Cisco Security Posture Assessment Service

ACTIVE TESTING TO PROTECT YOUR ORGANIZATION'S INFRASTRUCTURE SECURITY

Validate Your Current Security Posture

The Cisco SecureX Architecture™ is a context-aware, network-centric approach to security that enables organizations to embrace the new network security landscape while protecting business assets, critical services, and employees. Understanding the current state of your organization's security posture is critical to this approach and to building a comprehensive security solution that addresses the increasing sophistication and targeting of network attacks.

The Cisco® Security Posture Assessment Service provides a point-in-time validation of how well security architecture and designs have been implemented and how well they are operating. It provides a detailed assessment of wired and wireless networks, security devices, servers, desktops, web applications, and the related IT infrastructure by comparing discovered vulnerabilities with industry best practices and up-to-date intelligence from the industry and Cisco.

Because technologies, business processes, and security threats are always changing, an organization's security posture is never static. Many organizations perform periodic security posture assessments to maintain a current picture of their vulnerabilities and to prioritize remediation activities based on available resources and business risk.

Cisco Security Posture Assessment Service

Cisco security experts begin by conducting a detailed review of your security goals and requirements. Based on this information, they probe your IT infrastructure from the interior and perimeter, survey and map your wireless network, and attempt to socially engineer their way into your facility. This analysis is done in a safe and controlled manner, simulating activities typical of malicious attackers. Engineers then analyze the discovered vulnerabilities and compare them with industry best practices and up-to-date information from Cisco Security Intelligence Operations (SIO) to remove false positives. Based on the confirmed vulnerabilities, engineers analyze the results to determine which critical assets and data are exposed. The prioritized and actionable results of the analysis are then delivered to your organization in a formal report and an executive presentation.

Cisco Expertise and Resources

Assessments are performed by Cisco consultants, who draw on their extensive security experience in a variety of vertical industries and government agencies. This expertise is supported by a combination of best-in-class tools, methodologies, and unparalleled access to Cisco product development engineers to help you make the most of the sophisticated security features included in the Cisco products in your network. Exploitable vulnerabilities are evaluated using data from Cisco SIO, which is uniquely positioned to provide the global reach and security expertise necessary for successful global threat correlation, with hundreds of research analysts dedicated to the full-time collection and analysis of threat intelligence.

Service Summary

Building a robust security defense requires a clear understanding of the current vulnerability state of your network, applications, systems, and network-connected devices.

By taking a comprehensive approach to assessing the current state of your security infrastructure, these services provide your organization with the information it needs to understand and improve its security posture. Through this process your organization can improve risk management and satisfy compliance needs by reducing threats to the confidentiality, integrity, and availability of business processes and information.

Service Benefits Summary

- Reduce the risk of intentional or accidental access to IT assets and information
- Test current infrastructure security safeguards to help ensure that malicious activity does not successfully penetrate or disrupt service
- Proactively identify security vulnerabilities that pose a risk to your IT infrastructure
- Correlate vulnerability data with network topology information and identify risk posed to critical networks and assets
- Prioritize resources to address vulnerabilities based on business risk
- Improve the overall security state of network infrastructure by following recommended actions to mitigate identified vulnerabilities
- Achieve improved compliance with regulations and industry mandates that require security assessments
- Reduce the time and resources needed to stay current with new and emerging vulnerabilities

Flexibility for Your Unique Requirements

To provide flexibility in matching your unique business, infrastructure, and budget requirements, the service's four assessment components can be customized and delivered, independently or together, based on your specific business objectives:

- Internal security posture assessment
- Perimeter security posture assessment
- Wireless security posture assessment
- Physical security posture assessment

Internal Security Posture Assessment

Although external network security incidents often get more attention, your organization cannot afford to overlook the threat from internal, trusted sources.

This assessment focuses on vulnerabilities in your internal network and is conducted from within the trusted network with detailed procedures, customized based on the infrastructure and environment.

Perimeter Security Posture Assessment

This service identifies the security risk associated with your organization's Internet, partners, and customer and remote worker connectivity and services. It identifies vulnerabilities that can allow inappropriate access to the internal IT infrastructure from the outside.

Wireless Security Posture Assessment

802.11 wireless technology and services must be fully integrated into your organization's security framework and provide the same level of privacy and protection as the wired infrastructure. If not properly secured, wireless networks can be one of the easiest ways for unauthorized users to access critical systems and information. This assessment helps you to prevent such security breaches by identifying points of exposure, including unauthorized access points, weak access control, and wireless data leakage vectors, inside and outside your physical facilities.

Service Activities and Methodology Summary

- Identify business-critical networks and assets to qualify risk and prioritize recommendations and remediation efforts
- Identify and confirm the presence of security vulnerabilities in your IT infrastructure through expertise, tools, and the data from Cisco Security Intelligence Operations
- Emulate typical malicious activities through nondestructive means to confirm the presence of vulnerabilities and the level of unauthorized access that they can expose
- Provide a security posture assessment report containing:
  - Detailed analysis of simulated attacks to identify critical vulnerabilities
  - Comparison of assessment results with recommended industry best practices and your organization's operational requirements
  - Recommended prioritization of the vulnerabilities based on risk to the organization

Physical Security Posture Assessment

Controlling physical access to your network infrastructure is a critical component in the overall security of your infrastructure and critical data. The value of a secure network architecture and deployment is compromised if intruders can gain access to physical devices or other areas where sensitive data is stored. Gaining physical access to your facility, intruders might install network "back doors," keystroke loggers, software to call home, or rogue access points or remove other sensitive data. This assessment consists of a combination of onsite techniques with which engineers attempt to gain unauthorized access to your locations.

Why Cisco Security Services

Cisco is a leader in network security. Based on extensive training, sophisticated tools, and years of securing some of the most complex networks in the world, Cisco has developed proven methodologies for actively assessing your infrastructure and conducting a detailed analysis. Assessment services from Cisco and our partners include prioritized recommendations to help you successfully close security gaps.

Availability and Ordering

The Cisco Security Posture Assessment Service is available through Cisco and Cisco partners globally. Details might vary by region.

For More Information

For more information about Cisco Security Services, visit www.cisco.com/go/services/security or contact your local account representative.

C45-701656-00 02/12