LMNTRIX

BE THE HUNTER | NOT THE PREY

WHITE PAPER

DECEPTION TECHNOLOGY **GUIDE**

How Undetectable Deceptions Create a Hostile Environment for Attackers, Stops Lateral Movement, And Saves Your Critical Assets.

2021

LMNTRIX USA.
333 City Blvd West,
18th Floor, Suite 1805
Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE #05-19
EUNOS TECHPARK
+65 3159 0639

LMNTRIX Hong Kong.
14F, Manning House, 38-48
Queen's Road Central, Central
Hong Kong
+852.580.885.33

LMNTRIX Australia.
Level 32, 101 Miller Street,
North Sydney NSW 2060
+61.288.805.198

lmntrix.com

EXECUTIVE SUMMARY

The cybersecurity threats faced by businesses continue to grow in both number and persistence. The increase is not just down to attackers getting smarter. It is now easier for anyone to get access to sophisticated tools to launch attacks along with the instructions to use them.

Cybercrime-as-a-Service (CaaS) is now a reality. Organized business models link vulnerability researchers and malware developers with attackers over the dark web. For example, toolsets to launch attacks are available to buy or rent, along with lists of targets and stolen credentials to get the attack started. Ransomware-as-a-Service business models also exist where the developers share a percentage of the earnings from the attacks.

The reality is that the damage that security attacks cause businesses has reached a critical point. It is reported that data breach costs in 2021 rose from USD 3.86 million to USD 4.24 million, compared to the previous year. This figure is now the highest average total cost seen figures were first collated in 2004. Worryingly, the most common initial attack vector for these breaches was compromised access credentials.

This situation has prompted the President of the United States to issue an executive order on improving national cybersecurity. The key takeout is recognizing the need to enhance efforts in identifying, deterrence, protection against, detection, and response to threats. This capability enhancement includes post-incident investigation and analysis and better intelligence sharing.

The answer is to pivot from passive perimeter defenses to a proactive solution that can detect attacks within the perimeters early enough to prevent harm to the business. Deception-based solutions give security teams the ability to detect and contain attackers where damage is minimized. In addition, the team has the benefit of time and data to understand the attack and prevent reoccurrence.

The key benefit for security teams is that deception techniques allow the automation of threat detection with minimal false-positive alerts. As a result, lean security teams can focus on response and recovery actions, knowing that detection is assured and all alerts are actionable.

The key benefit for management is accurate attack metrics that can inform security resourcing to maximize investment returns from security controls and the teams that monitor them.

Deception technology can be complex to develop, configure and deploy. However, it must be done correctly if it has to be effective. As deception solution providers, LMNTRIX XDR delivers these benefits to businesses while managing the in-depth technical know-how to provide you with effective and proportionate deception services that maximize protection for your business-critical systems and valuable assets.

CONTENTS

AN OVERVIEW OF **CYBER DECEPTION**

INTRODUCTION

Organizations are facing ever-increasing threats from determined and capable attackers. Not only are the number of attacks increasing year on year, but they are also becoming more sophisticated, persistent, and resourceful. The number of reported breaches occurring each year shows the scale of the problem.

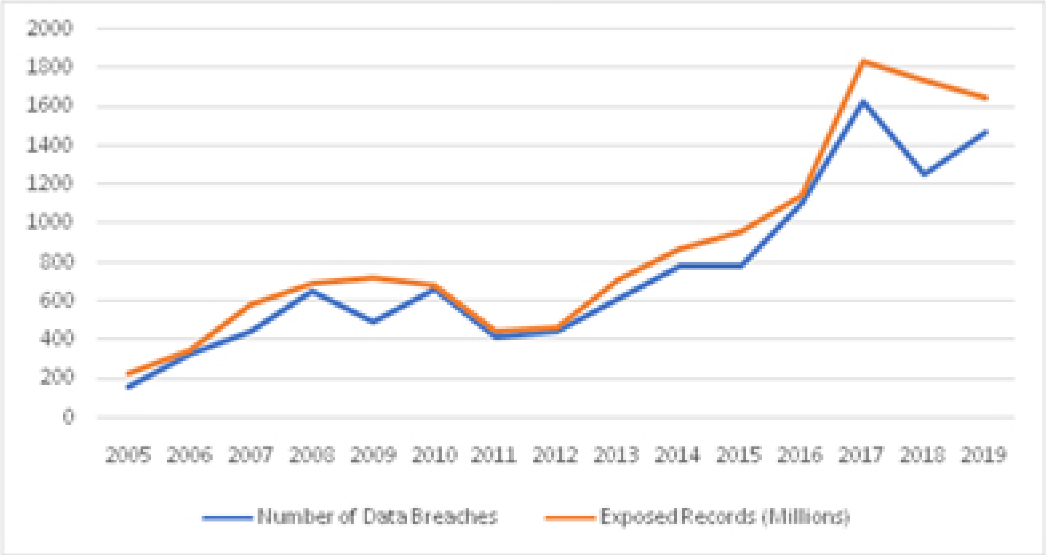


Figure 1 - Annual Number of Data Breaches in the US

It is now recognized in the United States that organizations face persistent and increasingly sophisticated malicious cyber campaigns. The threat level has prompted the President of the United States to issue an executive order on improving national cybersecurity. This order sets out a number of requirements, including the following critical needs that apply across all organizations:

The need to improve efforts in the identification, deterrence, protection against, detection, and response to threats, including post-incident investigation and analysis

- The need to facilitate better sharing of threat intelligence across all stakeholders
- The need to modernize cybersecurity with significant changes, including adopting the zero-trust philosophy
- The need to enhance supply chain security to counter weak links in interconnected systems
- The need to maximize the early detection of cybersecurity vulnerabilities and incidents
- The need to improve investigation and remediation capabilities through better information logging

One problem for the majority of organizations is that information systems remain relatively static. This stability allows potential attackers the benefit of time for inspecting the systems, passively monitoring for vulnerabilities, and actively probing for weaknesses in the defenses. It is an inherent problem with vulnerabilities regularly found in software applications and hardware endpoints. Where manufacturers identify vulnerabilities, security researchers, or other responsible parties, security patches are created and distributed before exploitation of the vulnerabilities is possible. This creates a window of opportunity for attackers for the period between the vulnerabilities being identified and patches applied. It creates risks for systems that are left unpatched or where patches are not yet available due to vulnerabilities identified by maliciously intended parties acting in bad faith of which manufacturers are unaware.

Another problem is the weakest link in information systems, the end-user. The greater adoption of cloud-based infrastructure combined with a recent and significant shift to working from home has dramatically increased the frequency and volume of information flow outside organizations' boundaries. As a result, while Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) all deliver significant operating benefits to businesses, they increase the threats to which the organization is exposed. These factors make protecting sensitive information more difficult to achieve, requiring fast and effective detection and response capability to keep systems secure.

To defend themselves from such attacks, organizations need to invest in comprehensive adaptive and intelligent defenses to resist attacks or halt attacks in their tracks and learn and adapt to withstand any subsequent attacks better. Defenses need to follow the principle of following a continuous cycle of detect, respond, and recover.

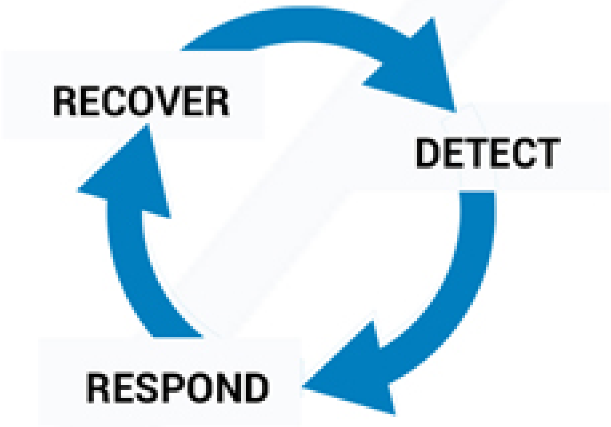


Figure 2 - Detect, Respond and Recover

Detecting attacks as early as possible in the kill chain will prevent system damage, compromise the availability and integrity of information, and exfiltration of sensitive information, compromising confidentiality. Therefore, efforts have focused on reducing this dwell time, the period between attackers gaining access to systems, and their detected presence.

Back in 2011, the global median dwell time for attackers was a staggering 416 days. Recent statistics show that technological advances in detection capabilities have reduced this down to just 24 days. However, that's still a significant period for undetected compromise of systems. For businesses with the capability to detect an attack, this global median dwell time is now 12 days. By comparison, dwell times for companies that have adopted deception-based solutions are on average five days. For those businesses that discover their systems are compromised when informed by external parties, this median dwell time is still a significant 73 days.

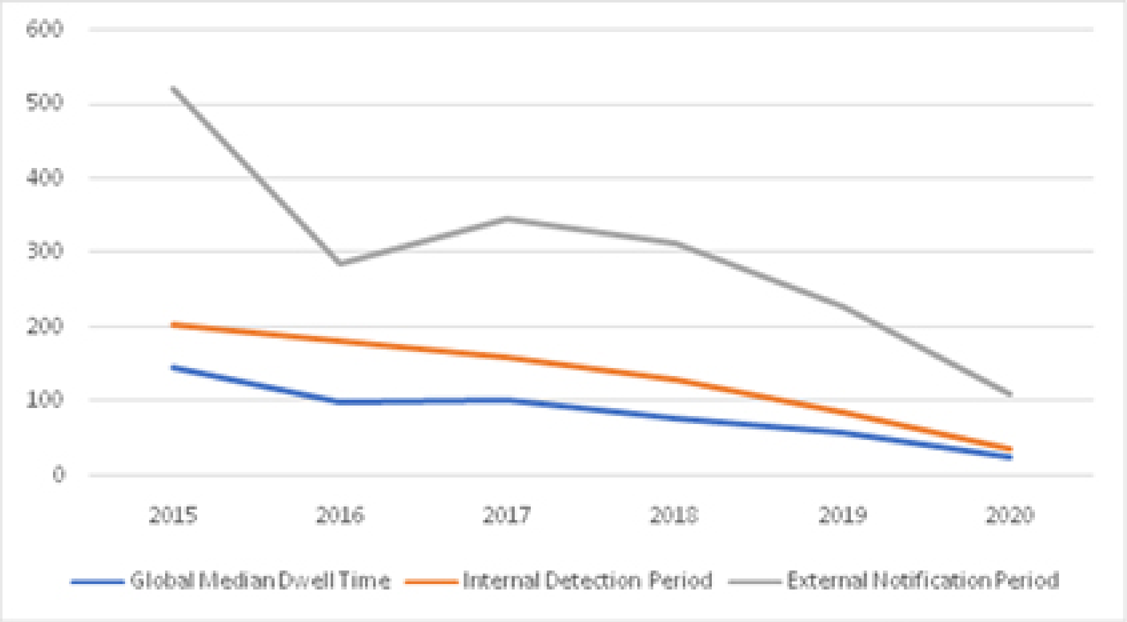


Figure 3 - Global Median Dwell Times (Days)

A key component in an integrated defense solution that provides early detection of attacks is deception. As this technology becomes more widely adopted, median dwell times are predicted to fall further.

WHAT IS CYBER DECEPTION

Cyber deception comprises a range of techniques employed to conceal networks or devices from attackers or create uncertainty and confusion by presenting attackers with an illusionary system that draws their attention away from the real systems.

The goal is to prevent the attacker from gaining a situational awareness of the real systems, preventing them from gaining sufficient understanding to launch an effective attack. In addition, using misinformation and misdirection techniques aims to alter the attacker's perception of reality so they cannot gain a foothold within the real system.

At the same time, the deception-based defenses should alert a security team to the attacker's presence and provide essential time for the team to analyze, identify, and mitigate the attack vectors that the attacker is looking to execute. This not only provides a means to halt the attack in its tracks but also provides a valuable insight into any potential unrecognized vulnerabilities. In addition, this can allow the security team to rectify systems to mitigate weaknesses before they are exploited.

Often attackers scan multiple potential targets looking for exploitable weaknesses, and they can be inherently lazy, going after the lowest hanging fruit. Deceptive measures that make systems look too difficult or time-consuming for an attacker can be sufficient to prevent an attack if there is an easier target to attack instead.

Fundamentally, a deception-based system aims to direct authorized users to the real system and malicious users to the deceptive system from the same common interface.

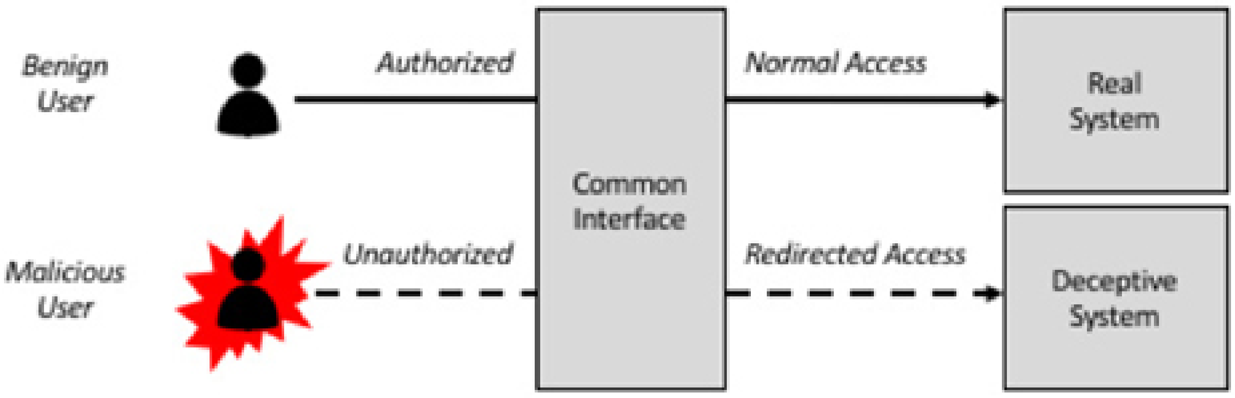


Figure 4 - Simplified Deception Strategy

An example of deception is to configure a password-protected function such that after a set number of failed attempts, the function prevents that user from accessing the function. However, rather than simply sending an error or blocking further attempts, the function continues to prompt for a password exactly as normal but ignores the data provided. As a result, the user is unaware that their access is blocked and will continue to attempt access. A legitimate user would be aware of this feature, but an attacker would be deceived into wasting effort and providing an insight into their password guessing tactics.

HISTORY OF CYBER DECEPTION

Deception is a fundamental human trait, employed since the dawn of time when people were hunter-gatherers, using physical camouflage techniques and hidden traps to gain an advantage over prey and predators. In the world of cyber security, the first reported use of cyber deception was in 1991. Bill Cheswick recorded that Bell Labs successfully deployed a honeypot that ensnared a real hacker. This was a manual process, with a member of the security team interacting with the hacker in real-time, manually feeding misinformation.

The basic purpose of a honeypot is to study attacks, analyze attackers' behavior, and gather intelligence.

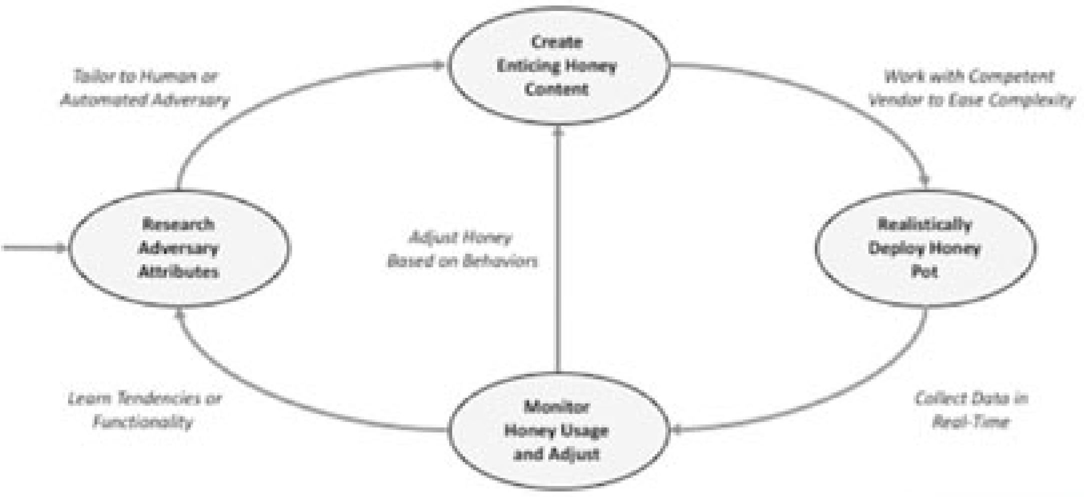

Create Enticing Honey Content
Tailor to Human or Automated Adversary
Work with Competent Vendor to Ease Complexity
Research Adversary Attributes
Adjust Honey Based on Behaviors
Realistically Deploy Honey Pot
Learn Tendencies or Functionality
Collect Data in Real-Time
Monitor Honey Usage and Adjust

Figure 5 - Simplified Honeypot Lifecycle

The original honeypots were heavily tailored for a specific type of attacker.

- Research metrics about the known, expected behavior of an adversary of interest and his motivations were used to construct content to structure an enticing honeypot. Typical content for a honeypot is data of value such as user credentials, documents, databases, and decoy endpoint devices.

- The deployed honeypot was hosted in a realistic environment that hid its intent while ensuring that an attacker could not move out of the honeypot environment into a real environment.

- Close monitoring of the honeypot was then undertaken once the bait was taken and an attacker's presence was detected. Thus, the honeypot's effectiveness is constrained by the efficacy of both the alerting mechanisms and the monitoring capabilities.

- Monitoring attacker behavior is used to adjust the honeypot content and functions to prolong the attack while maintaining the deception that the attacker was in a real environment.

- Monitoring attacker behavior also generated intelligence on the attacker's abilities, knowledge, tools, behavior, and motivations. This information could be shared with the wider security community and feed into the research for the next honeypot.

THE ROLE OF DECEPTION

Traditional security solutions focus on perimeter controls to prevent attackers from gaining access to networks and devices. Hardening techniques coupled with detection and blocking of suspicious actions are employed to create impenetrable layered barriers. What these solutions lack is the ability to manage sophisticated and well-resourced attackers who penetrate the perimeter. In addition, advanced detection controls such as next-generation firewalls and Intrusion Detection Systems (IDS) tend to also focus on the perimeter. In contrast, more recent detective solutions such as Sandboxes and Endpoint Detection & Response (EDR) are easily bypassed. Once inside a network, it is relatively straightforward for a sophisticated attacker to avoid detection by such systems, as evidenced by our Red Team and many others.

The key weakness of traditional controls is they focus on detecting malicious activity or unusual behavior. As a result, attack techniques that mimic authorized actions will not be recognized when employed to steal credentials or gather sensitive information. Artificial intelligence and user behavior analytics are being brought into play to address these issues but refine the ability to detect unusual traffic patterns, unauthorized data access, movements, or suspicious or malicious activity on a network or an endpoint.

Deception-based solutions are available to resolve these issues and close the gap in the detect and respond capabilities by detecting in-network threats. They also cover the significant risks to businesses from insider threats. Such attacks from inside the perimeter were inherently difficult to manage using perimeter centric security solutions.

Deception solutions integrate with existing security controls, enhancing their effectiveness and providing capabilities that traditional controls often lack. Their key advantage is that they will integrate seamlessly with other controls with minimal effort. Crucially, deception-based controls do not affect the performance of the real business systems that they protect, unlike some other security solutions.

DECEPTION TERMINOLOGY

A honeypot is a simple decoy, a computer that is part of the real system, configured to give the appearance of an attractive target for attack, normally by impersonating a known targeted device.

A honeynet is a simulation of multiple computers or systems as an extension of the honeypot concept. The honeynet will include simulated cyber defenses with phony vulnerabilities that are different from the device's actual defenses that are hosting the honeynet.

A honeytoken is falsified information held on a real system designed to either attract an attacker's attention away from more valuable information or provide the attacker with misleading information for them to act upon. In addition, the access or exfiltration of honeytokens can be used to raise the alarm that an attack is in progress as real systems will never access such information.

Breadcrumbs are items of misinformation placed on a system for an attacker to find. The information is intended to lead the attacker onto a decoy system, away from the real system. The information must appear credible and persuasive to be effective.

Network decoys simulate network and data center systems and servers, domain controllers, and data storage facilities, both on-premises and cloud-based.

Device decoys simulate endpoint devices and specialist devices such as components of industrial control systems, retail systems, elements of the Internet of Things (IoT), and other operational technology.

Application decoys represent simulations of applications and services deployed across networks. These can include operating systems, file servers, web servers, routers, switches, file shares, and business applications.

Data decoys are simulations of records deployed across networks. These can include databases, files, documents, registry entries, or any other type of information stored or in transit across networks.

Tags are unique identifiers embedded in live information that is inaccessible under normal circumstances. Access to the tagged information provides an alert trigger for detect and response processes. The benefit of Tags is that they can be deployed in cloud-based assets and information shares.

Personas are individual fake user accounts and profiles deployed across systems and publicly accessible resources to lure attackers who seek to contact and exploit users, typically utilizing social engineering techniques to compromise access credentials.

COMPONENTS OF AN ENTERPRISE **DECEPTION SOLUTION**

NETWORK DECOYS

Network decoys are configured to appear identical to real network assets and are deployed throughout the network. They are designed to detect attackers during reconnaissance and lateral movement phases of an attack. The underlying strategy is to hide in plain sight by creating a camouflaged environment where the attacker is tricked into believing that the fake system is real. For maximum detection capabilities over the widest attack surface, deception decoys should mimic and seamlessly blend in with the real network assets.

The believability of the decoys is critical. Any indication that the attacker is accessing a decoy asset will render this security control nugatory. The decoys should use the same operating systems, applications, and services as real assets to maximize the authenticity of the deception measures so sophisticated attackers cannot discern which assets are decoys and which are real. Decoy behavior should match the operating characteristics of the real devices to be credible. The highest authenticity level can be achieved by using the same "golden image" template in use for the real system on the decoys.

Network decoys operate using the same principles as a sandbox. They're an isolated network environment that mimics the business operating environment using emulation or virtualization techniques. Sandboxes are widely used to execute suspicious code without any risk to the business network. What happens in the sandbox stays in the sandbox. Network decoys offer the same protection for attackers executing a command while hiding the fact that the attacker is inside a protected environment. The key to success in preventing the attacker from detecting they are inside the decoy while ensuring there are no weaknesses that would allow the attacker to transit out of the decoy and pivot across to the live system.

DEVICE DECOYS

In addition to endpoint decoys, decoy services and data are deployed on devices to trap any attack that's compromised real assets. Deploying genuine-looking and attractive deceptive credentials and lures on existing systems and servers will aid in detecting an in-progress attack. Decoys deployed on devices will provide a capability to monitor live services and redirect attempted access back to the deception environment. Exposed credential mapping will provide visibility of lateral attack movement paths.

Comprehensive endpoint deceptions can cover a wide variety of application and memory credential lures, browser credentials and histories, and Identity and Access Management (IAM) access accounts, access keys and tokens, as well as Domain Name Service (DNS) entries for cloud environments. Creating an effective decoy will require active management of decoy credentials to maintain timestamping currency and coherence with active directory configuration. Active directory decoys can also be employed to hide high-value objects such as administrator or service accounts with privileged access credentials, presenting decoy credentials in their place without affecting the live environment.

Device decoys should be implemented using agentless deployment models to maximize effectiveness. While primarily the benefits are reduced management and processing overheads, this offers security benefits. Where a deployed endpoint agent extracts deception and monitoring capabilities from the deception-based solution, the agent's presence can be detected by attackers. Agents are also vulnerable to reverse engineering techniques employed by attackers. Gaining a detailed understanding of the functionality and its implementation helps identify weaknesses that enable circumvention or disablement.

Endpoint scan deflection techniques and the obfuscation of Active Directory information can also be employed to deflect attacker activities across to decoys for engagement. These techniques can reduce the risk of lateral movement and identify misconfiguration issues.

SERVICE DECOYS

Application decoys allow an organization to deploy internal decoy applications, such as SWIFT terminals, web applications with supporting backend processes and database functionality, or network directory services. Application decoys provide additional targets of interest for an attacker to interact within the deception environment. These decoy services can provide detailed information as to the intentions and capabilities of attackers as well as aid in the identification of the misuse of valid credentials by an attacker. This capability is valuable for detecting internal threat actors.

DATA DECOYS

Decoy data in the form of false databases or data stored on network or endpoint devices act similarly to decoy services in providing an attractive target. Decoy data should emulate valuable information assets such as commercially sensitive data, intellectual property, Personally Identifiable Information (PII), system configuration data, security control configurations, or privileged access credentials. Data decoys can also include decoy file servers and services, Server Message Block (SMB) shared drives, and network shared folders. The key to success is creating engaging, credible content that stands the scrutiny of a technically savvy and potentially suspicious attacker.

Access to decoy data can be used as the trigger for security response and redirect access to the deception environment. This redirection is valuable for countering ransomware attacks or another network and led malware.

BREADCRUMBS

Credential-Based Breadcrumbs

A key part of any attack is searching for access credentials for high-value systems and services or privileged accounts. Creating false user credentials and permissions as part of an Active Directory creates a tempting target for the attacker. False credential breadcrumbs can be placed in registry keys for decoy services. When the attacker accesses a decoy based on these false credentials, a validated alert is automatically triggered. Creating personas linked to false user credentials enhances authenticity and encourages attacker interaction to maximize engagement.

File and Data Breadcrumbs

File-based breadcrumbs or tags are the simplest to create, and false information can be placed in documents, emails, database entries, and recent file lists that direct the attacker to decoy systems. The misinformation can also include usernames and passwords. Also, false network topography and configuration information, such as Internet Protocol (IP) addresses and decoy firewall configurations, can be used to confuse and deceive an attacker. This is to make the false information as convincing as possible, down to document formats and versioning that provides the illusion of an official maintained document. False emails are particularly valuable as breadcrumbs as it's common for users to share sensitive information using internal email systems.

Network Breadcrumbs

A decoy network that communicates with real system assets such as the DNS server will create an enticing target if its appearance and behavior match the real assets. The network breadcrumb is intended to lure the attacker into conducting a man-in-the-middle) attack on the decoy network. This attack can then be used to feed misinformation directly to the attacker and trigger validated alerts. The Address Resolution Protocol (ARP) cache of IP and Media Access Control (MAC) addresses makes an attractive target for attackers and an ideal location to place network breadcrumbs.

Application Breadcrumbs

Application data in the form of session credentials, access histories, and stored passwords are another tempting target for attackers. Adding carefully crafted false information that appears valid can misdirect attackers onto decoy systems where their presence can be detected and alerts raised. Secure Shell (SSH) and Remote Desktop Protocol (RDP) credentials are of particular value for an attacker and ideal for use as an application Breadcrumb.

DECEPTION STORIES

A deception story combines breadcrumbs and decoys, including tags and personas, deployed as a cohesive deception environment that stands up to scrutiny by an attacker. The deception story needs to closely match the normal business systems and processes, both convincing and compelling. The individual elements must seamlessly fit together with no tell-tale indications that the business is using deceptions everywhere.

The fundamental principle of a credible deception story is its ability to direct attackers along a set path to the decoy environment where they can be contained. The breadcrumbs should draw attention away from real assets while supporting security controls monitor the attackers should they choose real assets over the decoys. Scenarios of possible attacker behavior will feed into the deception story to maximize the likelihood that one of the breadcrumbs will be taken.

Believability is key. The instant that an attacker suspects that deception-based controls may be deployed, their behavior will change. They will become more cautious, increase scrutiny of artifacts, and actively look for decoys. A good deception story will take this situation into account to ensure the robustness of the deception-based solution.

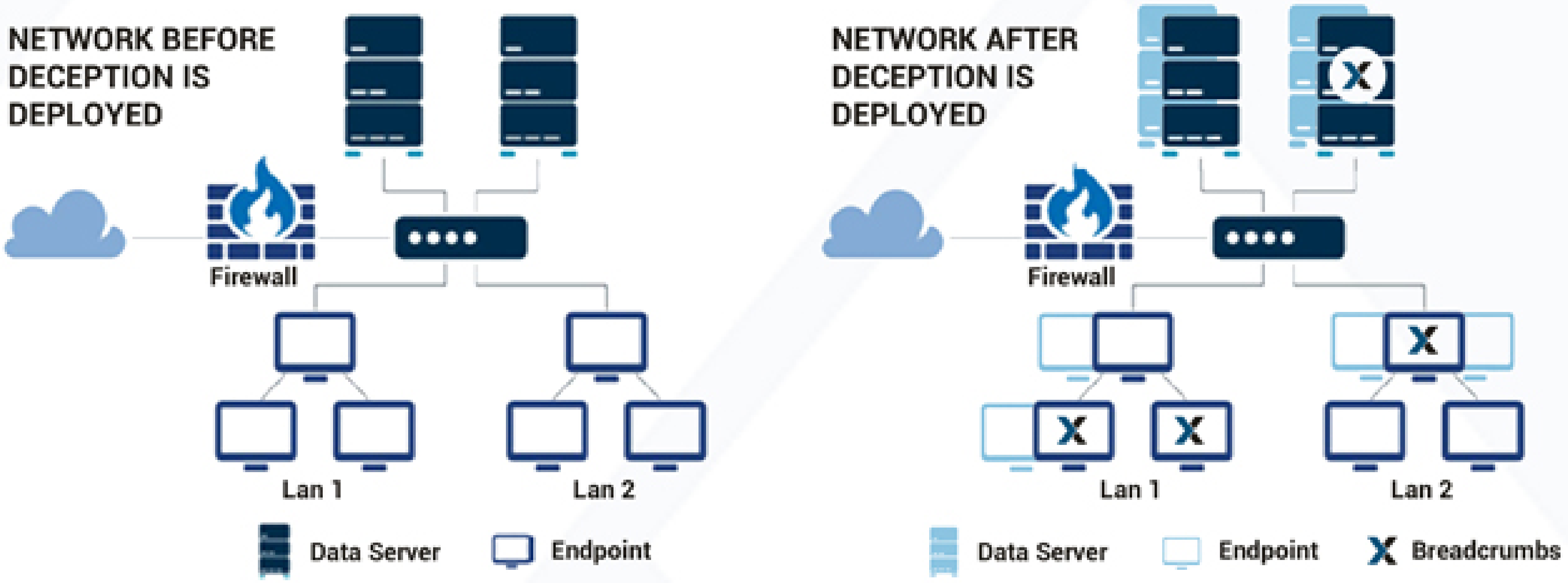


Figure 6 - Deployment of Decoys and Breadcrumbs

IMPLEMENTING **DECEPTION**

THE ART OF EFFECTIVE DECEPTION

Organizations must be aware of the legal implications of implementing deception-based solutions. Solutions that entice non-malicious third-parties into decoy systems not only breach laws in some countries, monitoring and responding to their actions is a waste of the security team's resources. In addition, decoys need to be deployed within boundaries that only a deliberate attack would breach, ensuring that anyone interacting with a decoy is a legitimate threat and fair game to be played by the security team. These factors are why it is crucial to look for a competent and respected security solutions provider to source and deploy deception-based solutions.

The benefits of deception-based solutions are:

- Early detection of attacks
- Minimum false positive alerts
- Automated alerting
- Minimal resources outside investigation and response
- Flexible, adaptable, and scalable
- Effective for previously unknown attack vectors
- Equally effective for internal and external attacks
- Real-time monitoring of attacker's actions
- Identification of previously unknown vulnerabilities
- Comprehensive information for the response team
- Intelligence gathering for lessons learned and community sharing

DECEPTION CHARACTERISTICS

Originally decoys were bolted onto production systems, a separate system in their own right. This approach evolved to the manual integration of decoys within these real systems. Machine learning techniques and heuristic processing enable automated deployment across real systems and are integral to information processing. This close coupling between the real systems and the decoys makes distinguishing the two a complex undertaking for an attacker.

Decoys need to be effective against both manual and automated attacks. These can be markedly different in behavior and actions. The former can be driven by curiosity, take pseudo-random actions that take attacks in an unexpected or illogical direction. The latter tend to be more formulaic, following defined actions towards predetermined goals.

The sophistication and deployment of decoys can vary considerably depending on the environment they are used in and their purpose. Therefore, a common classification method between decoy types is based on the interactivity available to the attacker.

- A low-interaction decoy will provide the attacker with limited resources to interact with in terms of accessible services and data. The purpose is to detect the presence of an attacker rather than engaging and gathering intelligence. The advantage of a low-interaction decoy is that it is simple to create and deploy, requiring limited resources to maintain and monitor. The disadvantage is that it will not trick an attacker into persisting with the attack and will be unlikely to detect the presence of a sophisticated attacker.

- A high-interaction decoy simulates a real and representative environment to the extent that a sophisti cated attacker will be fooled into interacting with the decoy. The decoy will often be implemented as a real system to provide a credible environment for the attack. The advantage of a high-interaction decoy is that it creates an environment where attackers can be monitored closely throughout a sustained persistent attack, providing valuable intelligence. The disadvantage is that this type requires significant resources to create, deploy and maintain.

- A medium-interaction decoy strikes a pragmatic balance between low and high. This type of decoy is easy enough to operate while providing enough intelligence to be of value. A medium-interaction decoy is unlikely to be effective against the most capable attackers with access to zero-day exploits. Still, it will suffice for the usual threats that an organization will regularly face.

The key decision for any business is the overall goal of the deception-based solution they are looking to implement. Such systems incur costs in terms of initial investment into the technology and the resources required to monitor and maintain the solution. These costs will be weighed against the potential harm should a persistent attack go undetected. For some businesses, one successful attack is all it would take to cause irreparable damage to reputation or incur overwhelming financial penalties due to a data breach.

Compared with traditional security controls based around perimeter defenses, deception solutions offer significant benefits in terms of improved effectiveness and lower costs. Significantly, the deployment of the deception solution can be tailored to the value of systems, such that systems with high-value assets or business-critical services can be more highly protected than other systems with no or limited value to the business. Furthermore, this tailoring can be dynamic, responding to operating processes or business practices changes. Conversely, traditional security solutions tend to be more static in implementation with lower flexibility and scalability.

There is a class of decoys that are created for specific purposes. For example, typically, security researchers investigating particular threat technology will create decoys designed specifically to attract the threat of interest. This approach enables in-depth research of the threat in a real-world environment to further their studies.

HIDING TECHNIQUES

Deception-based solutions are not just focused on creating enticing decoys that attract the attention of attackers. To be effective, they also need to hide the presence of the real systems so that the attacker is not presented with a choice of which environment to attack, alerting them that one is a decoy.

Deceptive hiding techniques are necessary to prevent an attacker from gaining access to information that reveals the network topology of the real system, its technologies, and assets. One mechanism is to prevent the use of scanning as part of an attacker's reconnaissance to gain network information. Intercepting communications to unused network addresses and simulating endpoints for those addresses will provide misleading topology information. An intelligent attacker will identify this information as invalid, but the additional effort required to identify real connections increases the likelihood that their scanning will be detected. Also, assigning fake names to unused network addresses can help obscure real devices names in a reverse DNS lookup. Another example of defensive tactics is the configuration of a firewall to send falsified host unreachable responses to disallowed packets which hides the presence of the firewall and its connected devices.

Attackers have three key methods of identifying the presence of a particular target on a system. First, they can directly observe its presence using techniques such as port scanning. Second, they can also deduce its presence based on responses to actions or learn of its presence from information available from alternate sources. A comprehensive hiding strategy needs to cover all these options to stand scrutiny by a capable attacker. Some examples of hiding techniques are:

CHANGE EXPECTED LOCATIONS	Locate files containing critical information such as credential details in obscure locations that an attacker may not discover Hide devices behind a Network Address Translation (NAT) device
CHANGE APPEARANCES	Use cryptography to hide information Disguise critical information using steganography techniques and embed it within other data Change filenames of files containing critical information to defeat automated searches Configure ports to disguise servers as workstations Configure high-value devices identically to low-value devices
CHANGE THE ENVIRONMENT	Create false records in the expected locations of critical information Publish false or incomplete network diagrams Hide network data using switches in place of hubs
CHANGE DATA FLOWS	Generate false, misleading information Configure firewalls to allow only predefined data flows Configure routers to defeat ping scans
ACTIVE DEFENSES	Generate large volumes of data in response to requests to overwhelm the attacker Actively attack the source of port scans using denial of service techniques

Figure 7 - Hiding Techniques

ACTIVE DEFENCE STRATEGY

An active defense strategy requires taking direct defensive actions to halt, nullify, or reduce the effectiveness of cyberattacks against an organization's systems. In addition, this defensive strategy aims to increase the resources required in terms of time and effort to attack a system successfully.

Using deception-based defenses increases the time spent by an attacker on false targets whose compromise will not impact business operations. At the same time, the defensive security team can analyze the attacker's actions and gather valuable intelligence that not only can improve their defensive readiness but can be shared with other potential targets.

Introducing deception into security defenses adds uncertainty to the kill chain. Even once an attacker becomes aware of the presence of decoys, the strategy still has value. An attacker will need to take additional measures to determine if they are interacting with a decoy or real device or system. They will also be conscious that the information they have gathered to date may be deliberately misleading, and their actions may be under scrutiny. This places significant psychological pressure to end the attack to prevent disclosing attack vectors, previously unknown vulnerabilities, and exploit techniques.

While the publicized deployment of deception can be a strong deterrent and valuable in discouraging attacks, the investment in deployment may be seen by some attackers as an incentive. Successfully attacking deception-based controls may be seen by some as a challenge and an indication that the organization has assets of value that require such protection.

DECEPTION BENEFITS

OVERVIEW

Deception is extremely effective for providing detection of attacks at all stages of the kill chain. It is particularly valuable at providing detection at the earliest stages of an attack before any damage or compromise has yet occurred.

Traditional security controls protect boundaries from unauthorized access using technologies such as firewalls, malware scanning, and intrusion prevention systems. Alternatively, they detect attempts to exfiltrate data using data loss prevention techniques.

However, these controls have limited value countering an attacker's presence within a system undertaking a continuous cycle of internal surveillance, privilege escalation, and lateral movement.

Deception techniques provide internal visibility of any actions taken by an attacker within a system, providing valuable intelligence on their behavior and intentions as well as hampering their efforts with misdirection and misinformation.

A critical advantage of deception-based defenses is that they can provide organizations with an edge over attackers. They can actively feed their adversaries misleading information that affects the observe and orient phases of the OODA loop.

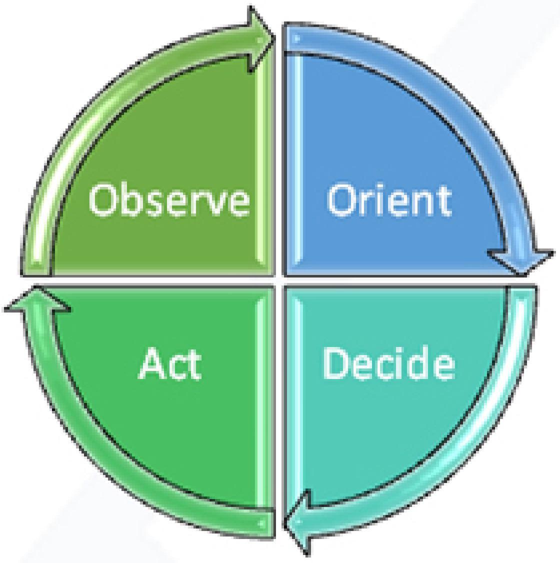


Figure 8 - The OODA Loop

Advantages come from creating the means to cycle through the OODA loop faster than the attacker by actively slowing them down. Deception creates uncertainty, misdirection, and misinformation. This gives the attacker less time for decide and act stages, thereby providing the security team with observable insights into the attacker's actions and reactions.

COUNTERING THE ATTACK CYCLE

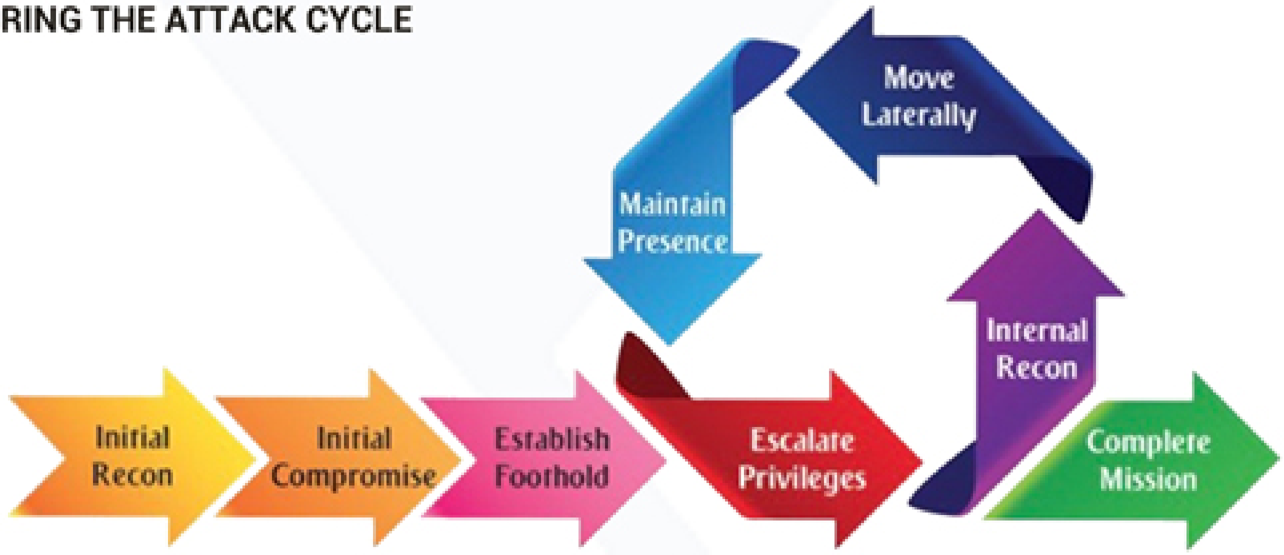


Figure 9 - The Attack Lifecycle

Attack Phase	Attacker Actions	Deception Capabilities
Establish Foothold	Install malware, establish outbound communications and remote access	Decoys alert on attempts to compromise systems or communicate with command and control servers. Misinformation moves the attacker to a decoy environment.
Escalate Privileges	Credential theft, man-in-the-middle attacks	Decoy credentials move the attacker to a decoy environment for alerting. MitM detection identifies credential theft and vulnerable credentials for lateral movement
Internal Reconnaissance	Critical systems, services, and information identification and intelligence gathering	Decoy applications, services, and data trigger alerts and move the attacker to a decoy network.
Move Laterally	Use of stolen credentials, mapped shares, and other techniques.	Decoy network trigger alerts and move attacker to decoy network.
Maintain Presence	Creation of backdoors, subversion of services, installation of malware, alternate ingress paths, and remote access	Decoys alert any attempts to compromise systems or communicate with command and control servers. Misinformation moves the attacker to a decoy environment.

Figure 10 - Deception to Counter the Attack Cycle

HALTING THE KILL CHAIN

The cyber kill chain is a sequential representation of the attack cycle derived from military concepts for phase-based actions. It's built around representing a cyber-attack against traditional perimeter-centric security controls, but here we can show how deception-based solutions can address all stages. This ability emphasizes the value of deception technology. Traditional security controls are ineffective at countering the reconnaissance and weaponizing stages that occur outside the system's boundaries.

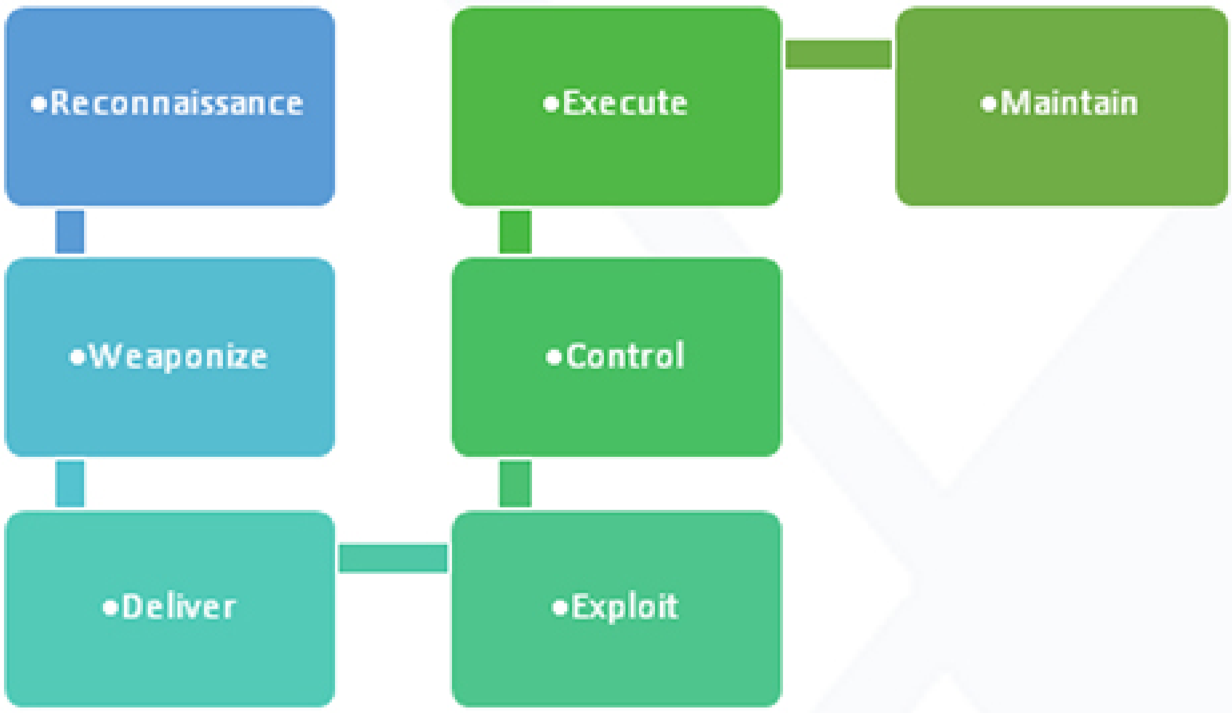


Figure 11 - The Kill Chain

Reconnaissance

Attackers select their target, collect information from publicly available sources, and examine accessible interfaces, such as networks, devices, applications, or services. The goal is the identification of exploitable vulnerabilities.

Deception-based solutions enable the early detection and monitoring of attackers during the reconnaissance phase. Alerting can trigger response, while breadcrumbs can direct attackers into a decoy environment.

Weaponize

Attackers develop means to exploit the vulnerabilities found during the reconnaissance step. The goal is to develop the means to gain access to the target's systems.

Deception-based solutions provide intelligence sharing on attack methods and system vulnerabilities that can pre-empt any attack.

Deliver

Attackers deploy the means to compromise the target's systems to gain undetected access.

Deception-based solutions misdirect attackers with misinformation and misleading situational awareness to halt or hinder attacks. As a result, an attacker contained within a decoy environment can be allowed to launch attacks while their behavior is closely monitored.

Exploit

Attackers loiter within a compromised system, looking for opportunities to move laterally and escalate privileges by exploiting vulnerabilities and weaknesses. The goal is to upload, install and execute malicious code to implement the attack goals.

Deception-based solutions enable the detection of exploit attempts with automated alerting and redirection over to a decoy environment where the effects of the exploit are contained.

Control

Attackers look to use command and control servers for the remote manipulation of the target's systems. The goal is to provide the means to exfiltrate information of interest.

Deception-based solutions allow the management of control actions within a decoy environment where decoy assets can be used to study the attacker's activities and deduce their goals. Decoys can also monitor communications and exfiltration attempts, potentially identifying the attacker.

Execute

Attackers initiate their end-attack, be that system disruption, data exfiltration, malware deployment, ransomware execution. This is the end goal of the attack.

Deception-based solutions allow the containment of the attacker within a decoy environment where the actions, tools, and techniques employed during the execute phase can be studied. Detailed intelligence can be gathered to inform the security solution and shared with the security community.

Maintain

Attacks look to maintain a presence on the compromised system. This provides the opportunity to initiate further attacks at a future date or use the compromised systems as a launchpad to attack other interconnected targets.

Deception-based solutions can simulate the characteristics of real-world systems to maintain the illusion that the attacker is within a live system. Additionally, temporal modification of decoy content can convince the attacker to maintain a presence in the decoy environment for intelligence gathering purposes.

INTEGRATION WITH SECURITY STACK

Deception should be used to supplement existing security controls, complementing the protection they provide. In the long term, the metrics of control effectiveness that deception-based solutions offer can be used to remove or replace ineffective or inefficient controls as necessary.

Deception should be viewed as a solution that delivers early threat detection and reliable alerting of in-network threats. Added benefits are shutting down unprotected attack vectors and unknown weaknesses in existing controls combined with comprehensive monitoring and forensic recording capabilities. These features deliver robust network-wide protection and improve the response and recovery abilities of the security team.

The deception solution should cover the entire environment to provide complete detection capabilities across a system. For example, endpoint solutions can detect credential-based attacks but not detect lateral movement or compromise to cloud-based resources. Similarly, network solutions will not detect ransomware or credential-based attacks.

An effective deception-based solution should include a mix of network, device, applications, and data deception techniques. These should be deployed around sensitive and critical areas of the environment such that they offer early detection and response capability irrespective of the attack vector and ingress point.

DEPLOYMENT STRATEGY

DEPLOYMENT LIFECYCLE

Successfully deploying deception technology requires formulating strategic goals and tactical aims if it is to be effective. Then, the deployment can be planned, implemented, and maintained by understanding what the deception-based solution is required to achieve

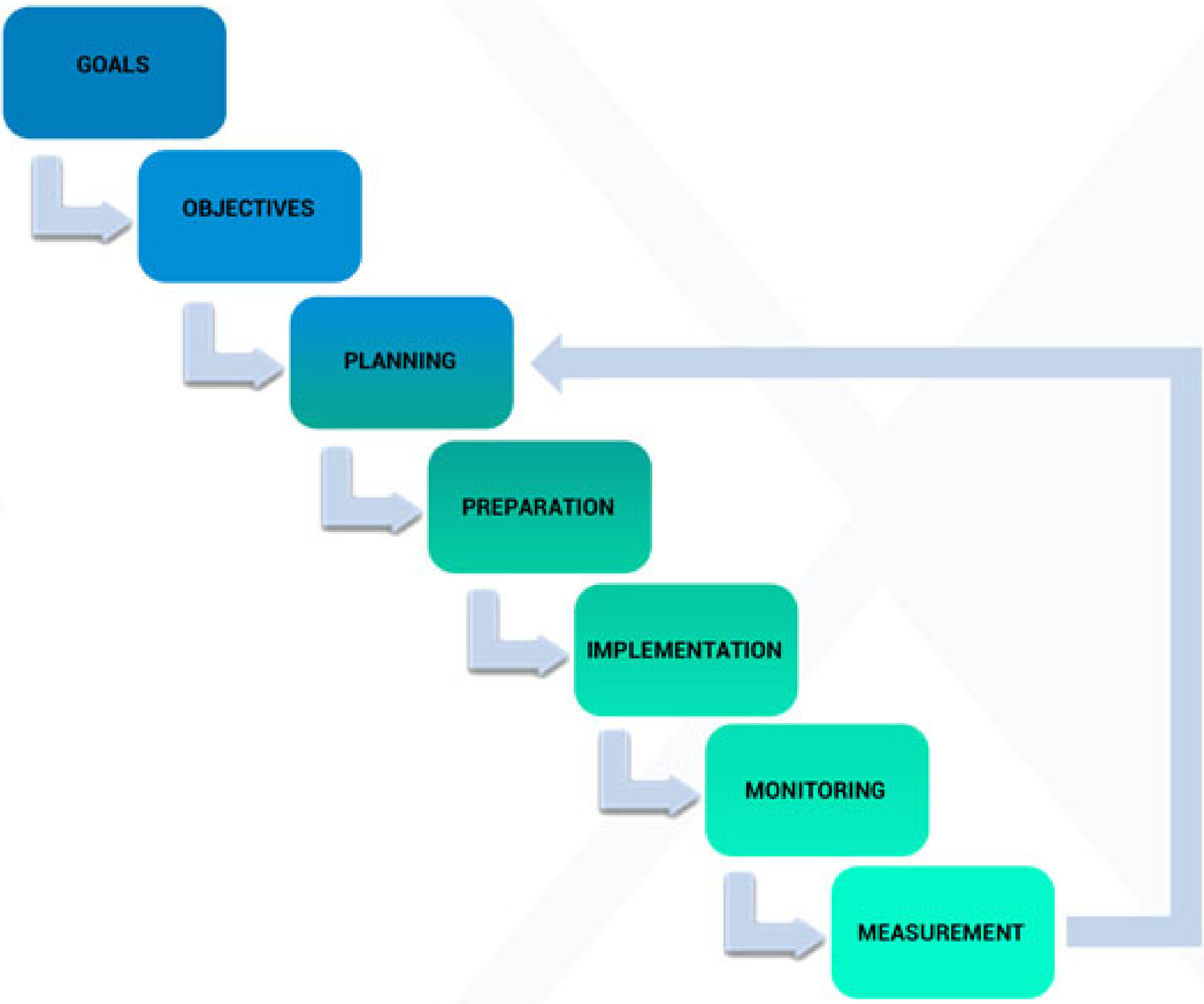


Figure 12 - Deception Deployment Strategy

Goals

The questions that need answering are:

- What are my valuable assets?
- Why would my systems be attacked?
- Who will typically attack my systems?
- What will their likely intentions be?
- What publicly available information can they leverage?
- How robust are my current security defenses?
- What are my known security weaknesses?
- The answers to these questions will aid the definition of the aims and goals of the deception-based solution, defining its purpose and priorities.

Objectives

Once the aims and goals of the deception-based security are known, the detailed objectives of the deployed solution can be defined. Key factors to consider include:

- What critical assets do I wish to protect from attack?
- What actions do I want the attacker to do?
- What information do I need to collect about the attacker's actions?
- What intelligence do I want to collect from the attacker?

With the objectives of the deception-based solution defined, the implementation can be planned.

Planning

Planning a deception program involves the creation of deception stories, the combination of decoys, breadcrumbs, tags, and personas that create a deception environment that fulfills the objectives. The process starts with identifying the ingress paths into the real environment. Then, breadcrumbs are spread around both the attack paths and the critical assets. These will lead the attacker to the deception environment.

The deception stories need to match the real environment to be convincing and compelling. In addition, breadcrumbs and tags must be engaging and believable, the decoy's behavior the same as the normal business systems and processes on the real systems. Finally, all the individual elements must seamlessly fit together with no tell-tale indications that the business uses deceptions everywhere.

The planning phase will examine how the business uses and stores information. It will look at which applications, services, and endpoints are critical for business operations. Additionally, it will determine which access credentials offer the greatest value to an attacker. This analysis will inform the preparation of decoys and breadcrumbs.

Preparation

The results of the planning phase should produce the deception stories that deployed solutions will follow. Preparing the decoys, breadcrumbs, tags, and personas requires a detailed technical understanding of the business's networks, systems, interconnections, processes, and operations. This process also needs to take into account the attacker's probable methods and tools.

This phase is the most challenging aspect of deploying a deception-based solution. Any errors or omissions will result in an unconvincing story that allows the attacker to identify the presence of deception technology and allow their avoidance, rendering them ineffective.

Implementation

Following the preparation of the deception solution, the next step is to deploy the technology across the operating environment and integrate it with existing security controls. Again, the deployment must be meticulous and robust; an attacker can exploit weaknesses and vulnerabilities within the deception environment. The implementation must be convincing. The deception environment needs to reflect the activity present in the real network in terms of network traffic, data flows, user interactions, and services.

Autonomous alerting triggered by interactions with personas, tags, breadcrumbs, and decoys is linked to the security monitoring facilities in place for the business. This alerting must be hidden from an attacker to prevent alarms themselves from providing information to the attacker.

Monitoring

An implemented and deployed deception-based solution provides the means for monitoring in-network threats to inform the response and recovery processes and allow intelligence gathering. The implemented solution will therefore need to record the information necessary to achieve these goals.

The monitoring requirements form part of the objectives of the deception-based solution, operational experience, and post-incident lesson learned exercises will allow these requirements to be refined as part of the standard improvement processes.

Measuring

Deception-based solutions provide a mechanism to accurately measure the effectiveness of security controls for key performance indications and metrics generation.

The effectiveness and reliability of existing security controls can be quantified using information gathered from tracing the ingress path and actions of an attacker. This information can also gauge if the deception stories derived from the solution are complete and correct.

The results from this stage are fed back into the planning stage to refine the deception stories as part of the continuous improvement process.

DEPLOYMENT SCENARIOS

Administrative Center

The administrative center of a business is typically the first place to start when deploying deception technology. This is because this type of facility typically hosts most business-critical functions and the most sensitive information. For example, systems holding sensitive, personally identifiable information of employees are part of the human resources and payroll functions, as well as commercially sensitive data and financial records. Thus, for an attacker looking to steal information for financial gain, the administrative center's network is the place to visit.

A typical deployment will include network and endpoint decoys plus breadcrumbs and tags distributed throughout the operating environment. Deception technology should be concentrated around the business-critical systems and valuable assets, though coverage of all network parts is prudent.

Deception servers and decoy endpoints provide the deceptive environment to contain attacks. In addition, breadcrumbs in the form of decoy credentials provide the mechanism to pivot an attacker out of the live system and onto a decoy device.

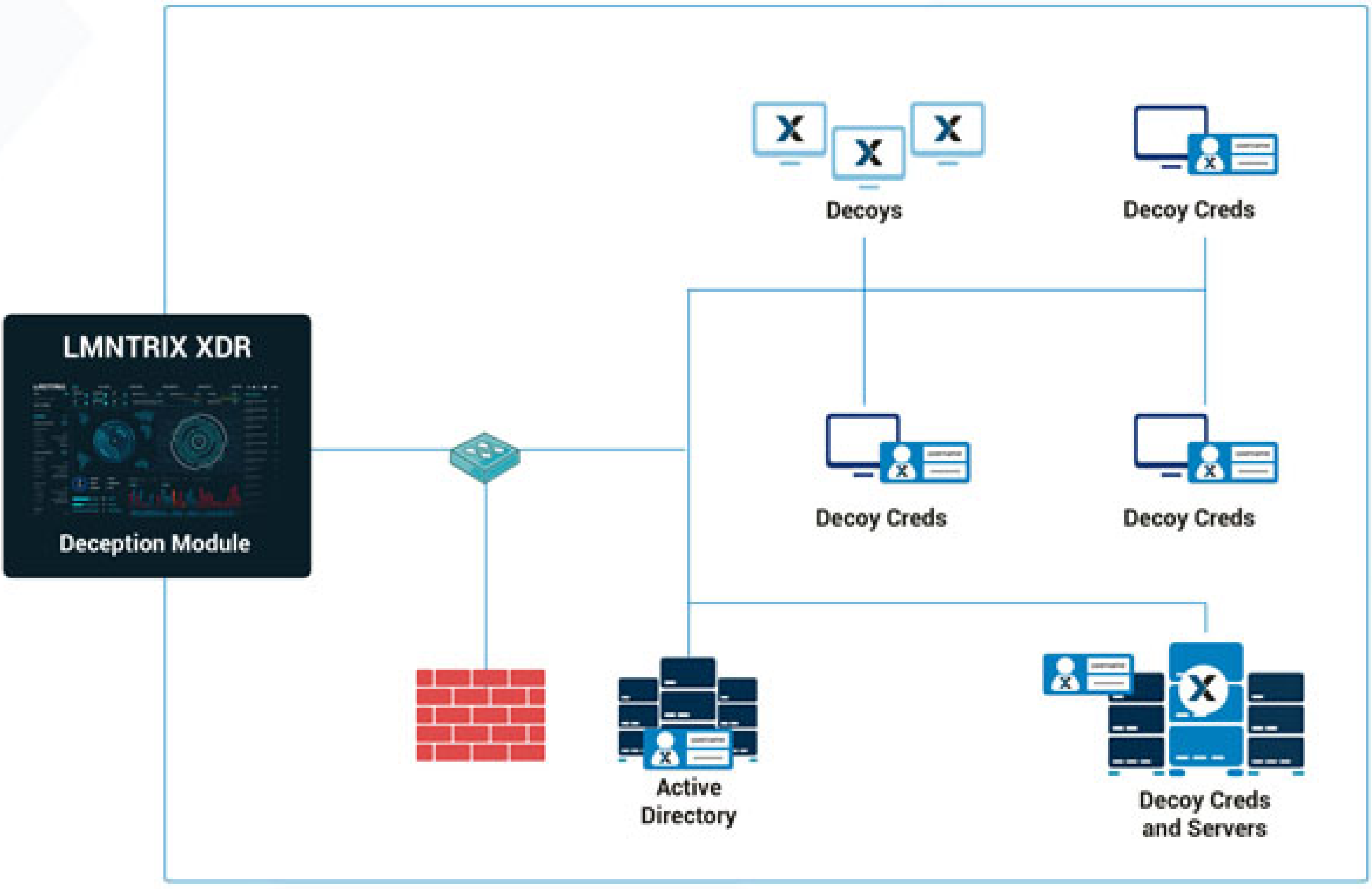


Figure 13 - Administrative Center Deployment Example

Production Facilities

Businesses that operate production plants or similar remote facilities such as distribution hubs or warehousing amenities utilize specialized systems that require protection. As a result, industrial control systems not only make attractive targets for attackers looking to disrupt business operations, but they also contain valuable intellectual property and other proprietary information valuable to competitors.

Remote manufacturing facilities often lack the capability of managing complex security controls onsite. In this situation, the deception environment can be established in a centralized location such as the administrative center or a data center. Breadcrumbs on the remote facilities network and endpoints pivot the attacker onto a virtual machine resident on the remote facilities network. Decoys support these for specialist devices such as Supervisory Control And Data Acquisition (SCADA) control systems and other Human Machine Interference (HMI) type equipment.

The attacker is then moved using a deception forwarder into the central deception environment. This relocation will be invisible to the attacker, with the advantage that the central security team can manage the attack. Additionally, maintenance and extension of the deception technology are managed centrally.

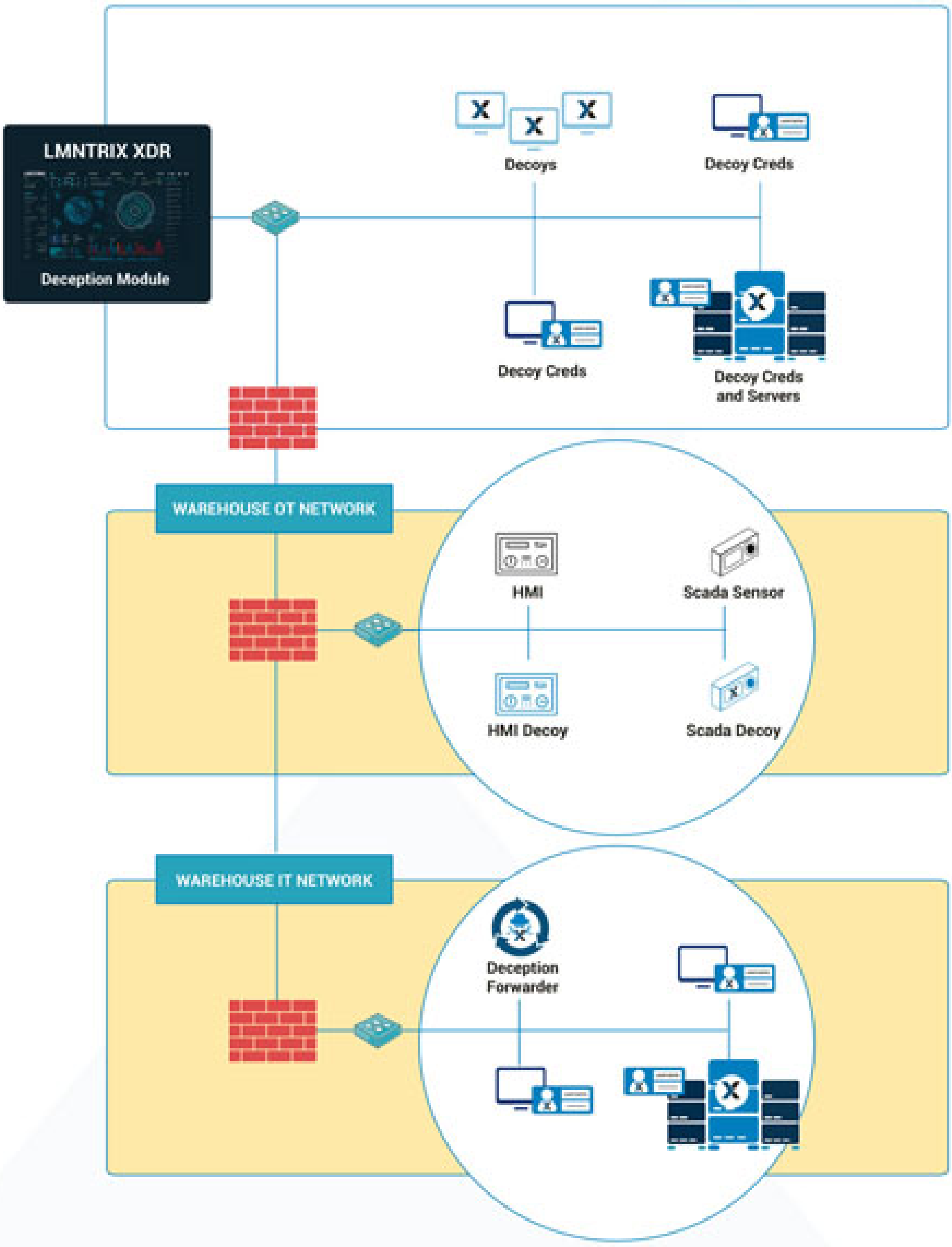


Figure 14 - Production Facility Deployment Example

Remote Facilities

Remote facilities often create challenges for traditional security controls where limited space and the lack of knowledgeable resources make implementing maintainable perimeter defenses difficult. In this situation, the deception environment can be established in a centralized location such as the administrative center or a data center. Breadcrumbs on the remote facilities network and endpoints pivot the attacker onto a virtual machine resident on the remote facilities network. The attacker is then moved using a deception forwarder into the central deception environment. This process will be invisible to the attacker, with the advantage that the central security team can manage the attack. Thus, maintenance of the deception technology is managed centrally.

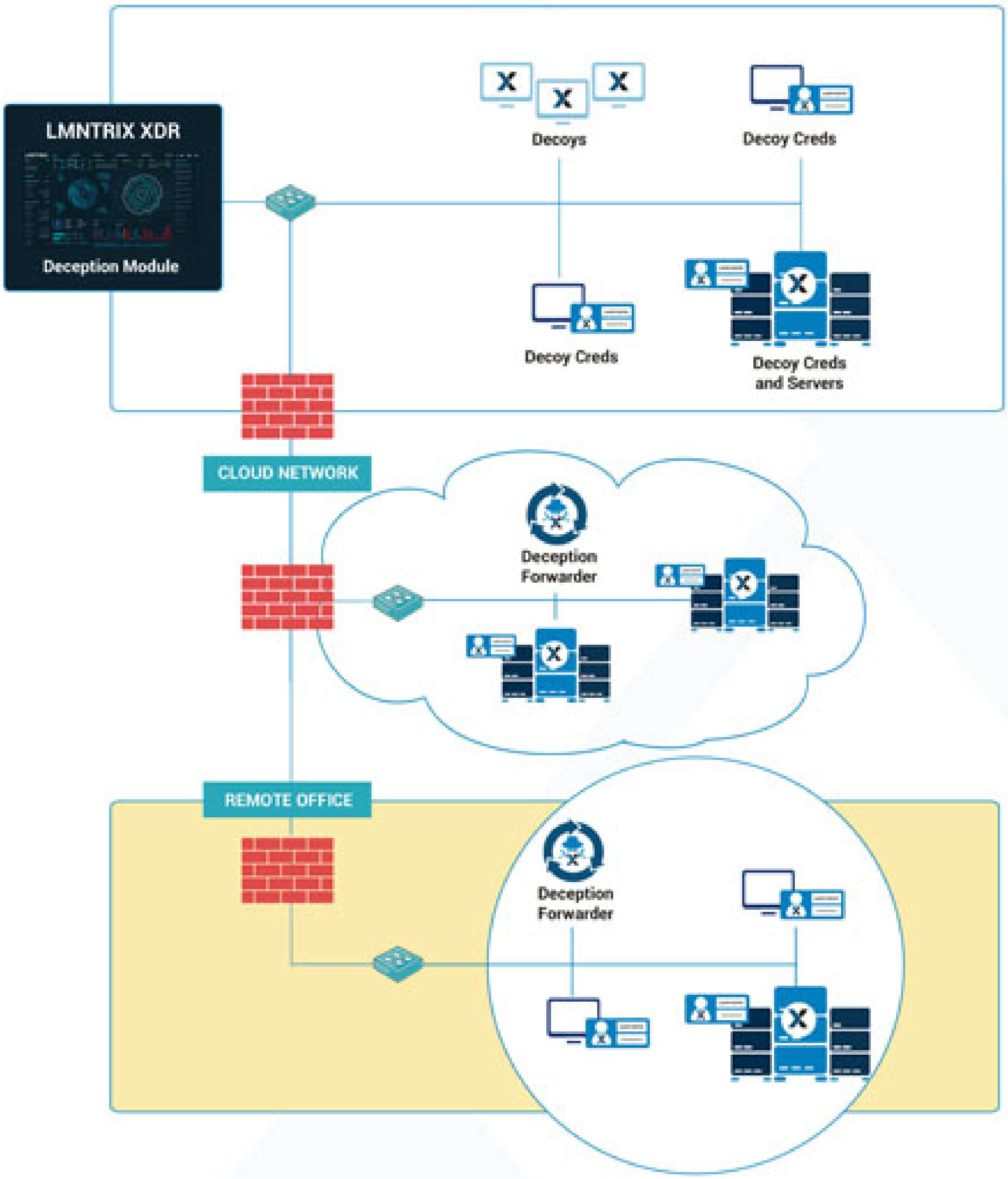


Figure 15 - Remote Facility Deployment Example

Cloud Environments

Deploying deception in a cloud environment requires a fully featured deception-based solution that can deploy network decoys and deceptive credentials for cloud assets along with decoy services and applications implemented using native cloud technologies. Additionally, compatibility with container-based technology and serverless processes is essential for implementing effective deception in cloud environments.

A deception environment can be established in a centralized location such as the administrative center, a remote data center, or as part of the cloud environment. Breadcrumbs on the cloud-based services and data storage facilities pivot the attacker using a deception forwarder into the central deception environment. This relocation will be invisible to the attacker, with the advantage that the central security team can manage the attack. Additionally, the maintenance of the deception technology is managed centrally.

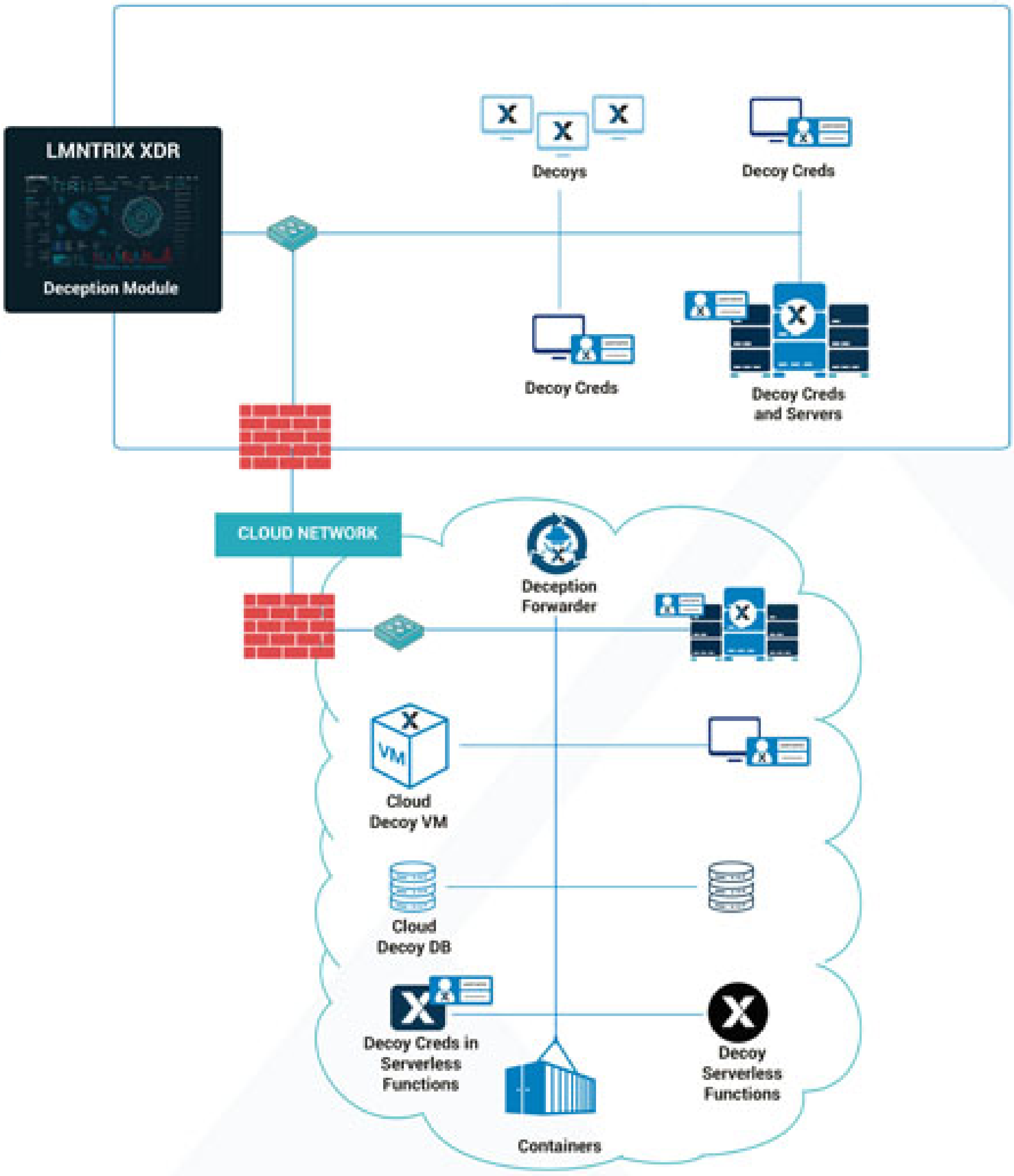


Figure 16 - Cloud Deployment Example

Supply Chain Providers

Systems that allow access to suppliers, partners, and other third-party providers as part of an integrated supply chain are particularly vulnerable to attack. Security integrity is dependent on the robustness of security controls in systems outside the security team's control. Attackers often exploit weaknesses in suppliers to launch attacks along a connected supply chain, exploiting trust relationships between parties to access systems that cannot be directly compromised.

A deception environment can be established in a centralized location such as an administrative facility or remote data center. Breadcrumbs can then be remotely deployed in the networks and endpoints of connected third parties, which pivot an attacker through a cloud-based central manager using a deception forwarder and then into the central deception environment. This movement will be invisible to the attacker, with the advantage that the central security team can manage the attack on third-party systems as part of the security controls for the business at risk at the end of the supply chain. Furthermore, maintenance and additions to the deception technology are managed centrally, transparent to the third party.

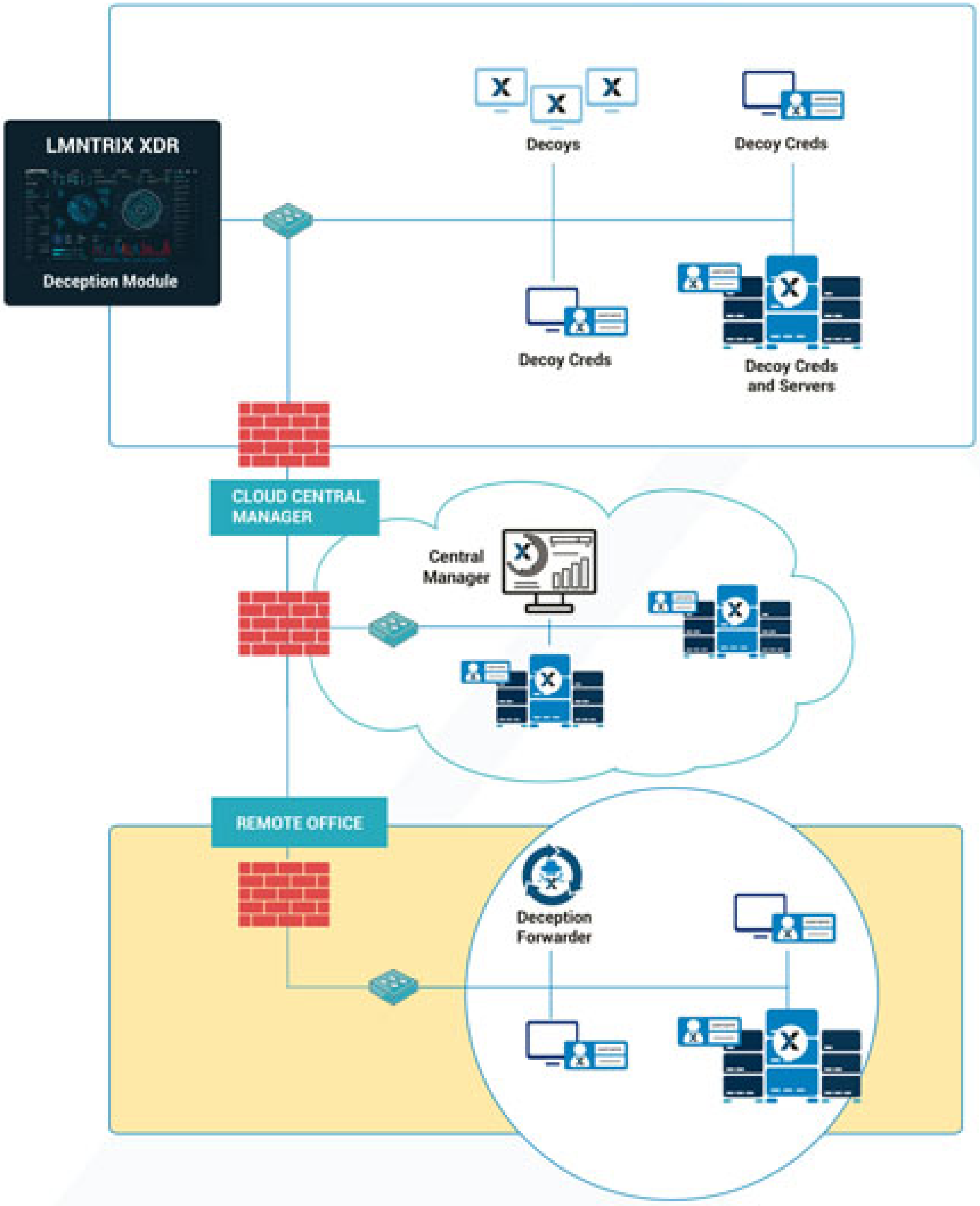


Figure 17 - Supply Chain Deployment Example

CURRENT **TRENDS**

Deception-based solutions are still in the early phases of market adoption. While the underlying technology is now twenty years old and entering maturity, its use was restricted to niche applications such as security research and state-managed protection of critical national assets and infrastructure in its early years. However, adoption across commercial businesses is now gathering pace due to the demonstrable benefits.

Deception-based solutions such as LMNTRIX's Deceive service are now available to significantly improve system security while at the same time decreasing resourcing requirements thanks to the elimination of false-positive alerts. Not many other solutions offer a better service with fewer resources.

The predicted growth in the adoption of deception technology is borne out by a recent survey of users of deception-based solutions. The results show that more than 80% of businesses planned to increase their spending on deception technology. There can be no greater expression of approval than the willingness to increase investment in a solution based on the benefits seen.

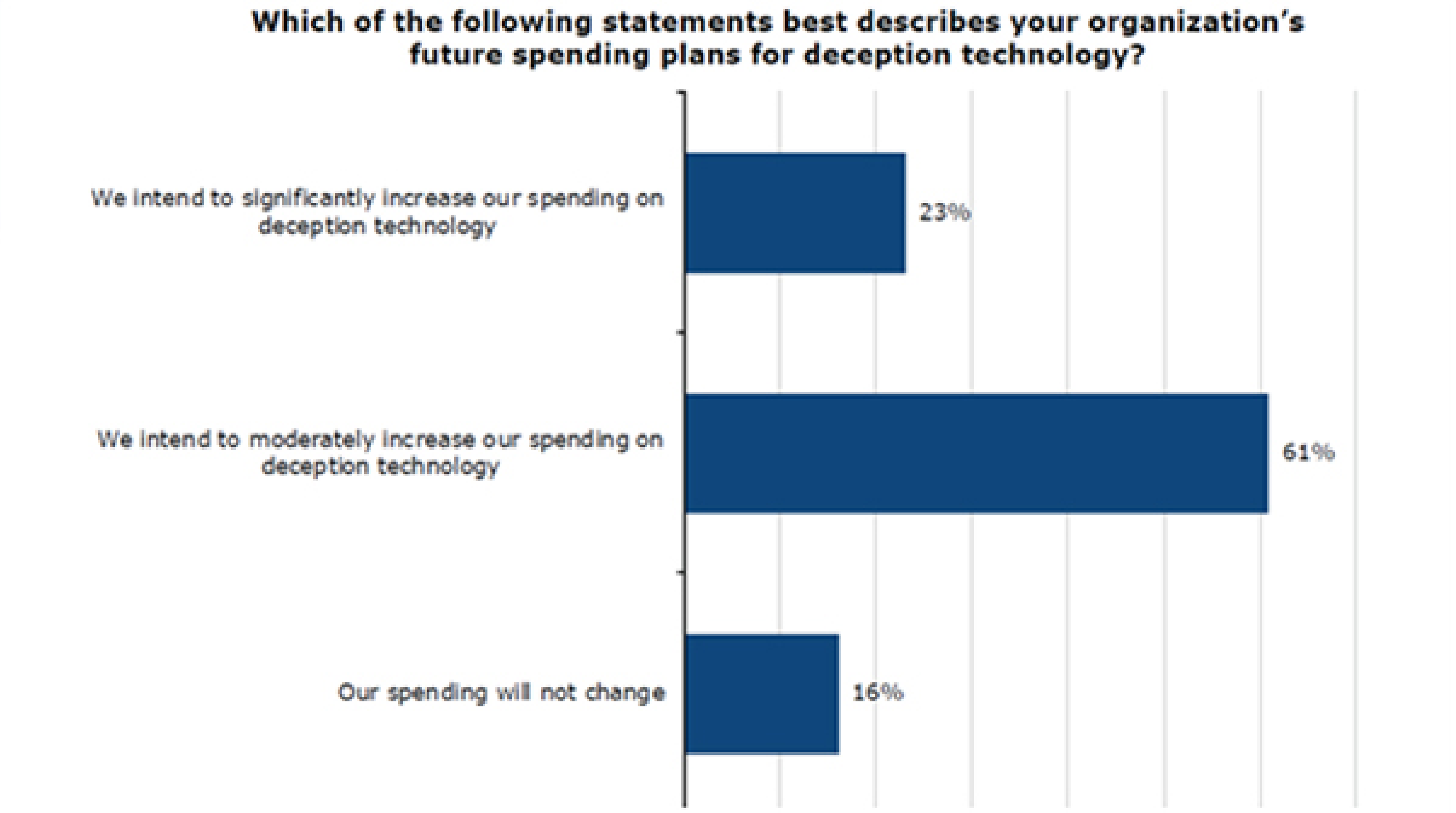


Figure 18 - Planned Investment of Deception Technology

This survey also looked at organizations considering adopting this technology but yet to invest to see why they were considering deception as an option. The results show that overwhelmingly the primary attraction was the ability to detect threats early in the attack lifecycle. Additionally, this technology feature brings an immediate business benefit in the potential cost reduction to remediate damage caused by an attack.

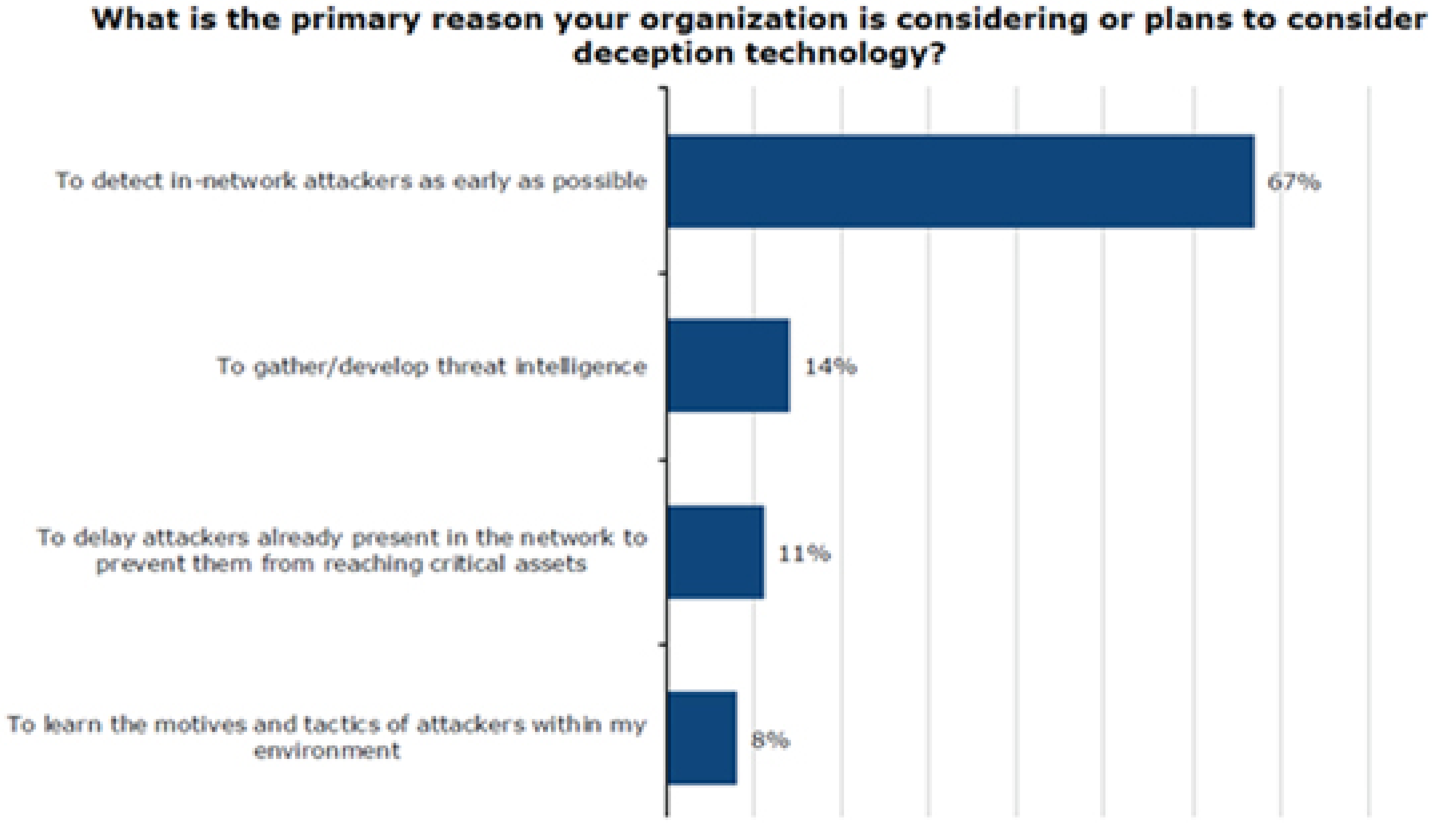


Figure 19 - Motivations for Investment in Deception Technology

A reactive response to threats currently drives the adoption of deception technology. A recent report into the cyber deception market found that the strongest demand was in Asia-Pacific markets. This adoption corresponded with companies in this region experiencing considerably high attack rates and suffering significant financial losses. Predictions are that as businesses worldwide become better informed and more aware of the benefits, growth in adoption will be seen across North America and Europe.

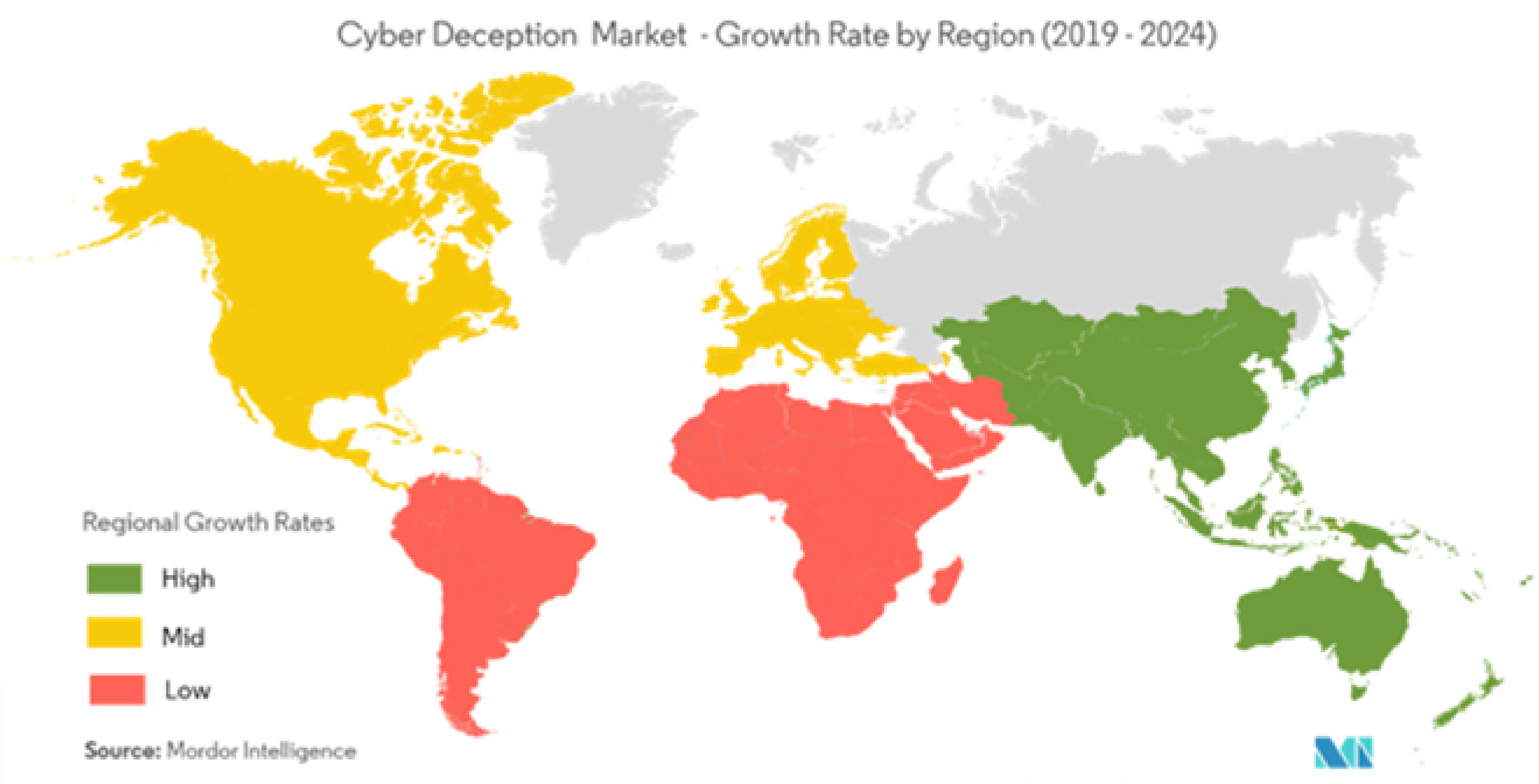

Cyber Deception Market - Growth Rate by Region (2019 - 2024)
Regional Growth Rates
🟩 High
🟨 Mid
🟥 Low
Source: Mordor Intelligence

Figure 20 - Region Adoption of Deception Technology

A key market differentiator for the future is the suitability of deception-based solutions for organizations moving across to a zero-trust-based approach to security. The deception philosophy dovetails seamlessly with the zero-trust model, working out of the box without the need for significant changes. The same is not true with traditional perimeter-centric security solutions built on the premise of trust within the boundaries.

SHIFTING POWER TO **THE DEFENDERS**

ASYMMETRIC WARFARE

The battle between hackers and the security team is a continuous process of evolution and revolution. Each side attempts to get ahead of the other. Traditionally attackers have had the advantage as security controls are designed to detect and respond to known attack vectors. However, each innovation in attack capability and the uncovering of zero-day exploits gives attackers the advantage until the security community develops and deploys countermeasures.

With each attack, the hackers gain knowledge about the target systems that are typically static for long periods. This is because significant changes to environments are costly and disruptive to business operations and so rarely implemented. Attackers, on the other hand, are constantly learning and adapting their methods of attack.

Attackers also get to pick when and where they attack. Therefore, the security team must be constantly vigilant for an attack that may never happen, which can be challenging for management to keep motivated and attentive.

Deception solutions change this threat environment. Autonomous processes monitor systems and issue alerts when an attack is detected. Security teams can now concentrate their effort on responding rather than detecting. A much smaller team can maintain systems and call upon support when an attack is detected. And the detection no longer requires prior knowledge of attack techniques or reliance on pattern recognition. Novel attack vectors and zero-day exploits will allow an attacker into a system, but they won't hide their presence when they start the kill chain.

ACTIVE COUNTERMEASURES

Advanced deception techniques create the opportunity to take active countermeasures against persistent threats rather than passively protect systems. Processes that hinder or nullify the attacker's actions by consuming resources and frustrating their activities reduce their effectiveness while gathering crucial intelligence. In addition, misinformation can alter the attackers' understanding of the system they are attacking, costing valuable time and forcing mistakes.

Deception solutions require the attacker to devote time and effort to determine if they are under the radar in a real environment or trapped in a decoy, under scrutiny, and potentially about to reveal their identity to law enforcement agencies. The deployment of a deception solution can itself act as a deterrent to attackers who may prefer to look for an easier target that can deliver financial gain quicker with less risk of being uncovered.

RISK REDUCTION

Business risk management is evolving, and cyber security needs to keep pace. Organizations that increasingly rely on processing information are looking to Digital Risk Management (DRM) processes to improve their risk management. DRM encompasses all aspects of business, including information processing and security. It's the identification of digital risk and the quantification of their business impact.

DRM has been developed to frame digital processing risks in a form that dovetail with conventional business risk, using a common language and understanding. The goal is to allow board-level executives to understand the digital risk profile of their business operations for informed decision-making. Technical risks can be balanced against the cost of doing business, supporting cost-benefit analysis of security decisions.

DRM's ultimate objective is to support digital resiliency in the operating environment, protecting digital assets from threats, minimizing business disruption and financial losses caused by attacks. To achieve this, DRM models have evolved to consider wider issues, including supply chain risks and perimeter security limitations.

Deception technology plays a critical role in reducing risk in the DRM models by enhancing security and providing security control metrics that support risk quantification. Its early detection capability with a high alert confidence level provides real-time metrics for malicious attacks as well as policy violations and misconfiguration issues.

With the trend for interconnected supply chains and on-demand business models, risk management is vital for today's businesses.

FITTING INTO THE NIST FRAMEWORK

Implementing deception-based security controls improves the robustness and dependability of a business's security posture, reducing business risk and providing a competitive advantage in a challenging operating environment. Mapping security controls to an established framework provides quantifiable evidence that not only informs risk management metrics but supports the demonstration of regulatory compliance. It also demonstrates reliance and due diligence to trading partners, the supply chain, investors, and end customers.

The NIST Cybersecurity Framework provides guidance for the management and reduction of security risks. The framework integrated industry standards and best practices using a common language accessible to all stakeholders and was ratified by the US Congress in the Cybersecurity Enhancement Act of 2014.

The NIST Cybersecurity Framework follows a five-step process.

- **IDENTIFY** – Develop an organizational awareness of important assets, security threats they face, the security controls in place, and the residual risks to the business.
- **PROTECT** - Develop and implement security controls to minimize risks to an acceptable level to safeguard critical business processes and assets.
- **DETECT** - Develop and implement security solutions that detect security incidents.
- **RESPOND** - Develop and implement security processes and practices to respond to security incidents.
- **RECOVER** - Develop and implement security processes and practices to restore services and data compromised by a security incident and resolve the incident's root cause.

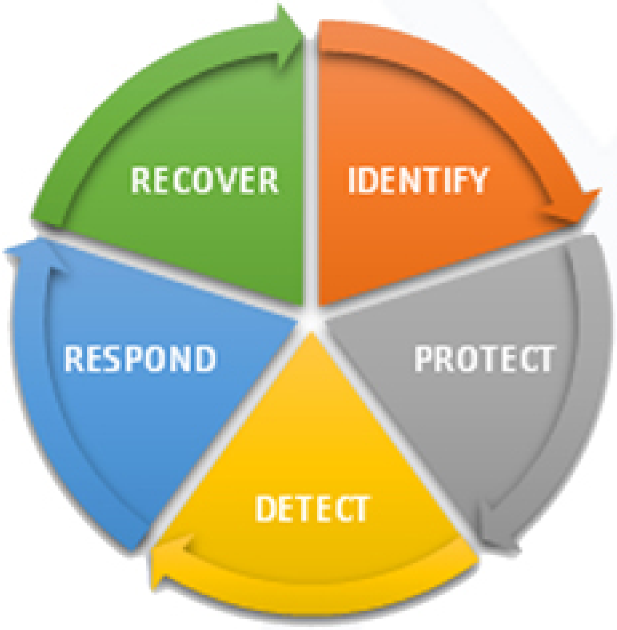


Figure 21 - NIST Cybersecurity Framework Steps

MONITORING AND ALERTS

A key benefit of deception-based security controls is the virtual elimination of spurious false positive alerts that can overwhelm security teams with traditional alerting mechanisms. This allows the response activities to focus on dealing with real incidents, improving responsiveness with fewer resources. In addition, the minimal false-positive occurrence rates also have benefits in boosting security team motivation.

The benefit of deploying decoys is that no normal business activity or user actions will interact with a decoy. Any interaction with a decoy must be due to an abnormal act, be that an internal or external attack. Any interaction with a decoy will automatically generate an alert to the security team that will include valuable information to aid response activities. Knowing which decoy was triggered allows the security team to focus on the attacker's actions when the alert was raised. This enables real-time monitoring of attacker activity. This real-time monitoring to replace traditional post-incident forensic analysis provides the response team with valuable information for the recovery phase.

These key capabilities that deception-based security controls bring to a business enable the use of leaner security teams that can detect, respond and recover far more effectively and quickly than would previously be the case with traditional security solutions.

INTELLIGENCE GATHERING

A key benefit of deception-based security controls is the quantity and quality of the information that can be gathered concerning each attack. By close monitoring of exactly what the attacker does and how they approach each step in the kill chain, the security team can uncover the previously unknown weaknesses and vulnerabilities in their systems that the attacker is exploiting.

This information allows the recovery team to resolve the identified issues and can be pooled with the knowledge base of the wider security community to identify weaknesses and vulnerabilities in other systems.

A significant risk to organizations is the leverage of zero-day exploits in widely adopted technologies and solutions. The vulnerability is unlikely to be independently identified and patched until the exploit is identified. Deception-based solutions can identify the exploitation of such vulnerabilities very early in the kill chain, and therefore severely limit the window of opportunity attackers have to take advantage of vulnerable systems.

Deploying high-interaction decoys in the deception environment can enable a security team to gather valuable intelligence on the attacker's actions and allow the defensive team to test the attacker and influence their actions to expand their knowledge of the attacker's abilities and resources. In addition, this captured information can be used to identify vulnerabilities, strengthen security controls, and share law enforcement bodies and the wider community as applicable.

INCIDENT RESPONSE

The main challenge with traditional security solutions for the response team is determining exactly where the attacker has been in a system and what exactly they did. For example, attackers may alter records, plant malware, or change configuration settings. Unfortunately, performing a forensic analysis on compromised systems to precisely determine what has been affected was often a painstaking and time-consuming activity, delaying the restoration of services.

Deception-based solutions provide detailed and valuable information on what the attacker was doing and how they did it. For example, detailed monitoring of an ongoing attack allows the response team to observe exactly how the attacker bypasses perimeter security controls, the lateral movement paths they took, and the services and data that attracted their interest.

An added benefit is that deception-based solutions can support automated response and restore processes. System configurations can be modified in real-time to block communication paths that the attacker tries to use to exfiltrate data or link to a command and control server. Compromised endpoints can be temporarily isolated from networks to halt attack paths. An intelligent deception-based solution can not only respond to counter the attacker's actions but predict their future actions and apply preventative controls to stop them in their tracks.

Adopting deception allows organizations to shift from a post-incident analysis and recovery process to a real-time response to ongoing incidents. This will significantly increase the likelihood of an attack being halted before a data breach occurs or harm caused to systems.

FORENSIC ANALYSIS

The data gathered from decoys in a deception-based solution provides valuable forensic information to inform response and recovery processes and intelligence gathering. High-interaction decoys capture and record detailed records of attacker activity for forensic analysis. The information shows exactly how the attack played out, what tools and techniques were used, what vulnerabilities were exploited. This is invaluable information for responding to attacks, recovering compromised assets, and improving the robustness of security controls. The processes for collecting forensic evidence can also be automated to ensure a comprehensive suite of records are obtained and shared as quickly as practical to limit the ability of the attack to use the same techniques on other targets.

The decoy environments provided by the deception-based solution are the ideal mechanism for collecting high-quality and exhaustive forensic evidence. They offer a safe environment to study attackers and gain valuable insights. A high-interaction environment will also enable the security team to influence the direction that an attack takes. This is invaluable if research into particular vulnerabilities or evidence of an attacker's capabilities is needed. By directing the attacker, placing obstacles to observe how they are circumvented, valuable information is obtained.

The benefit of a comprehensive deception environment is that forensic evidence can be obtained with minimal risk of the attacker breaking out of the decoy system and pivoting their attack onto the real business system.

THREAT HUNTING

The process of proactive threat hunting is a resource and time-intensive activity whose effectiveness depends on the hunt team's skills, knowledge, and abilities. The use of breadcrumbs that direct attackers to a decoy environment will give the hunt team a head start by trapping attackers and providing alerts to their presence. This significantly narrows the scope of the hunt activities, allowing a more focused hunt strategy on those aspects of the live environment that the breadcrumbs do not cover.

In addition, intelligence gathered from previous attacks by the deception-based solution, combined with shared intelligence from the wider security community, provides direction to the hunt activities. This allows hunts to target known attacker behaviors for current attack types, increasing the likelihood of success if an undetected attack is in progress.

The results of threat hunting activities can also inform the security controls to bolster the use of personas, tags, breadcrumbs, and decoys where deficiencies in coverage are identified. This will improve the robustness and effectiveness of the deception-based solution, increasing the likelihood of early detection of subsequent attacks.

DECEPTION USE CASES

EARLY DETECTION

Capable and sophisticated attackers can gain unauthorized access to systems protected by traditional perimeter defenses with relative ease if the system has discoverable vulnerabilities. If attackers have access to stolen or disclosed access credentials, then their task is made simple. And then, there are internal attacks, where an authorized user misuses their permitted access for malicious purposes. I'm all these cases, detecting the attacker's presence within the system inside the perimeter of the security controls is challenging.

Systems are also expanding in terms of the number and diversity of connected devices. The trends for integrating Internet of Things (IoT) technology into networks and remote access using personal devices are expanding the attack surface and the number of potential vulnerabilities. In addition, the growth in the working from the home culture in response to the Covid-19 pandemic means that systems allow access to devices whose configuration and security controls are outside the control of network administrators.

Deception technology brings the capability to detect attackers within the boundary of systems at the very start of the kill chain before any damage can be done. This ability gives security teams a significant advantage in halting attacks and closing down the ingress route to stop further attacks.

The more advanced and capable the deception environment, the longer the security team can let the attack play out. At the same time, the team can gather valuable intelligence to share with the wider community and inform future security strategies.

LATERAL MOVEMENT

Gaining access to systems is only the start of the kill chain; the initial ingress route into a system rarely gives an attacker access to valuable assets. Instead, ingress typically leads to slow and steady surveillance of the systems to identify the interconnections and where they lead. As a result, attackers maintain a low profile to avoid detection by standard monitoring and logging processes or more capable intrusion detection systems. This lateral movement across the network in search of the compromised organization's Crown Jewels represents most of the dwell time of an attack.

- Opportunities to escalate privileges
- Access to connected networks and devices
- Creation of back doors to ease future access
- Capability to delete traces of presence
- Upload of utilities to support actions

The challenge for security teams using traditional security controls is to detect an attacker's presence on their systems before the attacker has found a means to move across to a different connected system. For the most capable attackers, this time can be measured in minutes. System analysis tools that rely on behavioral analysis or pattern matching technology will be unlikely to detect lateral movement in its early stages.

Deception technology brings the capability to detect attackers within the boundary of systems at the very start of the kill chain before the attacker can move to connected systems. Significantly, they also bring the capability to misdirect attackers to move laterally to a decoy environment where the attack can be contained, and the security team alerted.

While the most capable of attackers may deduce the presence of decoys, this knowledge will mean that the attacker will need to spend more time and effort establishing if the next destination of their lateral movements is real or a decoy. This caution allows the security extra time to detect and respond to the attack.

An additional benefit of the deception strategy is that it provides detailed information about the vulnerabilities and misconfigurations that the attacker has exploited in the attack. This valuable information can resolve the security weaknesses and prevent further attacks using this particular attack vector. It can also drive improvements to the implemented deception environment where the attacker can successfully navigate real systems.

CREDENTIAL COMPROMISE

Once an attacker has penetrated a system and identified mechanisms that enable lateral movement, their next priority will be privilege escalation and discovering alternate ingress paths. One key technique is to find and target privileged user credentials that can be used to increase their levels of access without raising the alarm. Exploiting legitimate credentials in a manner that mimics normal user actions will keep activities under the radar of typical behavioral analysis and process monitoring techniques.

A typical attack vector is to implement an internal man-in-the-middle attack to intercept and record access credentials as they pass over networks, exploiting vulnerabilities in the protection mechanism applied to the network traffic. This technique uses the fact that internal network communications are often less rigorously protected than traffic that passes over external, third-party accessible channels.

Another attack vector is to access Active Directory information of privileges accounts using techniques that occur in normal operations that utilize Active Directory technology. This utilization of standard processes for malicious purposes is incredibly difficult for traditional security controls to recognize as abnormal behavior.

The challenge for security teams using traditional security controls is to detect an attacker's presence on their systems before the attacker has found a means to steal and exploit user credentials. However, security detection techniques that rely on behavioral analysis or pattern matching technology will be unlikely to the presence of a competent attacker keeping a low profile and performing actions that mimic normal user activities.

A deception solution can include planting false but believable credentials for an attacker to steal and utilize. These deceptive credentials can be configured to move the attacker across to a decoy system and trigger a security alert. The false credentials need to be managed identically to real credentials to be credible but in a manner that makes them more attractive to the attacker.

A second alert mechanism that can be employed is to monitor for the use of legitimate credentials on decoy systems and endpoints. For example, an attacker who has compromised legitimate privileges access credentials but later moves across to the decoy environment can be immediately identified.

The primary benefit of this deception strategy is that it provides a definitive indication that a capable attacker has established a presence inside a system. This valuable information can be used to respond to attacks early in the kill chain and indicate unresolved security weaknesses that require attention.

MALWARE AND RANSOMWARE

Malware and its ransomware offspring are evolving to be more capable, persistent, and difficult to detect. Traditional security controls rely on scanning content crossing boundaries and pattern matching techniques to identify known threats and derivatives. While this technique effectively spots and stops the known, they are less effective at detecting novel malware that doesn't follow a previously employed signature.

Another technique for spotting deployed malware within an environment is to look for tell-tale signs using behavioral analysis. However, this technique has limited success against sophisticated malware that is able to perform actions that mimic normal user activities.

The challenge for security teams is to detect the presence of malware and ransomware on their systems before the malicious code can either initiate a harmful action or spread to other connected systems.

Malware, in general, comes in a wide range of types that are typically characterized by their behavior.

- Worms are a type of malware that actively seeks to spread through systems so that a copy of the malware is installed on as many devices as possible. In addition, the worm's purpose is typically to install copies of other malware on the devices that it has compromised in a manner that is invisible to security controls. This allows compromised devices to be exploited at a later date as part of a more sophisticated attack.

- Ransomware is a type of malware that traditionally encrypts data. The owner of the affected systems will pay a financial settlement to obtain the key required to decrypt and restore the data. It is now also common for ransomware to exfiltrate data of perceived value over to a server controlled by the attacker. This stolen data can then be used to incentive ransom payment to counter the possibility that the compromised systems can be recovered without the need for decryption.

- Malware can also deliver resource-heavy applications such as crypto mining applications that hijack the computing resources of the compromised systems to perform operations that provide value to the beneficiary of the service using the resources of the target organization. In the case of crypto mining, the processing creates cryptocurrencies.

The key benefit of using a deception-based strategy to detect malicious code is that it's effective in not limited to certain types of malware. Traditional technology looks for code with a known signature or behavior to detect malware, unable to detect a completely novel form of malware not previously seen. The use of decoys to detect the presence of malware by its actions does not suffer this limitation, being able to detect any malware that is already inside a system.

Deception technology can detect ransomware early in the kill chain before it initiates its encryption phase. Ransomware will look for any accessible data, unable to distinguish between real and decoy information. As soon as it accesses hidden, deceptive shares placed on endpoint systems, an alert can be raised, and a response initiated.

INSIDER ATTACKS

Insider attacks are a significant challenge to detect before malicious actions result in loss or damage to systems. Insider attacks can vary from disgruntled employees seeking to disrupt systems to users seeking to exfiltrate valuable information for financial gain. In the typical operating environment, users include contractors, third-party service providers, and other associate users. As the attacker has legitimate access to systems, identifying such an attack relies on spotting unusual behavior that indicates malicious intent before the attacker can cause harm. Unfortunately, this represents an extremely limited window of opportunity for the security team.

Where attacks are by insiders, they tend to be unsophisticated in techniques but benefit from detailed system knowledge, including precisely where information of value is held. However, in some cases where the insider is technically savvy, they often look to cover their tracks by stealing access credentials of other users. This can be relatively straightforward using social engineering techniques or simply shoulder surfing a colleague. In addition, users tend to lower their guard when working in what they believe to be a safe environment, such as an office or other work area.

The nature of the insider attack depends on motivation. A disgruntled employee will typically use their own credentials to cause damage to the system as an act of retribution against perceived injustice. The greater threat is the insider looking to steal information over the long term using techniques that will hide or disguise their actions such that any investigation will not implicate them. This latter type of attack is incredibly difficult to detect and recognize before damage is done.

Deception technology can create an environment that legitimate users will not recognize as being a decoy. Planting decoy data that emulates valuable data that attracts the inside attacker's attention can provide a trigger that an inside attack is in progress. Creating decoy servers with mapped shares, data records, and documents identical to real servers in logical appearance can lure the attacker into believing they are accessing information worth stealing.

This deception strategy can provide a definitive indication that a legitimate user seeks information outside of that needed for their normal duties. In addition, this event can be used to trigger detailed monitoring of behavior to distinguish between accidental actions, non-harmful curiosity, and malicious intent.

SUPPLY CHAIN ATTACKS

Attacks that use legitimate user accounts of supply chain partner companies that have been granted access to systems have significant similarities with insider attacks. Having a legitimate reason to access systems makes it challenging for the security to detect that the account is being used maliciously before any harmful actions occur. Additionally, identifying unusual behavior that indicates malicious intent in just one of potentially hundreds or thousands of user accounts is challenging for the best traditional security solutions.

This attack vector is becoming more critical for larger organizations as attackers leverage weaknesses in small suppliers to gain access to their systems. These are the springboard for launching attacks up the supply chain by impersonating legitimate users. The more elements in the compromised chain, the harder it is for the end target to recognize that an attack is in progress.

Deception-based controls can create a decoy environment that attracts the attention of attackers leveraging access through the supply chain. An environment with decoy services and data that would be of value to the attacker can generate alerts to the security team that an attack is in progress.

There are potentially two purposes to the decoy environment. The first is to attract the attacker's attention using baited assets if the organization is at the end of the supply chain and, therefore, the ultimate target of the attack. The second is to provide decoy credentials for accounts with access to connected systems higher up the supply chain if the organization is a stepping stone in the overall attack strategy.

Whatever the attacker's intent, the deception-based controls provide the means to detect an attacker's presence leveraging access using the credentials of a legitimate third-party user. This valuable information can be used to respond to attacks early in the kill chain and to inform those organizations within the supply chain whose systems have already been compromised. Additionally, detailed intelligence can be used to identify how these affiliated companies may have been compromised, resolving their security issues to increase the overall robustness of the supply chain security.

INFRASTRUCTURE CHANGE AND MIGRATION

One of the key information security challenges that organizations face is managing major infrastructure changes. The period of transition where different systems are combined as a result of a merger or acquisition or in response to the decision to migrate to a new environment creates significant challenges.

Often, security teams are required to manage changes to security policies, processes, and technologies during the transitional phase without impacting security posture. Capable attackers will be aware when a particular organization is undergoing a period of significant change and see this as an opportunity to find weaknesses and vulnerabilities that exist during the transition.

Deception technology can be used to encase the affected systems in a protective shield for the duration of the change, providing an extra layer of protection during the period of increased risk. Deception technology can also be quickly adapted and scaled to give the new environment effective security controls. The nature of deception-based solutions allows rapid change that keeps pace with infrastructure change.

Another benefit is that in the case of mergers and acquisitions, deception technology can be deployed as part of the due diligence processes to assess the robustness of security controls in the organization of interest. This information can provide valuable insight into the impact of integrating businesses from the information security and governance perspective before integrating systems.

OFF-PREMISES ENVIRONMENTS

A significant percentage of organizations no longer rely on on-premises computing environments. The move towards using third-party managed remote datacenters or the cloud has brought significant business benefits and security challenges. Traditional security controls are not always applicable for protecting the latest technological advancements. In addition, the availability of serverless applications has created complex challenges for traditional integrated security solutions that were not developed to cope with such technology.

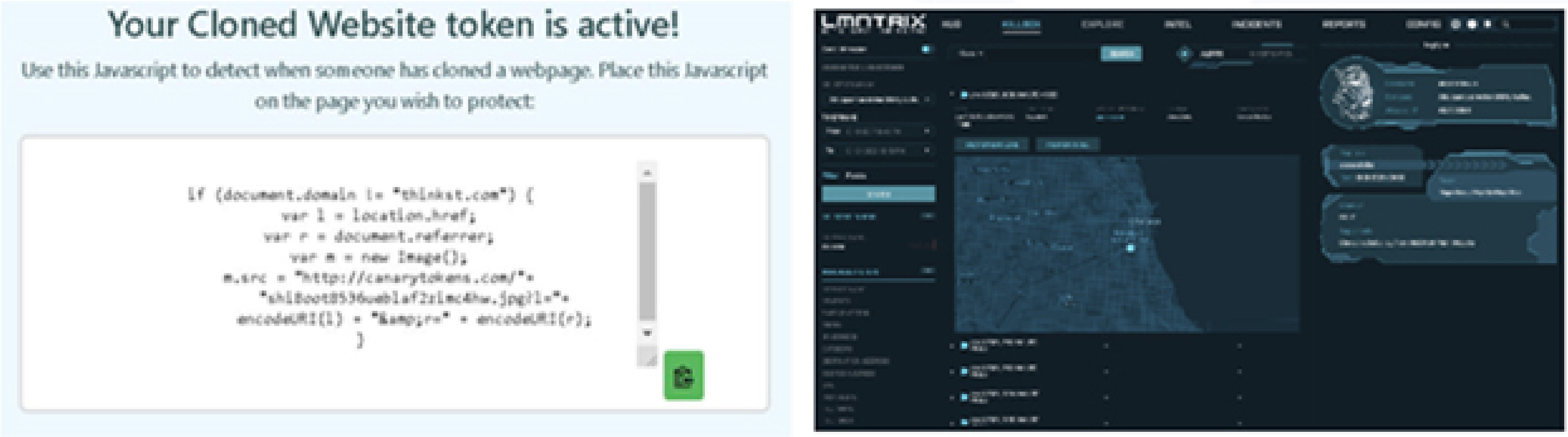
The advantage of deception-based solutions is that they can be deployed in any environment. Furthermore, the introduction of a novel environment can be quickly followed by the availability of a decoy emulation of that environment.

It can be argued that the move towards serverless applications makes it simpler to create effective decoys that are more capable and hence provide increased levels of protection. Deceptive services, applications, and data can be quickly deployed and evolved to develop novel defenses that can stay one step ahead of the most capable of attackers. This innovation in defenses has significant benefits thanks to the flexibility and scalability of the technology they employ.

WEBSITE CLONING

A common method of obtaining credentials for web-based systems is website cloning, creating a duplicate copy of a website that sits on an attacker's servers, mimicking the real site. Users are misdirected onto the cloned website where they enter their access credentials, oblivious to the deception. The attacker can then record the credentials and transparently move the user onto the legitimate website, so they are unaware their credentials have been compromised. This technique allows the attacker to use the credentials later or pass them on to other attackers as part of a Cybercrime-as-a-Service.

Deception technology can counter this threat and turn the table on attackers, deceiving the deceivers. Simple JavaScript code obfuscated and embedded in each webpage can detect if the domain does not match the expected value. An attacker cloning the webpage will clone this code, alerting the website owner that the cloning has occurred. This allows countermeasures to be deployed against the attacker that has cloned the web pages.



Your Cloned Website token is active!

Use this Javascript to detect when someone has cloned a webpage. Place this Javascript on the page you wish to protect:

```
if (document.domain != "thinkst.com") {
    var l = location.href;
    var r = document.referrer;
    var m = new Image();
    m.src = "http://canarytokens.com/"+
        "shi8oot8536uebla f2zlmc4hw.jpg?l="+
        encodeURI(l) + "&amp;r=" + encodeURI(r);
}
```

Figure 22 - Website Cloning Detection

THREAT INTELLIGENCE GATHERING

A key to preventing future attacks is the gathering and sharing of intelligence on current attacks. Knowing which groups are targeting which organizations, what attack vectors they favor, and what novel techniques they are using is valuable in ensuring security controls will be effective.

Traditional security controls operate based on containing and removing threats as soon as they are detected to limit the harm that the attacker can cause. This approach provides a snapshot of threat behavior during containment. Still, it offers little intelligence on their behavior during the initial stages of the attack or what actions they intended to undertake during the attack.

A forensic analysis of the compromised system may yield information on how the attacker ingresses the system and what actions they have carried out before detection. Still, the completeness of this information depends on the competence of the attacker in covering their footsteps. Also, it depends on the quality of the logged data available to be analyzed by the forensics team.

Deception-based solutions enable organizations to allow the attack to proceed while it remains contained within the deception environment. Assuming they are unaware that they have been discovered and that they are in a decoy environment, the attacker will behave normally as if the attack was ongoing. This allows the security team time to monitor the attacker's actions in fine detail to glean valuable intelligence. This information is of value for the incident response team to address the vulnerabilities that allowed the attacker to ingress into the system. It is also valuable for the wider community in preventing similar attacks and potentially for law enforcement officials in the attacker's jurisdiction looking for evidence to prosecute the attacker.

A highly skilled security team can also test the attacker's capabilities by actively engaging in actions that influence subsequent actions. A controlled environment allows the security team to play with the attacker to gain greater insight and uncover potential weaknesses and vulnerabilities.

CYBER DECEPTION EFFECTIVENESS

The use of deception-based solutions to combat cyberattacks has steadily gained ground in recent years. The enhanced detection capabilities, combined with the elimination of the noise of false alerts that traditional detection services can generate, make it an attractive addition to the suite of security controls.

The growth in low and slow multi-staged attacks where attackers move stealthily around breached networks to locate, gain access to, and exfiltrate sensitive information will see the use of this technology become more common. It's ideally suited to detect threats early in the attack lifecycle, limiting potential damage and minimizing remediation costs.

A recent survey of users of deception-based solutions has revealed some remarkable results on the perceived effectiveness of this technology.

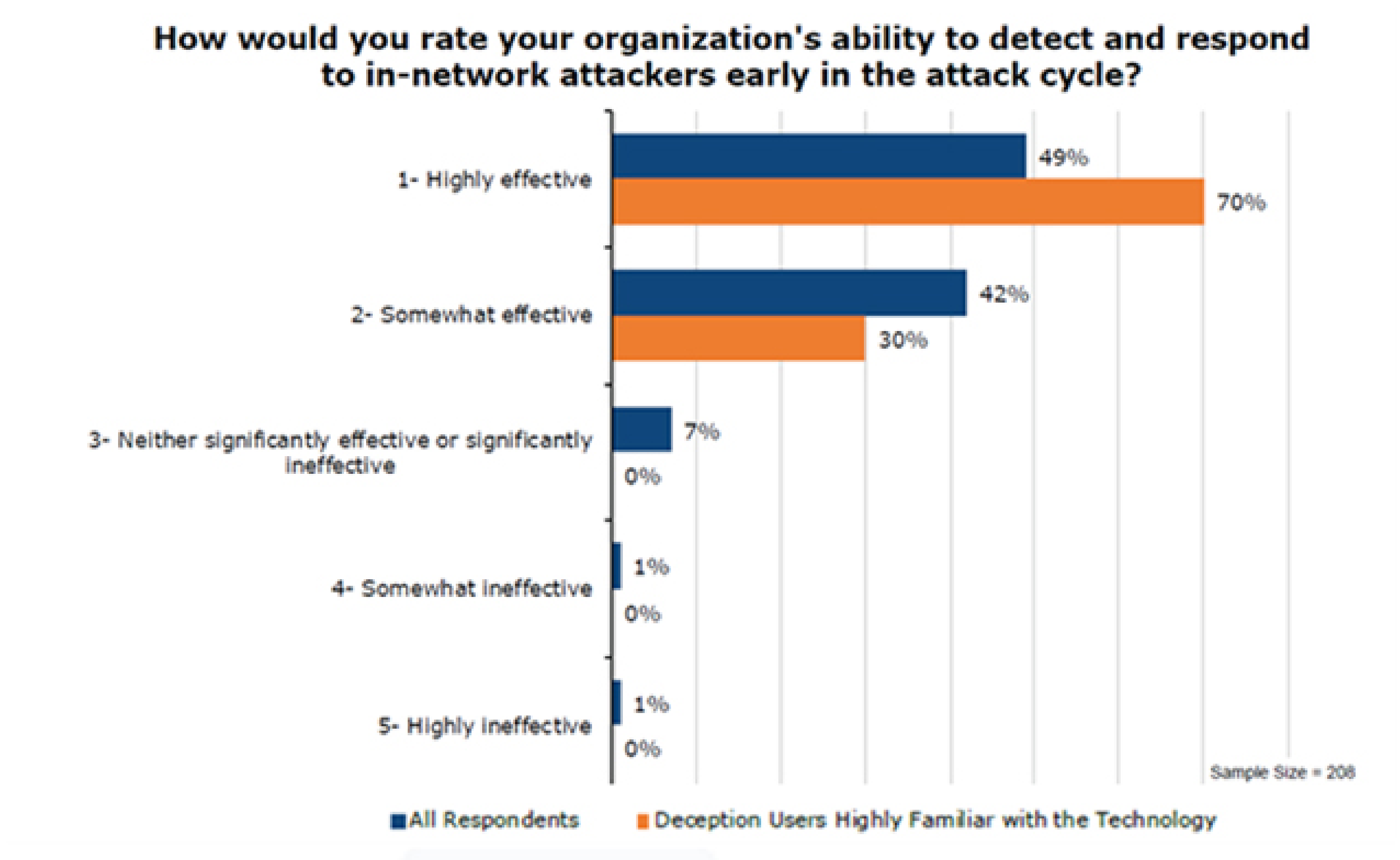


Figure 23 - Perceptions of Deception Effectiveness for Early Detection

This survey also looked at organizations that were yet to adopt this technology to see what difference it made to the security posture of businesses. The greatest benefit was seen in the speed of detection of an attack. Dwell time is the time taken to detect a threat measured from when the attack was initiated. The dwell time is when attackers are free to roam networks looking for useful information to use in their attack, sensitive information to exfiltrate, or opportunities to upload and install malware. This marked reduction in dwell time directly translates into minimization of threat impact.

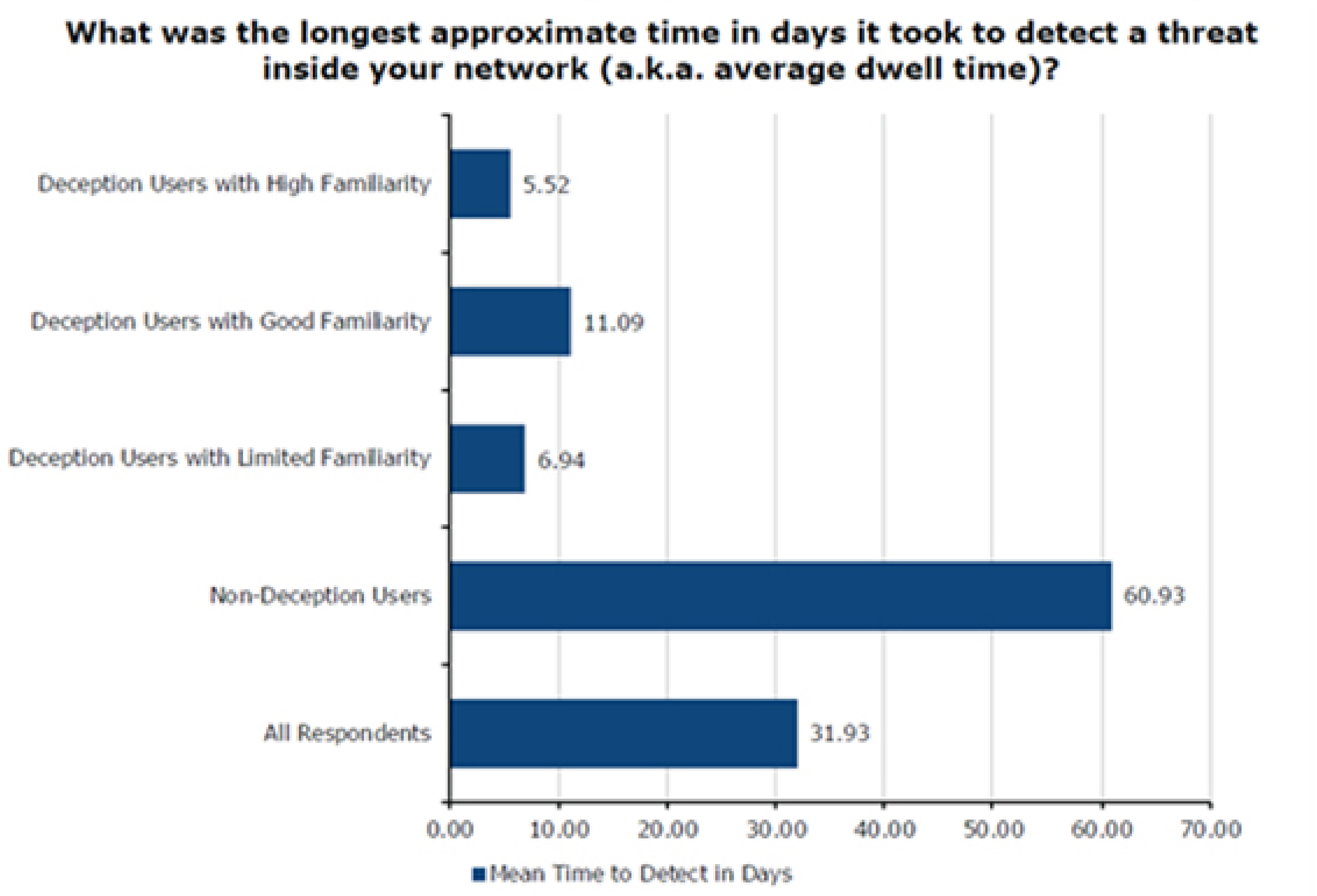


Figure 24 - Deception Effectiveness measured against Dwell Time

This survey asked each user of deception technology to list the benefits to their business from having decided to adopt this solution. The results show that this technology brings a host of benefits to businesses. However, which ones matter the most depends on the nature of each business. This demonstrates the wide-ranging advantages that this solution brings.

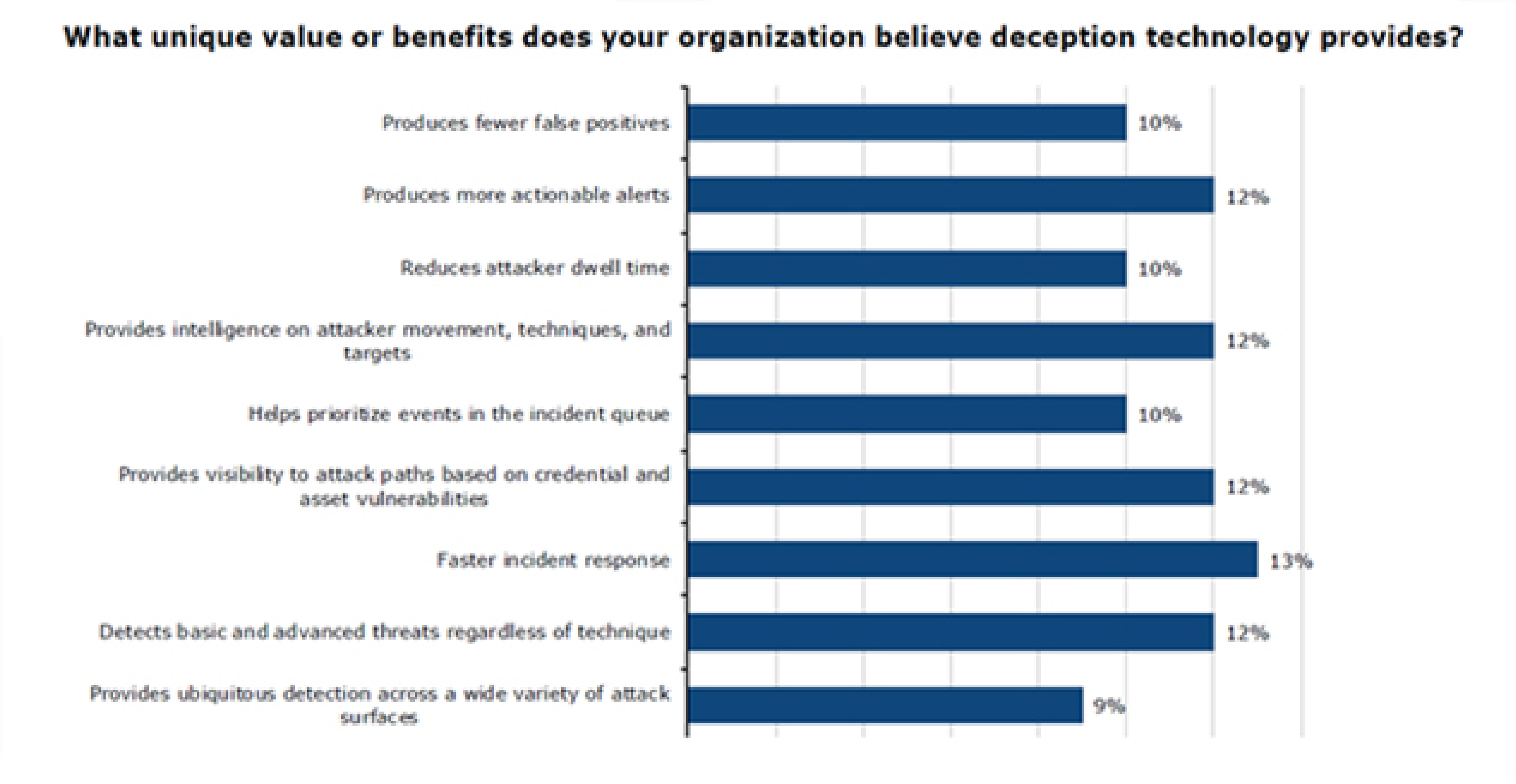


Figure 25 - Perceptions of Deception Benefits

Finally, this survey asked each user of deception technology to express their opinion of the value to the business brought by adopting this solution. More than half of respondents reported that they felt that they had achieved greater than expected value. Furthermore, more than 80% of respondents reported that they intended to increase their investment in deception technology. This is a far cry from some security solutions brought into enterprises only to bring no noticeable benefit to the business.

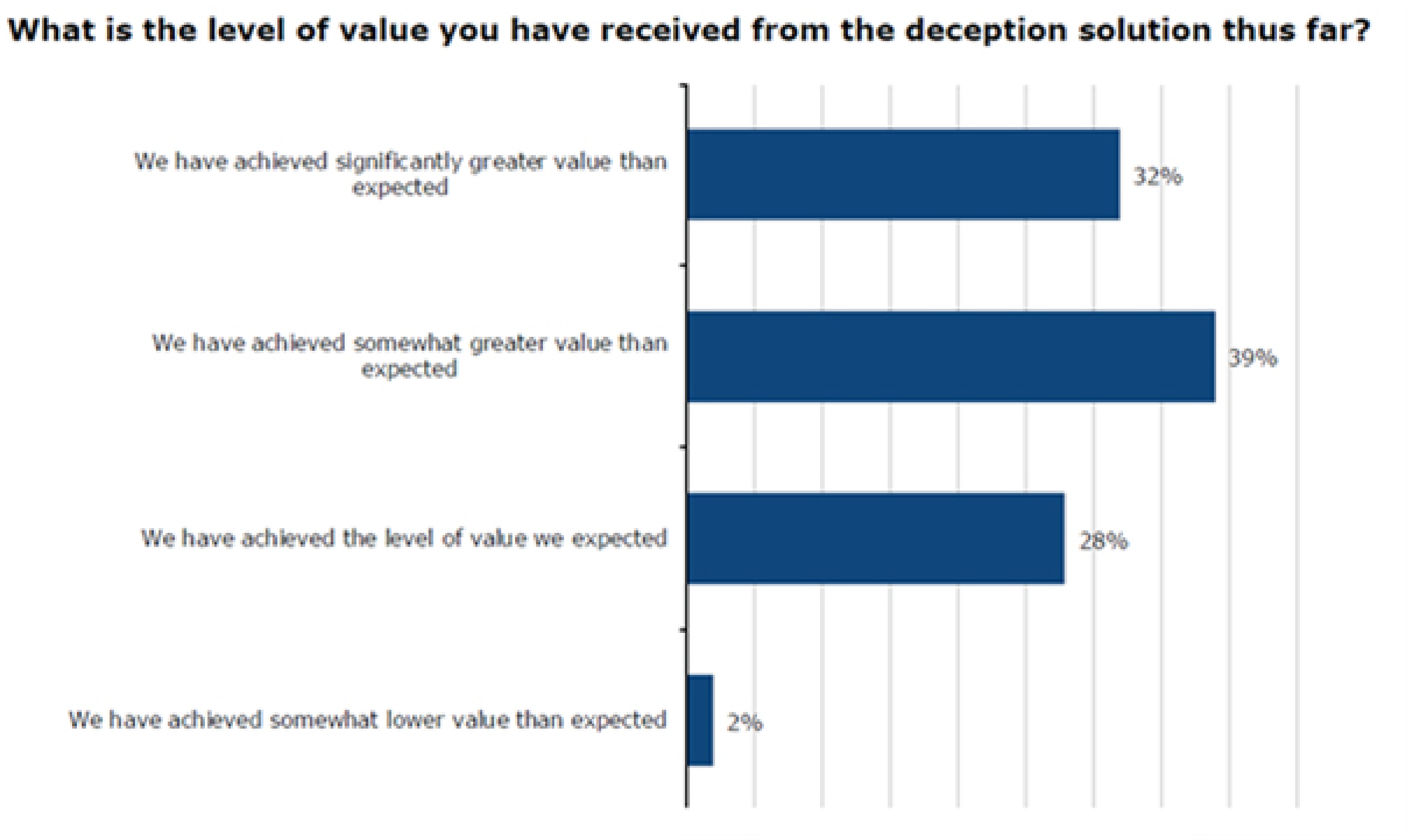


Figure 26 - Perceptions of Deception Value

HOW **LMNTRIX XDR** BENEFITS FROM DECEPTIONS

LMNTRIX XDR

The platform

LMNTRIX's Extended Detection and Response (XDR) platform is our cyber defense SaaS platform that provides a new utility model for enterprise security. It delivers pervasive visibility, threat hunting, validation, investigation, containment, remediation, and unlimited forensic exploration on-demand and entirely from the cloud. It is a single investigative platform for insights into threats on enterprise, cloud, hybrid, and Industrial Control System (ICS) networks.

The LMNTRIX XDR delivers unique advantages over current network security solutions. It is a holistic and multi-vector platform with an unlimited retention window of full-fidelity network and endpoint traffic, innovative security visualizations, and the ease and cost-savings of an on-demand deployment model.

LMNTRIX DECEIVE

Deception technology gives defenders an opportunity to reduce cyber dwell time by altering the adversaries' perception of the attack surface. Doing so slows down the attacker's ability to move laterally undetected, changes the economics and increases the attacker's risk, giving defenders more time to understand TTPs and ultimately eradicate the threat from the environment. LMNTRIX Deceive is an integral part of LMNTRIX XDR that allows organizations to quickly and accurately detect attackers, malicious insiders and malware already inside the network, engage with the attackers, and neutralize advanced cyber threats. With LMNTRIX, defenders can automatically create real, interactive OS decoys as well as emulated services and OS's, including enterprise OT and IoT devices. Then attackers can be lured to the decoys via breadcrumbs and tags that are continuously updated. Through a unique combination of adaptive intelligent deception, automatic terrain learning and visibility, LMNTRIX keeps the attackers guessing and dramatically reduces time-to-resolution from weeks and months, to hours and minutes

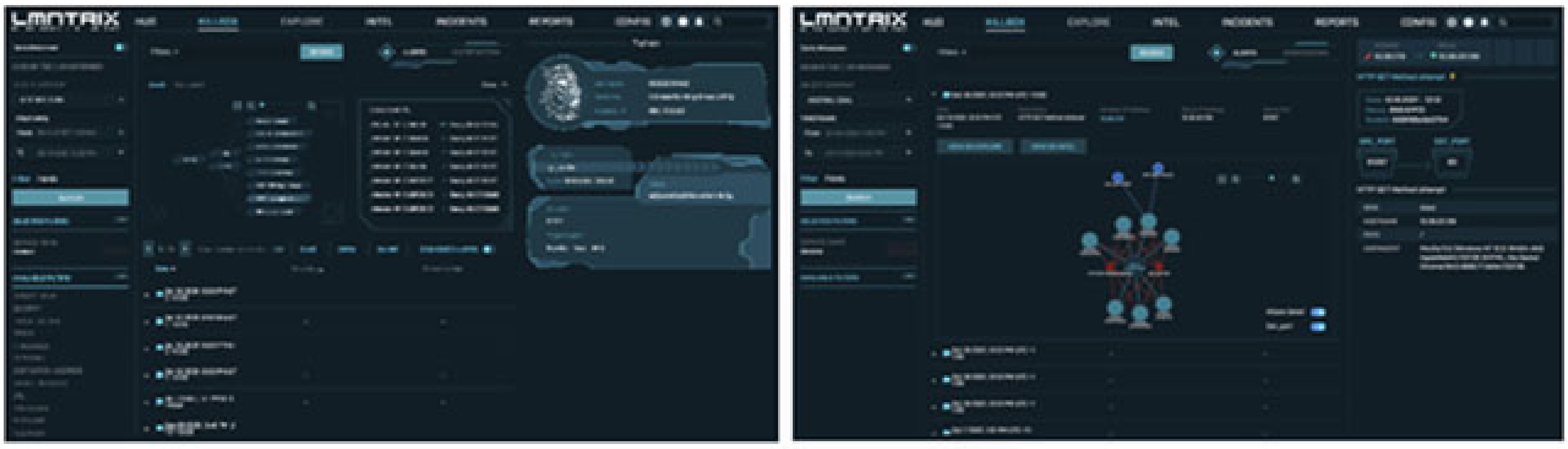


Figure 27 - LMNTRIX Deceive

LMNTRIX Deceive leverages an organization's network terrain to automatically create decoys and suggested breadcrumbs to alter the perception of the attack surface.

Key Benefits

- ✓ Reduce dwell time with a smart alarm system to detect threats inside your network
- ✓ Detect external attacks and insiders to expose reconnaissance and lateral movement
- ✓ Learn details of attack paths, resource interests and initial compromised foothold systems
- ✓ Remove blind spots for unknown assets including legacy systems, enterprise OT/IoT, and shadow IT
- ✓ Continuously profile and classify assets to facilitate deception layer creation and freshness
- ✓ Facilitate deception layer creation with full automation of decoys, including adaptation
- ✓ Decoy options to meet customer needs including real OS VM decoys, golden image OS decoys, and emulation decoys for low risk interaction and file uploads
- ✓ Lure attackers with breadcrumbs and tags on real assets and Active Directory to divert and defend
- ✓ High fidelity alerts you can trust
- ✓ Enable Red Team and Blue Team risk simulations to determine enhanced decoy and breadcrumb placement
- ✓ Native cloud based service running off the LMNTRIX XDR platform using on premise deployed deceptions, alerts reviewed, notifications configured, and devices managed.
- ✓ Change the parameters of cyber warfare, taking the attack to the attackers, exploiting their weaknesses to strengthen defenses.
- ✓ Seamless workflows into LMNTRIX Detect, LMNTRIX Hunt, LMNTRIX Respond and LMNTRIX Intel and LMNTRIX Recon

HOW DECEPTION WORKS

Deception becomes deterministic by publicizing decoys with breadcrumbs on real assets luring attackers, malicious insiders, and automated malware to the decoys. Instead of searching in vain for the bad actor within an ocean of good data, deception delivers actionable alerts and events from decoys, AD credentials, poisoned data, and traffic analysis. These alerts have extremely high fidelity. Using deception on-premises and cloud with fresh activity data creates persuasive deception layers that include devices, data, and behavior all designed to turn the tables on attackers. They pursue the lures to decoys so you can detect and defend.

Decoy Profiles

- Hardware — laptops, servers, routers, switches, cameras, printers, enterprise OT and IoT devices, etc.
- Software — OS, apps, databases, ports, services, applications, cloud assets, and similar data
- Decoys are unknown and obfuscated assets, no reason for employee access or use
- Consume attacker time with high and medium interaction decoys and distract from real assets

Breadcrumb, TAG & PERSONA Profiles

- Tags: Trigger an alert when copied, executed, or shared. Tags include files, documents, email, system resources, web services, databases, file shares, Custom exe, QR code, Slack/AWS API keys, etc.
- Breadcrumbs: Leads attackers to Decoys. Deployed on each machine's registry or memory. Breadcrumbs include pointers to databases, network shares, web services, application, or credential based
- Personas: Poisoned data, credentials, and profiles that attackers use (e.g. fake LinkedIn profiles)

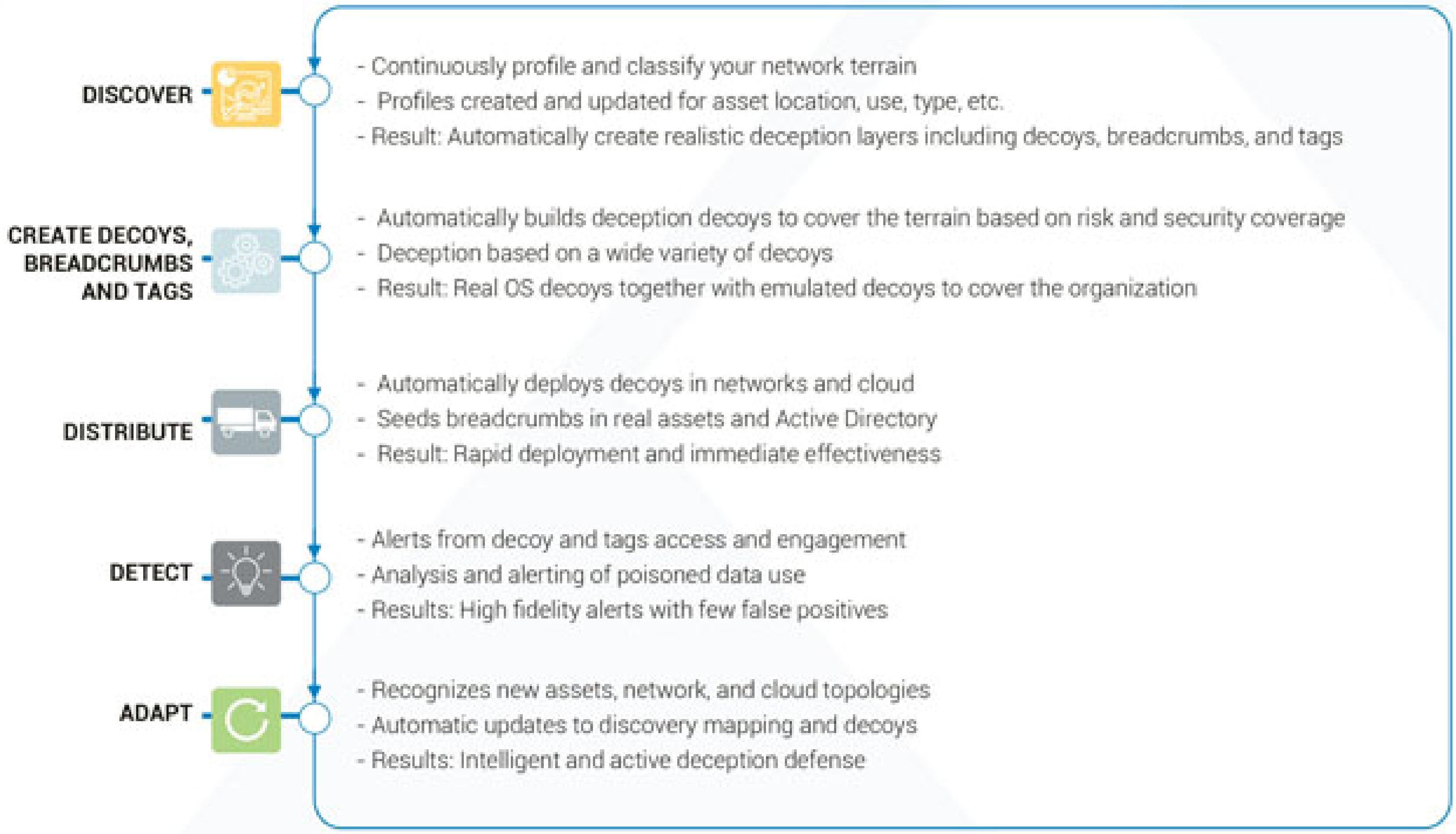
Detection of Post-Breach Attacks

- Data analysis showing the use of poisoned data (e.g. credentials)
- Monitoring attacker actions engaged with decoys and breadcrumbs
- Network analysis around decoys and data alerts

Active Deception

- Automates and adapts deployment of decoys, breadcrumbs and tags
- Detects lateral movement, attackers' reconnaissance and activities
- Visibility and forensics to learn TTPs (tactics, techniques, and procedures) and desired assets
- One platform with complete deception telemetry for analysis and hunting, and action

No impact to operations or users, no risk to data or resources



DISCOVER

- Continuously profile and classify your network terrain
- Profiles created and updated for asset location, use, type, etc.
- Result: Automatically create realistic deception layers including decoys, breadcrumbs, and tags

CREATE DECOYS, BREADCRUMBS AND TAGS

- Automatically builds deception decoys to cover the terrain based on risk and security coverage
- Deception based on a wide variety of decoys
- Result: Real OS decoys together with emulated decoys to cover the organization

DISTRIBUTE

- Automatically deploys decoys in networks and cloud
- Seeds breadcrumbs in real assets and Active Directory
- Result: Rapid deployment and immediate effectiveness

DETECT

- Alerts from decoy and tags access and engagement
- Analysis and alerting of poisoned data use
- Results: High fidelity alerts with few false positives

ADAPT

- Recognizes new assets, network, and cloud topologies
- Automatic updates to discovery mapping and decoys
- Results: Intelligent and active deception defense

LMNTRIX
BE THE HUNTER | NOT THE PREY

ABOUT **LMNTRIX**

LMNTRIX is the leader in intelligence led security-as-a-service. Working as a seamless, scalable extension of customer security operations, **LMNTRIX** offers a single MDR solution called Active Defense that blends our cyber defense platform called **LMNTRIX** XDR with innovative security technologies, nation-state grade threat intelligence and world-renowned Cyber Defence Centers. With this approach, **LMNTRIX** eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyberattacks. Our service differentiators include:

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, Network Forensics, UEBA and Deception Everywhere with completely automated attack validation, investigation, containment, and remediation on a single, intuitive platform.

LMNTRIX Tech Stack is a powerful proprietary threat detection stack that is deployed onsite, behind existing controls. It's made up of network sensors, endpoint agents and deceptions everywhere. It combines multiple threat detection systems, with machine learning, threat intel, correlation, static file analysis, heuristics, and behavior and anomaly detection techniques to find threats in real-time. It decreases alarm fatigue by automatically determining which alerts should be elevated to security events, and reduces false positives by requiring consensus across detection.

LMNTRIX Cyber Defense Centers - A global network of cyber defense centers that are complemented by our local partner SOCs, with highly trained and certified intrusion analysts who provide constant vigilance and on-demand analysis of your networks. Our intrusion analysts monitor your networks and endpoints 24x7, applying the latest intelligence and proprietary methodologies to look for signs of compromise. When a potential compromise is detected, the team performs an in- depth analysis on affected systems to confirm the breach. When data theft or lateral movement is imminent, our endpoint containment feature makes immediate reaction possible by quarantining affected hosts, whether they are on or off your corporate network while our automated network containment feature blocks the threat traversing your Firewalls or through our integration with cloud security solutions such as Zscaler, Netskope and Cisco Umbrella. This significantly reduces or eliminates the consequences of a breach.

TO LEARN MORE ABOUT **LMNTRIX** VISIT

https://lmntrix.com/

LMNTRIX USA.
333 City Blvd West, 18th Floor,
Suite 1805, Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65 3159 0639

LMNTRIX Hong Kong.
14F, Manning House, 38-48
Queen's Road Central, Central,
Hong Kong
+852.580.885.33

LMNTRIX Australia.
Level 32, 101 Miller Street,
North Sydney NSW 2060,
+61.288.805.198