

特发信息

risk  
CREW



## ABOUT US

Risk Crew is an elite London-based, information security governance, risk, compliance and testing consultancy. Experts in the cyber threat landscape, we excel in creating cost-effective controls and processes to meet these threats and comply with legislation, regulation and best commercial practices. We also put skin in the game and provide a 100% satisfaction guarantee on all our services. **Put us to work for you today.**



## CONTACT US

5 Maltings Place  
169 Tower Bridge Road  
London, SE1 3JB  
United Kingdom  
+44 (0) 203 653 1234  
information@riskcrew.com  
[www.riskcrew.com](http://www.riskcrew.com)

# RED TEAM TESTING

---

Service



## SERVICE

### Multi-vector attack simulations

A Red Team is a group of ethical hackers who execute a series of coordinated attacks on an organization's people, process and technology to simulate how an intruder could obtain unauthorised access.

Risk Crew will provide a certified and experienced Red Team to design and deliver multiple synchronized technical and social engineering attacks to test your organisation's overall defences. Simulated attacks will be based upon current threat vectors, methodologies and payloads. Attack sophistication, targets, objectives and timelines will be agreed in advance to ensure results serve your risk objectives.

*"Don't look at the hole in the donut, look at the whole donut"*

*Anonymous*



## METHODOLOGY

### People, Process & Technology

Simulated attack methodologies shall be determined based upon your specific risk objectives, however, include attempts to identify and exploit vulnerabilities in your people, process and technology.

Attacks shall be designed based upon data collected in surveillance and through open source intelligence gathering techniques. A typical Red Team test is comprised of selected social engineering attacks such as phishing, catfishing, telephone pretexting, smishing, vendor scams, road apples, piggy backing VoIP or RFID spoofing designed to provide information to support system and device technical penetration depending upon the stated objectives.



## DELIVERABLE

### Measurable results

The service results in a detailed report of our findings and remedial recommendations to holistically improve your defences against a real-world attack. Report shall include all photographic, video and audio evidence collected during the attacks along with suggested key performance indicators for implementation to monitor and measure improvement. We will present these findings in a workshop with your stakeholders to ensure their understanding.

