OFFENSIVE-DEFENSIVE STRATEGIES AGAINST ALL ODDS
Setting the context

Cyber attacks have evolved, and the techniques employed by the attackers have changed drastically in the recent years. The adversaries are spending anytime between 1-3 years in lateral movement within the customer environment or Advanced Persistent Threats (APTs) are a common occurrence today. The attackers are deceiving the cyber defense mechanisms put in place and taking time to study the environment and are launching the attacks at the most opportune moment to inflict maximum damage.

Currently, the typical approach is to counter these sophisticated APT attacks with such defensive strategies that are easily bypassed or deceived by the attackers.

This has resulted in many breaches going unnoticed for months and years.

Hence, what we propose here is an Offensive Defensive Strategy (ODS) combining Deception Technologies and Moving Target Defense (MTD) to deliver a coercive counterattack.

Through Deception, the attackers are caught as and when they enter the network and then through Moving target Defense they are deceived and misled that they never reach the crown jewels. This way, they are detected and tracked from the time they enter the network. The chances of false positives and negligible and that it’s a very offensive technique taking the fight back to the enemy.
Why Invinsense ODS?

Offensive Defensive Against All Odds

Combining the potential capabilities of Deception Technologies and Moving Target Defense is the immense potential of catching the attacker before they make the first move and then nullifying their attempts on real-time:

- Our offensive Security makes you and your system think and act like Adversaries.
- Our deception creates a trap for Adversaries which helps you see their actions and neutralize them.
- Our moving target defense helps prevent attack by diversion and dilution.
What is Deception?

Deception is the evolution of the idea of the honey pot — external sites that would attract people who had bad intentions so that they could be identified. While honey pots were often used by security researchers, it was not a popular threat detection technique for enterprises. Deception takes a new approach and moves decoys inside the network, offering more valuable insight into threats that have penetrated perimeter defenses.

Deception is a viable option to improve threat detection and response capabilities. Technical professionals focused on security should evaluate deception as a “low-friction” method to detect threats inside their environments and as an alternative or complement to other detection technologies.

Benefits of ODS

**Deception**
- Reduction in well time and the mean time to detection and remediation.
- Locate and remediate.
- Decreases dwelling time.
- Compromise Indicators (IOCs).
- Tactics, techniques, and procedures (TTPs) through engagement.
- Detect early recognition, credential theft, and lateral motion.
- Decoys around the new vital assets that are at risk.
- Reduced False Positives and Risk

**Moving Target Defense**
- Reduce resources needed for detection.
- Defend distributed data in untrusted networks.
- Reduce resources needed for detection.
- Well worth the effort and potential cost.
- Decrease attacker ROI.
- Scalable security solution.
- Enhances system efficiency.
- Significant layer of protection between defenders and attackers.
Integrated Approach Combining Deception and Unpredictability
Personalized Threat Intelligence

Reduced False Positives

With Dejavu’s cutting-edge deception technology, powered by a deep understanding of attacker behavior, the Blue Ninja sets irresistible traps to draw out malicious behavior earlier in the attack chain and buy your team the time and insight needed to respond effectively.
Use Cases of Deception Technology

- Perimeter Deception
- Network Deception
- Endpoint Deception
- Deception + Endpoint Detection & Response
- Deception + User Entity and Behavior Analytics
- Deception + Sandboxes
- Deception + Threat Intelligence
- Deception + Network Traffic Analysis
- Deception + Threat Hunting Platform
Moving target defense technology is designed to provide end-to-end protection against the most damaging cyberattacks. With the power of moving target defense, attackers are unable to accurately identify the resources they need to leverage in order to evade your current defenses. This proactive cyber defense solution guards your critical systems with a lightweight, easy to install agent that doesn't require any updates to keep securing critical infrastructure.
## Invinsense ODS – MTD Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature/Whitelist</td>
<td>Implemented at both network and endpoint</td>
</tr>
<tr>
<td></td>
<td>MTD assumes perfect security is unattainable</td>
</tr>
<tr>
<td>Sandbox</td>
<td>Devices placed at the perimeter to emulate files in a contained environment and assess risk</td>
</tr>
<tr>
<td></td>
<td>Introduces controlled changes, increases uncertainty, increases complexity, reduces window of opportunity, increases cost of attack</td>
</tr>
<tr>
<td>Artificial Intelligence</td>
<td>Machine Learning/Deep Learning work on principle of training set deployed on the cloud.</td>
</tr>
<tr>
<td>Behaviour Monitoring</td>
<td>Looks for behaviour anomalies of processes to make a decision</td>
</tr>
<tr>
<td></td>
<td>MTD focuses on having systems that are defensible rather than perfectly secure</td>
</tr>
</tbody>
</table>
## Invinsense ODS – MTD Techniques

<table>
<thead>
<tr>
<th>TECHNIQUE</th>
<th>DECEPTION METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polymorphism</td>
<td>Changes malware signature</td>
</tr>
<tr>
<td>Metamorphism/ Self-modification</td>
<td>Changes malware code on the fly</td>
</tr>
<tr>
<td>Obfuscation</td>
<td>Hides malicious activities</td>
</tr>
<tr>
<td>Self-encryption</td>
<td>Changes malware signature and hide malicious code and data</td>
</tr>
<tr>
<td>Anti-VM/sandboxes</td>
<td>Evades automated forensic analysis by changing behaviour in forensic environments</td>
</tr>
<tr>
<td>Anti-Debugging</td>
<td>Evades automated/manual investigation by changing behaviour in forensic environments</td>
</tr>
<tr>
<td>Encrypted exploits</td>
<td>Evades automated/manual investigation by changing parameters &amp; signatures</td>
</tr>
<tr>
<td>Behaviour Changes</td>
<td>Waits for real user activity before executing</td>
</tr>
</tbody>
</table>
Moving Target Defense

Real Life Scenario

Scenario 1
Attacker builds knowledge about the environment

Scenario 2
With practice and skill, can achieve accuracy in a standard/static environment

Scenario 3
In a changing environment, the attacker needs much more skill, effort and resources to hit

“You can execute a technique to hit the target; but it’s not feasible that you would succeed with a moving target.”
## Advantage of Invinsense ODS - MTD

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