SOLUTION BRIEF

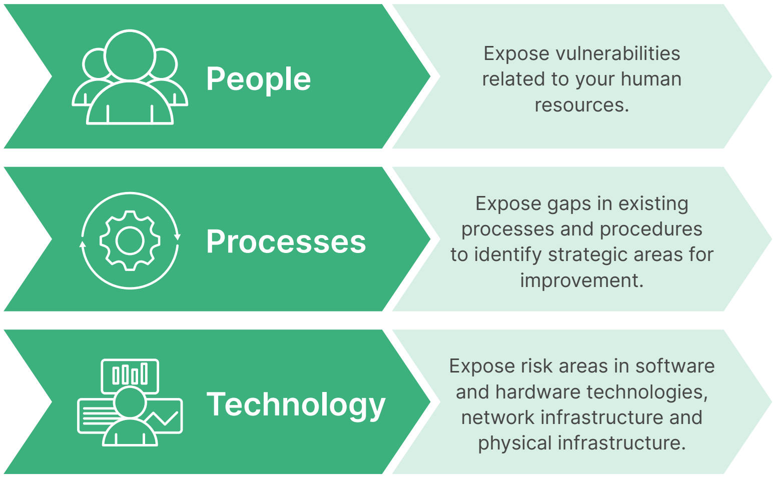
Test Your Cybersecurity Team Against the Latest Cyber Attacks Using the FortiGuard Red Team Assessment

Executive Summary

Organizations regularly face waves of malicious activity, ranging from technical intrusions to social engineering attacks. To protect against such threats, businesses strive to use the most-effective measures and defense tactics available. However, news about successfully prevented attacks does not always reflect reality. Threat actors are continually adapting their techniques and procedures, making it difficult for organizations to keep up with today's threats.

What you don't want is to learn that your network is not hardened against a threat after an attack is already underway. One of the best ways to prevent this is to test your people, processes, and technology through an effective Red Team Assessment. There are many security-testing tools and services on the market, including solutions for system and application security analysis, penetration testing, and employee awareness of information security issues. However, despite how effective these measures may be when it comes to some aspects of security, they do not provide the deep assessment most networks need to determine if they can withstand a sophisticated attack.

Red Teaming assesses system security by emulating a specific threat actor's tactics, techniques, and procedures (TTPs) to determine your organization's ability to detect and respond to incidents and resist the latest attacks, including advanced persistent threats (APTs). Ultimately, a Red Team Assessment focuses on exposing gaps in your organization's people, processes, and technology and provides a roadmap for improvement.



People

Expose vulnerabilities related to your human resources.

Processes

Expose gaps in existing processes and procedures to identify strategic areas for improvement.

Technology

Expose risk areas in software and hardware technologies, network infrastructure and physical infrastructure.

Red Team Assessment benefits include:

- Identifying critical vulnerabilities within your organization's infrastructure and technology
- Assessing your organization against those attacks you are most likely to encounter
- Determining if new or existing security measures are properly employed and can protect your critical systems and data
- Testing your security team's response capabilities and processes
- Understanding the gaps in your people, processes, and technology and providing recommendations to improve your organization's security posture

Common Red Team Objectives

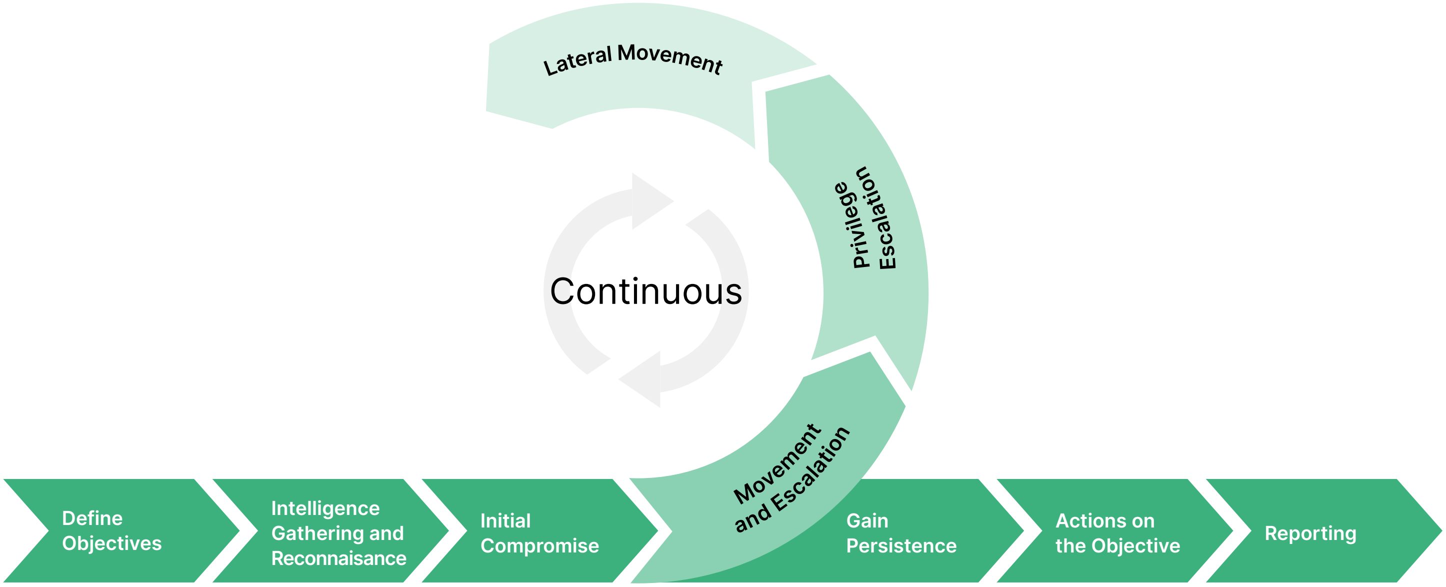
A Red Team assessment includes a controlled compromise against your existing environment, often utilizing one of the use cases below:

- Mimicking a threat actor targeting the organization and then launching a mock ransomware attack
- Accessing business-critical data and staging it for exfiltration
- Taking control of the Active Directory environment
- Gaining access to and controlling critical applications or systems, including process control systems
- Conducting a business email compromise to test the organization's response
- Accessing a segmented area of the network and gaining unauthorized access to systems

How the Red Team Operation Works

During a Red Team Assessment, our offensive security team, composed of experienced cybersecurity consultants, designs realistic attack scenarios leveraging both Open-source intelligence (OSINT) and proprietary threat intelligence from FortiGuard Labs relevant to your industry or organization. These operations are highly planned and executed systematically.

The following diagram outlines the steps of a FortiGuard Red Team Assessment:



To start, we assist you in defining the objectives of your assessment. Using active and passive reconnaissance, our experts gather information on your organization and its assets to determine the best vector for performing an initial compromise. Once that initial compromise occurs, our team looks to elevate permissions, move laterally across the network, and gain persistence by establishing command and control systems—just as would be done by today's threat actors. Ultimately, our experts perform actions on those objectives defined by the goals created for the Red Team Assessment.

It's also important to note that while the Red Team tries to compromise the organization, a Blue Team (your organization's security team) can actively defend against these attempts. Depending on the type of engagement, they can also be aware or unaware of the ongoing operation. The dynamic between these teams provides valuable insights into your organization's defensive capabilities.

Fortinet's Red Team Assessment Offerings

There are two primary approaches to our Red Team Assessment process. We can help you identify the one that is most appropriate for your organization and objectives.

Objective-Led Red Teaming is a structured approach that focuses on achieving specific objectives or goals deliberately and purposefully. Objective-Led Red Teaming aims to provide organizations with a strategic and targeted assessment of their capabilities, defenses, and preparedness in the face of specific threats or challenges.

Training-Led Red Teaming is a specific approach to red teaming that primarily serves an educational or training purpose that goes beyond traditional, Objective-Led Red Teaming. The primary purpose of Training-Led Red Teaming is to train and develop organizational personnel by simulating real-world adversarial activities and threats in a controlled environment.

Regardless of the type of Red Team Assessment you choose, Fortinet will ensure your organization's objectives are met while educating your team along the way.

Knowledge Is Power

In today's threat landscape, preempting attacks is a vital component of any cybersecurity strategy. Red Team assessments equip you with the knowledge you need to stay ahead of adversaries and secure your network's integrity.

An effective Red Team assessment isn't just about finding weaknesses. It's an investment in resilience, helping you safeguard your data, operations, and reputation. The vital insights you gain will enable you to stay vigilant and actively adapt to emerging threats. Our FortiGuard Offensive Services team is ready to help you defend your organization against the latest cyberthreats together.

Of the incidents handled by the FortiGuard Incident Response team, we have found that inadequate incident response procedures and a lack of network and system visibility and logging are consistently the top two contributing factors that enabled an intrusion.

FortiGuard's Red Team Assessment can help your organization identify and bolster these areas *before* your network is compromised.

Read the FortiGuard Incident Response Report

www.fortinet.com

May 31, 2024 2:29 PM

2586382-A-0-EN