Red Team Metrics™

Enhancing red teaming with risk analysis

IDART
Information Design Assurance Red Team

Fact Sheet

Red Team Metrics

Red Team Metrics helps red teams consider customers' core questions, identify relevant target metrics, analyze risk in adversary attack scenarios, assess outcomes, and communicate the risk issues and business impacts to the sponsor.

Red teaming (authorized, adversary-based assessment for defensive purposes) is a flexible tool that program managers and sponsors use to identify critical vulnerabilities; understand threat; deliver effective and secure components, systems, and plans; and consider alternative strategies and courses of action.

Because red teaming is applied in multiple problem domains and for different reasons, effective red teaming methods must be flexible and support customization. *Red Team Metrics* is one of several Sandia methods available to help customers achieve better results with red teaming.

The *Red Team Metrics* Process

Step one

The RED TEAM LEAD considers the customer's core business questions, the types of red teaming involved, and types of relevant metrics to identify the set of targeted metrics needed for the assessment.

Step two

The RED TEAM applies the targeted metrics to their assessment process. The metrics inform the process by helping guide the assessment's data collection, characterization, and analysis phases.

Step three

Risk is analyzed by the RED TEAM, based in part on the metrics identified and the data collected relative to them. The team analyzes the risk of various attack scenarios of one or more modeled adversaries.

Step four

Risk associated with various outcomes is assessed by the RED TEAM; a report is produced that communicates risk issues, supporting greater CUSTOMER understanding of business impacts.

Training course offerings*

Sandia currently offers this course in an eight hour version; depending on the needs of Sandia's customers, it could be extended to a multi-day course.

Who should attend?

Red Team Metrics introduces a pragmatic approach to using assessment metrics and will be helpful to program managers whose work must fulfill its mission in the presence of goal-directed, adaptive adversaries. The training course will greatly benefit red teams, especially project leads, whose assessments must deliver understandable and defensible results.

Prior experience with red teaming and/or red teaming methods and processes is assumed and highly beneficial.

* All IDART™ Courses are offered at the discretion of Sandia National Laboratories to individuals with need-to-know.

IDART™

Sandia's Information Design Assurance Red Team (IDART) has been performing assessments since 1996 for a variety of customers including government, military, and commercial industry.

Through its participation in a variety of government programs and leadership of industry conferences, the IDART team has assembled what is perhaps the widest vision of the use and practice of red teaming in the nation.

NNSA
National Nuclear Security Administration

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Red Team Metrics

Why *Red Team Metrics*?

Of the little published work on red teaming, most addresses how to perform adversary-based assessments, knowledge and skills a red team would need.

In Sandia's red team experience many of the biggest obstacles to successful assessments have more to do with why the assessment is needed, what the red team must deliver, who performs the assessment, and how the deliverables will be used to satisfy the assessment goals.

Sandia developed the *Red Team Metrics* concepts, methods, and materials to better equip red teams to deliver high-confidence analyses and communication products that effectively identify issues from the perspective of their sponsors or program managers who use adversary-based assessments.

The course introduces six classes of metrics that support red teaming: consequence, vulnerability, protection, adversary, attack, and threat-based metrics.

Course instructors

Red Team Metrics instructors are key members of Sandia National Laboratories' technical staff and IDART team, with years of experience in a breadth of security assessments.

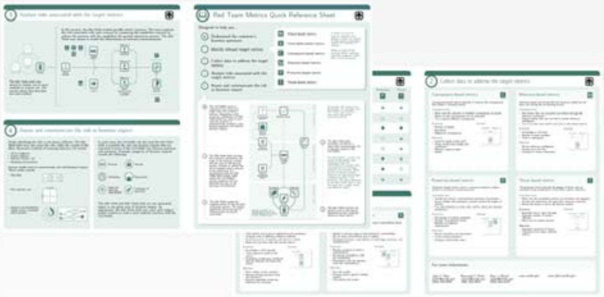
Their experience, knowledge, examples, and anecdotes afford course participants the opportunity to engage in meaningful discussion of red teaming.

Course outline

- Introduction and process overview
- Identify relevant target metrics
- Collect data to address target metrics
- Analyze risk associated with the target metrics
- Assess and communicate the risk or business impact
- Conclusion

Course materials

Participants will receive a handbook with all presentation materials, and a useful job aid that summarizes the course in the form of a quick reference sheet .



Course methods

Red Team Metrics instruction is available initially in an eight hour training session. Course extension is possible in order to provide opportunities for greater depth of discussion and extended exercises.

In the eight hour training, *Red Team Metrics* instructors blend mini-lectures with discussions and short exercises to illustrate and clarify course concepts. Instructors also demonstrate the use of a software application that supports adversary scenario modeling to help assess and communicate risk.

For more information or to schedule a course please contact:

Raymond C. Parks
Sandia National Laboratories
Information Design
Assurance Red Team
(505) 844-4024
rcparks@sandia.gov

Unlimited release { approved for public release. Sandia National Laboratories
SAND . Last revised on 03 December 2008.