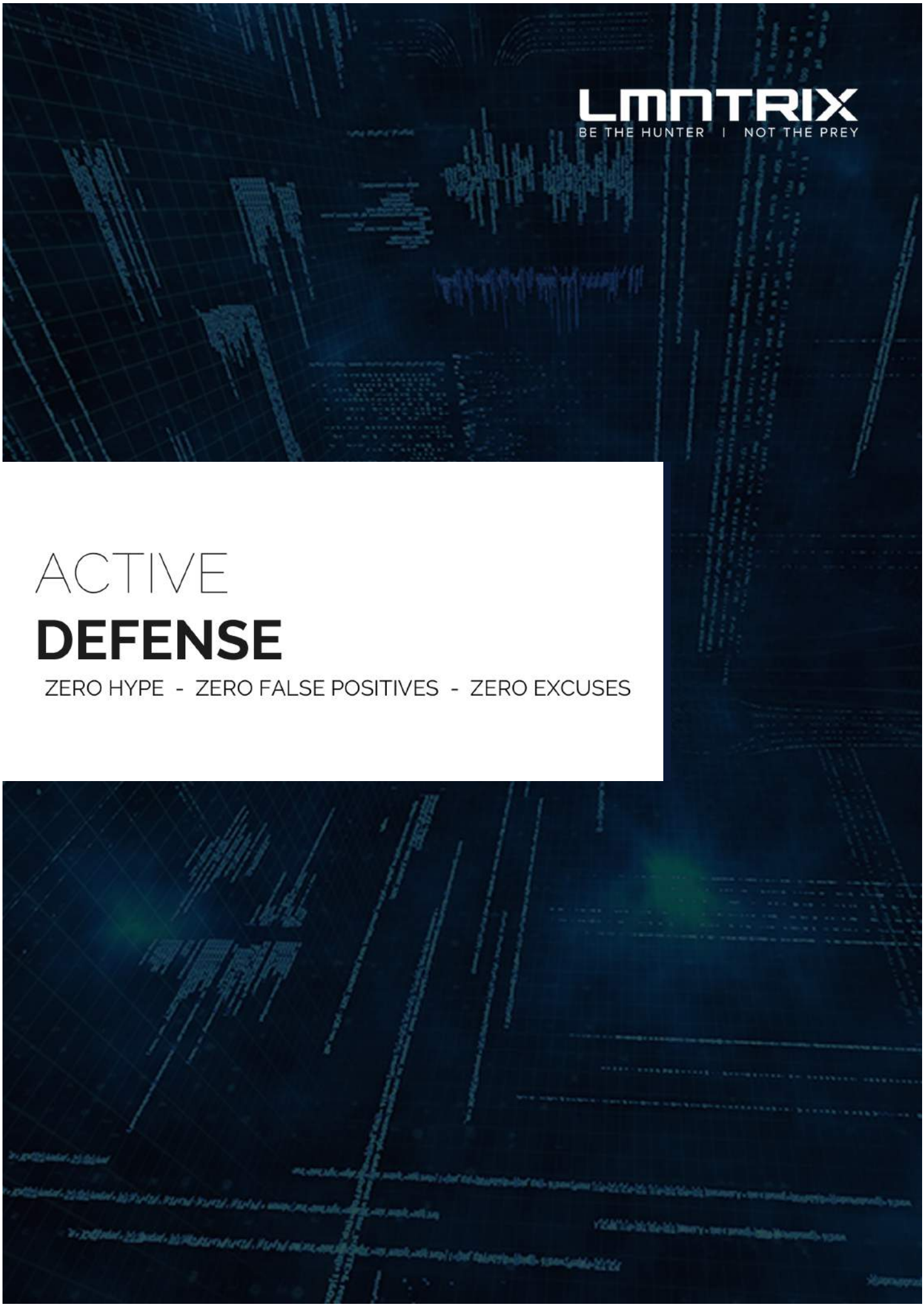

LMNTRIX
BE THE HUNTER | NOT THE PREY
ACTIVE
DEFENSE
ZERO HYPE - ZERO FALSE POSITIVES - ZERO EXCUSES

# TODAY'S REALITY: **UGLY.**

We are at a cybersecurity crossroads. Go one direction, it's just more of the same, and you will lose. You'll waste precious resources on the next silver bullet and the hackers will eat you alive anyway.

Go the other direction, embrace the future of cyber security and the tables will instantly be turned in your favor. Hackers hate us, because we ruin their business model when we keep yours safe.

First things first. It's not about the money. Here's why.

Target, Sony, RSA, Ebay, Anthem, the US Military, Heartland, Dropbox, JP Morgan Chase, Home Depot, Linkedin, Adobe, the NSA, and a thousand others that shall remain un-named, were investing millions of dollars per annum on their cyber security programs. Many had security forces of hundreds of experts together with shiny SOC's and the latest next generation sandboxes, firewalls, SIEM's, EDR, you name it, but when it mattered . . .

They. Just. Didn't. Know.

The truth is money doesn't buy security anymore.

With the median number of days before a breach is detected at 229 and 67% of companies only learning of a breach when an external entity tells them, it is obvious something needs to change.

According to Gartner, the current blocking and prevention tecniques are failing, and cybersecurity spending is incorrectly skewed, leading to budgets that cannot meet the threats. Currently, protection and prevention comprises 85% of total spend and detection, monitoring and intelligence only 15%.

Most organisations are relying on solutions that sounded great 15 years ago. 15 years! That's a few hundred years in digital years with the hyperfast pace of change.

Back then SIEM, IPS, NGFW, WAF, Email and Web Gateway dominated —with some malware sandboxing thrown in. Today, many know these approaches aren't working, but they keep doing them anyway because they don't think they have a choice.

LMNTRIX
BE THE HUNTER | NOT THE PREY

LMNTRIX
BE THE HUNTER | NOT THE PREY

# OUR EXTENSIVE RESEARCH HAS POINTED OUT **THREE SERIOUS PAIN POINTS.**

"Raise your hand if you identify:"

**1.Alert Fatigue.**
Only one percent of all attacks are detected through logs. This is an astounding number and SIEM has proven to be a particular failure. Interviews with IT teams delivered this frustrated indictment of SIEM: "Stupidly Irrelevant Electronic Messaging" (actually they called it something a whole lot worse, but we're too polite to say that here). They said SIEMs produced too many alarms. MSSPs aren't doing much better for those who depend on them. Even medium-sized organizations can receive as many as 200-300 alerts per month from their MSSP and are then left with no idea what to do with them. The result is that alarms drone on while hackers roam free.

**2.Lack of Breach Validation.**
The hackers roam free because companies have no way to confirm if these alerts are actual incidents. It is too time consuming and costly to investigate, and their security teams lack skills to respond to advanced threats. Imagine being told by the police that someone may have broken into your house but it was up to you to investigate further that's the situation most companies are in it's wrong and needs to be fixed.

**3.Fortress Mentality.**
Even though it should be clear by now that hackers are in the inside, organizations cling to the illusion that cybersecurity means keeping bad things out. This is about cyber-purity not true cybersecurity. It is a dangerous fantasy that does not reflect the inevitability of cyber intrusion. By holding onto it, organizations are unable to respond properly to threats. This mentality is why Gartner is correct in saying the current blocking and prevention techniques are failing, and cybersecurity spending is incorrectly skewed.

LMNTRIX
BE THE HUNTER | NOT THE PREY

**What** is also clear is that organizations are lousy at building their own SOCs (Security Operations Centers). When they do, all the shiny new kit, the NextGen Firewalls and AV, Sandboxes, and Endpoint Detection & Response solutions don't work just like their IPS, DLP and SIEM never worked. They sit idle, unpatched, untuned, unlistened to. Part of the challenge is finding, recuriting and retaining the best security team. But just telling the good from the bad is next to impossible for most companies let alone building a team of true experts. Even significant SOC investments fall flat a fact that many companies are now admitting as they abandon in-house SOC programs.

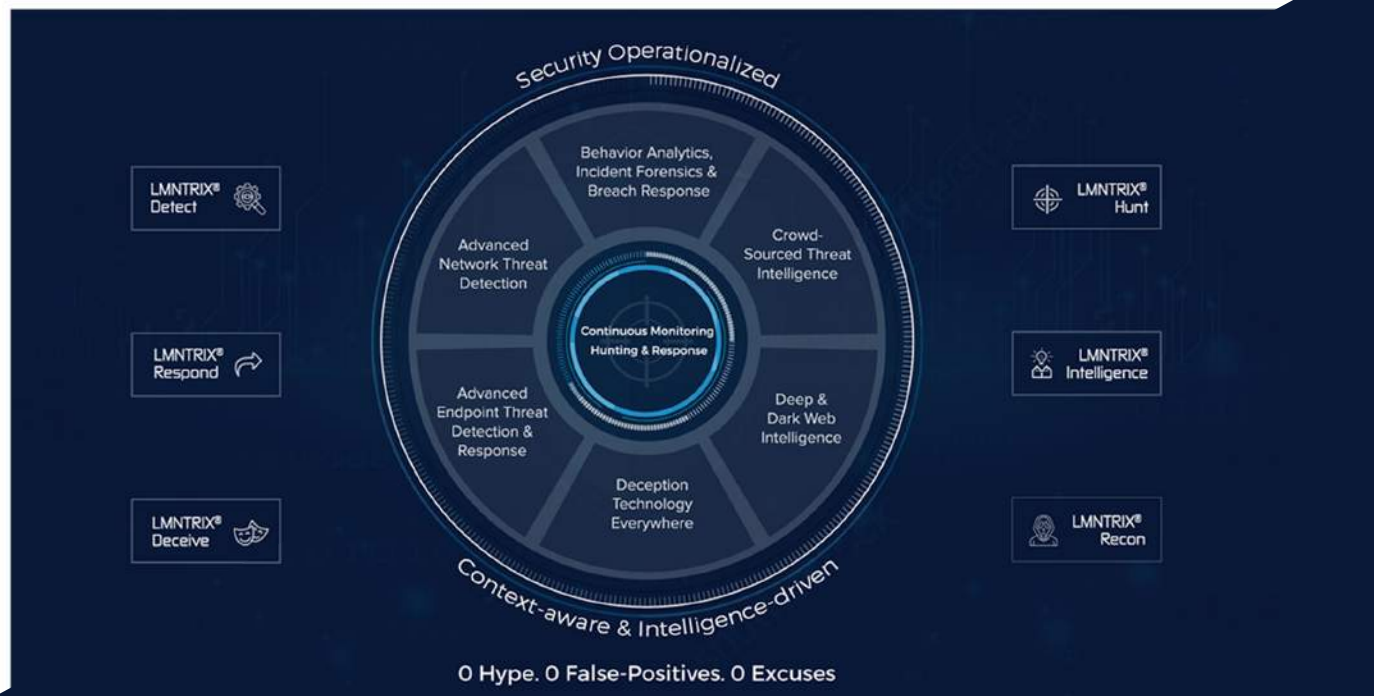
**Not** only that, we live in a networked world built on the weakest of foundations: insecure code. Insecure code leaves everyone with big vulnerabilities. This isn't going to change. Why? Because even if AI magically comes along to patch all the insecure code, it won't be able to patch all the insecure people. The other weak link will always be the human factor. Case in point. Recently Carlo's own mom opened a phishing email for the second time and he had to quarantine and rebuild her computer again. It didn't matter how many times Carlo had warned her about opening suspicious emails, she still did it. Mom!

The truth is that Carlo's Mom isn't alone. People like her work across most organisations. They are smart and good at what they do, but are impossible to train when it comes to cybesecurity. Continuous User Awareness Training does some good, but it will never be enough.

**The bottom line?** Organizations need to make a mental shift that sees them embrace a more dynamic approach to security that turns the battle in their favour. They need to think differently about how to detect and respond to threats.

Luckily, there's a way.

INTRODUCING
# ACTIVE DEFENSE.




At LMNTRIX, we think like the attacker and prize detection and response. When we hunt on your network and your systems, you cease to be the prey. We turn the tables on the attackers, shifting the cost to them and changing the economics of cyber defence. We strategically weave illusion into your entire network, coating every endpoint, server and network component with deceptions, creating a environment naturally hostile to a hacker. When attackers are unable to determine what data is real and what is not, their ability to make decisions vanishes and their attack is paralyzed.

We call this Active Defense. Active Defense is a validated and integrated threat detection and response architecture that addresses unknown and advanced threats that slip by perimeter controls.

Our methods are unique and powerful, combining advanced network and endpoint threat detection, deceptions everywhere, analytics and global threat intelligence technology. Wrapped around this technology is continuous monitoring that can be further strengthened by best-in-class threat hunting that is both internal and outward facing, capable of scouring the deep and dark web.

In short, the LMNTRIX Active Defense is a fully managed, security analyst delivered service. 24 hours a day, 7 days a week, it defends you.

lmntrix.com

LMNTRIX
BE THE HUNTER | NOT THE PREY

# THE NUTS **AND BOLTS**

**Active Defense** is composed of seven proprietary technologies. Each technology is powerful on its own. Put them all together and that power is unprecedented. An offering so smart, so multi-faceted and so robust that attackers are quickly worn down and sent packing.

**LMNTRIX Detect** is designed to catch those threats, known and unknown, that bypass your perimeter controls. It uses a proprietary virtual sensor to deliver integrated, multi-layer detect-in-depth capability.

**LMNTRIX Deceive** is an attacker's worst nightmare. Deceive weaves an illusive layer over your entire network, coating every endpoint, server and network component with deceptions. If an attacker doesn't know what's real, an attacker can't act.

**LMNTRIX Intelligence** taps the power of the community to protect you. We aggregates over 650 million IOCs from 300 threat intelligence sources including our global sensor network and then we correlate these findings directly to your real-time network data, mitigating threats long before others even know they exist.

**LMNTRIX Respond** keeps your endpoints safe by deploying light touch sensors and then using behavioral monitoring and machine learning in conjunction with our intrusion analysts to quickly identify, quarantine and block threats.

**LMNTRIX Hunt** is the hunter with a thousand eyes. We use proprietary packet capture technology combined with behavior analytics, retrospection, anomaly detection and proactive threat hunting to deliver visibility so pervasive and stealthy that even the most challenging threats are detected in real time.

**LMNTRIX Recon** is your canary in the coal mine. Recon looks outside your network to find evidence of a breach or one that might be in the works. Our team's knowledge and proprietary techniques go where others cannot, the deep and dark web, by using the attacker's platforms against them so you can be certain of your defenses.

**LMNTRIX ThinkGrid** is the perfect SIEM replacement because not only does it collect logs and help you meet your compliance mandates —it goes further, using machine learning algorithms that get smarter every minute. Our platform analyzes your data, finds anomalies, links them together and tells the story behind advanced threat activity and operations issues. Our algorithms don't require you to write rules, create thresholds, or anticipate every possible move a hacker might make. Most importantly our algorithms are based on your data, to ensure accuracy. Because the only way to know what's "abnormal" is to know what's normal for your organization.

LMNTRIX
BE THE HUNTER | NOT THE PREY

CONTINUOUS
**IS EVERYTHING.**

Continuous is the key. Hackers never stop and we don't either. We shift your security mindset from "incident response" to "continuous response." Continuous response assumes that systems are already compromised and require ongoing monitoring and remediation. Continuous means we are always alert and you stay safe.

No matter what subscription level you choose (and you can check those out below), one thing never changes: our people and their commitment to continuous. They are fierce, smart and always on — the best of the best. Together these highly trained, certified intrusion analysts form an ever vigilant, on-demand, global cyber defense centre (CDC) network.

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 before moving to contain and remediate the endpoint.

# HOW **ACTIVE DEFENSE FITS YOU.**

LMNTRIX BE THE HUNTER | NOT THE PREY

LMNTRIX Active Defense provides three subscription levels so you can appropriately supplement your team's skills and risk tolerance, keeping you safe and your costs in check.

## ACTIVE DEFENSE **SUBSCRIPTION LEVELS**

| SUBSCRIPTION ELEMENTS | FOUNDATION | ENHANCED | PREMIUM |
|---|---|---|---|
| LMNTRIX DETECT | X | X | X |
| LMNTRIX RESPOND | X | X | X |
| LMNTRIX INTELLIGENCE | | X | X |
| LMNTRIX DECEIVE | | X | X |
| LMNTRIX HUNT | | | X |
| LMNTRIX RECON | | | X |
| LMNTRIX THINKGRID | X | X | X |

## FOUNDATION

Foundation uses a combination of advanced network and endpoint detection sensors, to constantly monitor your network and accelerate your response with expert analysis from senior intrusion analysts who validate and investigate alerts and provide detailed compromise reports for each confirmed threat. We then go a step further and contain and remediate incidents for you so you can sleep through the night.

This service delivers a continuous network and endpoint monitoring service using behaviour of malware rather than signatures and is ideal for detecting encrypted threats that bypass perimeter controls and detonate on the endpoint.

The service includes exploit prevention, hunting down and blocking or quarantining malware missed by other solutions, automated network perimeter threat containment and helps reduce alert escalations by 95% by first validating breaches on your endpoints before escalating them to you. Furthermore, we help you reduce incident response time from days to minutes by finding all other infected machines and the exact location of malicious files on your network.

When data theft or lateral movement is imminent, our endpoint blocking and quarantine feature makes it possible to react immediately by blocking or quarantining affected hosts, whether they are on or off your corporate network, significantly reducing or eliminating the consequences of a breach.

LMNTRIX ThinkGrid provides unlimited log management and SIEM capability deployed onsite or in the cloud, so that you can meet your log management and compliance requirements.

Accountability and responsiveness is key. This is our stock in trade. We stay close to you and your specific needs. You will be paired with a designated investigation manager. Not only does this person have deep incident analysis and investigation skills, they are always current with your environment. They are deeply familiar with your specific network goals and provide the best incident management available.

Quickly engage remote expert incident responders from our CDC or engage onsite incident response from one of our locally certified partners, when needed, to investigate breaches, re-secure your network, remediate technical damage and assess the business impact so you can make prompt and accurate disclosure, if necessary.

The Foundation subscription level is the minimum service recommended to all organizations to help defend against todays evolving threat landscape.

LMNTRIX
BE THE HUNTER | NOT THE PREY

## ENHANCED

Enhanced adds intelligence and deceptions everywhere. LMNTRIX Intelligence adds an additional layer of detection capability against known, unknown and encrypted threats while LMNTRIX Deceive is a post breach strategy for detecting human attackers and red teams that have established foothold and now looking to move laterally.

The Enhanced subscription level offers a stronger security posture suitable for mid to large organizations that have a medium risk tolerance.

## PREMIUM

With the Premium subscription level our hunting team actively pursue adversaries in your network by deploying our hunting platform that uses retrospection, anomaly detection combined with behavior analytics and data science modelling techniques to find attackers hiding in remote corners of your network.

This service involves the proactive, stealthy, and methodical pursuit and eviction of adversaries inside your network without relying on IOCs. Our team of expert intrusion analysts and threat hunters 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 attack.

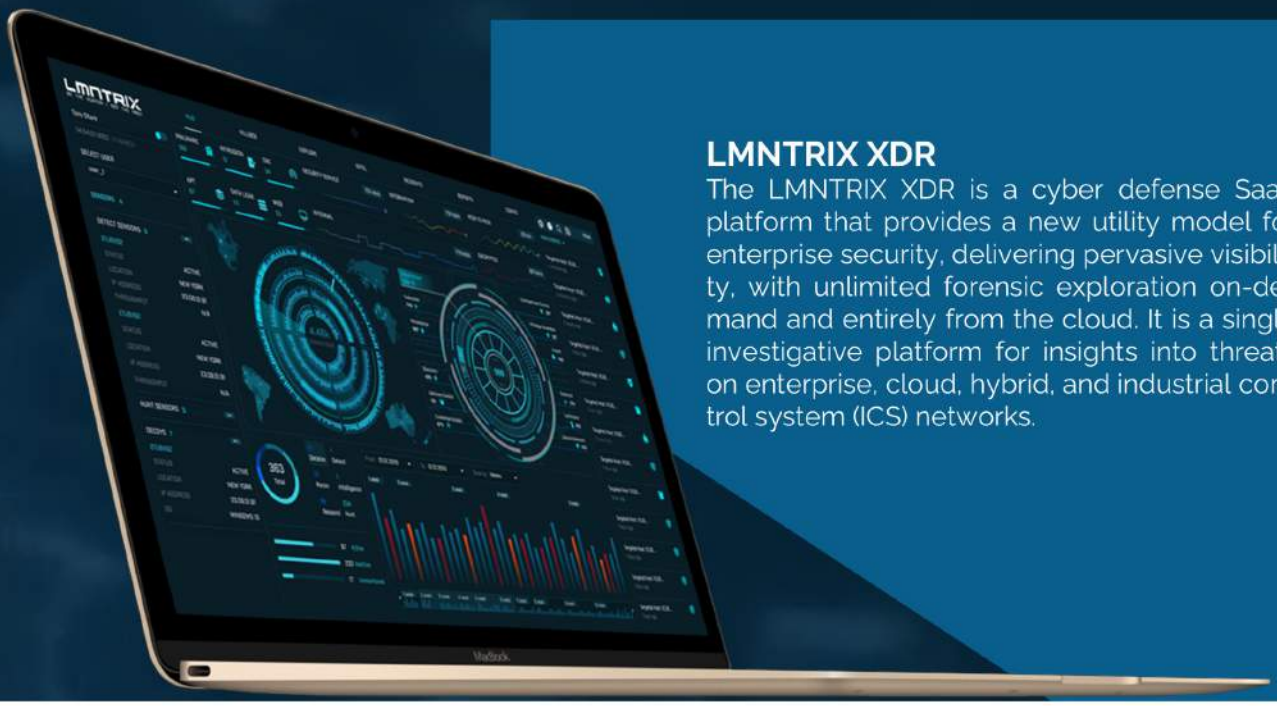
Our intrusion analysts leverage intelligence, deceptions, deep & dark web monitoring, multi-vector network threat detection, together with endpoint and network forensics capability on live systems to investigate, classify, and analyze the risk in real time. Detailed reports on exactly what happened and recommendations on how to contain the threat are immediately provided.

Finally, we complement your internal network hunting with external deep and dark web hunting services with the gathering of the most salient data publicly available on the internet about you and providing meaningful, timely, relevant, and actionable insights through a fusion of technology and subject matter expertise.

The Premium subscription level offers an Advanced security posture suitable for large organisations that have a low risk tolerance.

LMNTRIX

BE THE HUNTER | NOT THE PREY



## LMNTRIX XDR

The LMNTRIX XDR 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 system (ICS) networks.

## LMNTRIX Active Defense Features

| FEATURE | ACTIVE DEFENSE |
|---|---|
| 24 X 7 Monitoring | ✓ |
| End-to-End Management | ✓ |
| Endpoint Visibility | ✓ |
| Network Visibility (Selective PCAP) | ✓ |
| Log Visibility (on-premises & cloud) | ✓ |
| Additional Cloud Visibility (beyond log, endpoint & vulnerability | ✓ |
| Deceptions Everwhere | ✓ |
| Deep & Dark Web Intelligence | ✓ |
| Proactive Threat Hunting | ✓ |
| Active Threat Hunting | ✓ |
| Forensic Investigation | ✓ |
| False Positive Reduction | ✓ |
| Managed Remote Host Tactical Threat Containment | ✓ |
| Managed Remote Network Tactical Threat Containment | ✓ |
| Managed Remote Cloud-Based Threat Containment | ✓ |
| Unlimited Remediation Support | ✓ |
| Automated Known Threat Response | ✓ |
| Powerful Visualizations | ✓ |

# ACTIVE DEFENSE
# IN ACTION

LMNTRIX
BE THE HUNTER | NOT THE PREY

Let's use a real world example to show how Active Defense stacks up.

Deep Panda, or Shell Crew, continues to be a formidable threat group, actively attacking organizations and stealing data. Deep Panda is a prime example of an advanced persistent threat that is able to breach networks and then remain inside enterprises for years before detection.

The following diagram uses the Deep Panda threat profile to show how each element of the LMNTRIX Active Defense works together to deliver unmatched threat detection and response.

## ACTIVE DEFENSE IN ACTION

Data Source:
**Deep Panda Example**

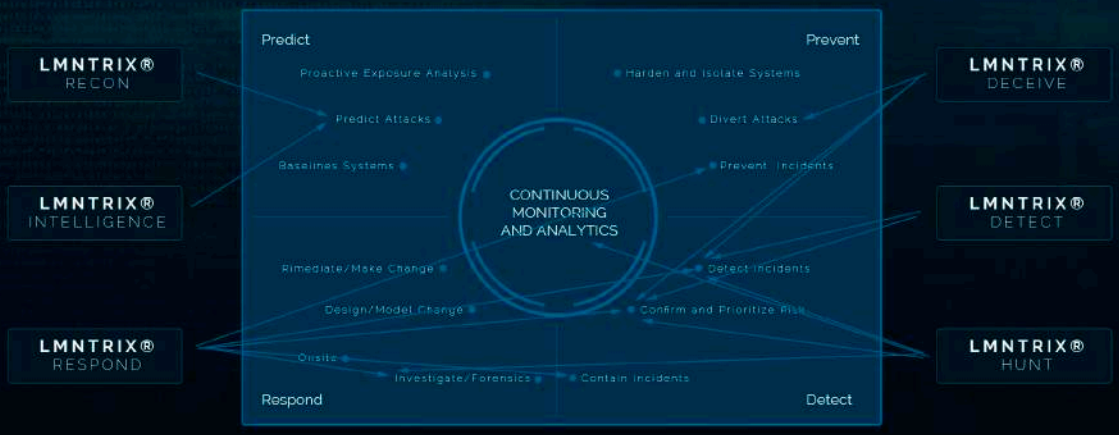
LMNTRIX
BE THE HUNTER | NOT THE PREY

| | |
|---|---|
| **LMNTRIX Intelligence**<br>Who could be attacking us? | Early detection of threats |
| **LMNTRIX Detect**<br>What was targeted? | Advanced intrusion attemps that bypass perimeter controls |
| **LMNTRIX Hunt**<br>How did the exploit occur? | 1. "Beaconing & suspicious communications<br>2. "Sticky-keys" backdoor<br>3. Malicious proxy tools<br>4. WinRAR using encrypted rar files<br>5. Recreate entire exploit |
| **LMNTRIX Deceive**<br>How did the attackers move around once inside? | 1. Lateral movement via RDP<br>2. The hacker is on your network |
| **LMNTRIX Respond**<br>Was the endpoint exploited?<br>Were others infected? | 1. Time/date "stomping"<br>2. Indicators about malicious files and code<br>3. Scope of infection |
| **LMNTRIX Recon**<br>What information did they steal?<br>Is it up for sale?<br>Did they leak it on the Deep or Dark web? | 1. Details of breached credentials<br>2. Copies of breached documents/files/sources code |

# LMNTRIX ACTIVE DEFENSE ALIGNS WITH GARTNER

LMNTRIX
BE THE HUNTER | NOT THE PREY

## LMNTRIX ALIGNS WITH GARTNER




12 Critical Capabilities of Gartner's Adaptive Security Architecture

The **LMNTRIX Active Defense** validated architecture was developed specifically to complement an organization's existing security program and enable a comprehensive adaptive security protection architecture as prescribed by Gartner.

The above image depicts how **LMNTRIX** works with clients and partners to deliver on all 12 Gartner capabilities that are necessary to augment an organisations ability to block, prevent, detect and respond to attacks.

For more information on LMNTRIX, visit:
lmntrix.com or info@lmntrix.com