The bridge to possible

Cisco Technical Security Assessment Services

Know your weaknesses and fortify your security

Today's networks are transforming rapidly as more and more applications, workloads, and data are moving to the cloud. And with the increasingly mobile workforce and hybrid work business models being used globally, there are rising numbers of users and devices accessing networks remotely. All these changes open your business up to greater security risk. According to Gartner, by 2025, 99 percent of security failures will be due to the organization's own mistakes.[1] This is because security is incredibly complex and difficult to manage, and the breadth of what needs defending is ever-expanding, yet protecting your business has become more critical than ever.

One key to maintaining a strong security posture is regularly testing for vulnerabilities in your infrastructure, defenses, and response. You can't effectively manage security issues that you do not understand fully. Your infrastructure, Wi-Fi, devices, and physical premises all need protecting and should be able to restrict attacks. Even your own employees can be susceptible to phishing attempts by hackers, jeopardizing your organization's security. Once an attacker has penetrated, recovery can be a long, drawn-out process. In addition to financial consequences and compromised data, these events often play out in the public eye and can harm your business reputation.

So how can you stay ahead of the bad actors? You need to:

- Know where you stand by discovering, prioritizing, and addressing shortcomings and gaps.
- Continually test your organization to maintain optimal security health.
- Strengthen your internal security team by measuring their response to threats.

Do you have the in-house skillsets you need to assess your vulnerabilities and maintain a vigilant security posture? Cisco® can help.

Benefits

- **Awareness.** Vulnerability assessments and attack simulations highlight the weaknesses attackers use to compromise your organization, providing the knowledge you need to address them effectively.
- **Competitive edge.** Instead of assuming you've made the right security investments, you can become a data-driven organization and measure them.
- **Confidence.** By knowing and addressing your security weaknesses, you are working to prevent future attacks and helping to reduce risk, avoid regulatory fines, and prevent breaches that could potentially be catastrophic.
- **Experience.** With more than 35 years of experience plus countless awards and accolades for our security experts, services, and products, Cisco is on your side providing industry-leading security expertise.

[1] Gartner, 2019

The bridge to possible

Service options

Identify your weaknesses

- Internal Penetration Test
- External Penetration Test
- Application Penetration Test
- Wireless Penetration Test

Strengthen your resiliency

- Red Team Threat Simulation
- Social Engineering/Phishing Assessment
- Device Configuration and Build Review

Why Cisco?

Cisco is a top leader in network security. Based on extensive training, sophisticated tools, and 35+ years of experience designing, implementing, and securing some of the most complex networks in the world, Cisco has developed proven methodologies for actively assessing your infrastructure and designing a security solution that aligns with your business goals and successfully closes security gaps.

Next steps

To learn more, visit www.cisco.com/go/as or contact your Cisco sales representative or authorized partner for assistance.

Cisco Technical Security Assessment Services

Service details

Penetration Testing

Internal and External Network Penetration Testing provides a practical security evaluation of a specific network by trying to gain access to valuable systems and data in an attempt to identify exploitable vulnerabilities. This helps uncover vulnerabilities often missed by vulnerability scanning. These tests contribute to improvements in organizational security posture by demonstrating the security weaknesses attackers are likely to exploit. Application Penetration Testing identifies flaws in application logic or implementation by attempting to gain access to the underlying server or database, bypassing authentication and authorization, and testing for injection vulnerabilities. The results identify common areas for exploitation of your application security. Wireless Penetration Testing identifies weaknesses in wireless configurations an attacker is likely to exploit and attempts to gain access to your internal assets. The results of the testing help you identify where your wireless LAN (WLAN) access needs to be strengthened.

Red Team Threat Simulation

The Red Team models the threat of real-world cybercriminals, but without the risks of a real-world attack. During a Red Team engagement, our security experts use cutting-edge hacking techniques and unique proprietary and public tools to extract sensitive organizational information and test your defenses. Our objectives are to replicate real-world attack scenarios, assess the effectiveness of many layers of your security controls in preventing and limiting breaches, and identify any weak spots. The information gained will help you drive future security investment where you most need it.

Social Engineering and Phishing Assessment

By executing phishing campaigns using text- or voice-based communications, we help identify individuals likely to be phished, evaluate your prevention measures, and gather metrics on the effectiveness of your organization's security awareness training. Each campaign is carefully constructed to evaluate perimeter defenses with your oversight, providing an opportunity for your personnel to learn how to avoid becoming a victim of one of the most popular ways by which remote attackers infiltrate networks.

Device Configuration and Build Review

To help harden your device configurations against exploits and malicious threats, this service provides a deep dive into the configuration of critical or common builds. Our experts deploy detailed analysis tools and conduct manual investigation of specific configurations identified by tools and humans. With our findings, you can understand current weaknesses and likely sources of threats in the future. We also help you reliably and safely identify weaknesses that are hard to pinpoint at the network level.