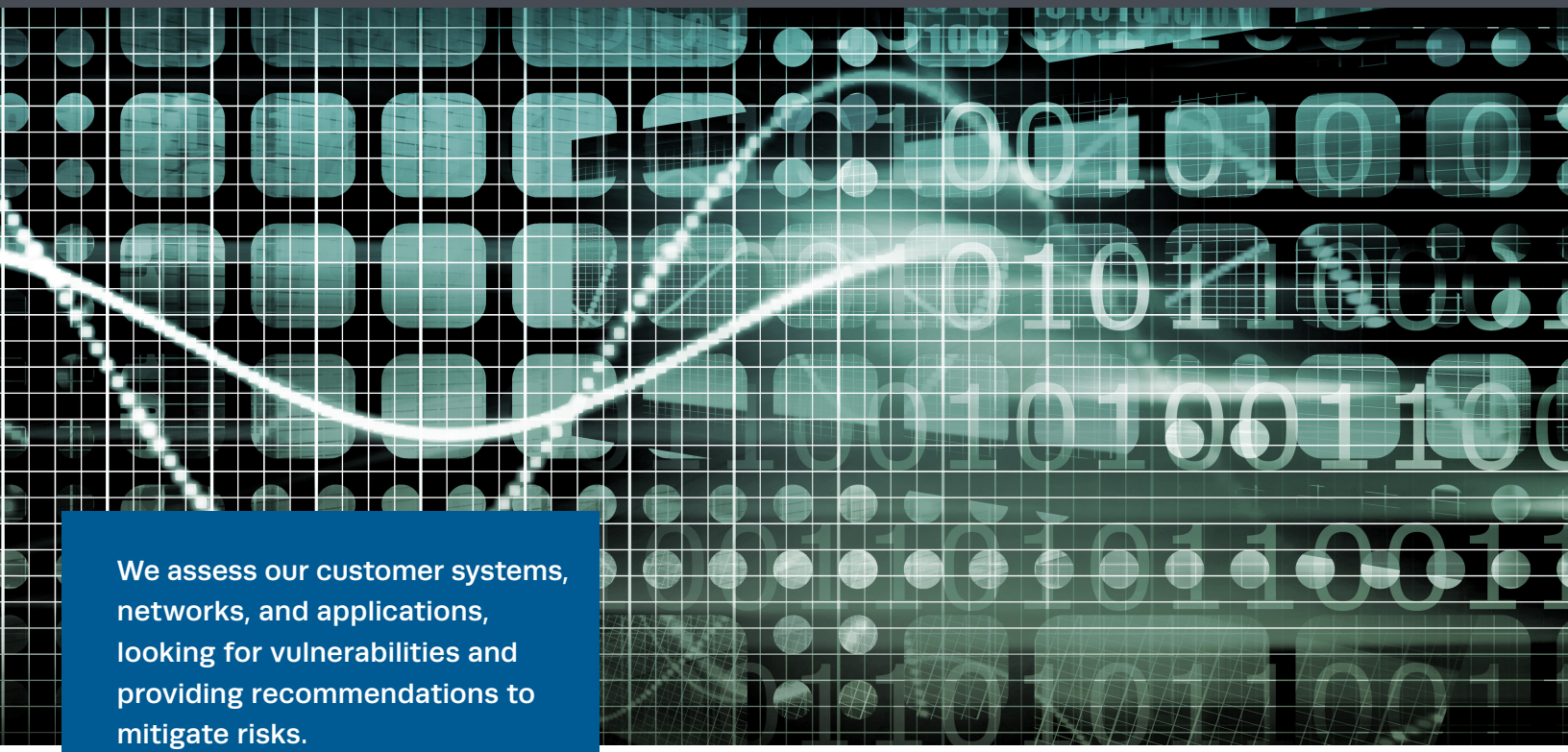
# Cyber Assessments



**We assess our customer systems, networks, and applications, looking for vulnerabilities and providing recommendations to mitigate risks.**

## Cyber Security Assessment and Mitigating Cyber Risk

MITRE's Cyber Assessment experts enable organizations to improve their security programs. We have supported over 20 different sponsors with over 600 security assessments in the last 18 years.

Our numerous sponsors have told us that commercial cyber security assessments often do not fully meet their needs. That testing can be compliance-oriented—focusing on locking in products and services—not oriented toward mission needs. MITRE understands customer environments and the importance of accomplishing a mission. During testing we focus on risk to business/mission execution so an organization can apply its scarce resources where needed most to reduce risk.

MITRE structures the findings from cyber security assessments into frameworks that organizations can use to evolve their security programs and practices. We offer technical expertise in security solutions, software engineering practices, and systems engineering to thwart common and advanced threats. Sponsors benefit from the breadth and depth of our experience applying cyber assessments in domains ranging from national security to civilian e-commerce missions.

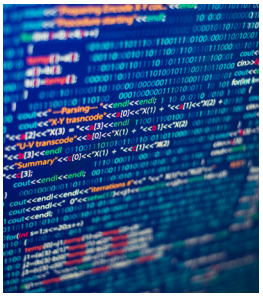
**MITRE has completed more than 600 cyber assessments in the last 18 years. Our methodology is key to our success.**

## Differentiating Among Types of Cyber Assessment

The majority of MITRE's cyber assessments work is performed in conjunction with Vulnerability, Penetration, Red Team/Adversary, and Security Control Assessment.

**Vulnerability Assessment** focuses on adequacy and implementation of technical, management, and operational security controls. It strives to identify vulnerabilities present in a system or its components.

MITRE



**Penetration Testing** is designed to drive organizational behavior change and has somewhat limited technical value. Its objectives include developing or measuring capabilities of network defenders and their processes and developing or measuring an individual or group risk profile. It can be used to draw attention to a specific problem in a high-criticality system. Practitioners may develop re-usable models of adversary actions to exploit known or suspected weaknesses as a by-product.

**Security Control Assessments** evaluate the security posture of systems when compared to the requirements established for the system. In other words, does it do what it originally set out to do in terms of safeguarding the information and enabling successful execution of the business/mission.

**Red Team/Adversary Assessments** are similar to a penetration test but more targeted. The goal of a Red Team assessment is to emulate cyber adversary attacks with specific goals defined by the assessment's campaign parameters. A goal of a Red Team assessment is NOT to find as many vulnerabilities as possible, but to find and exploit vulnerabilities that achieve their goals. The Red Team persists and attempts to achieve the goals and other objectives of the campaign. Red Team assessment is a thorough engagement that helps organizations determine if and how their critical assets could be compromised.

Even more testing capabilities exist at MITRE including product-focused vulnerability assessments which illuminate cases where the system may be vulnerable but the security of the application compensates for it. However, the inverse is equally as likely. Compliance Assessments are conducted periodically to ensure that the tested organization continues to meet compliance standards.

In all of these assessment types a standardized, but flexible, methodology is important to focus on meeting mission needs. Standardization also improves the quality of results and allows identification of systemic and root causes.

## Addressing the Challenges in Cyber Assessment

MITRE has identified several challenges in Cyber Assessment.

Practitioners and sponsors tend to trust the results of automated tools excessively. Automated tools do not identify all risks; nor do the tools understand the business/mission context that the system under assessment enables. To address this challenge, MITRE blends deep mission knowledge as well as augmented assessment techniques and processes to reduce errors in assessment results.

There are also many interpretations of the various forms of cyber security testing. Terms are often used confusingly or not widely understood. Polling people from industry, academia, or government will likely result in different explanations for the same terminology. Sponsors are asking for one thing, expecting something different, and needing another thing entirely. MITRE brings our extensive cyber assessment experience to enable common understanding to cyber assessment so that our sponsors achieve their outcomes.

*For information about MITRE's cybersecurity expertise and capabilities, email cybersecurity@mitre.org*

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

**The MITRE Corporation** www.mitre.org