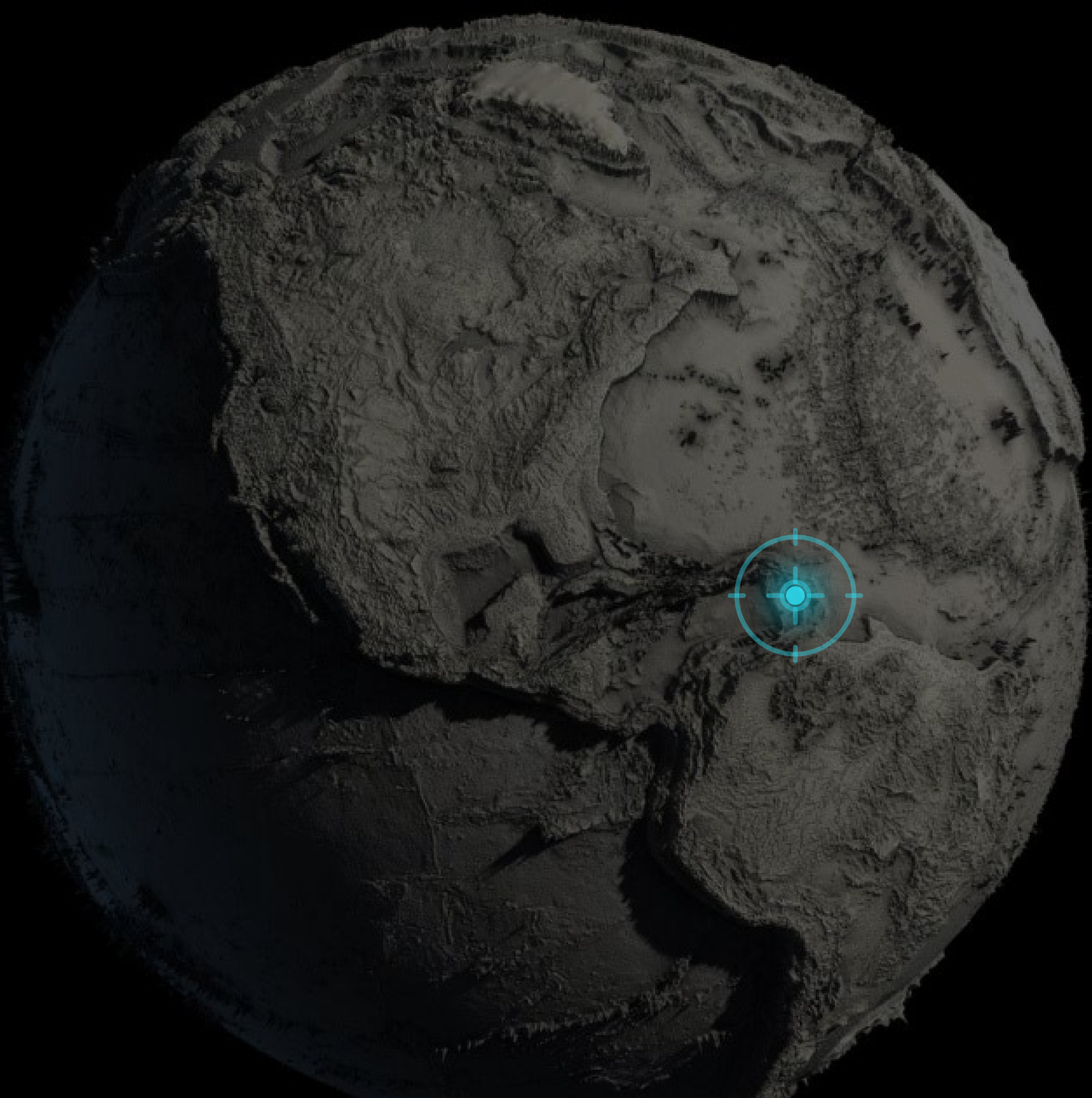
LMNTRIX
BE THE HUNTER | NOT THE PREY

TURNING INWARD

How Managed Detection and Response turns the table on attackers by focusing on the business, not the border



EXECUTIVE SUMMARY

For decades, cyber attackers have had the upper-hand against enterprises. This advantage grew more pronounced with the ever-increasing proliferation of digital technology; as modern market expectations changed, enterprises sought to digitise anything that could be digitised.

While the efficiency gains of modern technology cannot be disputed, every new business process brought online gave attackers one more potential avenue of compromise. With the ubiquity of mobile devices, an increasingly remote workforce, and the emergence of IoT, enterprise attack surfaces have never been larger.

This sprawling digital footprint is where attackers found their most significant advantage.

Adversaries only need to be successful once in order to completely compromise an enterprise. With more and more elements of the business exposed to the internet, finding a way in is only a matter of time.

It used to be said that the only certainties in life were death and taxes. As anyone who has worked in cyber security will tell you, a determined attacker will always find a way in. Considering this, the saying needs to be updated for the 21st century; the only certainties in life are death, taxes, and cyber-attacks.

The advantage given to adversaries from an increased attack surface was only compounded by the traditional defensive strategies employed against them. Enterprises fell victim to their own optimism. In thinking they could completely secure their environments from the outside world, they used medieval thinking to solve a modern problem.

It didn't work.

They sought only to fortify their borders, focusing on the perimeter. They thought if they built their walls high enough, they'd never be breached. With every defence looking outward, once an enterprise was inevitably compromised, they had little capacity to detect the intruder. As long as the external alarms weren't triggered, businesses thought they were safe. This false sense of security gave attackers all the time in the world once they were inside a network – they could move laterally, spending months combing the environment for the most damaging and valuable data.

Depending on their motives, they might seek to shut down operations, steal IP or pilfer customer data. With no one looking for them, they could stroll along and sight-see across the enterprise, picking up souvenirs like a tourist in a market.

But now the holiday's over.

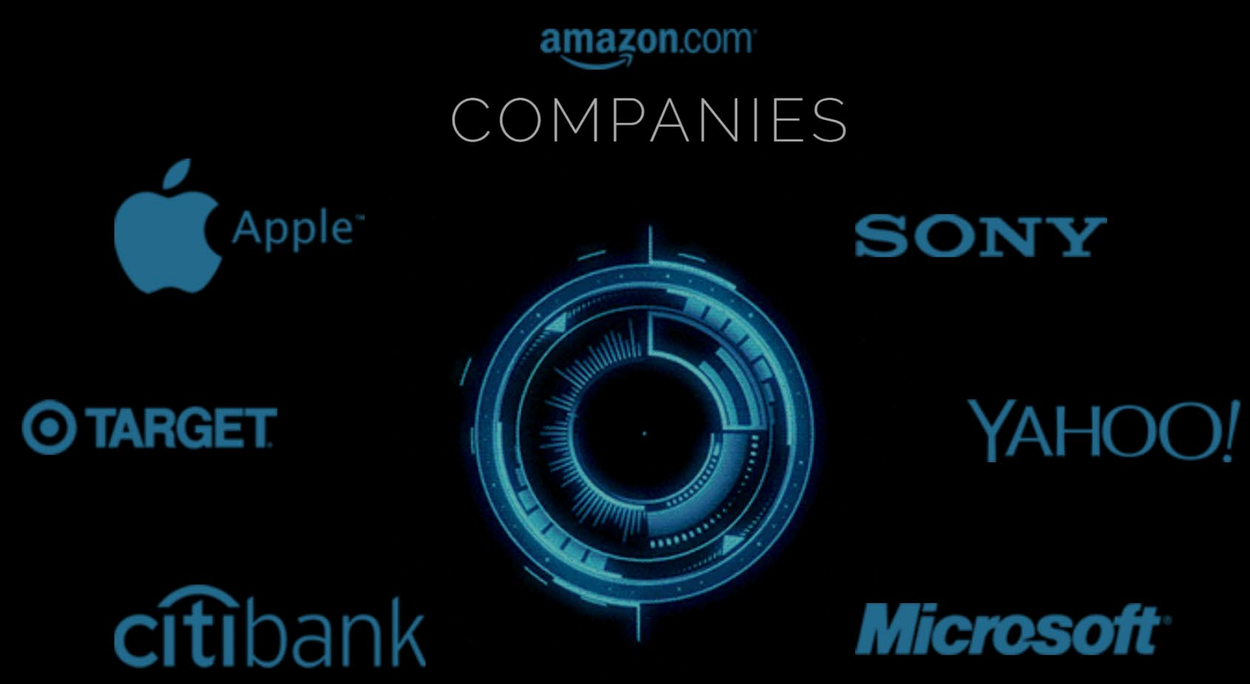
Managed Detection and Response (MDR) reimagines cyber security. It takes the traditional security mind set and turns it on its head. By realising that an enterprise's borders can never be completely secured, it turns the attention inward and, in doing so, it turns the tables on attackers.

By focusing on the detection of attacks that breach the perimeter, breaches can be rapidly recognised and responded to. This significantly reduces the time an attacker has within a network and nullifies their ability to do material harm.

This whitepaper will explore how this inward focus takes the advantage away from cyber attackers and finally levels the playing field.

INTRODUCTION

Perhaps the greatest proof that any determined attacker will eventually succeed is the calibre of names included in post-breach headlines. The list is a who's who of global organisations and includes the likes of Target, Sony, Yahoo, and Equifax.



All were incredibly successful, multi-million-dollar global companies, but all were unable to protect themselves from motivated adversaries.

Recognising the reality of cyber security – that no perimeter is impenetrable – is what lies at the heart of MDR. As a defensive strategy, it shifts the focus from prevention and to detection. Rather than looking outward, MDR turns the attention inwards and seeks to mitigate the damage once an attacker breaches the perimeter. Perhaps the best definition of MDR comes from Gartner:

> "A focus on threat detection use cases, especially advanced or targeted attacks that have bypassed existing perimeter controls (e.g., next-generation firewalls [NGFWs], secure web gateways [SWGs], network intrusion detection systems [NIDSs], endpoint security)... Delivery of services usually using a vendor-provided stack of network- and host-based controls (e.g., commercial, open source or provider-developed). These tools are not only positioned at the traditional internet gateways, but are also inward-facing to detect the threats not typically discovered by traditional perimeter security technologies."

While still a relatively new approach to cyber security, the MDR market is growing rapidly, with Gartner predicting: "By 2020, 15% of organisations will use MDR services, up from fewer than 5% (in 2018)." Further, Gartner also predicts that by 2020, 60% of enterprise security budgets will be allocated to detection and response, up from less than 30% in 2016.

There are many reasons behind this growth, but perhaps the two most prominent are the growing realisation of the consequences of a data breach, and an increasing frustration with traditional methods.

Every year, various studies attempt to quantify the cost of a data breach and every year the results are sobering. According to a recent IBM and Ponemon Study, the average cost of a data breach is US$3.62 million. If that figure weren't enough to give any business executive pause, this study's focus was only on breaches involving stolen customer records – it does not include data for breaches in which intellectual property, trade secrets or confidential business information were taken.

Adding to the business realisation of the gravity of a data breach is the global trend towards legislation mandating impacted consumers be notified in the event of a breach. Like with Europe's GDPR or Australia's NDB scheme, fines of up to US$26 million can be imposed on organisations who fail to notify customers of a breach in a timely manner.

With the reality of a breach so stark, it is no wonder the traditional controls are now being questioned. In the same Ponemon study, the average time it took to identify a breach was 191 days. That's more than six months that an attacker spent undetected within the victim organisation's network.

Below, we'll outline three of the most common ways in which traditional controls and strategies fail, and highlight how MDR solutions, like the LMNTRIX Active Defense solution using the LMNTRIX Grid, overcomes these deficiencies.

The average cost of a breach is
US$3.62 million
Ponemon 2017

LMNTRIX ACTIVE DEFENSE SOLUTION:
A validated threat detection and response architecture that hunts down and eliminates the advanced and unknown threats that bypass perimeter controls.

The LMNTRIX Grid is a cyber defense SaaS platform that provides a new utility model for enterprise security, delivering pervasive visibility, with 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 systems (ICS) networks.

1. TRADITIONAL DEFENCES CAN'T DETECT OR RESPOND TO TARGETED TACTICS

The SIEM, SOC and MSSP model was conceived in the late 90's and not much has changed since then in the way networks are monitored and managed. During this same time period, the way attackers target, compromise, and exploit organisations has changed significantly – in favor of the adversary.

The tech industry loves to boast about 'agility', but traditional security strategies couldn't be more cumbersome.

Most MSSPs rely on signatures and rule-based detection. This is effectively static pattern-matching and the tactic frequently fails to identify threats – both advanced and basic. The reason signature-based detection fails, is because it only works if attackers use the same code all the time. Attackers are always one step ahead against these tools because once a campaign or malware variant has been identified, a few slight tweaks to the code means they can bypass defences all over again.

This matter is made worse with the focus on prevention, rather than detection. Once an attacker has successfully penetrated the perimeter, traditional MSSP and SOC models have little – if any – ability to detect the intruder.

Even if these legacy providers could detect the threat, they then offer little in the way of response because the customer is ultimately responsible for containment and engagement.

MDR solutions like LMNTRIX were borne as a necessity to help close the gap left in the market from the traditional models.

Rather than rely on signature-based methods, the LMNTRIX Grid uses advanced techniques such as machine learning, intelligence, endpoint detection and response (EDR), behavioral analytics, sandboxing, retrospection, deception and forensics capabilities to rapidly detect any malicious behavior. Critically, this capability is driven by a threat analyst who hunts down and isolates suspicious behavior. This proactive threat hunting means attackers have nowhere to hide. In short, it takes a human to catch a human.

Further, instead of just notifying the customer that a threat has been detected, LMNTRIX then responds to the threat and evicts the attacker from the network – nullifying their ability to do material harm.

"More than 90%
of our clients that were breached had an existing SOC or MSS"
Carlo Minassian
Founder & CEO LMNTRIX

$1.27 million dollars
wasted responding to erroneous or inaccurate malware alerts.
Ponemon 2015

2. ORGANISATIONS LACK RESOURCES TO PROPERLY INVESTIGATE, ANALYSE, AND PRIORITISE ALERTS

Most enterprises have invested in Security Information and Event Management (SIEM) or use an MSSP whose service relies on one. SIEMs promise to provide real-time analysis of security alerts generated across an environment. While the promise of the SIEM has proven seductive, the reality is another matter.

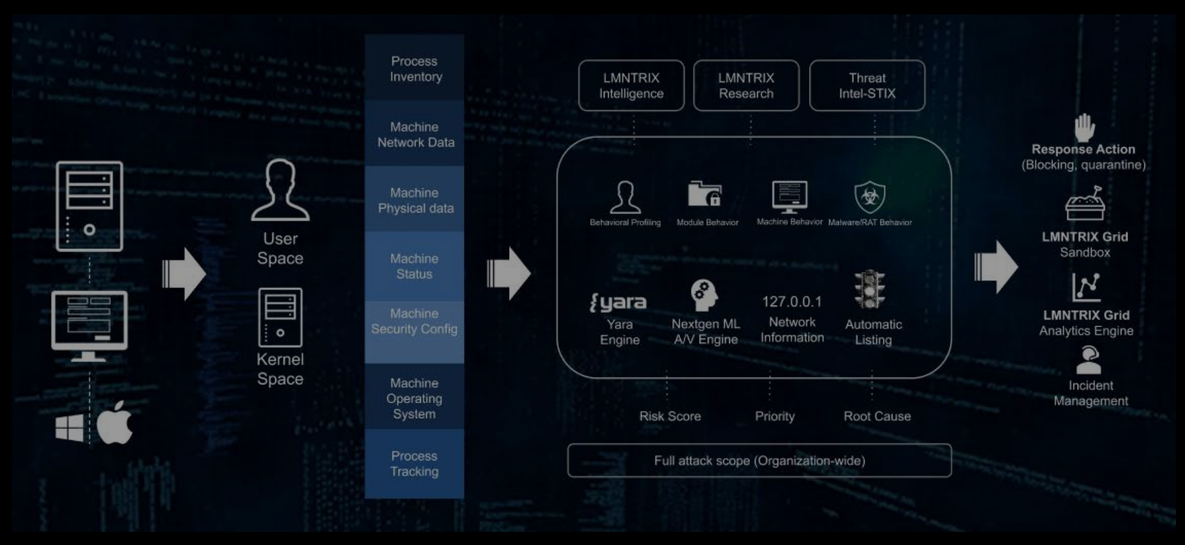
> Security information and event management is a crucial and widely used security technology, yet many security architects struggle to get value from their often expensive deployments.
> Gartner 2016

Not only are these technologies extremely expensive, they are notoriously difficult to run and manage. One of the biggest issues with SIEMs is the sheer volume of alerts and false positives they generate.

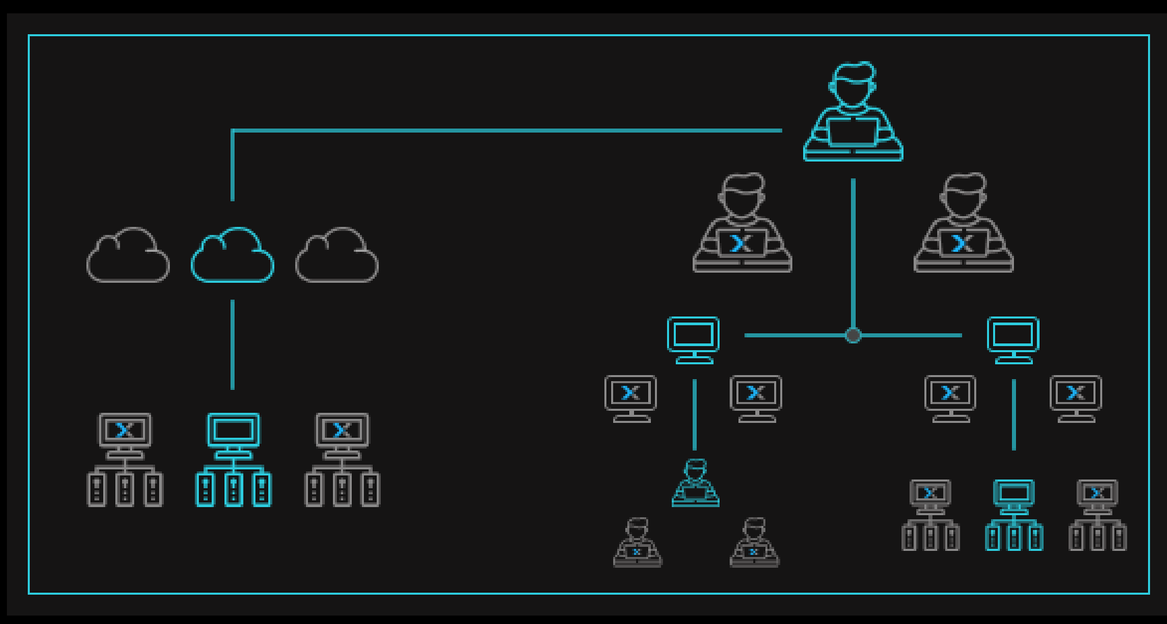
According to a survey from Enterprise Management Associates, 79 per cent of security teams reported they were overwhelmed by the volume of alerts. This phenomenon results in what is known in the industry as 'alert fatigue'. This is where analysts have no choice but to ignore alerts as they attempt to weed out the serious threats. Alert fatigue is a serious issue in cyber security. One recent survey reported 72 per cent of security teams suffered from alert fatigue. Unfortunately, this static gives attackers the perfect cover to slip by undetected – SIEMs promised to help find a needle in a haystack, but all they've done is provide more hay.

In other words, even if the traditional security model was able to detect an intrusion, it is unlikely it would be acted upon because the alert would be drowned out by thousands of false positives.

The LMNTRIX Active Defense solution was designed specifically to address this challenge. Rather than inundate the client with a flood of false positives, LMNTRIX analysts validate every breach before it is escalated. By continuously monitoring the network for anomalous behavior and reverse engineering malware, rather than relying solely on logs and alerts, clients are only notified of actual breaches.



By thinking like the attacker, the intruder can be tricked into giving themselves up. LMNTRIX enshrouds every endpoint, server and network component in a deceptive parallel universe. From the instant an attacker penetrates a network, all they can see is an illusive mirage where every single data packet is unreliable. As this deceptive environment is completely separated from the real network, the moment an attacker attempts to interact with data, analysts are immediately notified, and the threat can be mitigated.



LMNTRIX enshrouds every endpoint, server and network component in a deceptive parallel universe

3. THREAT INTELLIGENCE DOESN'T FACTOR THE HUMAN ELEMENT

Not only do MDR providers have a better idea of what's happening inside an organisation's network, they have a broader view of what's happening on the outside too.

Traditional threat intelligence platforms focus on sharing signatures in an attempt to try and keep up with the shifting tactics of attackers. This reactive approach waits for an attack to be levelled and discovered and does little to guard against sophisticated attackers who are constantly updating their methods.

This level of threat intelligence is better than none – but not by much.

The best way to gain the upper-hand against a cyber attacker is to understand the person, not just their tools. When hackers steal data, it almost always finds its way to an online black market – the deep and dark web – the back alley of the cyberworld where illegally obtained data is bought and sold.

Advanced MDR solutions like LMNTRIX shine a light on the deep and dark web. Whether an attacker has stolen data and is looking to sell it online, or if someone is planning to breach an organisation and is seeking advice on how to do so, the attacker's own platforms can be used against them and the attack can be prepared for in advance.

This is true intelligence. Getting to the heart of the human behind the attack and staying one step ahead in order to anticipate their actions.

ADVERSARY INTELLIGENCE
from hundreds of threat researchers embedded deep within the adversaries' development ecosystem that provide insight into the earliest stages of the attack

VICTIM INTELLIGENCE
gained from over a decade on the front lines investigating the world's most consequential breaches

MACHINE INTELLIGENCE
derived from analysis of global detection technology provides real-time visibility into attack telemetry and proliferation

GEO-POLITICAL ANALYSIS
by experts from diverse domains who rigorously track and analyse the financial and political dimensions of thousands of cyber threats worldwide

CONCLUSION

No cyber perimeter is impenetrable. It never will be. This fundamental truth may be difficult to accept, but it must form the basis of any effective security strategy.

Whereas the traditional security approaches have focused on bolstering the border, not enough attention has been given to detecting attacks that bypass these defences. This lack of inward-focus gives attackers almost unfettered access to an organisation's network once they successfully evade the firewalls and anti-virus that the business depended on for defence.

MDR solutions, like the LMNTRIX Active Defense using the LMNTRIX Grid, finally give organisations the ability to rapidly respond to attacks before they cause serious harm. The reason they're able to do this is because they've accepted the reality of cyber security – a motivated attacker will eventually succeed.

By thinking like the attacker, and by using humans to catch a human, MDR turns the tables. Proactive forensic and investigation methods mean adversaries have nowhere to hide. They might be able to breach the perimeter, but once inside they won't be able to steal data or IP, destroy critical infrastructure or bring business to a halt.

Through advanced MDR solutions, enterprises can finally become the hunter, not the prey.

ABOUT LMNTRIX ACTIVE DEFENSE

The LMNTRIX Active Defense is a validated and integrated threat detection and response solution for addressing advanced and unknown threats that bypass an organisation's perimeter controls.

We use a combination of advanced network and endpoint threat detection, deceptions everywhere, analytics and global threat intelligence technology. These are complemented with continuous monitoring together with threat hunting both internally as well as on the deep and dark web. It is a fully managed, security analyst delivered service that defends against zero-day attacks, and advanced persistent threats from our cyber defence centre, 24 hours a day, 7 days a week.

LMNTRIX
BE THE HUNTER | NOT THE PREY

CONTACT US

LET US HELP YOU IMPROVE YOUR ENTERPRISE NETWORK SECURITY.

WE'D LOVE TO HEAR FROM YOU.

GENERAL

Email: info@lmntrix.com

Tel: +1.888.958.4555

SALES

US
333 City Blvd West, Suite 1805, Orange,

CA 92868 USA

Email:sales@lmntrix.com

Tel: +1.888.958.4555

HONG KONG
Room 1102, 11/F, Kenbo Commercial Building, 335-339

Queen's Road West, Sai Ying Pun, Hong Kong

Email: sales@lmntrix.com

Tel: +65.3159.0639

AUSTRALIA
Level 5, 155 Clarence St, Sydney, NSW

Email: sales@lmntrix.com

Tel: +61.288.805.198

SINGAPORE
60 KAKI BUKIT PLACE, #05-19, EUNOS

TECHPARK

Email: sales@lmntrix.com

Tel: +65.3159.0639

UK
Kemp House, 152 – 160 City Road, London, EC1V 2NX

Email: sales@lmntrix.com

Tel: +44.808.164.9442

MEDIA

Email: press@lmntrix.com

Tel: +1.888.958.4555

CAREERS

Email: careers@lmntrix.com

Tel: +1.888.958.4555

SOCIAL MEDIA

FACEBOOK

CRUNCHBASE

TWITTER

LINKEDIN

SUPPORT

Email: cdc@lmntrix.com

Tel: +1.888.958.4555

For more information on LMNTRIX, visit:

lmntrix.com or **info@lmntrix.com**

LMNTRIX
BE THE HUNTER | NOT THE PREY