures (TTP) of a threat actor based on all available threat intelligence and attempts to breach the target organisation through weaknesses found in associated attack vectors (people, process, and technology systems).

The document is intended for organisations considering the procurement of RT testing services to ensure their resiliency against sophisticated cyber attacks. Due to the inherent risks associated with RT testing, the information is intended to provide potential buyers with confirmation that Risk Crew possesses the qualifications, skills, and experience to deliver effective RT testing thus minimising the risk associated with tests conducted by inexperienced personnel, which could have an adverse impact on the organisation.

Information detailed herein is based upon framework requirements as established in the TIBER-EU Framework Services Procurement Guidelines dated August 2018.

2. Company Details & Overview

Risk Factory Limited	(trading as Risk Crew Limited)
Registered & trading address:	5 Maltings Place, 169 Tower Bridge Road, London, SE1 3JB, United Kingdom
Contact number:	+44 (0)203 653 1234
Website:	www.riskcrew.com
Registration number:	07864266
Incorporation date:	November 29, 2011
VAT number:	124975201
Insurance:	Professional Indemnity Limit: 5,000,000.00

Risk Crew are a CREST-certified testing company

CREST Company ID: 7790344 - 2

Established in 2011 and headquartered in London, United Kingdom Risk Crew is a privately-owned, product-agnostic, information security governance, risk and compliance management services provider serving customers across Europe.

RT testing is a core competence.

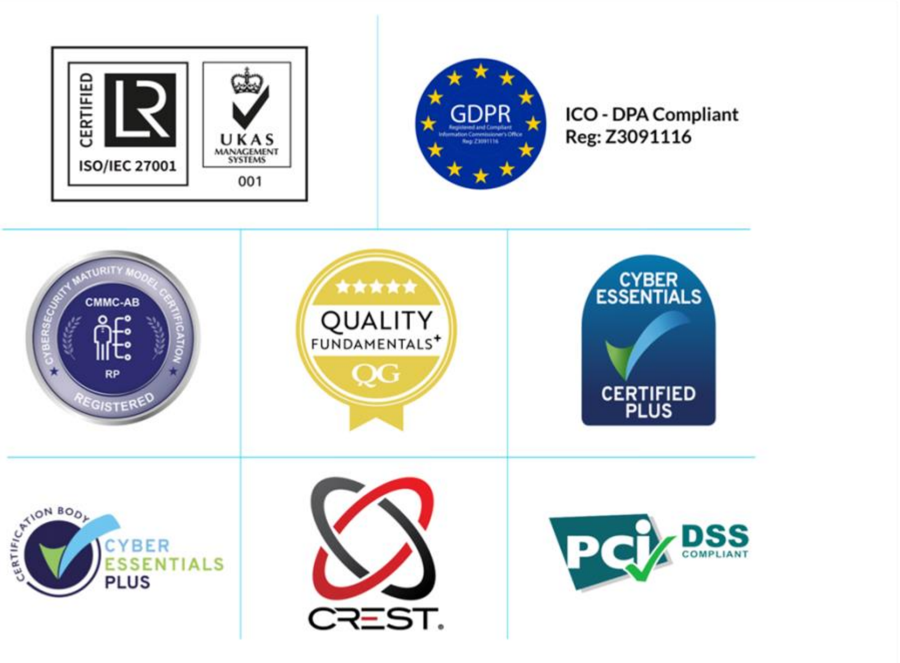
2.1 Testing Services

Risk Crew provide the following portfolio of cyber security testing services:

- Red Team Testing
- Social Engineering
- External Network Security Penetration Testing
- Internal Network Security (Assumed Breach) Testing
- Web Application Security Penetration Testing
- Risk-Driven Application Security Penetration Testing
- Mobile Application Security Testing
- API Security Testing
- Cloud Security Testing

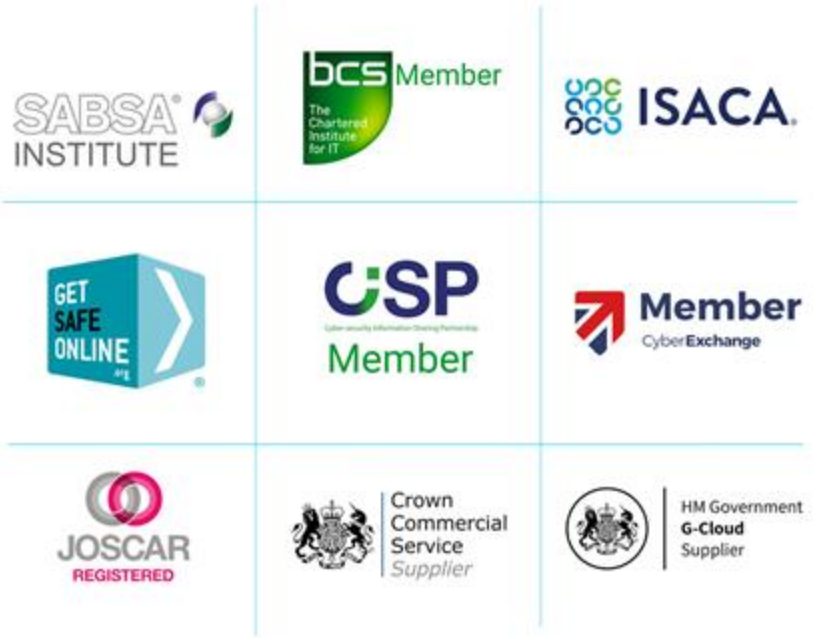
2.2 Accreditations & Certifications

Risk Crew holds the following industry accreditations:



2.3 Memberships

Risk Crew are members of the following organisations:



3. Professional Requirements Profile

As an industry-recognised, specialist Red Team (RT) provider, Risk Crew ensure minimum requirements for all of testing engagements to ensure only qualified and experienced professionals are utilised and deliver the highest quality deliverable possible.

At a minimum, Risk Crew RT engagements meet or exceed the following basic requirements.

- ✓ Company professional references from previous engagements shall be provided upon request.
- ✓ Company professional indemnity insurance is in place to cover activities which were not contractually agreed, or a result of accidents, misconduct, or negligence.
- ✓ All RT activities are overseen and ensured by a RT Test Manager.
- ✓ RT Test Manager possesses a minimum of five years' experience in delivering intelligence-led red team tests.
- ✓ RT Test Manager possess professional qualifications and certifications that meet or exceed those established in the TIBER-EU Framework Services Procurement Guidelines dated August 2018.
- ✓ RT Tests Manager C.V. and references are provided to the client upon request.
- ✓ Background checks are competed on all RT members.
- ✓ Enhanced background checks are conducted upon request on all RT members as may be required by local or national authorities.
- ✓ All RT members possess professional qualifications and certifications that meet or exceed those established in the TIBER-EU Framework Services Procurement Guidelines dated August 2018.
- ✓ RT Team members C.V. are provided to the client upon request.
- ✓ RT members possess a broad range of knowledge and skills to include basic business knowledge, OSINT, reconnaissance, threat intelligence analysis, threat actors, TTP, threat vectors, red team testing, penetration testing, social engineering, vulnerability analysis, exploit development and payload creation, physical penetration, and combinations thereof.

4. Reputation, History & Ethics

Founded in 2011, Risk Crew has been providing product-agnostic cyber security testing and information security governance, risk, and compliance services to clients across the European Union for over 10 years.

At Risk Crew we set out to do something different. We wanted to form a company of information risk professionals *for* information risk professionals. Our industry is product-lead. Marketing professionals have sold us the idea that security is a product. We believe that security is a process – not a product. The company was founded on the principle that "cyber security" is an oxymoron and that real cyber security is risk management.

As a result, we have developed and enjoy a reputation in the industry and more importantly – with our customers – for designing and delivering creative, cost-effective cyber security testing and risk management services that meet both customer-specific risk appetites as well as, regulatory, legislative, and commercially recognised best practices.

Risk Crew are a hand-picked group of information security risk management and testing professionals selected for their knowledge base, communication skills and passion for what they do. Our consultants are not typical – they take things personal. Your problems become their problems and they don't give up until they're solved. There is no stronger customer service ethic.

Crew members are chosen for their vision, innovative thinking, and facility to embrace change. Given the constant changes in threats, vulnerabilities and technology, effective risk professionals are those that expect it.

Our history of over a decade of success is built on our reputation for:

- Thinking deeply – We take nothing for granted and think beyond current beliefs, preconceived ideas, and prevailing opinions.

- Questioning assumptions – We do not assume answers to problems, we verify them.

- Detecting cause and effect – We confirm the causal relationship between events to confirm the source of a problem.

- Delivering pragmatic, measurable results – We include key performance indicators in all of our services to confirm their ongoing effectiveness.

These ethics are programmed in our DNA along with a strong belief in knowledge transfer and complete customer satisfaction. Which is why we back all of our services with a 100% guarantee. Nobody else in our industry does that.

5. Governance, Security & Risk Management

Corporate governance, security and risk management are critical to Risk Crew. We practice what we preach and have implemented a comprehensive and detailed corporate governance administrative framework to ensure the ongoing quality and dependability of our business processes. Our established operating policies and procedures and quality assurance processes are subject to annual compliance auditing.

Risk Crew operations are certified to ISO/IEC 27001:2013 and recertified annually. We have a documented risk appetite and conduct annual risk assessments and maintain a risk treatment plan managing all risks to well below our stated appetite. We have an established information classification scheme and maintain an information asset register with assigned owners also verified annually. Customer sensitive information – such as RT testing details and associated findings are classified as "Confidential" encrypted in storage and in transit, assigned information owners who restrict and document "need to know" access.

All staff are subject to extensive background checks prior to employment and receive initial and continuous security awareness training. We have established information security policies and procedures; a dedicated and experienced Information Risk Manager and staff are subject to random and annual compliance auditing.

Business information technology systems are subject to monthly vulnerability scanning and quarterly security penetration testing Security incident reporting procedures are in place and Incident Response, Business Continuity and Disaster Recovery plans are tested annually.

Our robust ISMS and bespoke security control framework provides a clear governance structure and processes, which are effectively established, implemented, operated, continuously monitored, tested, reviewed, maintained, and improved.

We provide assurances to our customers that the security of and risks associated with their business systems and confidential information (together with any other business risks) are adequately addressed. Indexes to internal policies and redacted content samples can be provided to customers upon request.

6. Tester Competence & Qualifications

Risk Crew Red Teams are assembled and comprised of the following professionals:

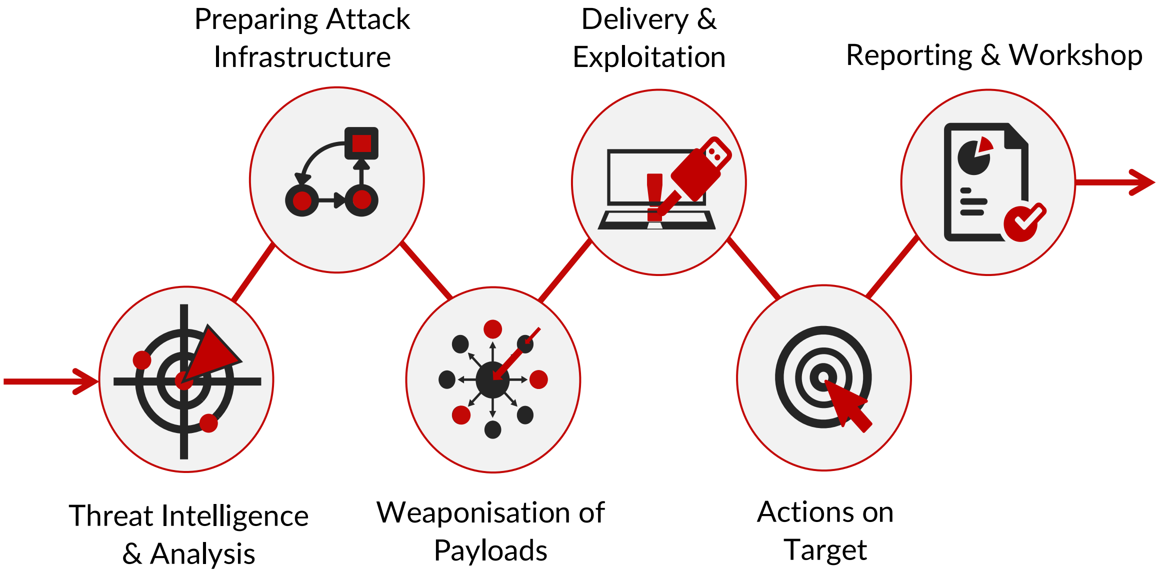
Tester Name	Location	Seniority	Qualifications	Testing Skillset
John Hannay	UK	Senior	CRT, CCT-APP, OSCP, CSPA, CRTSA	Web Application Mobile Application Network Testing Assumed Breach API Testing Cloud Testing Red Team Testing Social Engineering
Hugo Valette	UK	Senior	OSCP, CSPA	Web Application Mobile Application Network Testing Assumed Breach API Testing Cloud Testing Red Team Testing Social Engineering
Matt Graham	UK	Senior	OSCP, CRT	Web Application Mobile Application Network Testing Assumed Breach API Testing Cloud Testing Red Team Testing Social Engineering
Holly Grace-Williams	UK	Senior	CRT, CCT-APP, CompTIA Pentest+, GIAC	Web Application Mobile Application Network Testing API Testing Cloud Testing Red Team Testing Social Engineering
Dave Hewson	UK	Senior	CRT, CCT-APP, OSCP, CSPA,	Web Application Mobile Application Network Testing API Testing Cloud Testing

				Red Team Testing
Gaston Perez-Martin	UK	Senior	CRT, OSCP, GIAC, CEH	Web Application Mobile Application API Testing Assumed Breach Network Testing Cloud Testing
Gabriel McLeish	UK	Mid-Level	OSCP, CPSA, CEH	Web Application Mobile Application Network Testing Assumed Breach API Testing Cloud Testing Red Team Testing
Jake Kelly	UK	Mid-Level	OSCP, CEH, GIAC	Web Application Network Testing Cloud Testing Social Engineering
Ross Brimble	UK	Mid-Level	OSCP, CEH	Web Application Network Testing Cloud Testing Social Engineering
Rish Verma	UK	Senior	CRT, CCT-APP, OSCP, CSPA,	Web Application Mobile Application Network Testing Assumed Breach API Testing Cloud Testing Red Team Testing Social Engineering
Mahendra Singh	India	Mid-Level	OSCP, CEH, ECSA, CSPA	Web Application Mobile Application Assumed Breach Network Testing API Testing Cloud Testing

Juan Manuel-Garcia	Argentina	Senior	OSCP, GPEN, CEH, CHFI, CEI, CEICP	Web Application Mobile Application Network Testing API Testing Cloud Testing Red Team Testing
Diego Ceballos	Argentina	Mid-Level	OSCP, CEH, CISSP	Web Application Mobile Application Network Testing Assumed Breach API Testing Cloud Testing
Ivan Huertas	Argentina	Mid-Level	OSCP, CEH, CISSP	Web Application Mobile Application Network Testing API Testing Cloud Testing
Dario Escarlon	Argentina	Junior	CEH, CISSP,	Web Application Network Testing Cloud Testing

7. Methodology

While each RT engagement is customised to meet our client's specific requirements, Risk Crew typically deploy the following methodology as a guideline:


Preparing Attack Infrastructure
Delivery & Exploitation
Reporting & Workshop
Threat Intelligence & Analysis
Weaponisation of Payloads
Actions on Target

Phase 1: Threat Intelligence & Analysis

The first step is to collect all applicable threat intelligence from an established Threat Intelligence (TI) provider and available open-source intelligence (OSINT) resources associated with all the Attack Vectors associated with the client. This will include but not be limited to the following activities:

Threat Intelligence

Risk Crew will begin by contacting their Threat Intelligence (TI) provider and soliciting current and applicable threat intelligence associated with the target organisation. TI plays a crucial role in the RT process. It provides the RT with a comprehensive report that formulates threat scenarios aimed at mimicking potential threat actors' attacks against the live systems that underpin the critical functions of the target organisation. These threat scenarios form the basis of the attack scenarios the RT provider will deliver.

Creating accurate and realistic threat intelligence is a complex activity. This means that the TI provider must have adequate knowledge of the threat actors, their motives, skills and TTPs, as well an understanding of how the core elements of the target system interact and operate. In addition, the TI provider must have a good insight into the targeted entity. It needs to know for example: what the target's critical functions are; how the target operates; who the crucial employees are and whether they are "viable" for the attack; and what the target's vulnerabilities are. The TI report provides the RT with the information needed to simulate a real-life and realistic attack on the target's live systems underpinning its critical functions.

Social media analysis

The RT also researches and assesses publicly available personal and professional information associated with the target organisation. This typically includes email addresses, social media profiles, phone numbers, employee ID numbers, and so on and of course any employee credentials that have been previously compromised. This information will be utilised for targeted phishing attacks against employees of interest in future phases of the engagement.

The RT also seeks to harvest information about the target organisation's technical stacks by analyzing the social media profiles of relevant personnel or previous key members of staff. Information may be disclosed in job descriptions such as "Was responsible for the deployment of Crowdstrike across the entire estate". This would allow Risk Crew to craft tailored payloads against the security controls in place.

Internet facing assets discovery

The RT enumerates external facing assets utilising numerous techniques such as subdomain enumeration, domain name historical analysis, passive, and active scanning, and "Whois" querying. This information allows the RT to discover external services which could present vulnerabilities and therefore allow the Red Team to gain a foothold on the target organisation's systems.

The RT also analyses existing DNS records, particularly those relating to the flow of emails to and from the target organisation to identify if the current configurations could allow the team to spoof emails. In addition, other records may disclose the usage of certain SaaS applications which could be used as whitelisted public Command & Control (C2) channels by the RT, or simply act as a good pretext for social engineering attacks.

Preliminary phishing

The RT typically sends phishing emails, Vishing or Smishing communications to entice target employees to click on a link, which in this phase will not deliver malware. However, should a member of staff fall victim to the attack, the RT would harvest information such as browser versions, Operating System versions, the usage of .NET within the organisation, the public IP addresses of target organisation's VPN, out of office email footers and whether the link was also followed by a third-party security vendor. This information could then be used to tailor specific payloads in future attacks against the organisation.

Phase 2: Preparing Attack Infrastructure

With the information collected in the first phase, the RT then begins preparations with goal of gaining their initial foothold on the target organisation's internal network. Consequently, the RT will conduct the following activities:

Building a lab environment

The RT typically builds a lab environment which replicates the technology stack identified in the threat intelligence and reconnaissance phase of the engagement. It will include the Anti-Virus, Endpoint Detection & Response, Web Gateway, and next-generation firewall products. The lab will be used by the RT to ensure their payloads bypass (or trigger insufficient noise on) the tools in question before these are delivered to the target organisation.

Configuring attack servers

The RT typically configures a server dedicated to targeting the organisation's employees in social engineering attacks. The RT will also then determine appropriate pretexts for the phishing emails. The RT will determine a C2 channel which is acceptable for the engagement. For instance, the client may not authorise the usage of a public C2 channel over known SaaS applications which would allow the traffic to go undetected by security products. In that case, the channel would need to communicate directly to Risk Crew's cloud infrastructure. Following channel approval, the RT would then build and configure the attack servers and appropriate forwarders (i.e., reverse proxies).

Acquiring domain names

The RT would also typically acquire domain names for the C2 channels (if appropriate), and the phishing pretexts described above. The RT would use tools to discover trusted domain names which have a history and are available for purchase.

Phase 3: Weaponisation of Payloads

With a lab environment replicating the target organisation's security technology stack, the RT would then create payloads and plan attacks against the external facing assets, this step would include:

Creating payloads

The RT would typically design payloads which could be delivered to the target organisation's employees via social engineering means. For instance, they will create Office documents with executable code (in the form of VBA macros) and test these inside the lab environment created in the previous phase of the engagement. Should a legal requirement exist to introduce guard rails, the RT will include Active Directory Domain Names or IP addresses in the documents to ensure the payloads do not execute on devices outside of the target's perimeter. In addition, the RT would design multiple phishing templates with varying goals, such as enticing the client's employees to divulge a password, tricking them into executing documents or social engineering them to respond to specific emails to gain information.

Planning attacks against external infrastructure

Next, the RT would identify external facing services which likely do not have two-factor authentication in place, these could then be targeted in the next phase with credential stuffing attacks. Consequently, the RT would create wordlists containing usernames gathered in the reconnaissance phase and spray these against weak passwords. With client approval, the RT may test certain internet facing assets (such as web or mobile applications) which could allow them to gain a foothold on target's internal infrastructure.

Phase 4: Delivery & Exploitation

Given that the payloads have now been tested and validated against a replicated lab environment, the RT would then seek to deliver them in order to gain an initial foothold inside the target's internal network. The delivery methods will include but not be limited to:

Phishing, Smishing & Vishing

Based on the activities of the previous phases, phishing attacks against the target organisation are launched. The RT would then attempt to get a foothold in the target system by delivering malicious attachments or malicious links via email, text message or voice mail attack vectors.

From there, they would attempt to turn this foothold into persistent access to the internal network. This will ensure that the next phases can be conducted without having to execute this phase again. The attacks involve gaining credentials to systems and intercepting two factor authentication codes by social engineering the victim if required. For instance, should access to Office 365 require a second factor of authentication, the phishing landing page will include a form to capture that code.

Attacking the external perimeter

Next the RT would typically attempt to identify and exploit security vulnerabilities associated with the exterior-facing systems to gain unauthorized and undetected access to the insider of the network. Prior client approval is vital since the OSINT may have mistakenly classified an internet facing asset as belonging to the client, and therefore RT would be breaking the UK Computer Misuse Act.

In addition, the RT may perform brute forcing and password spraying attacks using the lists designed in the Weaponisation of Payloads phase (above). It should be noted that this technique may be utilised to simply distract the organisation's security team stakeholders while conducting the next phase of the engagement.

Bypassing Physical Access Controls

The RT could also attempt to bypass visitor and physical access security controls deployed at the client's operating locations to obtain the stated testing objectives. To do so, the RT would typically deploy the following methodology:

Reconnaissance: The RT would conduct reconnaissance of the target locations with the objective of identifying potential vulnerabilities in physical, human factors and/or monitoring controls, which if exploited, could result in undetected or unauthorised access. Information gathered during reconnaissance shall be used to attack site-specific attacks conducive to exploit.

Design Attacks: The RT would then design site-specific attacks to test the effectiveness of the following access control areas:

Perimeter & Building Access Controls

- Perimeter fences, gates, walls, etc.
- Building fire escapes, evacuation points, smoking areas, loading bays etc.
- Staff and visitor car park surveillance
- Offices, conference rooms, storage, and common areas.

Security Policy Compliance

- Compliance to visitor identification procedures
- Compliance to visitor badging requirements
- Compliance to visitor escort requirements
- Compliance to no-tailgating policy
- Compliance to escorted visitor requirements

Reception Visitor Procedures

- Visitor challenge requirement
- Visitor identification requirement
- Visitor badging requirement
- Visitor sign-in procedures
- Visitor escort procedures
- Prohibiting visitor tailgating

Device & Information Controls

- Sensitive information is not left unattended
- Sensitive information is not discarded
- Computer devices signed-in are not left unattended
- Capturing information displayed on unlocked user screens

Phase 5: Actions on Target

Once the RT have obtained access to the target systems, the last phase of the engagement is to complete any objectives specifically identified by the client. For example, purposes these could typically include:

- **Gaining access to specific target(s):** The RT could try to identify these systems as well as the client's employees with access to them. From there, either the systems are targeted directly, or such employees are compromised and monitored for the purpose of gaining access to the targets. The actions on target phase are useful to demonstrate the real impact of a breach as well as to assess the last layer of security controls which can detect and prevent an incident from having devastating consequences for the business.

- **Data exfiltration:** The RT could recreate the scenario of a threat actor attempting to exfiltrate sensitive data from the network. This helps to assess the ability to detect and prevent such activities.

- **Detection exercise:** Should the RT go undetected in their activities, and in order to provide a simulated real-world exercise and training for the client, the RT could deliberately increase the noise of their attacks to prepare the client's Incident Response capability for future attacks.

Phase 6: Reporting & Workshop

Upon completion of attacks, The RT then documents the findings and remedial recommendations. The goal is to produce a document which becomes an effective tool for improving the client's security defences and increases resilience to cyber-attack.

The result of this process is a report containing details of the threat actor's simulated, the attack vectors, successfully exploited, the security controls circumvented as well as detailed recommendations to help the organisation improve its security controls to ensure that such a threat would be stopped as early in the attack chain as possible.

The report is structured in the following sections:

- **Executive Report:** An initial, self-contained executive summary report will be delivered. This is a non-technical report which mainly focuses on contextualising the identified issues and scenario outcomes into business risk.
- **Attack Vector Mapping:** The attack vectors described in the report will consist of the real attack paths taken by the Red Team which will help the client understand areas focus their defences
- **Risk Mitigation Roadmap:** This section of the report will provide high level risk management information with short, medium, and long term suggested actions to prioritise risks against resources. It will focus on identifying relevant flaws in processes and procedures rather than specific vulnerabilities, so that the root cause of the issues can be tackled.
- **Key Risk Metrics:** This document shall provide metrics resulting from the attacks and suggested metrics to include in future RT testing.
- **Evidence:** Any evidence that proves that systems, staff, or locations were compromised which could include password hashes, sample command & control traffic, body cam footage or screenshots.

Following the submittal of the report of findings and recommendations, the RT would then conduct an on-site workshop meeting with the client's stakeholders. The RT Leader and a Team Member would attend to explain attack methodologies and present evidence. The objective of the workshop is to add significant narration around the reporting.

We believe that it is important that the RT explain what, how and where they found and exploited vulnerabilities, as well as providing significant remediation advice in a face-to-face session.

8. Designated Threat Intelligence Providers

Threat intelligence-based scenarios that simulate the tactics, techniques, and procedures (TTPs) used by real-life threat actors are essential to the success of Risk Crew's red team testing engagements. Current threat intelligence provides specific and detailed information about a target organisation's attack surface and ensures actionable and realistic testing scenarios are used by the RT.

Risk Crew typically obtains TI from the following commercial providers:

Darktrace: www.darktrace.com

Private Company Founded 2013 United Kingdom

Darktrace is a UK-based TI provider. Founded in Cambridge, UK, in 2013 by mathematicians and machine learning specialists from the University of Cambridge, together with world-leading intelligence experts from MI5 and GCHQ provide target-specific cyber threat intelligence to both government and business sectors.

Digital Shadows: www.digitalshadows.com

Private Company Founded 2011 United Kingdom

Digital Shadows is a UK-based TI provider. Founded in the UK in 2011, they are a cyber threat intelligence company which provides sensitive data exposed through social media, cloud services and mobile devices.

Both TI providers meet or exceed requirements as those established in the TIBER-EU Framework Services Procurement Guidelines dated August 2018.

9. Contact Details

For more information regarding Risk Crew's Red Team testing methodology, qualifications, skills, or experience, contact:

Andy Wilson

Technical Account Manager

T: +44 (0) 203 653 1234

E: andy.wilson@riskcrew.com | **W:** www.riskcrew.com