Shelter from the Storm

RED TEAM

Essential KPIs & Metrics

THE PLAYERS INVOLVED

RED TEAM

In an information or cyber security context, a Red Team is a group of ethical hackers that design and execute a series of coordinated technical and social engineering attacks on an organisation's people, operating facilities, and technology to simulate how an intruder could obtain unauthorised access to its systems or information assets.

Technically, a Red Team is an independent group that challenges an organisation to improve its effectiveness by assuming an adversarial role or point of view – seeing the organisation through a threat actor's perspective. Think of them as a stand in for the offensive team. The Red Team emulates **Tactics, Techniques, and Procedures (TTPs)** of threat actors to test the effectiveness of the security controls implemented holistically across the organisation.

BLUE TEAM

If the Red Team is playing offence, then the Blue Team is playing defence. A Blue Team is a group of designated stakeholders within the business responsible for identifying, minimising and managing the impact of a cyber security attack. This could be a security operations centre (SOC) or any group of individuals professionally responsible for detecting, assessing and appropriately responding to a cyber-attack.

The Blue Team is the first and most critical line of defence in the business. It is entrusted with verifying the ongoing security integrity of the systems and the data it processes, stores and transmits. How fast and effectively a Blue Team can discover and respond to a breach is mission-critical to the business's risk objectives.

PURPLE TEAM

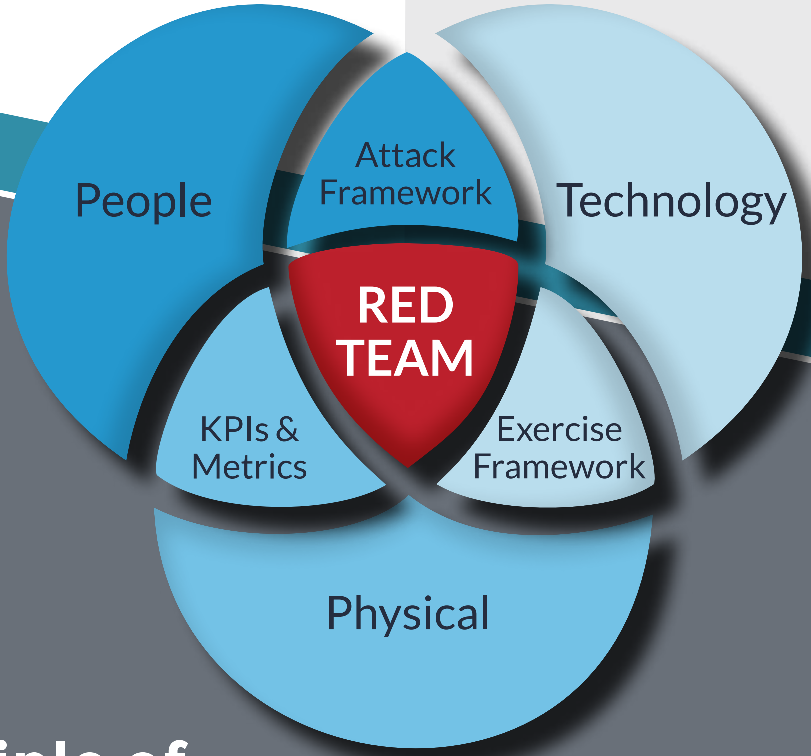
If a Red Team is playing offence and a Blue Team is playing defence, a Purple Team is like the referee. Purple Team is the term used to describe a Red Team and Blue Team that work against each other transparently in unison for purposes of knowledge transfer and to improve the business's overall security. Essentially, "Purple Teaming" is synonymous with Red Team vs. Blue Team exercises.

A Purple Team is a group comprised of key members of both the Red Team and the Blue Team. A Purple Team Exercise is an open engagement where the attack activity is transparent and explained in detail step-by-step, to the Blue Team as it occurs. They are "hands-on keyboard" exercises where Red and Blue Teams work together — with the Red Team openly explaining and discussing each specific attack TTP with the Blue Team in order to improve their identification and response capability.

THE RED TEAM APPROACH

Red Team Testing seeks to test all of the security controls you have implemented across your business in your people, process, and technology against real-life cyber-attack methodologies based on open-source available information.

This holistic, intelligence-led testing approach differs from conventional security penetration testing, which seeks to assess the security controls deployed in the systems that host your sensitive data. It's an effective methodology for testing the organisation's exposure and not just its technology.



The driving principle of conducting a Red Team Test is: "KNOW THYSELF"

This testing has a proven methodology for understanding how well your business would fare against a real-life cyber-attack.

ATTACK FRAMEWORKS

There are several industry-recognised frameworks providing Red Team attack methodologies that emulate the TTPs of threat actors. The top three are recognised as follows and can be found at the links:

THE MITRE ATT&CK FRAMEWORK

Commonly acknowledged as the industry standard it defines the terminology for Adversary Tactics, Techniques and Common Knowledge.

THE LOCKHEED MARTIN - CYBER KILL CHAIN FRAMEWORK

This industry-recognised framework details how threat actors work and the steps they perform during a breach.

THE UNIFIED - CYBER KILL CHAIN FRAMEWORK

This academic framework brings together a number of differing cyber kill chain methodologies for a more unified approach.

The attack framework selected by your Red Team should be applicable to the threat actors the team seeks to emulate and the business's cyber risk objectives.

The frameworks should be repeated for each consecutive test so that selected key performance indicators and metrics can be duplicated and continuous improvement can be assessed and evidenced.

EXERCISE FRAMEWORKS

Heavily regulated industries often require that Red Team engagements follow industry-specific frameworks in conducting the tests. Before you scope your Red Team test you should consider and research any regulatory or jurisdictional requirements. The following are the most recognised and can be found at the links:

G-7 Fundamental Elements for Threat-Led Penetration Testing

The Group of 7 nations provided guidance on performing Threat-Led Penetration Testing.

CBEST Intelligence Led Testing – Bank of England

The United Kingdom regulation for financial institutions operating in England.

Threat Intelligence-Based Ethical Red Teaming – TIBER-EU

The European Union regulation for financial institutions operating in the EU.

Red Team: Adversarial Attack Simulation Exercises – ABS (Association of Banks of Singapore)

Framework issued by the Bank of Singapore for financial institutions in Singapore

Intelligence-led Cyber Attack Simulation Testing (iCAST) – HKMA (Hong Kong Monetary Authority)

Framework issued by the Hong Kong Monetary Institution for financial institutions in Hong Kong.

Financial Entities Ethical Red-Teaming – Saudi Arabian Monetary Authority

Framework issued by the Saudi Arabian Monetary Authority for financial institutions in Saudi Arabia. ng.

Framework for the Regulatory Use of Penetration Testing and Red Teaming in the Financial Services Industry – GFMA (Global Financial Markets Association)

Framework issued by the Global Financial Markets Association to create a global framework that would meet multiple countries' regulatory requirements.

RULES OF ENGAGEMENT

Regardless of the attack or exercise frameworks utilised for testing, all Red Team engagements should follow clear and documented "Rules of Engagement". The rules of engagement (ROE) establish the responsibilities, relationships, and guidelines among the Red Team, the customer, the system owner, and any stakeholders required for the execution of the execution.

Comprehensive ROE detail the purpose of the test, its specific goals and objectives along with which attack or exercise frameworks should be used in testing.

Rules specify the key performance indicators and metrics to be captured during testing.

They identify the threat actors and associated TPPs to be emulated, define and document the exact scope and depth of the testing.

Additionally, rules identify points of contact both sides along with applicable escalation procedures and contact details.

Red Team testing ROE establish the ground rules: what tools can and cannot be used in testing and how far can testers go. The ROE establish what is "in bounds" and what is "out of bounds"? It is all documented – in minute detail – and should be agreed by signature and attached to the service level agreement approved for the engagement.

WHAT IS A KPI?

A (KPI) KEY PERFORMANCE INDICATOR IS A QUANTIFIABLE VALUE USED TO TRACK PROGRESS TOWARDS A KEY BUSINESS GOAL

A KPI or a key performance indicator is a quantifiable value used to track progress towards a key business goal. They are measurements that provide a high-level perspective for making strategic decisions. So, KPIs provide direction towards achieving desired results and therefore can help a business make better-informed decisions.

A GOOD KPI SHOULD BE:

- Clearly Defined
- Relevant to the Business
- Able to Show Performance in Achieving a Goal

Since the purpose of conducting Red Team testing is to assess your business's ability to withstand a real-world cyber-attack, the goal of the KPIs you select should be to assess the business' performance in identifying, minimising, and managing the attacks simulated in the exercises.

ESSENTIAL RED TEAM TESTING KPIs

While there are many measurements you can take to evaluate your business' performance under a cyber-attack, these are the five essential KPIs to capture in each test (and repeat in subsequent tests) — so that you can document and measure your improvement:

Mean Time to DETECT

Mean Time to RESPOND

Mean Time to INITIAL ACCESS

Mean Time to ACT

Time to Full REMEDIATION

Mean Time to DETECT

Mean time to detect: Mean time to detect or discover (MTTD) is a measure of how long a problem exists before the business becomes aware of it. It's an essential Red Team KPI for obvious reasons — if the business is not aware of a security incident — it cannot respond and manage it. For Red Team testing, the KPI should measure the duration of time between the start of the Red Team TTP activity and the identification of the activity by the business (Blue Team). To calculate the testing MTTD, add all the TTPs detection times associated with the test and divide it by the number of attacks. Tracking this KPI allows you to show (document) improvement in the business' incident detection capability.

Mean Time to RESPOND

Mean time to respond (MTTR) is a measure of how long it takes after a problem is detected — for the business to respond and assess it. This is an essential Red Team KPI as it is critical that a business responds to assess a security incident before it escalates. For Red Team testing, the KPI should measure the duration of time between the time the Red Team TTP activity is detected and the time it takes for the business (Blue Team) to respond and start their assessment of the activity. To calculate the testing MTTR, add all the TTPs response times associated with the test and divide it by the number of attacks. Tracking this KPI allows you to show (document) improvement in the business's incident response capability.

Mean Time to INITIAL ACCESS

Mean time to initial access (MTTIA) is a measure of the length of time it took the Red Team to gain initial access to your systems after initiating the attack. This is an essential Red Team KPI as it indicates the strength of your perimeter security controls and your end user's vulnerability to social engineering attacks like phishing. For Red Team testing, the KPI should measure the duration of time between the time the Red Team TTP activity is initiated and the time it takes for them to obtain unauthorised access to your systems. To calculate the testing MTTIA add the duration of start and stop times for each of the attacks implemented by the Red Team intended to obtain unauthorised access – and divide the sum by the number of attacks. Tracking this KPI allows you to show (document) improvement in perimeter and phishing controls.

Mean Time to ACT

Mean time to act (MTTA) is a measure of how long it takes after a problem is responded to before the business takes action to address it. This is another essential Red Team KPI as it is critical that a business act as soon as possible to address a security incident before it escalates or disrupts operations. For Red Team testing, the KPI should measure the duration of time between the moment the business (Blue Team) responded to a Red Team TTP activity, to the time a solution to address the TTP is implemented. To calculate the testing MTTA, add all the TTPs reaction times associated with the test and divide it by the number of attacks. Tracking this KPI allows you to show (document) improvement in the defence posture of the business holistically.

Mean Time to Full REMEDIATION

Time to full remediation is the measure of how long it takes after a vulnerability is identified and exploited by the Red Team. The risk is either accepted or remediated, and documented on the business's risk treatment plan. This essential KPI indicates the business's ability to follow through in addressing risks raised in the testing. Calculating the time to full remediation should be obvious. Tracking this KPI allows you to show (document) commitment to risk management.

WHAT IS A METRIC?

A METRIC IS A QUANTIFIABLE MEASURE USED TO TRACK PROGRESS AND EVALUATE SUCCESS

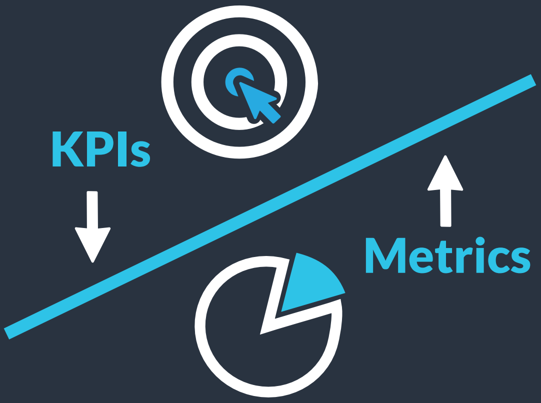
Metrics measure specific activity or process. The provide a granular view relevant to a specific activity and are used for tactical decision making.

Red Team testing metrics are measurements used to track the progress and performance of the TTPs associated with the attacks implemented by the team that are critical to the successful outcome of the test (unauthorised access).

It's important not to confuse metrics with KPIs. Red Team KPIs are tied to specific goals while metrics are data points in the testing.

KPIs are tied to specific goals

Metrics are data points



Testing data points (metrics) should be captured and documented by both the Red Team and the business (Blue Team) that measure their performance.

ESSENTIAL RED TEAM TESTING METRICS

There are many measurements you can take to evaluate the performance of your Red Team test. Things like the number and type of vulnerabilities identified, the number and type of vulnerabilities exploited, or the number of successful phishing attacks — make sense. While these are good metrics they don't represent the strength and the weaknesses of the Blue Team – which is what you should seek to understand.

The metrics you collect should provide insight into the business' (Blue Team's) strengths and weaknesses and fairly measure their performance in defending the systems. Consequently, we suggest that you select these metrics with your Red Team provider as its essential that they be derived from the TTPs implemented in the test i.e., how well or how poorly did they respond to specific attacks?

Your metrics should be focused on measuring Red Team attack progress and business (Blue Team) detection and response durations. The best way to do this is to have your Red Team set up an Excel spreadsheet in conjunction with the business (Blue Team) documenting specific details for each attack.

TTP Maps

Hostname & Host Types

Action Timestamp

Response Timestamp

Kill Chain Step Maps

Type of Detection Expected/Lacking

Detection Timestamp

Business Unit Reaction

TTP Maps

Attack TTPs should be mapped to the testing framework task used (i.e., Mitre ID). This allows a heat map to be created which identifies the Blue Team's strengths and weaknesses in detection capabilities for each attack.

Hostname & Host Types

Documenting these allows the Teams to see which operating systems have which strengths and weaknesses.

Action Timestamp

Documents when TTPs are initiated by the Red Team. The timestamp should be synchronised with the Blue Team (and/or SOC's SIEM).

Response Timestamp

Documents when TTPs are responded to by the Blue Team The timestamp should be synchronised with the Blue Team (and/or SOC's SIEM).

Kill Chain Step Maps

Similar to TTP Maps, this also measures the detection and response capabilities strengths and weaknesses of the Blue Team.

Type of Detection Expected/Lacking

Allows the team to map which controls are performing well, and / or which are underperforming.

Detection Timestamp

Documents when TTPs are detected by the Blue Team The timestamp should be synchronised with the Blue Team (and/or SOC's SIEM).

Business Unit Reaction

Identifying reaction times from specific parts of the business (IT versus marketing) may provide insight into which departments need more collaboration with security.

Whatever metrics you select we suggest that you keep them simple and straightforward — and that they are agreed with your testing supplier in advance of testing. Most importantly, they should be meaningful to improving the performance of your defensive capabilities.

RED TEAM SUCCESS

Red Team exercises are a critical component of your business's cyber risk management strategy, so it's vital to measure the success of these exercises in order to determine their effectiveness. Measuring the success of a Red Team exercise can help you determine whether you need to make changes to your security strategy – and that kind of information is invaluable.

You don't know what you don't know – UNTIL YOU TEST WHAT YOU THINK YOU KNOW

GET STARTED WITH RED TEAM

Risk Crew CREST Accredited Red Team Testers can give you a security view from the outside to secure your defences on the inside.

Request a Quote 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