Infopercept
Secure . Optimize . Strengthen

An introduction to Offensive Defensive Strategy for Strengthening your Cyber Security Posture

Table of Content

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 a person's motive was only the gratification received from breaking into any network. Nowadays, the motives are multi-fold and the rewards immense. As can be seen as an alarming trend, is that many of these attacks are going unnoticed and very many of these adversaries are spending anytime between 1-3 years in lateral movement (say, moving within the network to identify the crown jewels to inflict maximum damage) or Advanced Persistent Threats. These attacks are making a mockery of the cyber defense technologies and strategies that we are putting into safeguard us from the same kind of attacks.

Current Challenges:

We are spending a lot of time in finding out the vulnerabilities / control deficiencies within the environment and plugging those. That is purely a defensive strategy and that lacks the thinking to succeed in today's environment. What we need is an adversary mind-set that will help us go ahead and approach the scenario with a refreshed Game Plan. As highlighted earlier, the adversaries are spending sizeable amount of time in Lateral Movement. Once they are in inside the perimeter, they spent enormous amount of time and efforts in understanding the landscape, the crown jewels etc. and wait for the right time to launch an attack. However, all our strategies, tools and manpower spent very less amount of time in detecting and responding to lateral movements within the network.

What shall be the approach then?

What we have been seeing repeatedly is that we are finding it exceedingly difficult to even detect these types of attacks, forget putting strategies to combat the same. Henceforth, what we propose here an integrated strategy of combining Deception Technologies and Moving Target Defense. 'Deception' is an age-old strategy used in warfare with the intent of forcing one's enemy to commit mistakes. Same goes with the use of 'Honeypots', which are nothing but well-laid traps for the attackers to be lured to commit mistakes. Deception Technologies solve the problem of removing false positives and catching the attacker as they enter the network. What this does unlike the traditional technologies that involves behavioural analysis and signature based detection, is that you know exactly when an attacker enters your network thereby preparing oneself for the inevitable. On the other hand, Moving Target Defense (MTD) as a strategy is introducing controlled changes in environment thereby increasing uncertainty and reducing the attack surface. This increases the cost of attacks and requires extreme skill sets that does not work in a static environment. Combing the might of Deception technologies and Moving Target Defense, we have an Offensive Defensive Strategy to combat Cyber Threats, thereby nipping it in the bud itself.

Deception Technologies

Deception Technology is a Defense practice in cybersecurity which aims to deceive attackers. This is done by the distribution of a collection of traps and decoys across your organization's systems infrastructure, to replicate legitimate assets.

The main objective of employing deception technologies in the environment is to reduce the false positives and catch the attacker before they commit any misdeeds.

Deception technologies must be designed in a way to entice the attackers so that they consider it to be a worthy asset and inject a malware. Upon injection of the malware into the decoy, automated static and dynamic analysis of the injected malware is conducted and reports are automatically generated and sent to the Information Security team of your organization.

Deception occurs more in cyber-warfare than in any other field. The reason could be the ease of impersonation in a virtual world. People do it on the Internet very extensively, be it intentional or unintentional. And since impersonation on the internet is easy, many hackers exploit it.

Types of impersonation:

- **Phishing :** It is a particularly dangerous kind of impersonation for social engineering that has increased recently in frequency and severity. Here, a perpetrator sends an email to a large group of potential targets, urging them to visit a website with a familiar-sounding name to resolve a bogus issue. For example, a fake email from "PayPal, Inc" may state that "Security updates require you to re-enter your username and password." The information provided by the victim is then used to commit identity theft or enable espionage.

- **Spear Phishing :** It is like phishing except that in this case the attacker targets individuals rather than the mass, and it is usually more customized. The hacker finds out personal information about the user and makes use of it in his email to make it appear more authentic.

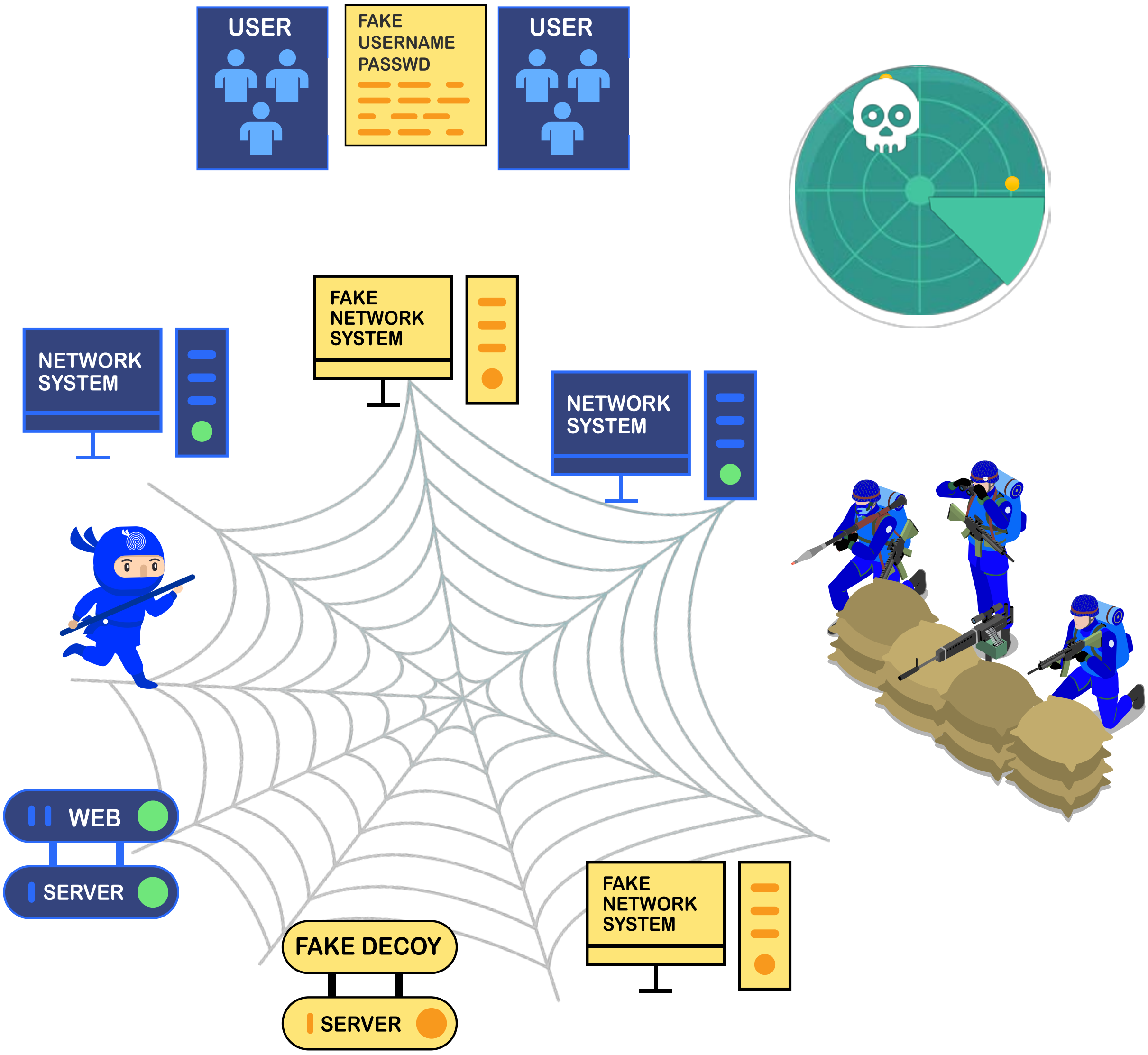
- **Whaling :** Another example could be of Business Email Compromise (BEC) email fraud, also known as "CEO Fraud" or "Whaling". It has become a major financial cyber threat, affecting businesses of all sizes globally. In such attacks, the targets are usually high-profile employees such as a CEO or a CFO to steal sensitive information. Email fraud can take the form of a "con game" or scam as it provides lucrative business for cybercriminals and internet con artists. So, what can be the solution to this problem? Something that can beat attackers at their own game. The answer to this could be in deception itself.

Solution: Turning deception into a weapon - Using Deception Technology.

The idea behind deception technology is to prevent cybercriminals from inflicting significant damage. It is akin to using a decoy to run in a real or virtual operating system to trick the fraudsters into thinking they have breached the security systems.

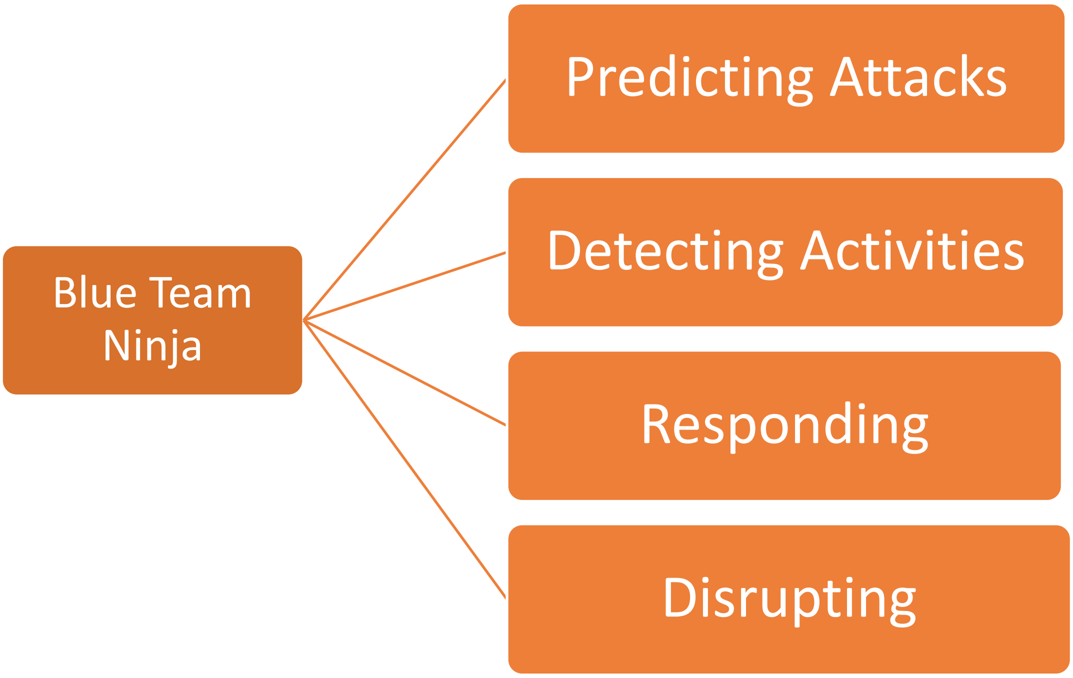
The distributed deception platforms have grown well beyond basic honeypot trapping techniques and are designed for high-interaction deceptions, early detection, and analysis of attackers' lateral movement. Apart from this, the platforms give security teams an upper hand by changing the asymmetry of an attack. It always forces the perpetrator to be on their toes and be on a constant vigil, lest their presence in the system be revealed.

Fig: Your Blue Team Ninja



What is your Blue Team Ninja?

Your Blue Team Ninja is a real-time detection technique whereby attackers are tricked and lured into our fake decoys strategically placed within the environment. This puzzled arrangement for attackers, traps and keeps the attackers engage. With this cutting-edge deception technology, powered by a deep understanding of attacker behaviour, the Blue Team Ninja sets irresistible traps to draw out malicious behaviour earlier in the attack chain and buy the security team the time and insight needed to respond effectively.



What Type of Activities Do Deception Systems Detect?

- Credential Theft: It detects the theft of login credentials like username and password details of users from directories such as OLAP where they are stored.
- Lateral Movement: It detects the movement of a hacker across networks.
- Hacking into directory systems: It detects an attack on the file systems or directories of the end-users.
- Man-in-the-middle: This potentially occurs when communication between two parties are involved. The hacker tries to infiltrate the network and change communication between the involved parties unknown to them.
- Access to sensitive information: When the cyber-criminal tries to steal sensitive and/or confidential data.
- Geo-fencing: When the attackers attempt to hack into deception files that provide virtual geographical location when opened.

Advantage of using Deception Technologies:

- **Reduced risk:**

It is true that no security solution can stop all attacks from occurring on a network, but deception technology helps to give attackers a false sense of security by making them believe they have gained a foothold on your network, whereas in reality progress is almost nil. Moreover, as their movements have been closely monitored and recorded, the knowledge is used to further secure the network. It is a low risk methodology as it has no risk to data or impact on resources or operations and in addition to that it also reduces the noise. It also makes it easy to deploy solutions for detecting and responding to threats important in this age of staff shortages. So, low risks and great results, a near perfect solution.

- **Automated Alerts:**

Another great advantage deception technology comes with is automated alerts. The threat to corporate networks is always on a rise but the budget to handle the deluge of new threats is rarely increased. With automated alerts, manual effort and intervention can be eliminated. Also, deception technology is designed in a manner that allows it to be scaled easily as the organization and threat level grows.

- **Reduced complacency of the IT workforce:**

IT teams are sometimes overwhelmed by the amount of data to be analysed and constantly checked for breaches. This could potentially lead to several false positives and alert fatigue. This could result in them becoming complacent and ignoring a real threat. Thus, when a hacker attempts to access the deception layer, a real alert is sounded and enables the admin to take care of it.

Moving Target Defense

The current game of hide-n-seek between the attackers and defenders in cybersecurity is unfair. The defenders plan the security architecture of an information security system, to prevent threats from attackers who have their own new and sometimes unpredictable ways of compromising a system. Speaking in technical terms, most of the current security systems are static in nature, hence giving the attackers the time to study a system, find its vulnerabilities, and plan an attack. They have an asymmetric advantage, which gives the security architects a hard time predicting a possible exploit.

So, what is the way out of this never-ending game? What if we make our security systems dynamic? What if we give the same asymmetric disadvantage to the attacker? Moving Target Defense systems is the solution we need. It is a whole new revolution in the field of cybersecurity. Instead of defending unchanging infrastructure by detecting, preventing, monitoring, tracking, or remedying threats, moving target Defense dynamizes the attack surface and imposes uncertainty in attack reconnaissance and planning. A dynamic, moving target attack surface imposes asymmetric disadvantages on cyber opponents. It invalidates the collected information and thereby prevents the attacker from building a weaponized attack. This may not end the game but would surely throw the ball in the attacker's court. Some of the developing moving target techniques are system randomization, bio-inspired moving target Defense, dynamic network configurations, cloud-based moving target Defense, and dynamic compilation.

Amongst the advantages of a moving target strategy, the first prominent advantage is that it frustrates the attacker. With a continuously and dynamically changing attack surface, the difficulty of the attack goes up with time. Attackers are forced to spend resources for monitoring and assessing a changing attack surface for an indefinitely long period. Secondly, it can be a considerable advantage when an organization goes for scaling. In a static scenario, the expansion of an organization invites more attacks as there is a greater possibility of a vulnerability left exposed. While in the case of a dynamic security system, the asymmetric disadvantage imposed on an attacker increases. Hence, moving target strategies increase system entropy and efficiency over time and scale.

Such systems also increase the worth of existing controls and methods since it uses orchestration techniques. Speaking in a simplified way, if an endpoint is exploited, shift the attack surface there, or if your cryptographic key is stolen, move your data and change the key. We are shifting around our real data. There is a considerable decrease in the requirement of threat detection once moving target strategies are applied. In the static approach, we detect the threats (attacker) and work on mitigating them. Whereas in the dynamic approach, we focus on increasing the difficulty of the attack instead of finding the undetected attacker.

Moving target defense strategies are becoming pivotal in the cybersecurity domain. It has even adopted new cloud-based technologies like containers, infrastructure as a code, and orchestration. It has already started making a noticeable impact in both the private and government sectors. The thought of moving the asymmetric disadvantage from the side of the organizations to that of the attackers is a compelling motivation for development and research. It is strengthening innovation and an embrace of the existing security technologies. As organizations are moving to cloud, newer ways of handling configuration management and security come along with the dynamic environment which cloud infrastructures provide.

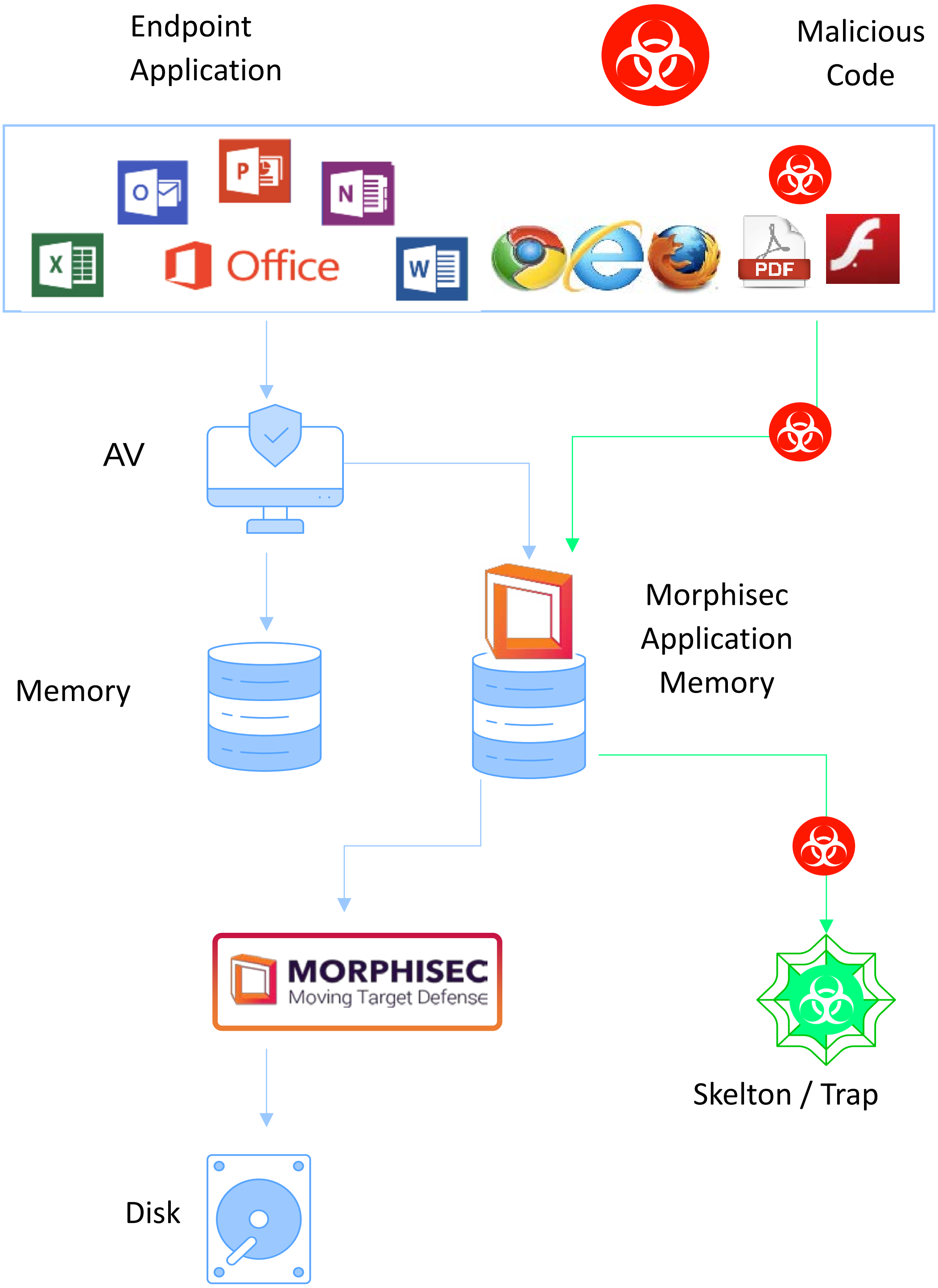
It is a perfect opportunity from a business perspective too. As this technology is evolving, it is becoming possible for even the smaller enterprises to leverage the benefits of moving target strategies into their security frameworks. It safeguards the data in untrusted networks and environments too. Hence security teams can convince the management to adopt this technology without breaking policies or compromising security standards. With Moving Target Defense Technology, Cybersecurity experts like us have an unfair advantage over the attackers and the tables are completely turned in favour of enterprises.

Our Approach:

It has been observed that 76% of breaches are caused by file less, in-memory attacks and that up to 80% of the attacks happen at the endpoint. The existing solutions are knowledge based and are defenseless against unknown and evasive threats. There is a refreshed view of looking at things here. The objective is to prevent (tactics) the attack from happening than detect (techniques) it when it surfaces. This reduces the surface area and thereby reducing the risks massively. The idea is to introduce controlled changes, increases uncertainty, increases complexity, reduces window of opportunity thereby increasing the cost of attack. Operating Systems and Applications are the real battlegrounds, and we are presenting a solution here at the OS and applications levels where the informative intelligence collected by the attacker to launch any attack is made futile.

The solution morphs the application memory and prevents any in-memory attacks being launched. It prevents zero-days, targeted and unknown attacks with no prior knowledge in one shot. The memory that is used at various points in the attack kill chain is clearly shielded thereby preventing such attacks from materializing.

We take the Moving Target Defense paradigm to the next level by creating environmental modifications to the application and the operating system, in a manner untraceable by attackers. By forcing attackers to fight on an uncertain battlefield, Moving Target Defense completely changes the rules of conflict.



Moving Target Defense - Common Practices:

In practice, there are three main categories of Moving Target Defense security:

(1) network level MTD,

(2) host level MTD,

(3) application level MTD.

1. Network level MTD includes several mechanisms that have been developed over the years. IP-hopping changes the host's IP address, thus increasing the network's complexity as seen by the attacker. Later, this idea was extended to allow maintaining the hosts IP mutation in a transparent manner. Transparency is achieved by keeping the real host's IP address and associating each host with a virtual random IP address. Some techniques aim at deceiving the attacker at the phase of network mapping and reconnaissance. These techniques can include using random port numbers, extra open or closed ports, fake listening hosts, and obfuscated port traffic c. Other techniques provide the attacker with fake information about the host and OS type and version. This includes random network services responses which prevent OS identification.
2. Host level MTD includes changing the hosts and OS level resources, naming and configurations to trick the attacker.
3. Application level MTD involves changing the application environment to trick the attacker. Address Space Layout Randomization (ASLR), which was introduced by Microsoft, implements a basic level of MTD. It involves randomly arranging the memory layout of the process's address space to make it harder for an adversary to execute its shellcode. Other techniques involve changing the application type and versioning and rotating them between different hosts. Some application level MTDs use different settings and programming languages to compile the source-code, generating different code in every compilation.

Information System Component	Deception Method
Network	Route change; random addresses, names and ports
Firewall / IDS	Policy change
Host	Change host address, replace host image
OS	Change version and release; change host ID; Change memory addresses, structures, resource names
Application / Application Code	Randomize addresses of storage fragments, filter input data that cause failures, rotate application among different hosts; multilingual code generation; different code generation

Benefits of the Moving Target Defense:

Endpoints:

- Prevention of in-memory zero days or file-less attacks
- Application Virtual Patching against in-memory attacks for commonly used applications
- Protection from Mimikatz Credential Stealing attacks
- Enhanced Lateral movement attack prevention by WMI coverage
- Prevention of Shell Code Injections

Servers:

- Enhanced Lateral movement attack prevention by WMI coverage
- Prevention of Shell Code Injections
- Protection from Mimikatz Credential Stealing attacks
- Application Virtual Patching capabilities against in-memory attacks on default applications installed on servers (e.g. browsers, adobe etc.)

Other Benefits:

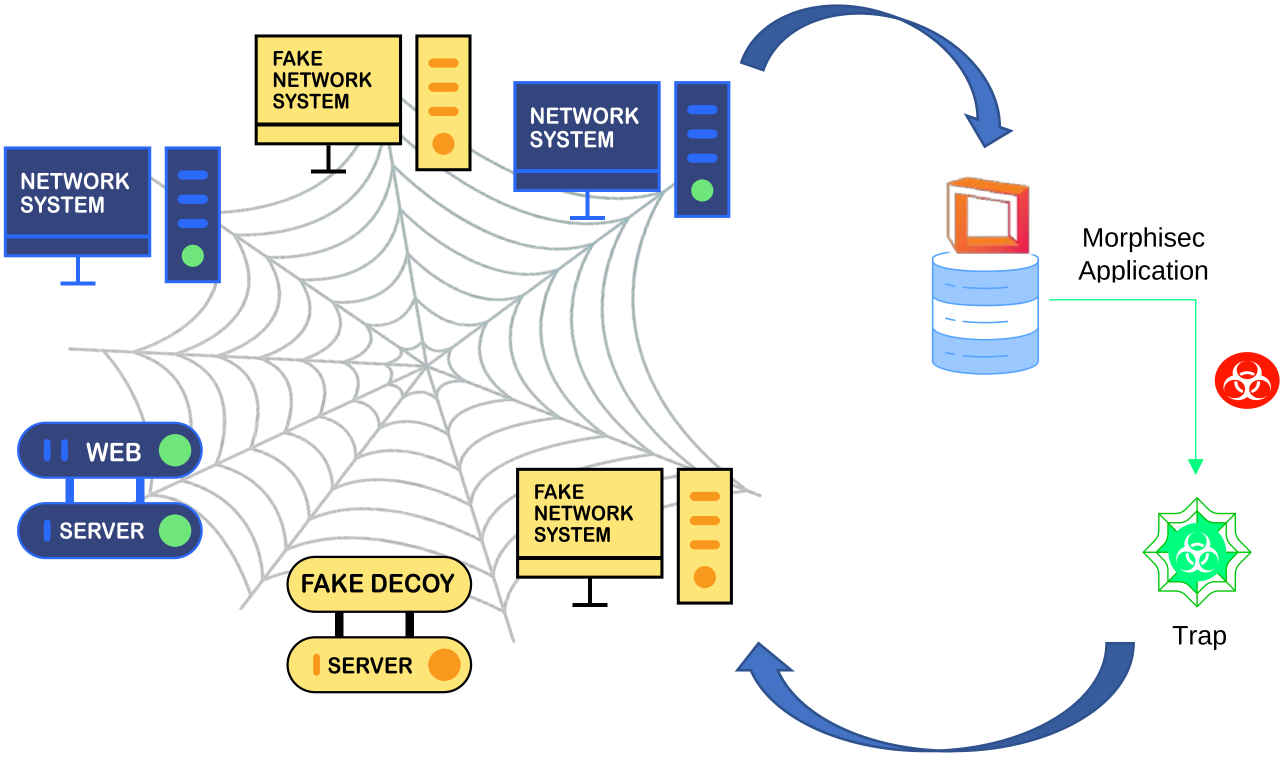
- MTD Prevents Advanced in-Memory Attacks with no prior knowledge
- Compliments existing Security Stack and reduces the residual risk level lower than the acceptable limits
- Shields commonly used Applications from memory-based attacks thus acting as an Application Virtual Patching shield
- Signature-less solution which does not require frequent updates thus saving costly man-hours for day to day management
- Light-weight Agent(2MB) ensures faster deployment and quicker ROI
- No Performance Impact on Applications and Stability Issues with Operating System ensuring faster Adaptability by end-users
- Simple solution which does not require additional manpower and skillsets for management

An Integrated Approach

We have seen the benefits of using Deception Technologies to remove false positives and to detect any attacks before it materializes. And we also looked at the Moving Target Defense as a Strategy to prevent attacks. What if we combine these two to bring to the table the advantages and benefits of both and much more?

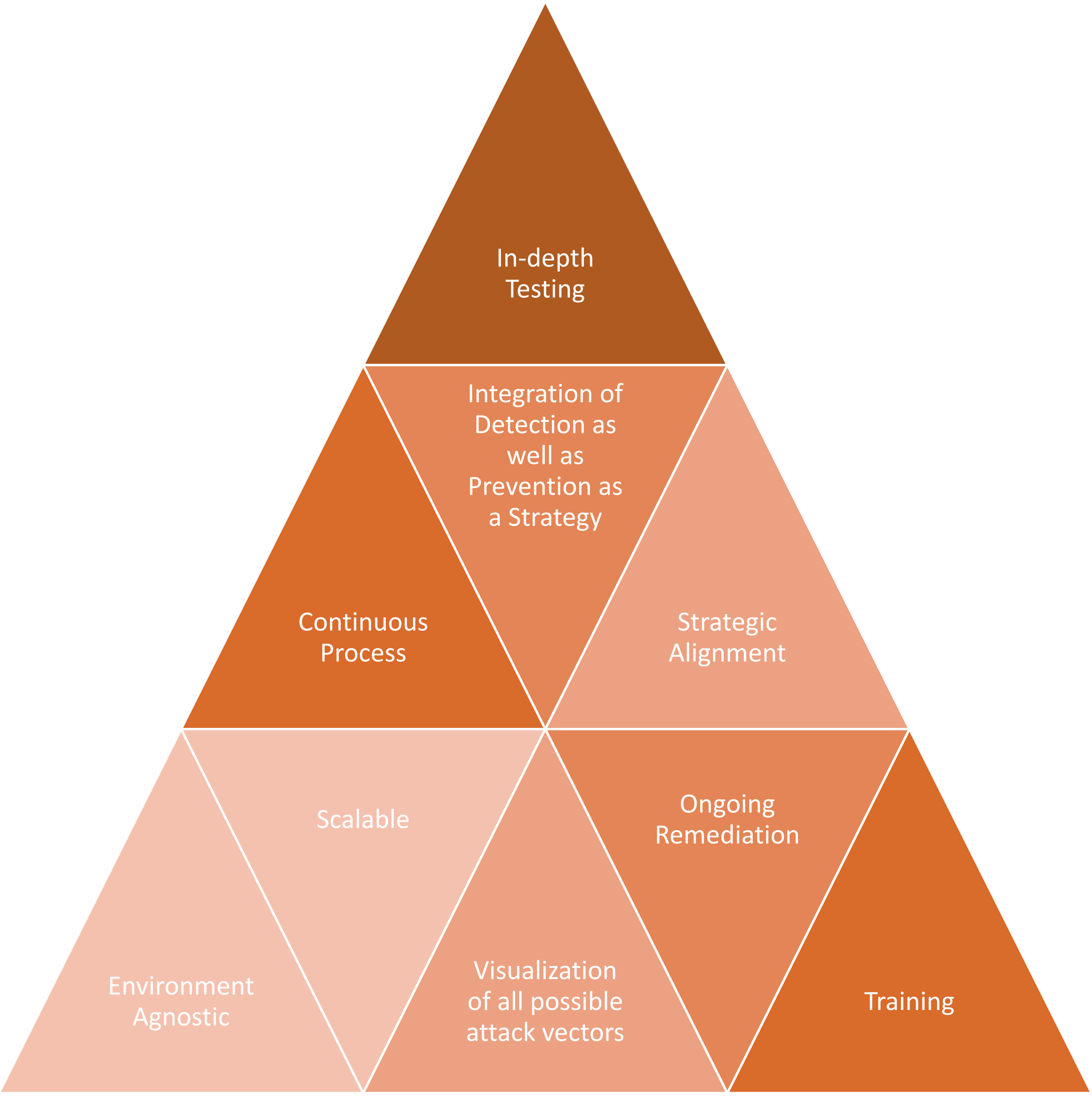
In this integrated approach what we are trying to do is to efficiently use these 2 technologies under the able guidance of a Blue Team. If the Decoys can detect an attacker, then they are engaged for a fixed short period to not alert them. Post which, they are blocked out whereby they might sense that a cyber defense solution is doing the same. The alert that goes the Blue Team makes them prepare themselves to use the MTD solution to wisely open another service or ip to lure them back to the environment. Again, the same techniques as mentioned earlier follows. This goes on till the time attacker feels frustrated and leave it altogether. What we achieve here are 2 things. One, we can detect any attack before it manifests. Second, is the preventing the further damage by using preventive measures. Further, by the time the loop is closed we would have gotten as much information about the attacker as well as the techniques employed that it can be used to further tighten the counter measures. There are quiet some use cases that we can use that have diffused so many such attacks from materializing. This is a great approach to secure the organization assets in a cloud environment whereby we can lure the attackers and beat them in their own turf

i.e. Deception and Unpredictability.



Key Benefits of this Approach

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



Way Forward

This methodology is proving to be a game changer in devising a Cyber Defense Strategy for any Organization. It is a highly evolved approach that marries the advantages of Detection as well as Prevention that gives the power to any cyber team. 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.

Infopercept

Contact Us

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Company's / 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.

Phone
+91 989 885 7117

Email
E: sos@infopercept.com
W: www.infopercept.com

USA	UK	INDIA	KUWAIT	SRI LANKA
New York	London	Ahmedabad | Bangalore Hyderabad | Mumbai	Kuwait City	Colombo