Solution Brief

CORE SECURITY
A HelpSystems Company

SECURITY CONSULTING SERVICES

A complete solution for peace of mind

Do you know if you're vulnerable?

On average, companies that never pen-test have over 20 vulnerabilities, and the scarier news might be that those vulnerabilities are left open for an average of 431 days! [1] Also, with 78% of all companies studied having at least 1 vulnerability, how confident are you about your security? [2]

More than just penetration testing

Security Consulting Services (SCS) is a complete service provided by Core Security to ensure that vulnerabilities are minimized and that your defenses are running in top shape by offering the following:

+ Red Team
+ Penetration Testing
+ Software Security Assessment
+ Attacker's Tactics and Techniques
+ Actionable and easy-to-follow results

With SCS it's easy to assist security professionals with security decisions, evaluate and measure cyber risks, and meet compliance, all while providing an additional proof point of security.

Data that's useful!

Testing is useless unless it achieves actionable results. With SCS you get reports written by experts that highlight key data and exactly how targets were compromised as well as recommendations on best practices.

1. https://info.whitehatsec.com/rs/whitehatsecurity/images/2015-Stats-Report.pdf

2. https://info.whitehatsec.com/rs/whitehatsecurity/images/2015-Stats-Report.pdf

What does SCS test?

SCS tests 5 major areas of security: applications, security awareness, likelihood of attack, cloud infrastructure, and networked device security.

DETERMINE IF AN APPLICATION IS SECURE

+ Mobile, web, desktop
+ Built in-house, by third party, or customized

SECURITY AWARENESS

+ Understand the level of security awareness of the organization against phishing attacks.
  - Targeted phishing campaign
  - Defense readiness
  - User awareness

LIKELIHOOD AND IMPACT OF AN ATTACK

Determine the likelihood of an attacker compromising the network and the impact it would have.

- External facing
- Corporate
- Wireless

CLOUD INFRASTRUCTURE

+ Determine the security posture of any cloud based infrastructure.

NETWORKED DEVICE SECURITY

+ Determine if networked devices are secure.
  - Cameras
  - VoIP phones
  - Networked speakers
  - Sensing and monitoring
  - Devices
  - Gateway
  - Data engines
  - Applications
  - Internet of things

SCS Service Offered

RED TEAM

Testers use all the industry leading tools and methods real hackers use to evade detection while discovering exploitable areas of the network, applications, credentials, and devices.

SCOPE

Networks, applications, users, and any vector an attacker is likely to take advantage of.

ACTORS

Consultants mimicking attacker's techniques and tactics. Liaison with internal security team is optional.

OBJECTIVES

Simultaneously test for vulnerabilities while also testing for defense readiness of the internal security team.

OUTCOME

+ Identify vulnerabilities exploited and attack paths
+ Description of techniques and tactics
+ Level of readiness of your defense team
+ Fixes and mitigations

PENETRATION TEST

Evaluate the resilience of your organization against real-world attacks. Consultants will find and exploit vulnerabilities to get access to privileged systems and information.

SCOPE

Enumerate components and systems. Networks, applications, and users are usual targets.

ACTORS

Consultants mimicking attacker's techniques.

OBJECTIVES

Think of worst case scenarios:

+ Cloud admin creds stolen
+ IP documents extracted

OUTCOME

+ Identify vulnerabilities exploited and attack paths
+ Description of techniques and tactics
+ Fixes and mitigations

SOFTWARE SECURITY ASSESSMENT

Assess the security of an application or group of applications and their ability to resist attacks. Evaluate your defensive programming practices.

+ Assess a system or groups of systems that are logically connected and cooperate to provide business functionality
+ Find as many vulnerabilities as possible
+ Evaluate the code quality in terms of security
+ Create running proof-of-concepts of the findings

The Process