An introduction to Red Teaming with Breach & Content Attack Simulation Strategy for Strengthening your Cyber Security Posture

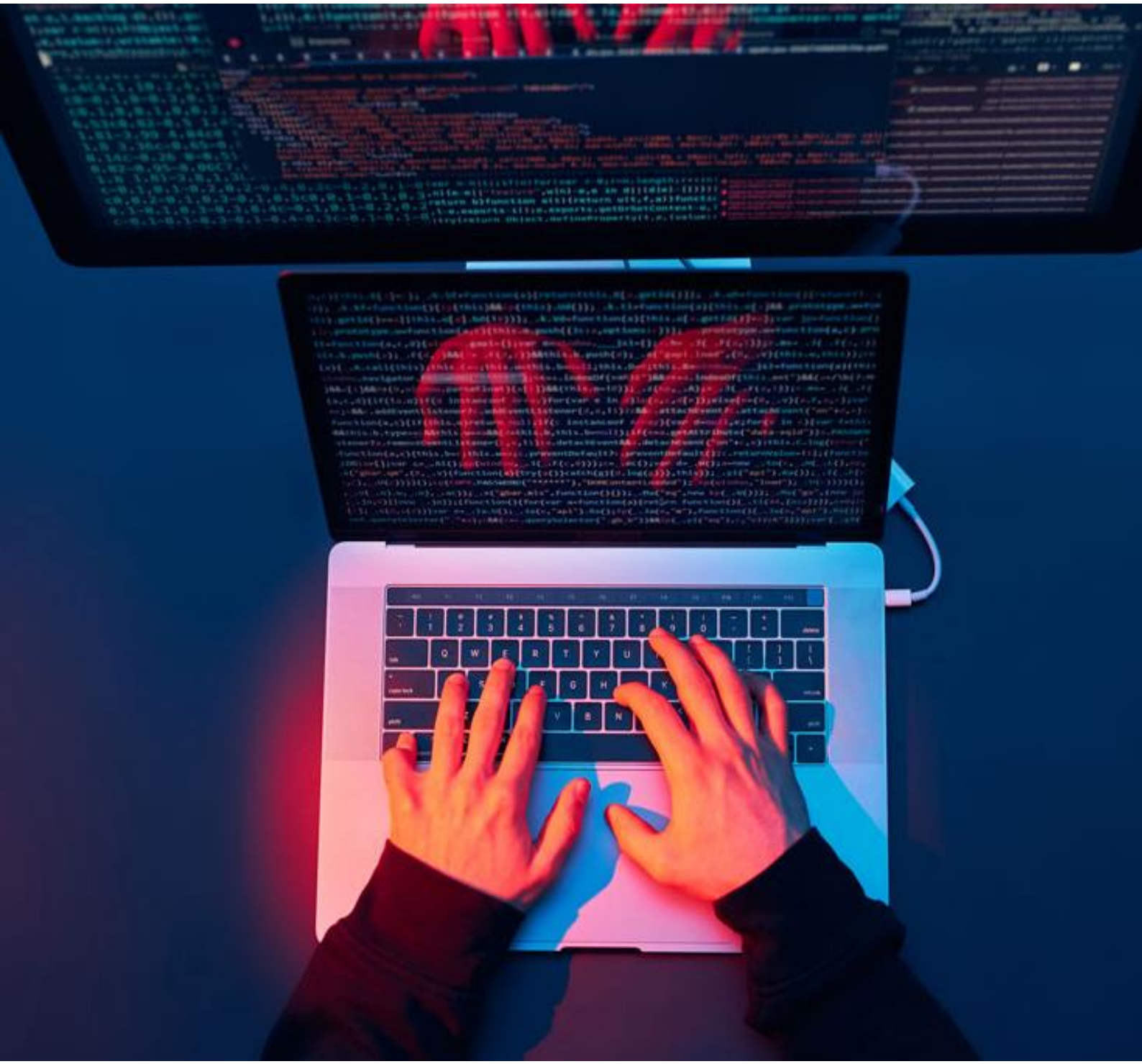


Table of Contents

Contents

Setting the Context

This whitepaper explores a completely new approach to combating cyber threats in the changing environment that we are in today. As any reader is aware, the cyber-attacks these days have evolved from the time of that of a hacker sitting in one corner of the world and trying to break into your network.

Current Modus Operandi:

With the advent of excessive processing power that is available to anyone today and the explosion of Cloud and IoT, the hackers are equipped with Bots / Botnets that helps them launch sophisticated attacks. These bots or automated scripts help them launch any sort of attack and explore the vulnerabilities within the network. Once the vulnerabilities are identified, then the attackers try exploiting those to inflict maximum damage. One thing that is standing out here is the ease with which the sweep is possible and the continuous nature of such targeted attacks. These are not one-time efforts and there is nothing stopping a determined hacker go on an all-out attack. So, it can be briefly summarised as the cyberattacks are today a combination of human effort as in sophisticated hackers and that of the excessive micro processing power that is derived from automated machines or bots / botnets. What we are trying to defend against is not just the unknown men alone; it is the combined might of man and machines.

What is the new strategy then?

For this, it becomes imperative for us to address both these aspects of Automation and determined hackers all under one roof. That brings us to the question as to how to practically address these 2 in a single integrated approach. Henceforth, we would like to introduce you to the Approach of Integrating Red Team Exercises with the Power of Automating Breach and Attack Simulation. This Approach considers a detailed Red Team exercise comprising of Testing with a real hacker mindset on real time basis along with an ongoing process of Breach and Attacks Simulations. This ensures that we have a continuous process of detecting and responding to Cyberattacks and a seamless process to strengthen the overall cyber security posture of an organization. The most sophisticated Red Team combined with a State-of-the-Art ‘Breach and Attack Simulation’ Tool is a Military Grade Defence that will provide the much-needed relief to the management who has been caught in this battle to protect its most valuable assets.

Red Teaming

The main objective of a Red Team Exercise is to perform a goal-oriented assessment of organizational defences on real time basis from the perspective of a real attacker. The scope includes all the available attack surface from the agreed vantage point (internal or external) and will cover the network and application layers as well as physical security and staff security awareness. The assessment will use legal, non-destructive attack vectors to gain access to and compromise customer networks.

With no pre-determined guidelines or instructions, cyber security experts will look for vulnerabilities and exploits in the following areas:

Technology: Digital infrastructure, corporate and mobile applications, routers, switches, and a variety of endpoints.

People: Employees, independent contractors, high-risk departments and business partners.

Physical: Office, warehouse, substations, data centres and associated buildings. A comprehensive report detailing vulnerabilities listed by criticality and severity is produced after the assessment, and certified cyber security experts present steps to improve the security posture of the company.

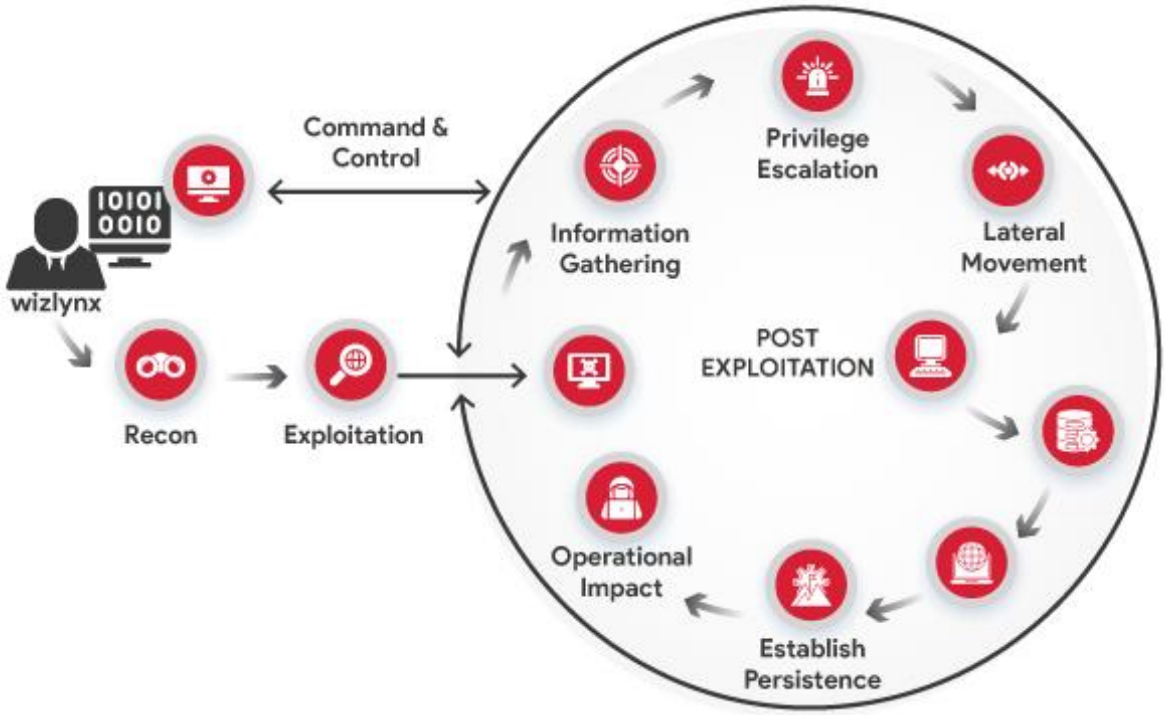
Red Team is designed to benchmark an organizations security controls and processes, particularly around physical security (for example access to buildings and computers/data held within it), general security awareness of staff, network security, procedures, and monitoring.

Red Team operator traits: An effective Red Team is comprised of a team of individuals who can contribute the overall success. Diversity is crucial, but the Team must comprise of the core operator traits. A Team can be even more successful when multiple Team members contribute in multiple areas.

Our Approach:

Our Approach to Red Teaming exercise can be summarized as below:

GET IN	STAY IN	ACTION
• Reconnisance • Enumeration • Exploitation	• Persistence • Lateral Movement • Continuous Enumeration	• Action on Objective • Operational Impact is assessed here



Red Teaming Exercise

Our Approach to Red Team exercise goes beyond Penetration Testing and Vulnerability Assessments. The focus is on Tactics, Techniques and Procedures (TTP). Red Teaming exercises relies heavily on well-defined TTPs that are critical to the successful simulation of realistic threat and adversary techniques. Red Teaming results are much more than just a list of flaws identified during the tests. It provides a deeper understanding on how an organization would perform against an actual threat and determine what a security operation team's strengths and weaknesses are.

Red Team is designed to benchmark an organizations' security controls and processes, particularly around physical security (for example access to buildings and computers or data held within it), general security awareness of staff, network security, procedures, and monitoring.

The end game of a Red Team attack is to provide an organization with a complete 'warts and all' look at its security posture. Usually Red Teaming takes place during the assessment stage of a business' security process - particularly if it is looking to invest in or upgrade its information security, or if it is carrying out a regular risk audit.

It is particularly valuable to businesses for two key reasons:

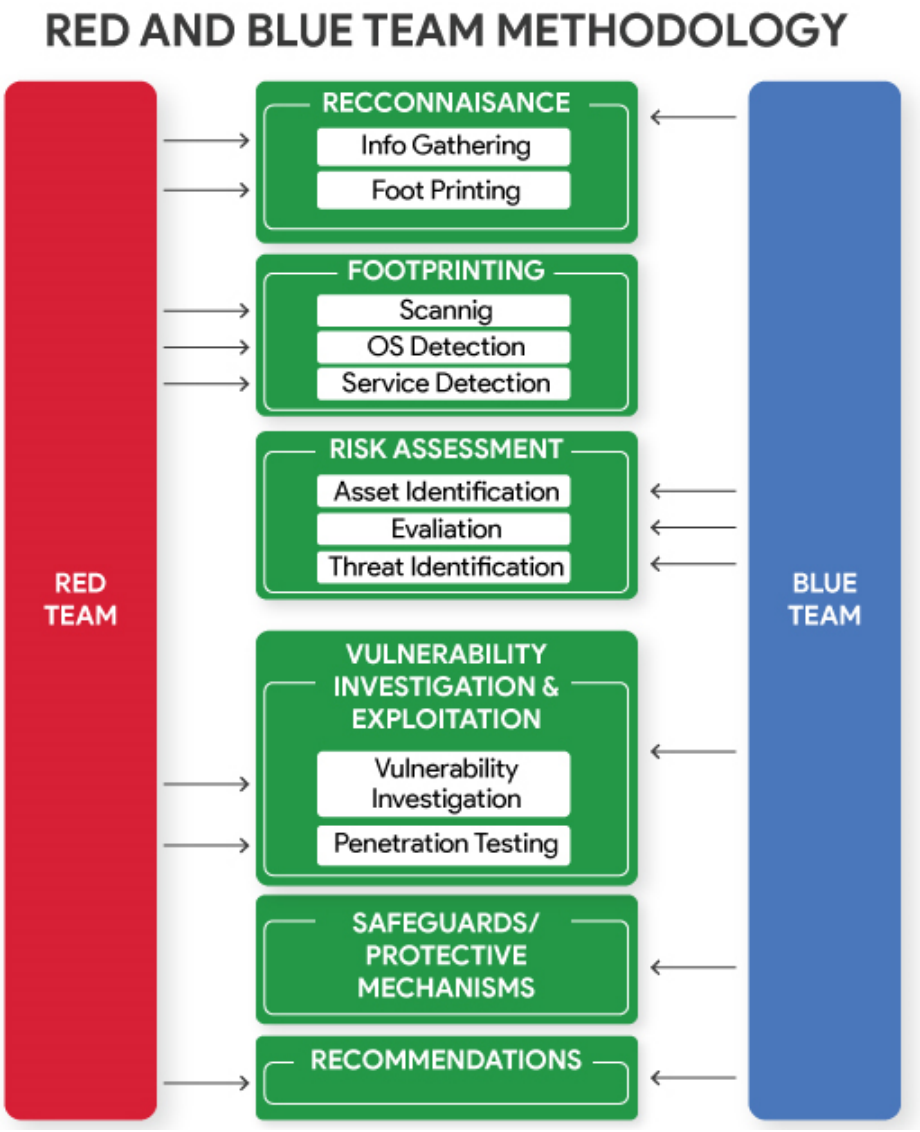
1. There is no procedure or automated tool in the market that can test an organization's security as intelligently as the human mind.

2. Red Teaming tests an organizations' security posture from many angles allowing them to pinpoint any holes or gaps more accurately in security and ensure that the right policies, procedures and technology are put in place.

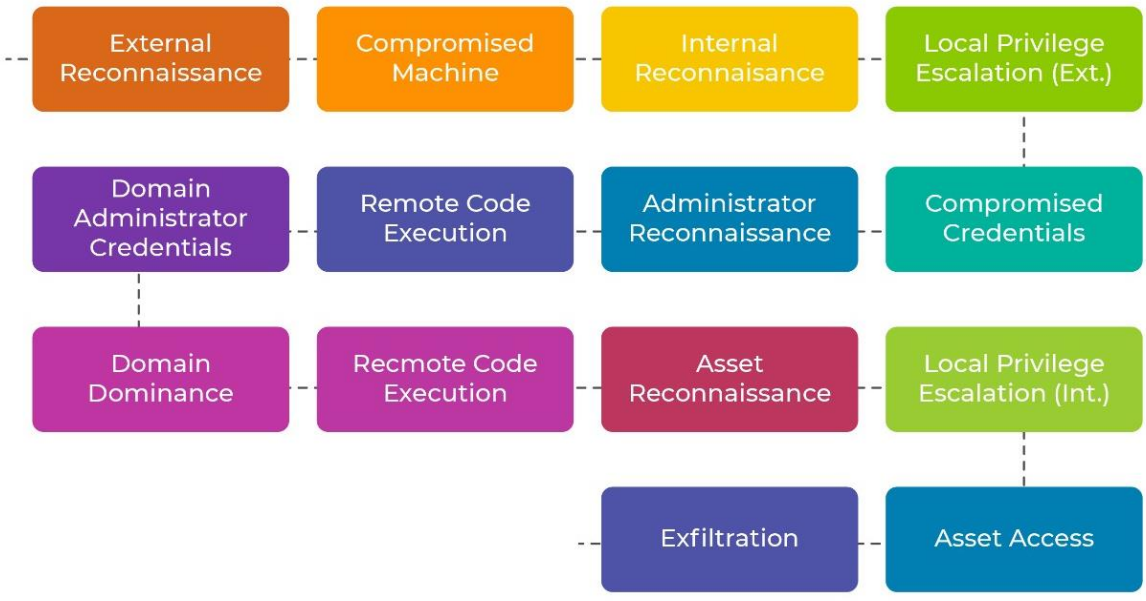
Red Team is an all-out attempt to gain access to a system by any means as in a real-life cyber-attack. The entire environment is within scope and their goal is to penetrate, maintain persistence, pivot, exfil, to examine what a determined enemy can do. All tactics are available including social engineering. Eventually the red team will get to a point where they own the entire network, or their actions will be caught, and they will be stopped by the security administrators of the network they are attacking. At that time, they will report their findings to management to assist in increasing the security of the network. They keep copious notes as this information is valuable later to fix the weaknesses they exploited. Not many organizations do this, but they usually have an organic red team, so the information gleaned from the red team is extremely sensitive. Red team actions are controlled by the manager of the red team.

Traditional Penetration testing uses similar tactics as that of a red team (may be limited by management and the scope of the test). However, it is executed in a controlled fashion usually dictated by management and/or asset owners. Typically, the limiting scope of a Penetration Testing is time (execution time of the event) in which a report will be made to the management. Often in a Penetration Testing exercise, before a flaw is exploited, management and system/network engineers must OK the attack to ensure it doesn't affect day to day operations. The goal is to find weaknesses in the systems/networks to increase/improve the security posture. The Penetration Tester's actions are controlled by business management and/or the asset owners. However, Red Team exercises are simulations of real-life cyber-attacks and the team goes beyond traditional means to perform a concentrated attack with all the defences in place to exploit the vulnerabilities.

Our Approach is to bring out various security loopholes and control weaknesses, how to address the same and train the internal team to be prepared for such scenarios thereby improving the overall cyber security posture of the organization.



Methodology of Red Team



Breach and Attack Simulation

Breach and Attack Simulation has gained utmost importance in the recent times due to the immense value it brings to any organization in its preparedness to combat any kind of cyber threats.

It employs a remarkably simple approach as can be seen below:

1. **Launch: Simulate a Breach:**

   • Run the tool from any machine on any platform of your choosing, whether it's a public cloud instance or on-premises server. Try different attack scenarios such as stolen credentials, infected internal server, or an external attacker.

2. **Attack: Go ahead and evaluate the controls present and then identify the gaps:**

   • The automated tests would run in the background

   • Working from the given attack configuration, the tool scans for potential victims in your network, attacks them and propagates further into the network. You can keep track of progress as you watch the tool generate a map of your network from the attackers' point of view.

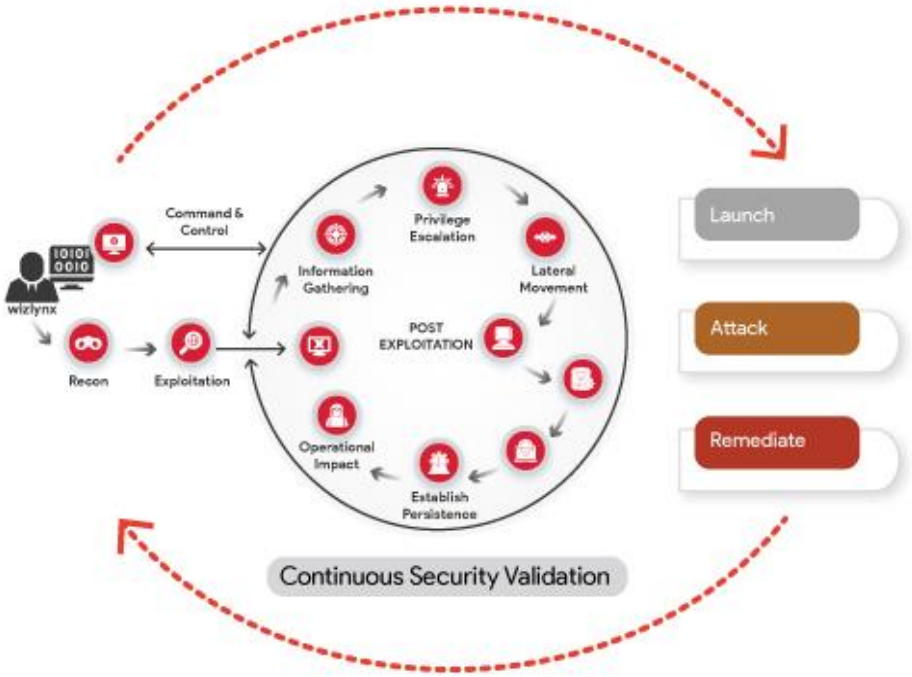
3. **Assess: Remediate the gaps with the insights available:**

   • Remediation based on the tool's findings and recommendations

   • The tool generates a comprehensive report detailing the simulated attack flow, highlighting immediate threats and potential security issues. By providing specific and actionable recommendations, per machine, you can use the report to harden your network

Infopercept's Integrated Approach

As highlighted earlier, the best possible solution to prepare your organization against the current scenario is to integrate the best of Red Team exercise and Breach and Attack Simulation. Here is how it is done to maximize the value to any organization looking to have an ongoing program to strengthen the defences against cyberattacks.



This approach comes with a whole of key benefits that shall be music to the ears of any CISO.

Key Benefits of this Approach

In-depth Teasting	Continous Process	Environment Agnostic
Scalable	Visualization of all possible attack vectors	Ongoing Remendiation
	Training	

Way Forward

It is especially true in case of Security that ‘one size doesn’t fit all’. Hence, this methodology will facilitate any type of industry or organization to perfectly simulate a threat actor TTP and check one’s readiness against preventing real attacks. It is a highly evolved approach and marries the advantages of Human Intelligence and Artificial Intelligence. This strategy is developed to beat the adversaries in their own game by taking the game to the next level. This approach is an integrated plug-and-play model that seamlessly fit into your Cyber Program and enhances the overall Cyber Security Maturity of the organization. This shall give the Management the much-needed confidence and the ammunition to fight the menace.

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/whitepapers