Assessment Choices

Assessment Choices

When Choosing Sandia Makes Sense

Do you need a risk assessment, a vulnerability assessment, a red team assessment, or some combination of the three? How do you know that different providers even mean the same thing when they use the same terms? And—perhaps most important—how do you determine in advance that the quality of assessment you'll receive will address your needs?

The challenge

If you have systems and assets you must defend, you have no doubt faced the challenge of decoding the wide variety of available service offerings and assessment types. In many ways, the world of security audits and assessments remains stuck in the Wild West phase: no common lexicon, few common standards, and more than a few snake oil salesmen promising cure-alls and quick-fixes.

What you need to know

To answer this challenge, you first need to consider several questions:

- Do you employ commodity or custom systems and components?
- Does your system perform a specialized function or mission?
- How essential is your mission to national security?
- How susceptible is your system to national security-related threats?
- What are the potential consequences of mission failure?
- How diverse and uncertain is your operating environment and adversaries?
- Does your system involve physical, cyber, chemical, radiological, or nuclear technical components?
- Do your stakeholders include private, government, or military interests?

Assessments at Sandia

Many providers offer assessments and red teaming services that differ little from checklist-based penetration tests or security audits. At Sandia, assessments and red teaming are much more than checklists. Sandia's red teaming approach is based on principles of systems engineering and includes a family of advanced methods and tools. Sandia assessments are also strengthened by multi-disciplinary technical programs across the lab. When technical expertise is required to assess a custom or highly specialized system, few organizations In the world can match the breadth and depth of knowledge a Sandia red team can apply to a problem. These domains include physical, cyber, chemical, biological, radiological, nuclear, energy, and control systems security.

Sandia applies assessment and red teaming to enable or improve efforts that allow you to:

- Assess
- Analyze
- Predict
- Decide
- Train
- Design

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.

Assessment Choices

As a rule, the more complex your system, the more consequential your mission, and the more varied your adversaries, then the more you need a specialized assessment team and approach.

Your choices

It is essential that you understand the choices available to you. Of course, various providers use terms differently, but in general …

- If you need to know whether and how someone can breach your security, perform a *penetration test*.
- If you need to identify and mitigate vulnerabilities of your commodity system from a neutral perspective, perform a *vulnerability assessment*.
- If you need to know if your systems and policies are performing adequately from a compliance or standards perspective, perform a *security audit*.
- If you face capable or adaptive adversaries and need to understand and mitigate the vulnerabilities of your custom or critical system, perform a *red team assessment*.

In addition, a complex system may require different combinations of these assessment approaches to provide the information you need. Only some groups can bridge multiple assessment methods across multiple threats.

Sandia's red teaming and assessment experience

Sandia has assessed high-consequence systems for a range of U.S. and local government, military, industry, and critical infrastructure providers. Critical infrastructure sectors Sandia's red teams have assessed include

- Electric generation and transmission,
- Oil and gas production & distribution,
- Banking and finance,
- Telecommunications,
- Water (local and supply), and
- Transportation.

Sandia engages in research and development that advance assessment science and tools through internal and externally funded research programs to improve our accuracy, effectiveness, and reproducibility of our results.

When to choose Sandia

Sandia is effective in providing a range of assessments adapted to provide answers you need for complex and high-consequence systems, particularly when facing a range of capable adversaries or when existing within uncertain operating environments. We rarely provide audit or compliance-based assessments to systems that are well defined. In these situations, often with widely distributed or numerous systems, in order to gain efficiency with quality, Sandia has used its breadth of assessment skills to produce customized compliance-based assessment methods and train others in their use.

For more information contact:

Ray Parks
Sandia National Laboratories
Information Design Assurance Red Team
(505) 844-4024
jfclem@sandia.gov
www.sandia.gov/idart

Jennifer Depoy
Sandia National Laboratories
Critical Infrastructure Systems
(505) 844-0891
jdepoy@sandia.gov
www.sandia.gov/scada

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.
060307