protiviti®
Global Business Consulting

Red Team and Adversary Simulation

Gain Visibility into Your Response to a Targeted Attack

Protiviti’s Red Team services go far beyond a typical penetration test to develop and execute targeted cyber attacks in a manner that simulates an advanced persistent threat with motivations that target the organization or industry.

Protiviti leverages threat intelligence data and conducts extensive reconnaissance and information gathering before ever touching a client's network, systems or physical locations. This allows us to develop a test plan that **assesses both the configurations and processes** that are meant to secure the organization, as well as the ability of the organization to **identify attacks** while they are happening.

During a red team exercise, Protiviti will leverage multiple attack vectors and exploitation techniques to assess the organizations maturity in the following categories and answer these key questions:

People

- Are our employees susceptible to common social engineering attacks, such as phishing, vishing or physical social engineering?
- Do our physical locations have proper security controls to prevent an on-site network breach?
- Have employees, vendors or contractors unintendedly exposed data about our organization on the internet?

Process

- Are our corporate processes and policies adequately designed to stop external attackers from gaining unauthorized access?
- Do we have proper incident response processes to detect and mitigate an ongoing attack?

Technology

- Is our technology environment susceptible to attack?
- Are our system, application and network configurations designed to prevent unauthorized access?
- Do we have the proper security technologies to monitor for, detect and respond to a breach?

How Protiviti Can Help

- Security Control Tuning
- Collaborative Purple Team Testing
- Threat Emulation
- Red Team and Attack Simulations

> “As data breaches continue to make headlines, organizations are asking, ‘are we prepared?’ A Red Team answers that question by simulating advanced persistent threats (APTs) and conducting targeted attacks to test how an organization will react and respond in a live event.”
>
> **— Krissy Safi**
> **Managing Director, Attack & Penetration**

INNOVATE. TRANSFORM. SUCCEED.

Red Team and Adversary Simulation

Our Approach and Methodology

Security Control Tuning: Perform manual and automated testing of key security technologies (EDR, SIEM, AV, IPS/IDS, etc.) and incident response staff using modern attacker tactics, techniques and procedures to assess and establish a baseline of security control behavior, while gaining visibility into the effectiveness of the organization's toolsets.

Purple Team Exercise: Act as a sparring partner for the organization's incident response "blue team" to simulate various attack techniques while providing guidance and education on how to respond to such an attack. The team will work collaboratively through multiple scenarios to assess and determine each point at which a targeted attack could be mitigated and assist with guidance on implementing defensive controls.

Threat Emulation: Perform threat profiling or modeling exercises to determine possible risk areas for the organization. Based on output from profiling and modeling, perform targeted technical threat emulation to assess the organizations resilience against a specific threat actor or risk scenario, such as ransomware.

Red Team and Adversary Simulation: Simulates real-world threats and attacks with no, or minimal, scope restrictions to assess the technologies, processes and people that are meant to secure an organization.

Healthcare Company

Red Team Exercise

Business Requirement

After a significant incident had major impacts on the network of a large healthcare organization, the board of directors and audit committee wanted to better understand the organization's resilience to similar attacks in the future. The organization had mature vulnerability and patch management programs and conducted regular penetration tests but had not executed a Red Team exercise previously.

Solution Delivered

Protiviti met with the key client stakeholders to define specific objectives and targets of the exercise. The Protiviti team executed a variety of attacks including physical social engineering, phishing, application-based attacks and network exploitation to compromise the network and demonstrate an attacker's ability to successfully escalate privileges, laterally move to sensitive systems and exfiltrate data.

Business Results

The client leveraged the results of the Red Team exercise to develop a go-forward security strategy to close the identified gaps and implement technologies and processes which would alert the security team to malicious activity on networks and endpoints more quickly, significantly increasing the overall security posture of the enterprise.

Protiviti.com/TechnologyConsulting **TechnologyConsulting@Protiviti.com** **TCblog.Protiviti.com**

protiviti®
Global Business Consulting