Introduction
Red Team Engagement

While penetration testing attempts to recognize and exploit vulnerabilities in a given scope, such as a web application – Red Team participation focuses on breaching predetermined assets or ‘flags’ by being agnostic to a specific fixed target scope and concentrating on possible effects. Our Red Team Cybersecurity Participation may illustrate the danger presented by APT (Advanced Persistent Threat). These detailed, dynamic safety tests are best used by organizations seeking to improve a mature defense organization.

Infopercept has been a pioneer in these advanced projects and has grown a world-class team of offensive security engineers and analysts.

With some of the leading professionals in the industry, our team is made up of practitioners in a wide variety of developments and is supported by evidence to prove this.

By harnessing this unique combination of attack capabilities, we can determine:

- Attack method to damage the critical business resources.
- Where bugs reside throughout your network, apps, IoT software, and personnel.
- Effectiveness of your security surveillance and alerting capabilities.
- Weaknesses in the policy and processes for responding to incidents.
- Priorities and illustrated effects on the future security measures.
Focused on The Aim. Determined Impact

Each Red Team collaboration focuses on a collection of unique ‘Flags’ – sensitive business properties such as domain controllers, proprietary data, or credit card data. These flags are decided on a customer-by-client basis to establish a tailored commitment and a specified scope for the length of the project. We recognize that your security issues are separate from your corporate processes and business. The involvement of the Red Squad – or other safety determination in this matter – should still take that into account.

Example:

A Software as a Service (SaaS) firm is one such example. Email servers, executive computers, and domain controllers were among the flags that were seen through businesses. However, we were able to recognize specific flags to their company as a result of our operation.

Since application availability was so important to this company’s growth, taking control of the main web application became a worthwhile goal. Access to the user account (or other stores) was another red flag, so it was added to the list. Infopercept showed quantifiable business threats – and how to minimize them – by focusing on these particular data points.

Scenarios Customized for Special Threats

The Red Team commitments involve custom simulations that mimic real-world tactics that may be used by a foreign adversary to achieve a foothold within a network. These scenarios describe dangers that are unique to a particular situation or environments, such as a malicious insider, a hacked mobile device, malicious hardware installation, or other unique threats.

Example:

A Bank with customer banking both on premises and online will have multiple opportunities for adversaries. With advanced infrastructure including Transaction servers, Payment Gateway Integrations, Mobile Banking Applications there arise thousands of potential flags. Our Experts identify flags to target specifically for such case-based scenarios.
About INFOPERCEPT

Infopercept’s vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners’ cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint
© Infopercept Consulting Pvt. Ltd. 2021

Publisher
H-1209, Titanium City Center, Satellite Road, Ahmedabad – 380 015, Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

Global Offices
UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

By accessing/ proceeding further with usage of this platform / tool / site / application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions, kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.