Technical Validation

Illusive Networks

Agentless, Authentic Deception Technology at Scale

By Tony Palmer, Senior Validation Analyst

May 2020

This ESG Technical Validation was commissioned by Illusive Networks and is distributed under license from ESG.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Introduction

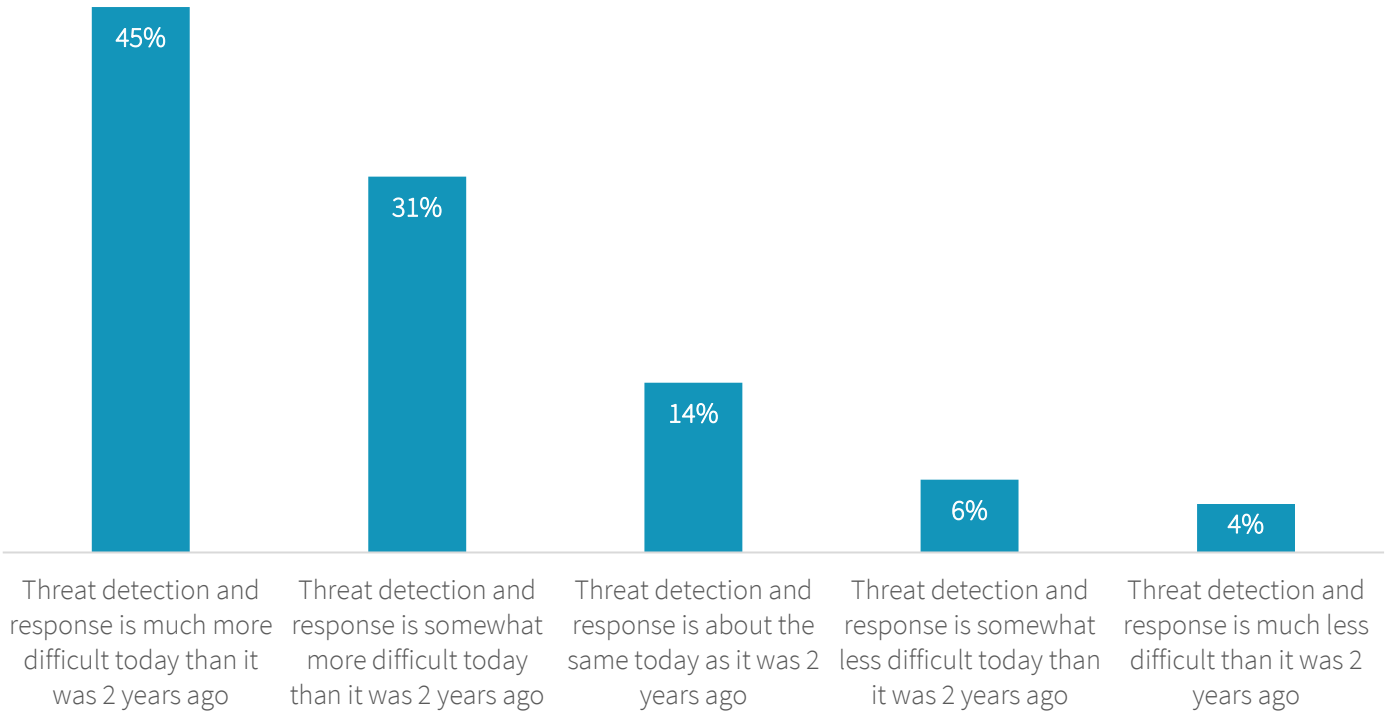
ESG evaluated the Illusive Networks Platform with a focus on validating its ability to simply and efficiently preempt attacks before they occur where possible, protect against attackers inside the perimeter, and respond to incidents with fast data-driven decisions, regardless of where assets are located, or where the attacks originated. Illusive's ability to scale deception technology quickly and easily was also of interest.

Background

Research from ESG and the Information Systems Security Association (ISSA) reveals that 74% of cybersecurity professionals believe that the ongoing global cybersecurity skills shortage has impacted their organizations.[1] Based upon this research, it's clear that most organizations don't have enough cybersecurity staffers, don't have some necessary cybersecurity skills, or both—a daunting situation. Meanwhile, the number of security incidents that businesses must investigate and respond to has grown exponentially; the proliferation of new systems and applications is creating more security incident scenarios, while a burgeoning number of detection tools are generating more alerts.

According to ESG research, more than three-quarters (76%) of organizations say that threat detection and response is more difficult today than it was two years ago (see Figure 1), the result of increasing threat volume and sophistication. This includes advanced techniques, tactics, and procedures (TTP) using fileless attacks and macros targeting PowerShell, .net, programming libraries, and APIs. The increasing threat detection and response workload, increasing attack surface, and the number of disparate threat detection and response tools, along with the ongoing global cybersecurity skills shortage also contribute to the increasing difficulty of threat detection and response.[2]

Figure 1. Difficulty of Threat Detection and Response



Source: Enterprise Strategy Group

[1] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.
[2] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The traditional endpoint security architecture based on multiple independent point products requires analysts to log into multiple systems and manually cross-correlate alerts. Additional tools are often employed to combine, correlate, and analyze security tool data. Both tactics slow the detection, investigation, and remediation process, leading to longer mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

The Illusive Platform

The Illusive Platform is built on agentless automation that is designed to have a light operational footprint to minimize the impact on IT. Illusive engineered their deception technology to disarm the attacker with a goal of eliminating their access to useful data, disabling decision making, and depriving them of the means to reach their targets. The Illusive Platform provides centralized management across environments of any size. The Illusive Platform's virtual machine-based decoys utilize native or tailored golden images, eliminating the need for manual configuration or physical presence in the locations where decoys are being installed, enhancing decoy authenticity by ensuring conformance to organizational standards and practices. Three modular components can work together or be operated separately to preempt, detect, and respond to cyberattacks.

Figure 2. The Illusive Platform

Source: Enterprise Strategy Group

Attack Surface Manager

Illusive Networks Attack Surface Manager is designed for the pre-breach stage before an attacker lands in the network. In high impact cyberattacks, attackers almost always conduct lateral movement from the system they've gained a foothold on to the ultimate target. To do this, the attacker uses attack tools to automate and accelerate credential harvesting, network discovery, and privilege escalation. This process, called "living off the land," uses the connectivity native to the organization. Attack Surface Manager enables organizations to manage their attack surface perpetually to preemptively cut off malicious access to "crown jewels."

Attack Detection System

Illusive Networks Attack Detection System (ADS) is responsible for post-breach, early detection of cyberattacks. ADS is designed to stop attackers by deploying lightweight deceptions on every endpoint that block attackers' ability to make safe decisions as they attempt to explore and traverse the network. Deceptions placed on endpoints mimic credentials, connections, files, and other data that look to an attacker as though they will facilitate lateral movement. Continuous

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

machine learning automation designs, deploys, and manages deceptions that reflect the naming conventions and other practices of the organization so that the attacker cannot tell real assets from deceptions and the attacker's first wrong choice triggers an alert. The net of deceptions catches attackers at or close to their point of entry by covering the entire endpoint inventory. ADS includes Illusive's endpoint forensics functions, which provide the forensics components of Illusive's Attack Intelligence System. As soon as a deception is activated, forensics are captured from the compromised machine, giving responders the data needed to determine how to react, including visibility on how close the attacker is to critical business assets and domain admin credentials.

Attack Intelligence System

Illusive Networks Attack Intelligence System is the set of response capabilities responsible for the collection and parsing of incident forensics to facilitate rapid and precise understanding of attacker activity. Illusive captures source forensics from the endpoints where attackers are operating and target forensics from highly interactive decoys—deceptive surrogate systems that attackers would be interested in compromising. Source forensics include volatile and non-volatile data from the endpoint, as well as real-time screenshots, while target forensics provide continuous visibility into the tools, methods, and intent of the attacker. This intelligence is compiled into a Forensics Timeline that provides unified access to a tremendous amount of incident data, designed to accelerate the entire incident handling process: immediate triage, investigation of the overarching incident, and remediation.

Illusive integrates into existing security strategies and stacks with a large and growing ecosystem of technical integrations with a variety of different security solutions, including but not limited to:

Endpoint detection and response (EDR)—Illusive deceptions can enhance the detection capabilities of EDR solutions, and EDR solutions then can enable organizations to immediately quarantine or isolate detected threats.

Privileged access management (PAM)—Illusive Networks has partnered with PAM solution vendors to seamlessly incorporate privileged account management into the deployment and administration of the Illusive Platform and enhance deployment security.

DNS management solutions—Illusive Networks and DNS management solutions work together to automate the mapping of deceptive hostnames, so that DNS deceptions are easy for teams to deploy without additional manual or scripted mapping.

Security information and event management (SIEM)—The integrated combination of Illusive and SIEM aims to deliver high-fidelity alerts and on-demand forensics that can be accessed through the SIEM to shrink the time and overhead required to find and neutralize threats.

ESG Technical Validation

ESG performed evaluation and testing of the Illusive Platform. Testing was designed to validate the value of using Illusive attack pathway discovery and elimination to preempt attackers; data-based deceptions that appear genuine and legitimate to detect and respond to attacks; and the efficiency and ease of deployment, use, and management of the platform.

Attack Pathway Discovery and Elimination

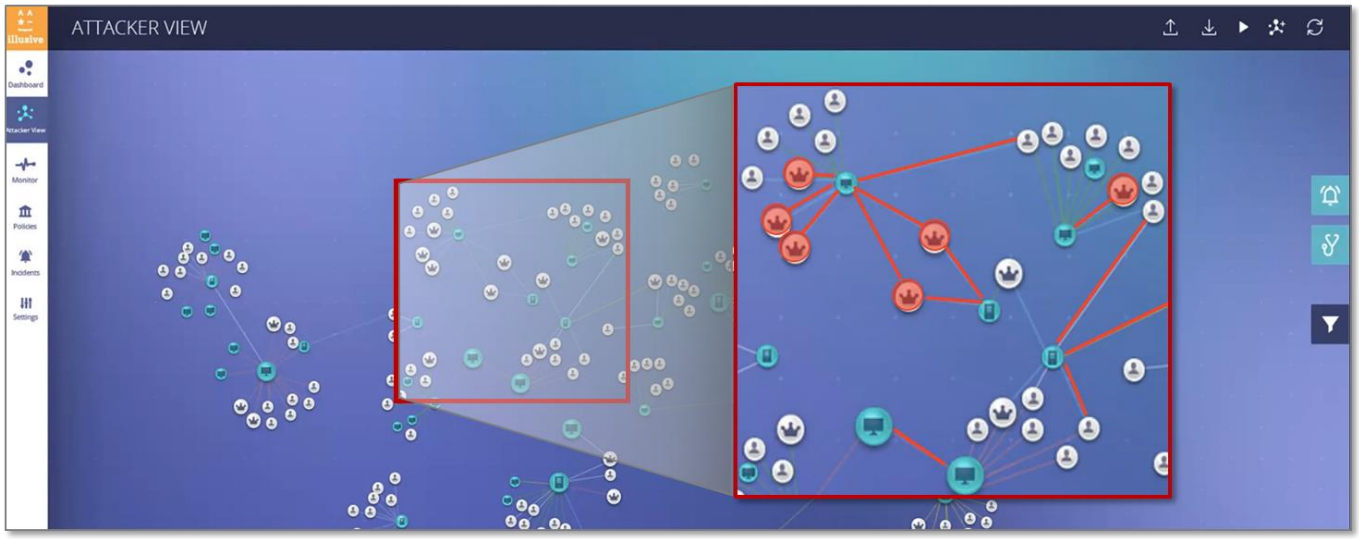
Identifying and removing excess, high-risk, and rogue connections has historically been a manual process and especially difficult to execute across an enterprise. The Illusive Platform is designed to continuously reduce an organization's attack surface without agents, with the goal of guaranteeing ongoing cyber hygiene that pinpoints and eliminates the most common paths attackers use to move laterally through an organization's network once they are inside the perimeter. This use case is an illustration of what attackers could do if they were present and how Illusive enables the eradication of conditions that pose an unacceptable risk.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

ESG Testing

First, ESG examined automated attack path and high-value asset discovery. Credentials and connections proliferate within an organization's network and attackers use threat tools like mimikatz to automate and accelerate credential harvesting, network discovery, and privilege escalation. The Illusive Platform provides the automatic discovery and mapping of the access footprint across an organization, defining attack paths to high-value systems, shown in red in Figure 3.

Figure 3. Automated Attack Path Discovery



Source: Enterprise Strategy Group

Once attack paths are identified, Illusive can remove conditions that are often exploited by attackers as they move laterally. As a result of normal system and application use, credentials are commonly stored in browser caches and in Windows' memory by the Local Security Authority Subsystem Service (LSASS). The Illusive Platform uncovers a wide gamut of basic yet frequently overlooked lateral movement paths that attackers use to move from a staging area established inside the perimeter to the data they want to steal. These paths include:

- Domain user credentials—referencing Active Directory (AD) groups.
- Local admin accounts—including the ability to discover local admins that share the same password.
- Domain admins—presence of domain admin credentials on systems and devices across the organization.
- Shadow admins—high-privilege users and groups that are not part of typically known privileged user groups.
- Connections to high-value systems—saved connections to systems tagged as being critical to the business.

The Illusive Platform enables adaptive and scalable decision making where removal of high-risk connectivity will have the greatest positive impact in reducing overall attack risk. The Illusive Platform's Pathways feature continuously computes the distance between endpoints and high-value systems, the risk levels associated with each system, and the connections that depend on each system in the chain. This data is automatically presented in a filtered dashboard view to focus analyst attention on the most critical conditions in the organization. It provides details on the systems in each path and enables elimination of unneeded connectivity. The Illusive Platform also provides on-demand summary reports designed to give security leaders and line-of-business IT leaders visibility into the organization's risk posture.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Illusive Platform's Action Engine feature can be configured through rules to provide automated remediation of cyber hygiene violations. When violations are detected, cleaning actions can be designated to execute in the background in real time. Examples include disconnecting orphaned remote desktop connections and associated credentials, disabling local admin accounts, and detecting and disabling accounts that are not covered by an organization's privileged access management (PAM) solution until those accounts are outfitted with stricter privileged credential polices.

Why This Matters

The critical lack of cybersecurity skills presents a challenge to organizations: How do they simply and efficiently protect their data and IT resources? A solution focused on easing the management burden is needed to ensure that cybersecurity analysts spend less time on the care and feeding of tools and more time protecting the organization.

ESG validated that Illusive continuously reduces an organization's attack surface without the use of agents, identifying high-value assets, then pinpointing and eliminating the paths that attackers use to move laterally inside the perimeter. Automated remediation of cyber hygiene violations can execute cleaning actions in the background in real time to remove vulnerabilities without human intervention, freeing time, effort, and resources for more strategic activities.

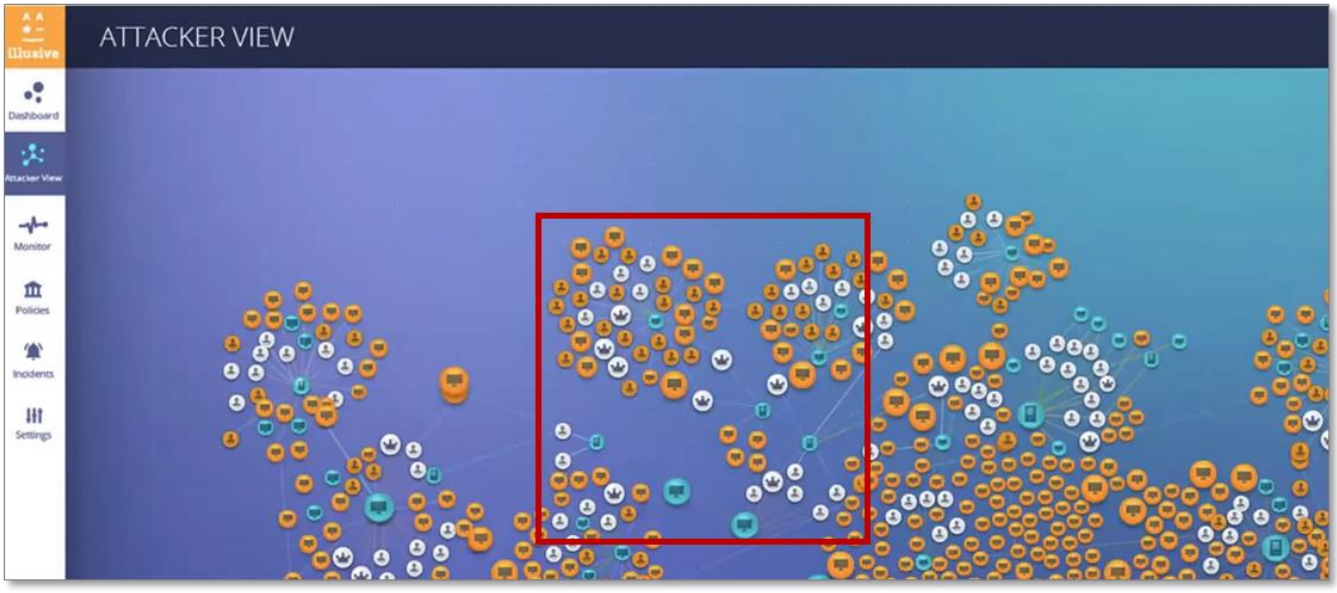
Deception Authenticity

High authenticity of deceptions is key. Attackers need to believe that deceptive data is real for deception to function effectively. The Illusive Platform's data-based deceptions are designed to appear genuine and legitimate to attackers, luring them into engagement, and ultimately identifying and stopping them. These deceptions can be placed on the attack paths that were cleaned up by the Illusive Platform, as discussed earlier, and can reveal attackers on the network as soon as they attempt to move laterally.

ESG Testing

ESG explored Illusive's automation of the adaptation and custom fit of deceptions to the individual endpoints where they are deployed. This ensures that deceptions accurately reflect the data, credentials, and connections that an attacker would expect to find on any given endpoint on the network they find themselves in.

Figure 4. Deceptions Deployed



Source: Enterprise Strategy Group

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

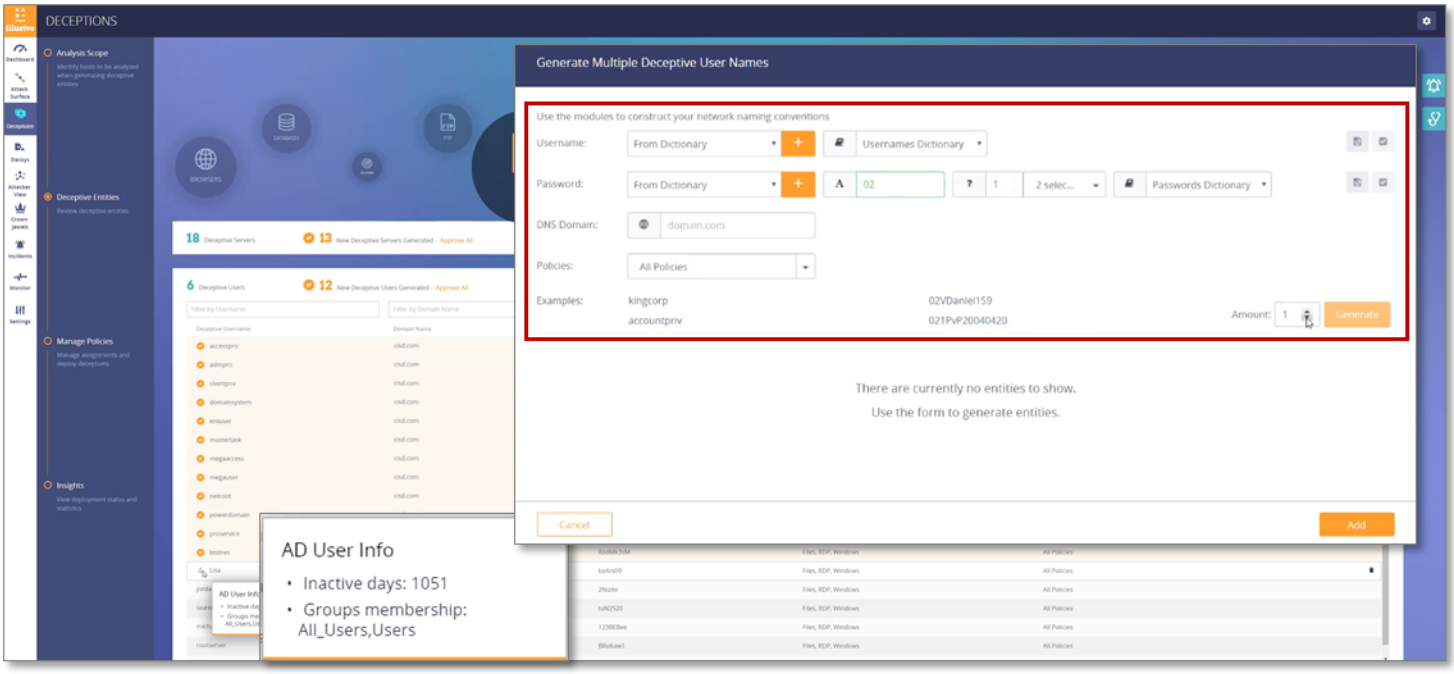
Figure 4 shows the same network view after deceptions are deployed. The orange icons represent deceptive users and systems deployed on the network and their apparent locations.

Attackers leverage tools like Honeypot Buster—a tool used to identify honey tokens, honey breadcrumbs, and honeypots commonly deployed by deception vendors—to evade decoys and other types of deception technology. Illusive allows organizations to create Deception Deployment Profiles to boost deception density and complexity on specific systems as needed. Illusive offers three different profiles for deception distribution and complexity levels that organizations can toggle between depending on the needs of the system they are trying to protect. Illusive's agentless automation capabilities alleviate organizations' need to spend time tweaking and refreshing deceptions so that Honeypot Buster can't find them; Illusive's footprint is so light that Honeypot Buster has no way to detect them.

Illusive deceptions are pushed out to endpoints and systems through an executable file that is copied and deleted in the span of less than half a second every 20 hours. The traffic sent between the Illusive management server and an organization's endpoints is extremely lightweight to minimize impact on remote sites. Because there are no resident agents running on the endpoints, there's nothing for advanced attackers to spot or circumvent. Deception solutions that require an agent to get full deception and forensic capabilities from the solution are traceable by attackers due to the agent's presence on all endpoints. Agents are also susceptible to reverse-engineering, where attackers learn how the agent works and how to circumvent or break it.

ESG looked at how an analyst deploys deceptions. Figure 5 shows the deceptive users view. It took just a few clicks to define the parameters that fit the environment and generate as many deceptive users as desired that are visible in Active Directory and look very much like real users. Illusive also leverages real inactive AD users.

Figure 5. Deceptive Users

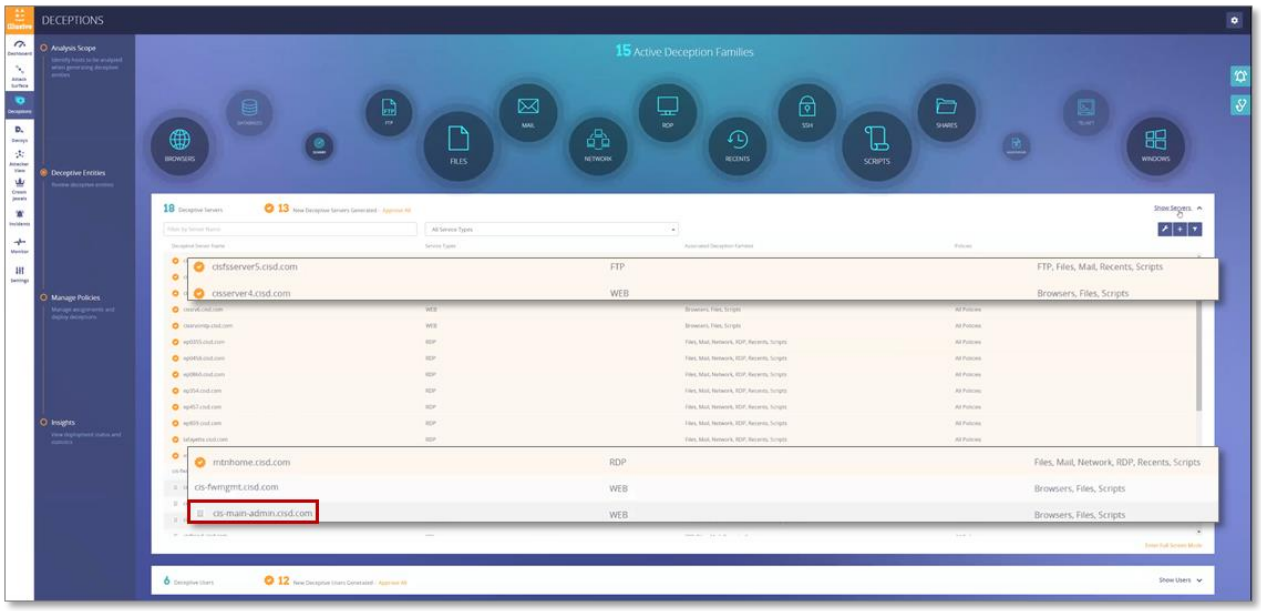


Source: Enterprise Strategy Group

Next, ESG looked at the deceptive servers view, seen in Figure 6.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 6. Deceptive Servers



Source: Enterprise Strategy Group

As with deceptive users, Illusive discovers inactive servers in Active Directory and uses them to create authentic deceptions. The orange icons identify server deceptions generated by Illusive, created using naming conventions learned in discovery and configured using data analyzed from active, real systems.

Why This Matters

Organizations tell ESG that threat detection has been growing more challenging.[3] Malicious actors are becoming more sophisticated and are crafting more devious and evasive attacks. Recent attacks have been specifically designed to evade new artificial intelligence-based methods of detection. Organizations need a solution that can supplement existing systems and help them to be more effective.

ESG validated that Illusive cloaks the entire environment with agentless deceptive information that looks and feels highly authentic, then silently alerts analysts, collects detailed forensics, and provides high-fidelity incident notifications with a low rate of false positives. Taken together, these capabilities make it exceedingly difficult for attackers to successfully move laterally toward critical information and systems. The net effect is that attacks can be thwarted in their earliest stages before any critical data is impacted or affected.

Deployment Efficiency and Ease of Use

Illusive Networks is engineered to easily scale deceptions up to millions of endpoints. Up to 150,000 endpoints can be protected using a single server. Security operations center (SOC) employees are armed with a low volume of high-fidelity incident notification reports with immediately actionable information to stop attacks, rather than the massive volume of alerts—replete with false positives—that need to be investigated before they can be confirmed as attacks. With this data, SOC and IT employees can be more self-sufficient and less reliant on other departments to carry out complete incident investigations.

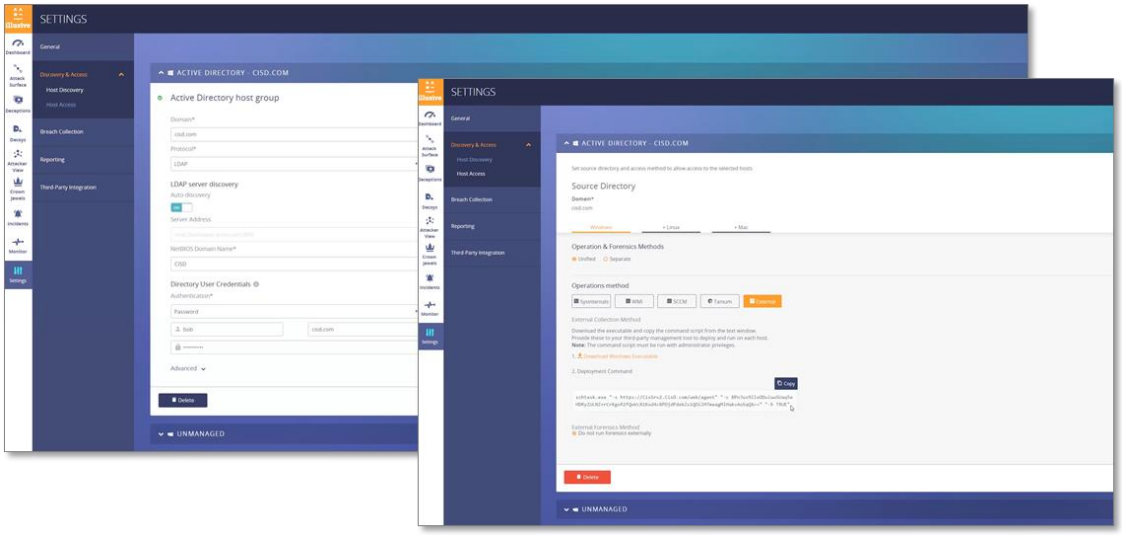
[3] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

ESG Testing

Illusive simplifies deployment by automating much of the process. First, the platform communicates with Active Directory using an account to understand all users, configurations, and values, to identify what machines are the highest-value assets.

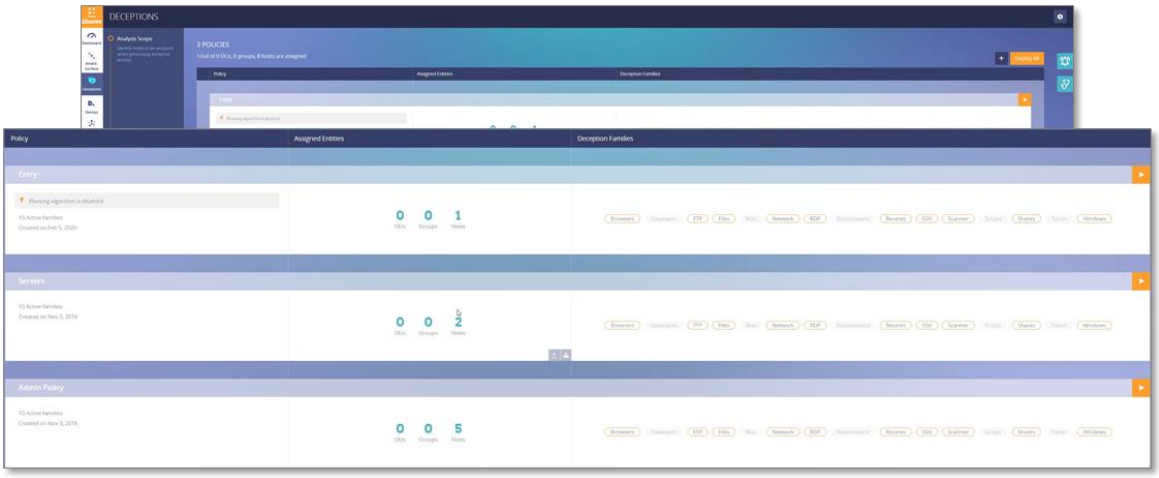
Figure 7. Host Discovery and Access



Source: Enterprise Strategy Group

Once discovery is complete, organizations can set the desired operational method for host access: Sysinternals, Windows Management Instrumentation (WMI), Microsoft Endpoint Configuration Manager (formerly SCCM), or Tanium. External tools like BladeLogic, Chef, or others are also available. Illusive provides a parent key to the management server and discovery happens in the background.

Figure 8. Host Discovery and Access



Source: Enterprise Strategy Group

The point and click interface to define policies that are appropriate to each type of endpoint is simple to use. ESG was able to assign and unassign policies in seconds with just a few clicks.

Although Illusive automates routine functions at scale, the platform also allows for human oversight where needed. In manual mode, once an analyst has reviewed the suggested deceptions, they are deployed through a one-click process.

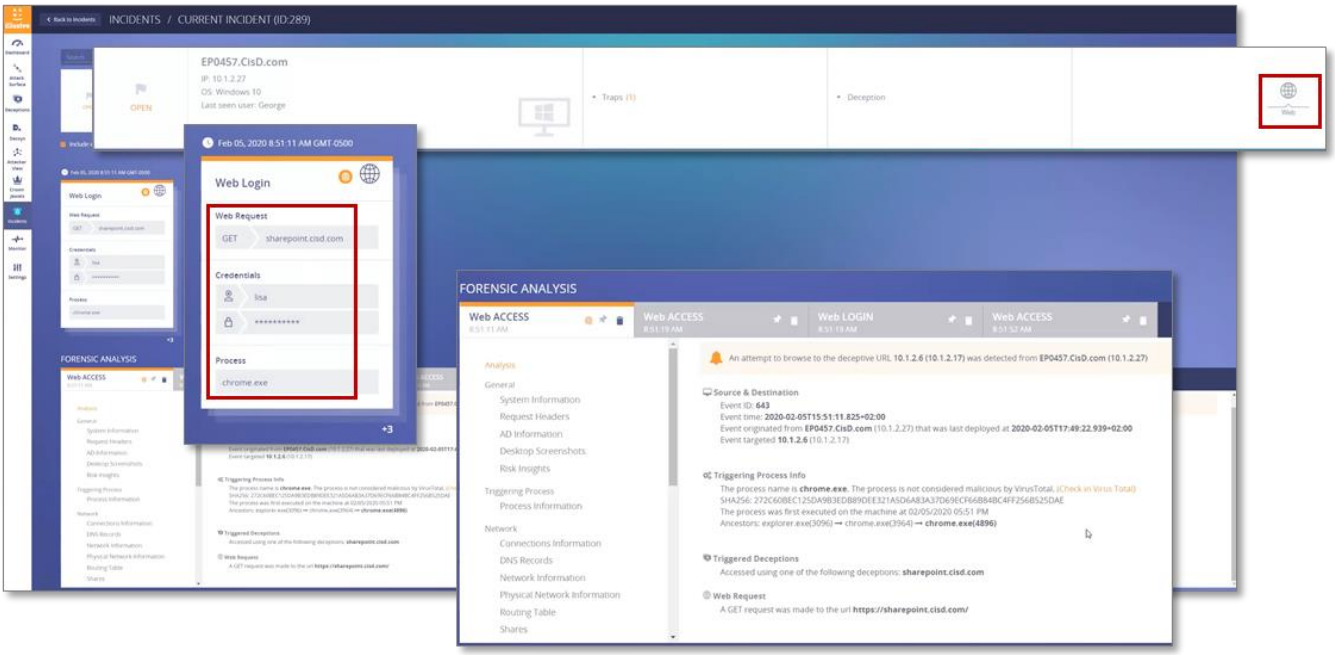
© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

ESG's testing in a simulated environment confirmed that deployment takes milliseconds per machine. 100,000 endpoints can be fitted with deceptions in approximately seven hours. When deployment is complete, a snapshot is saved to record the deceptions that were planted.

In addition to automated deception creation, refreshing deceptions is also automated. The solution learns how each customer's network is configured, including naming conventions for users, systems, applications, and communication patterns. The Illusive Platform recommends and automatically deploys deceptions that are tailored to reflect what the organization has on its network. The goal is to help organizations deploy the best, most reliable set of deceptions for each machine or user that they can to increase chances to fool—and detect—an attacker.

Finally, ESG triggered an incident to observe the forensics and response deployed by Illusive to detect and remediate the threat. We ran mimikatz on a system in the test network and obtained a set of saved credentials. The credentials were indistinguishable from legitimate credentials observed on the network. With those credentials, we attempted to log in to SharePoint. While the system looked like it was authenticating us, what was really happening was that forensics were taken from the endpoint we were working on, and an alert was triggered in the Illusive platform. Ultimately, the system prompted for credentials repeatedly, but because we're not really authenticating to the domain, we never left the page.

Figure 9. Incident Details



Source: Enterprise Strategy Group

The incident details shown in Figure 9 contain a wealth of details about the incident, including the machine the attempt was executed from, the last user to log in to that machine, the site that login was attempted against, and detailed analysis of the collected data including source, destination, the triggering process, and the deception that was triggered by it. In addition, we were able to see the screenshot collected, which showed the login attempt in progress.

Illusive in the Real World

Finally, ESG spoke with two large customers, a US-based financial services organization, and a multinational company in the energy sector. Both organizations are using Illusive on their production networks and ESG's goal was to understand how they are using the solution and what impact the solution has had on their businesses.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The financial services organization provides community banking services including personal, business, and online banking. Illusive covers approximately 12,000 endpoints and the CISO describes Illusive as "foundational to their cybersecurity strategy." The bank did their first proof of concept in 2017 initially to detect lateral movement and protect their Swift systems. "The first 90 days were illuminating," said their CISO. "Illusive's deception technology was game changing, filling visibility gaps we didn't know we had. It would have taken years to find and fill those on our own." Next, they used the platform to improve their cyber hygiene, integrate with their existing security systems, and build out their forensic capacity. The CISO reports that they have consistently achieved 95% confidence that Illusive will be tripped within three lateral movements of an attacker. This depends on the depth and breadth of coverage in an environment and they use this metric as a benchmark of their coverage. They found that with 10,000 endpoints and 65-70 deceptions configured on each, they can consistently get to 98% confidence. Also, Illusive allows them to delay deploying EDR for a couple of years, nor did they need to move from certain platforms to others. As the CISO put it: "It fills in-between gaps, making the entire stack more robust."

The energy company has a much larger network to cover, with about 120,000 endpoints deployed globally across nine regions, even though they are a fairly small company, with less than 500 employees and a "one-man show" approach to cybersecurity since their entire security operations center (SOC) is outsourced. They deployed Illusive to be more proactive and improve their security posture. Like the bank discussed earlier, the first thing they noticed was the deep visibility provided by the platform. Service and support are key criteria for this company when choosing any IT solution. The cybersecurity director we spoke with said, "Illusive made it easy to deploy, providing education to smooth the rollout and addressing issues quickly." In fact, during the pilot, Illusive detected two brute force attacks that were completely missed by their SOC and prevented a potentially serious incident. The director added, "I never recommend vendors, but Illusive is saving my job and my company. Illusive detected and stopped two attacks that no other technology could even detect."

Why This Matters

The global cybersecurity skills shortage is continuing unabated. According to ESG research, 44% of organizations said that they have a problematic shortage of cybersecurity skills, with nearly two-thirds (62%) indicating that they will increase their cybersecurity budget relative to last year.[4] CISOs clearly see the need to invest in solutions that make their existing staff more productive, effective, and efficient.

ESG validated that we could use the Illusive Platform to deploy deception sensors across the network with just a few mouse clicks—the effort was the same to deploy one or thousands of decoys. The automation and flexibility of the system made it quick and easy to configure deceptions to mimic the characteristics of existing hosts and users on the network.

The Illusive Platform utilizes existing network connectivity, requiring only minimal configuration of DNS services. This enables a centralized management process for flat and distributed networks, without the need for VLAN or tunnel configuration. ESG found that this speeds deployment, simplifies management, and minimizes the number of systems required to operate the software. Taken together, these capabilities reduce operational staffing and support requirements, freeing up valuable resources for more strategic activities. Illusive's extremely lightweight data-based deceptions minimize hardware requirements, reduce required maintenance, and eliminate the need for network upgrades.

[4] Source: ESG Research Report, *2020 Technology Spending Intentions Survey*, February 2020.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

It's clear that most organizations find acquiring cybersecurity staff, especially those with necessary cybersecurity skills, a challenging situation. Meanwhile, the number of security incidents that businesses must investigate and respond to has been steadily increasing, along with the sophistication and complexity of those attacks. Detection tools are generating more alerts, making identifying and remediating a modern cybersecurity incident a daunting task.

Traditional endpoint security architectures based on independent point products require analysts to log into multiple systems and manually cross-correlate alerts. Additional tools are often employed to combine, correlate, and analyze security tool data. These tactics slow the detection, investigation, and remediation process, leading to longer mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR). Organizations need a solution that can integrate with existing cybersecurity products and solutions to reduce the number of alerts and minimize the size and vulnerability of the attack surface, all while improving cyber hygiene.

The Illusive Platform was designed and engineered by people steeped in nation-state cyber intelligence and cyber defense. As former nation-state attackers themselves, they operate with a deep understanding of hacker behavior. Illusive invited ESG to examine and audit challenges from some of the world's most advanced and aggressive red teams, including those of Microsoft, Mandiant, Cisco, and the NSA. Red Teaming is a multi-layered attack simulation designed to measure how well a company's systems, networks, applications, people, and physical security controls can withstand an attack from a real-life adversary. When defending against read teams, it didn't matter how much control the red teams had over the network, nor did it matter whether they were aware that there were deceptions on the network, if they had inside knowledge of device vulnerabilities, or even if Illusive gave them hints. In each exercise, the red team was unable to compromise the network without being detected by the Illusive Platform.

Through hands-on testing, ESG has revealed that the Illusive Platform:

- Reduces the attack surface by identifying attack paths, removing excess connectivity, and providing analysts with actionable data to enable informed decision making.
- Cloaks the entire environment with agentless deceptive information that looks and feels authentic, then silently alerts analysts, collects detailed forensics, and provides high-fidelity incident notifications with a low rate of false positives.
- Requires minimal configuration, using existing network connectivity, which enables a centralized management process without the need for VLAN or tunnel configuration.
- Reduces operational staffing and support requirements, freeing up valuable resources for more strategic activities.

In addition, ESG found that Illusive is invisible to legitimate and non-malicious users. Legitimate end-users won't encounter deceptions while carrying out their day-to-day tasks. Internal users will only trip deceptions when performing malicious actions. The Illusive Attacker View in the solution's portal provides a map of an organization's network from the attacker's point of view, showing the layout of a network and how endpoints are connected. This provides visibility into the way an attacker would visualize a network upon breaching a perimeter and reveals attack vectors that lead to sensitive assets. This allows organizations to track attack locations and progress in real time, as well as shut down unnecessarily vulnerable attack paths with exposed connections and credentials.

Organizations seeking to enhance their security posture with highly realistic, efficient, easy-to-deploy deception technology should take a close look at Illusive's real-time, automated platform.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

www.esg-global.com

contact@esg-global.com

508.482.0188