Introduction Red Team Engagement

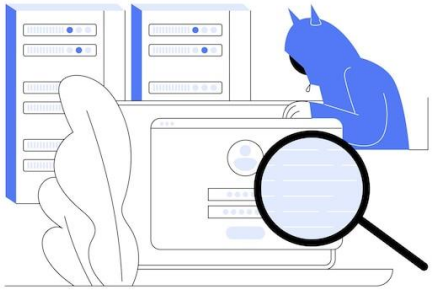
While penetration testing attempts to recognize and exploit vulnerabilities in a given scope, such as a web application – Red Team participation focuses on breaching predetermined assets or 'flags' by being agnostic to a specific fixed target scope and concentrating on possible effects. Our Red Team 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 is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com
www.infopercept.com/knowledge/datasheets