CSW Cyber SecurityWorks

CSW Red Team Services

Introduction

Organizations today face a constant barrage of cyberattacks. The security team's ability to detect and respond to these attacks can mean the difference between an internal exercise and headline news. To sharpen their skills, it's important that security operations teams test their ability to identify, contain and eradicate threats periodically

CSW Red Team services provide a safe platform for security operations teams to test their ability to effectively defend against cyber-attacks. Our Red Team testing methodology is performed by the industry's top security testers, based on thousands of worldwide engagements and customized for individual scope. Specializing in adversary simulation, the CSW Red Team uses a variety of tactics, techniques and procedures (TTPs) to help clients uncover vulnerabilities, test security procedures and identify areas of improvement.

Why Red Teaming?

Traditional approaches have focused on using targeted penetration testing to validate whether controls are working, and key information assets are protected. Penetration testing is very narrow and there are likely many other channels through which an attack could occur. An often-overlooked avenue is your physical security and the human factor. This is where a thorough holistic approach to information security testing is required - Red Teaming.

CSW Red Teaming will run a real-world scenario that's designed to measure how well your organization's defence and response capabilities will withstand social, physical, network and application attacks from a simulated adversary.

CSW Red Team services will be extremely customized based on each customer's unique area of concern. Our methodology is performed by the industry's top security testers, based on thousands of global engagements across different industry sectors.

Based on Customer's needs, CSW will customize the areas of concern.

- Intellectual Property Theft
- Customer Data Theft
- AD Forest Takeover
- Protected Network Access
- Device Access

During the engagement, the team attempts to evade security tools and stay hidden on the network. Clients should expect the initial intrusion and lateral movement to start as stealthily as possible.

This progression will help security operations teams identify and measure which threats they were able to detect versus which threats they were unable to detect. Using this information, teams can quantify their security posture at that point in time.

Our Approach

During a client engagement, the CSW Red Team will use any means necessary – just as an attacker would –without causing damage to the client's infrastructure or resources. This approach is designed to simulate a real-world adversary and test the security operations team's ability to respond to advanced threats.

Benefits

The key benefits of CSW Red Team service include:

- Measure the risk of critical assets
- Uncover unknown vulnerabilities.
- Identify strengths and weaknesses
- Measure improvement over time.

When it comes to information security, no organization is bulletproof. However, by practicing incident response to simulated attacks, security operations teams can improve their threat detection and response capabilities, become more effective in threat hunting and uncover vulnerabilities that may have gone unnoticed. As a result, security operations teams can be better prepared to stop real attackers early in the attack process and ultimately prevent material damage to the business.

CSW Red Team engagement can provide clients with insight into their security strengths and weaknesses, as well as provide a baseline from which future security improvements can be measured.

Deliverables

At the end of each engagement, clients will receive a detailed, two-part report that contains information relevant to both senior business managers and technical teams.

- **An Executive Summary**
outlines the scope of the engagement, key findings, the business impact of those findings and prioritized recommendations. This section also highlights key strengths that were identified throughout the engagement process.

- **A Technical Summary**
includes detailed information on the vulnerabilities and risks uncovered and recommended remediation steps to reduce future exposure.

We will conduct a live read-out with the appropriate organization stakeholders to review each vulnerability identified during the assessment, answer any questions that the team might have around each vulnerability, and discuss mitigation/remediation strategies.

Powered by Qualys.

PCI Security Standards Council
APPROVED SCANNING VENDOR

Corporate Office Address:
IITM Research Park, No.6 A-Block, 3rd Floor,
Kanagam Main Road, Taramani, Chennai - 600 113.

P: +91 44 4208 9337 | E: info@cybersecurityworks.com
W: www.cybersecurityworks.com