Red Team Metrics Quick Reference Sheet

Designed to help you ...

- ✻ Understand the customer's business questions
- 1 Identify relevant target metrics
- 2 Collect data to address the target metrics
- 3 Analyze risks associated with the target metrics
- 4 Assess and communicate the risk or business impact

- **At** Attack-based metrics
- **V** Vulnerability-based metrics
- **C** Consequence-based metrics
- **Ad** Adversary-based metrics
- **P** Protection-based metrics
- **T** Threat-based metrics

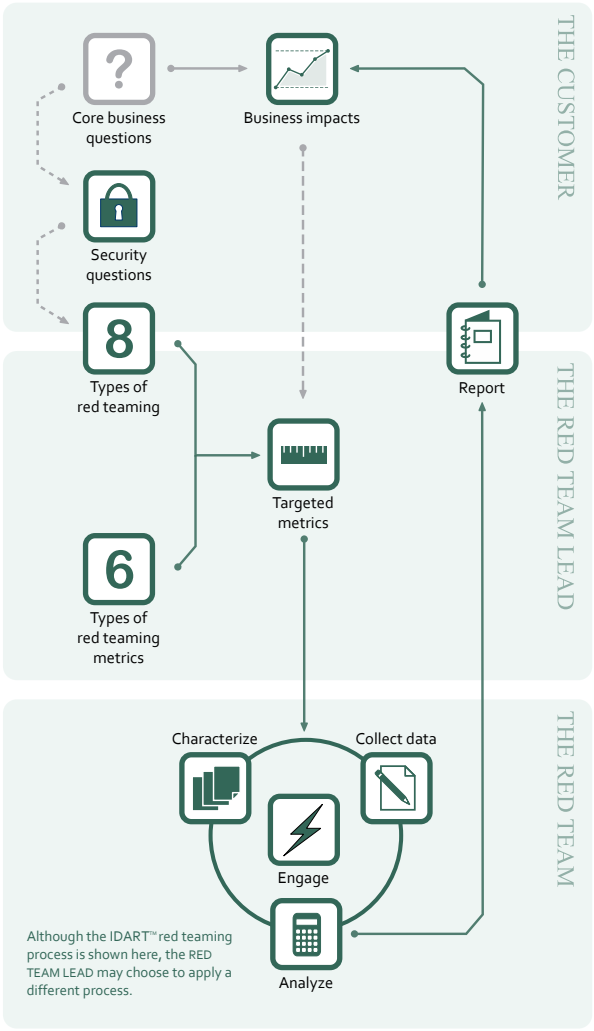
A metric is a unit of measure. Analysts and decision makers use metrics to help measure important aspects of a problem of interest.

These six types of red teaming metrics represent empirical categories rather than a strict taxonomy.

✻ The CUSTOMER wants to understand how adversaries might harm the customer's business. Depending on the customer's preference, the RED TEAM LEAD may need to work with the customer to understand the customer's core business questions and relevant business impacts.

1 The RED TEAM LEAD considers the customer's perspective, the types of red teaming involved, and the types of red teaming metrics available to identify the set of targeted metrics relevant to the assessment. It is assumed here that the RED TEAM LEAD already under- stands the CUSTOMER's security questions and has identified the type of red teaming to be employed.

2 The RED TEAM applies the targeted metrics to the red team assessment process. The metrics specifically inform the task of collecting data during the assessment.



In practice, this process can be iterative. For example, the RED TEAM may identify a new metric during the assessment phase.

4 The RED TEAM LEAD assembles and delivers a report that communicates risk or business impact to the CUSTOMER.

The RED TEAM is not the sole source of the metrics and measured values the CUSTOMER will consider when assessing the core business questions and impacts. Other sources of metrics include financial and operational data, traditional analyses, and forecasts. The report delivered by the RED TEAM LEAD is thus one input into a larger report assembled by others.

3 The RED TEAM analyzes risk based in part on the metrics identified and data collected relative to these metrics.

1 Identify relevant target metrics

Relevance of the type of metric to the type of red teaming: ● High ◒ Medium ○ Low ◌ Maybe

		Attack (At)	Vulnerability (V)	Consequence (C)	Adversary (Ad)	Protection (P)	Threat (T)
Design assurance red teaming	Da	●	○	◒	●	◒	○
Hypothesis testing	Ht	●	○	○	◒	○	○
Red team benchmarking	Bm	○	●	●	◒	●	●
Behavioral red teaming	B	○	◌	◒	●	◌	◒
Red team gaming	G	◒	○	●	●	○	◒
Operational red teaming	O	●	●	○	●	●	◒
Penetration testing	Pt	●	●	○	◌	●	○
Analytical red teaming	A	○	○	●	●	◒	◒

2 Collect data to address the target metrics

Vulnerability-based metrics (V)

Vulnerability-based metrics count or measure vulnerabilities found or weaknesses discovered.

CONSIDERATIONS:

- Decide in advance when to stop looking for vulnerabilities
- Do not share vulnerabilities out of context
- Distinguish between vulnerabilities of technology, processes, and implementation

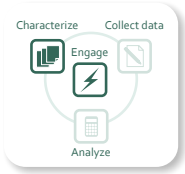
EXAMPLES:

- Boolean existence (is there a vulnerability?)
- Percentage of platforms with vulnerability
- Reachability (can the attacker reach vulnerability?)

METHODS:

- Scan system
- Execute attacks against multiple systems
- Characterize system

SOURCES:



Protection-based metrics (P)

Protection-based metrics count or measure protection systems (extant or posited as countermeasures).

CONSIDERATIONS:

- Include less obvious, unconventional measures of protection
- Assess whether protections actually protect targets of interest
- Pay close attention to what, why, and for whom you measure protections

EXAMPLES:

- Percentage of systems protected
- Number of protections/layers
- Number of incidents/ compromises

METHODS:

- Review interviews and documents
- Count actual protections
- Compare red and blue views

SOURCES:

The SOURCES box in each section-two module is designed to illustrate the relative likelihood that the team will collect values for the given type of metric during the specified phase. The strength of the source relationship is indicated by the darkness of the icon.

2 Collect data to address the target metrics

Adversary-based metrics

Ad

Adversary-based metrics describe the adversary model the red team uses during the red teaming process.

CONSIDERATIONS:

- Use metrics consistent and relevant through adversary continuum
- Choose metrics you can find in current adversary intelligence
- Try to use same metrics and units as attack metrics

EXAMPLES:

- Knowledge or skill level
- Number of team members
- Tools or techniques

METHODS:

- Review adversary intelligence
- Analyze past activities
- Compare to known adversaries

SOURCES:

Attack-based metrics

At

Attack-based metrics describe the capabilities and commitment required to undertake a given attack successfully.

CONSIDERATIONS:

- Take special care to ensure objectivity and consistency
- Compare costs of different collection methods
- Avoid discussions of specifics with decision makers
- Make sure you know who will see the metrics

EXAMPLES:

- Knowledge or skill required
- Time required to perform attack
- Probability of detection; likelihood defender will detect attack

METHODS:

- Elicit subject matter expertise
- Measure during execution (time attackers)
- Execute repeatedly; divide detections by successes

SOURCES:

Consequence-based metrics

C

Consequence-based metrics describe or measure the consequences that attend a successful attack.

CONSIDERATIONS:

- Work with customer to establish consequences of concern
- Make sure consequences can be measured
- Try to equate different consequences

EXAMPLES:

- Number of deaths
- Downtime
- Nightmare consequences achieved

METHODS:

- Interview target system staff
- Assess results from models and simulations
- Measure response under attack

SOURCES:

Threat-based metrics

T

Threat-based metrics describe the degree of threat and are calculated using combinations of the other metrics cited here.

CONSIDERATIONS:

- Make sure constituent metrics are consistent and objective
- Assume adversaries will apply resources creatively
- Ensure threat is real to decision makers

EXAMPLES:

- Expected cost to repair damage
- Expected number of systems affected
- Mean time to restore services

METHODS:

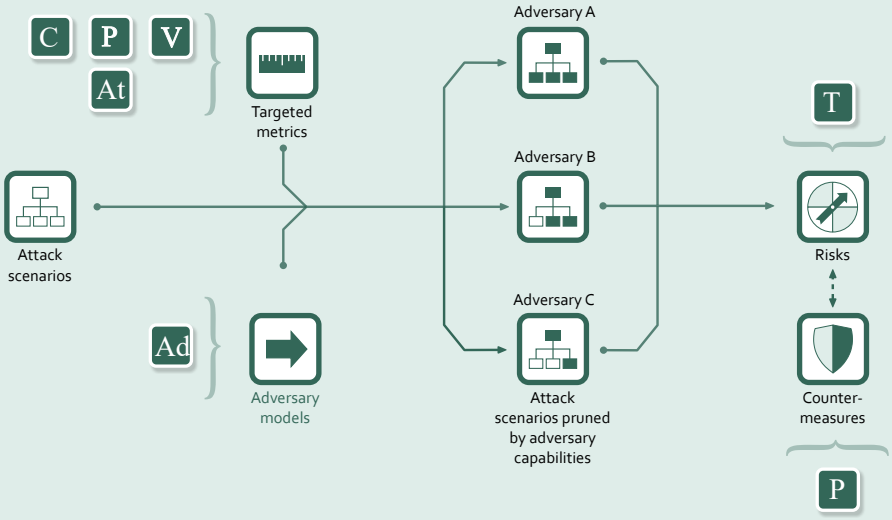
- Repeated simulation of attack
- Calculation from other collected metrics

SOURCES:

3 Analyze risks associated with the target metrics

The RED TEAM LEAD may choose to employ one or more methods to analyze risk. The process shown here describes one such method.

In this process, the RED TEAM models possible attack scenarios. The team analyzes risks associated with each scenario by comparing the capabilities required to achieve the scenario with capabilities the posited adversaries possess. The RED TEAM may choose to model the effectiveness of notional countermeasures.



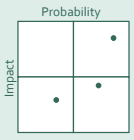
4 Assess and communicate the risk or business impact

Simply identifying risks is not always sufficient. The RED TEAM LEAD must also assess risks within the context of the effort. Illustrative methods of assessing adversary risk include:

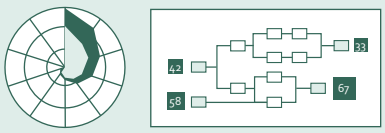
- Ad hoc judgment
- Expert judgment
- Decision analysis
- Modeling and simulation

Various modes exist to communicate risk and business impact. These modes include:

- Raw data
- Risk matrices



- Scenario risk distributions (spider charts, annotated attack graphs)



- Risk dashboards

In some cases, the CUSTOMER will also want the RED TEAM LEAD to translate risks into business impacts expressed in terms of the CUSTOMER's key business questions and operations. Example categories of business impacts include the following:

- Finances
- Security
- Scheduling
- Opportunity
- Legal and reporting requirements
- Continuity of operations

The RED TEAM and RED TEAM LEAD are not necessarily expert in any given area of business impact. As appropriate, the RED TEAM LEAD may work with subject matter experts to craft a more tailored interface with the CUSTOMER.

Sandia National Laboratories Information Design Assurance Red Team™
http://idart.sandia.gov | idart@sandia.gov | | SAND2017 - 9681 TR

IDART Information Design Assurance Red Team