LMNTRIX

BE THE HUNTER | NOT THE PREY

WHITE PAPER

EDR: PUTTING THE X FACTOR IN XDR

LMNTRIX XDR ENDPOINT SECURITY GUIDE

2023

LMNTRIX USA.
333 City Blvd West, 17th Floor,
Suite 1700, 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 INDIA.
VR Bengaluru, Level 5, ITPL Main Rd,
Devasandra Industrial Estate,
Bengaluru, Karnataka 560048,
+91-22-49712788

LMNTRIX Australia.
Level 25, 100 Mount Street,
North Sydney NSW 2060
+61.288.805.198

lmntrix.com

LMNTRIX
BE THE HUNTER | NOT THE PREY

CONTENTS

EXECUTIVE SUMMARY

With increased access and use of the Internet since the late 1990s, we are witnessing the popularity of the Internet skyrocket to unimaginable heights. For example, in 1995 there were only about 16 million internet users worldwide, which constituted only 0.4% of the world's population. From there, this number doubled almost every year to reach 248 million, or 4.1% of the global population, in December 1999. This number has now increased to about 5.38 billion people in March 2022. Ultimately, this means that 67.8% of the global population now has access to or uses the Internet.

As a result of this increased growth, the Internet has now changed the way people live, provides them with more knowledge than ever before, and allows businesses to be more efficient, productive, and serve their customers better. It is not all good news, however. With increased internet usage comes increased risks.

Probably the most significant of these risks is the increased risk for data breaches, data loss, and other cyberattacks that surface as Internet usage increases. This is an especially relevant consideration for businesses and other organizations where data security is a chief concern when one considers that cyber attacks increased by 31% from 2020 to 2021 and the cost of cybercrime is expected to reach $10.5 trillion by 2025.

Security risks have always accompanied Internet use, and it is for this reason that the world came to know earlier, traditional antivirus solutions. However, over time, cyber attackers have become more sophisticated and are now employing advanced attack methods that are capable of evading more traditional security solutions.

As a result, organizations now need more effective and efficient solutions that could not only help them identify any threats, but also help them respond faster to these threats. And faster identification and responses are vital.

For example, it takes security teams, on average, about 287 days to identify and contain a data breach, and data breaches cost companies about $200,000 on average. During this time, the resulting damage from a breach can be devastating.

This is where Endpoint Detection and Response or EDR becomes an invaluable tool. It helps our customers identify and respond to threats much faster than traditional solutions and enables their security teams to hunt for threats proactively, instead of taking a reactive approach as they would have with more traditional security solutions.

In this white paper, we will discuss EDR in more detail, look at some use cases, and we will aim to provide a concrete framework for threat hunting with EDR.

Introduction to EDR

Before looking at the threat hunting process in more detail, it's important that we first understand what EDR is, why the need for it arose, and the capabilities it offers. Comprehending these aspects lays the foundation for implementing threat hunting strategies and processes based on using EDR.

What is EDR?

The term Endpoint Detection and Response (EDR) was initially coined by Gartner's Anton Chuvakin to describe systems that could detect suspicious activities on endpoints and use automation that enables security teams to identify and respond to security threats quicker and more effectively. EDR refers to an integrated endpoint security system that continuously monitors and collects endpoint data and has automated responses and analysis capabilities and features.

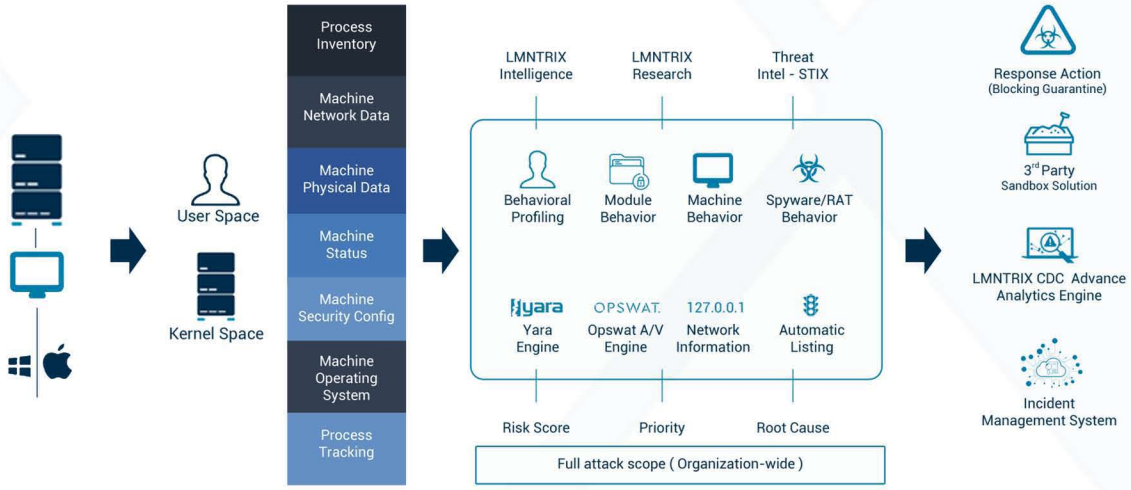

Figure 1 - How EDR Works

Considering the above, the key components of EDR are:

⊙ **Endpoint monitoring and management.** The first component allows EDR to monitor endpoints and collect data in relation to, for example, activity volume, processes, connections, and data transfers into a central location.

⊙ **Analysis.** Once the data is collected, EDR analyzes the data and provides insights on how an attack occurred, how future attacks might occur, and what strategies organizations might implement to prevent those attacks.

⊙ **Automated incident response.** EDR uses pre-configured rules to identify an incoming attack and to trigger an automated response. These responses include logging off users, sending alerts, or rolling back a system to a previous safe state.

The Need for EDR

Now that we have a broad overview of EDR and its components, the question is: Why the need for EDR solutions? In other words, why were EDR solutions developed? To answer this question, let us consider a brief evolution of cyber threats.

The Evolution of Threats

Traditionally, antivirus software was able to provide sufficient protection against cyber threats. However, during the early 2010s, attackers implemented new methods that did not rely on the installation of malware or an application to execute malicious code. By using these new methods, attackers were then able to bypass traditional security measures and software.

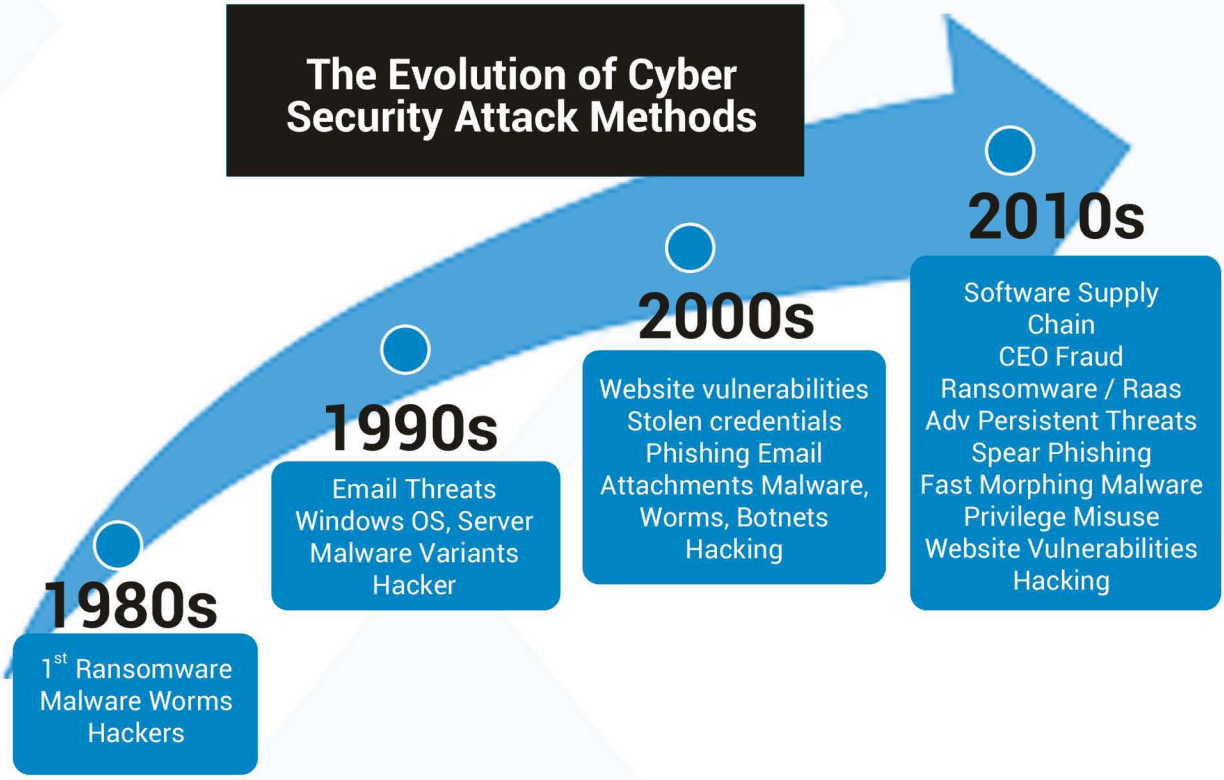

Figure 2 - Evolution of attack methods

The first example of these new methods is using document-based malware. This is so attractive because, while most users understand that they should not download or run any applications from unknown sources, they do not understand that document files like PDFs, Word, Excel, or PowerPoint documents are similarly capable. The result is that they are more likely to download and open these files.

Attackers take advantage of this misunderstanding by incorporating Macros in these files which, in turn, run malicious code on the users' machines. Now, some might think that a simple solution to prevent this is by disabling Macros. Unfortunately, because Macros help users to automate tasks and are vital to many business processes, doing this impacts productivity and efficiency negatively. Hence, disabling Macros is not a viable solution.

For this reason, because organizations use Macros as a productivity tool, they are still prevalent. Moreover, the fact that Macros are still easier to get onto a user's machine compared to other applications also contributes to their continued popularity under attackers.

The second method attackers often implemented is using fileless attacks, because this method, as the name implies, does not rely on the installation of any files but rather operates in-memory, it can evade traditional security measures. They became popular as a result of a leak of NSA infiltration tools, which allow attackers to move laterally through systems and exploit vulnerabilities in operating system protocols. Probably the most well-known example of fileless attacks is Eternal Blue attacks that exploit the network file sharing protocol SMB or Server Message Block.

Because traditional tools could not reliably identify these attacks, as is the case with document-based malware, there was no viable solution for these attacks. Despite this, SMB still forms a crucial component of organizations' network communications. It's important to remember that these are only two examples of how attackers can bypass traditional antivirus software, and there are myriad other ways that a potential threat can bypass your traditional controls.

Figure 3 - Top 15 Cyber Threats

EDR is Born

Since the evolution of the attacks mentioned above, the inadequacies of traditional antivirus software soon became apparent, and its effectiveness for detection continued to decline.

As a result, antivirus software vendors started using alternative techniques to distinguish between legitimate and malicious software. These techniques, which included cloud-based analysis, behavior analysis, and machine learning, were designed and used with signatures to allow organizations to identify both known and unknown threats. For this reason, these new tools were referred to as next-generation antivirus (NGAV).

Flowing from this, vendors also created new tools that gave organizations more visibility into their networks and systems. This new collection of tools was described by Anton Chuvakin, as mentioned earlier, as EDR in 2013. They typically, like NGAV, implemented machine learning, and behavior all analysis to monitor systems and identify any malicious activity.

Despite the improvements these tools facilitated, they weren't without their problems. For instance, they produce far more alerts compared to traditional tools and, could lead to stakeholders underestimating the importance of alerts given by the tool. Moreover, early EDR tools relied on organizations collecting vast amounts of data and having more security expertise compared to traditional tools to operate efficiently and effectively.

The Evolution of EDR

Despite the advances that EDR has brought to security and threat management, attackers are becoming more sophisticated and they are able to adapt to these advances by using new attack methods. A case in point, the LMNTRIX researchers are able to bypass every single NGAV and EDR tool on the market today, which means APTs and Nations State attackers could easily do the same. As such, these tools also need to adapt to ensure that companies' and organizations' data stays safe. Fortunately, since 2013, these tools have evolved significantly and vendors are continuously improving these tools to adapt to ever-increasing and evolving security risks.

One of these evolutions is Extended Detection and Response or XDR. This term describes the extension of EDR and SIEM and promises to reduce alert fatigue and false positives by integrating endpoint, network, system, application, and cloud data. This amalgamation enables better visibility and context into advanced threats through the use of analytics.

Sitting between EDR and MDR in terms of capability, it enhances on EDR solutions in terms of the types of activity it can monitor and the range of attacks it can detect. Where EDR improved on malware detection over antivirus capabilities, XDR extends the range of EDR to encompass more deployed security solutions while also offering containment capabilities using integrations with enforcement points.

While we may argue that this is the aim of security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools, they never quite lived up to the promise.

With a laser focus on threat detection and incident response, XDR is now poised to deliver what these other technologies couldn't a unified, workable detection, and response platform.

Generally, XDR should provide the following capabilities – at a minimum:

- Extend telemetry beyond endpoint signals
- Correlate security data to improve accuracy and consolidate alerts into incidents
- Expand, coordinate, and automate response actions across the environment

Based on these requirements, we can see how an XDR platform might be considered as an improvement and/or replacement of other security technologies – assuming the particular XDR solution actually delivers on its promise.

For example, if an XDR platform natively provides network telemetry signals, it might allow a company to replace their current NDR or Deception solution. The added benefit, which we'll discuss below, is that network telemetry is fully integrated into the XDR platform out of the box. This negates the need for expensive and complex integration and ultimately can lead to better protection due to the signals being natively built into the XDR analytics engine.

Taking the key XDR capabilities above, we can see how each might replace existing technology or add capabilities that may otherwise be missing.

- Extended telemetry potentially provide signals and data that would otherwise require additional technologies such as NDR, Network Forensic, UBA Rules, CASB, CSPM, Deception, Machine and Underground Intelligence, etc.
- Correlate security data potentially replace expensive and complex SIEM technology
- Expand response actions potentially replace expensive and complex SOAR technology

Consolidating these technologies into a single, unified offering also makes these technologies accessible to security teams that might otherwise not have the budget or bandwidth to deploy and support them.

Another evolution on EDR is **Managed Detection and Response or MDR**. Managed Detection and Response (MDR) is the term used for specialist threat detection and response capabilities delivered via an outcome-based approach. The goal of MDR is to rapidly identify and limit the impact of security incidents to customers while the focus of these services is on remote threat monitoring, detection, and targeted response activities on a 24/7 basis.

MDR providers may employ a combination of host and network-layer technologies, as well as advanced analytics, threat intelligence, forensic data, and human expertise for investigation, threat hunting, and response to detected threats. These make up an MDR's technology stack, and deployment is on the inside of the client network on all chokepoints and endpoints. Most MDR do not rely on the use of logs or legacy SIEM.

MDR takes off where MSSP stops, and it's considered the next iteration for threat detection and response. Most threats detected by MDR cannot be found in logs or a SIEM and cannot be identified by an MSSP or the client's internal SOC. Furthermore, threats detected by an MDR are typically automatically validated, investigated, contained, and remediated. Unlike MSSP, an MDR does not send unvalidated alerts or false positives to clients and expect them to conduct the investigation.

MDR also offers the opportunity to repurpose security budgets where the MDR would use equivalent or better technology in their stack, such as next-generation AV, SIEM, MSSP, IDS, sandboxing, and others. Unlike MSSP that simply relies on logs, the main weakness of MDR is that it can get expensive as MDR takes advantage of a completely separate technology stack that needs to be deployed on the inside of the client network. MDR also has a negative side-effect in that it makes log-based approaches such as the existing client SOC and MSSP look ineffective as it detects threats that simply cannot be identified from logs this naturally doesn't fare well for any executive that invested in those solutions.

Traditional AV vs. EDR

We have now looked at EDR in more detail, and we have a broad overview of where traditional antivirus software falls short. As such, we now need to consider the differences between these solutions in more detail.

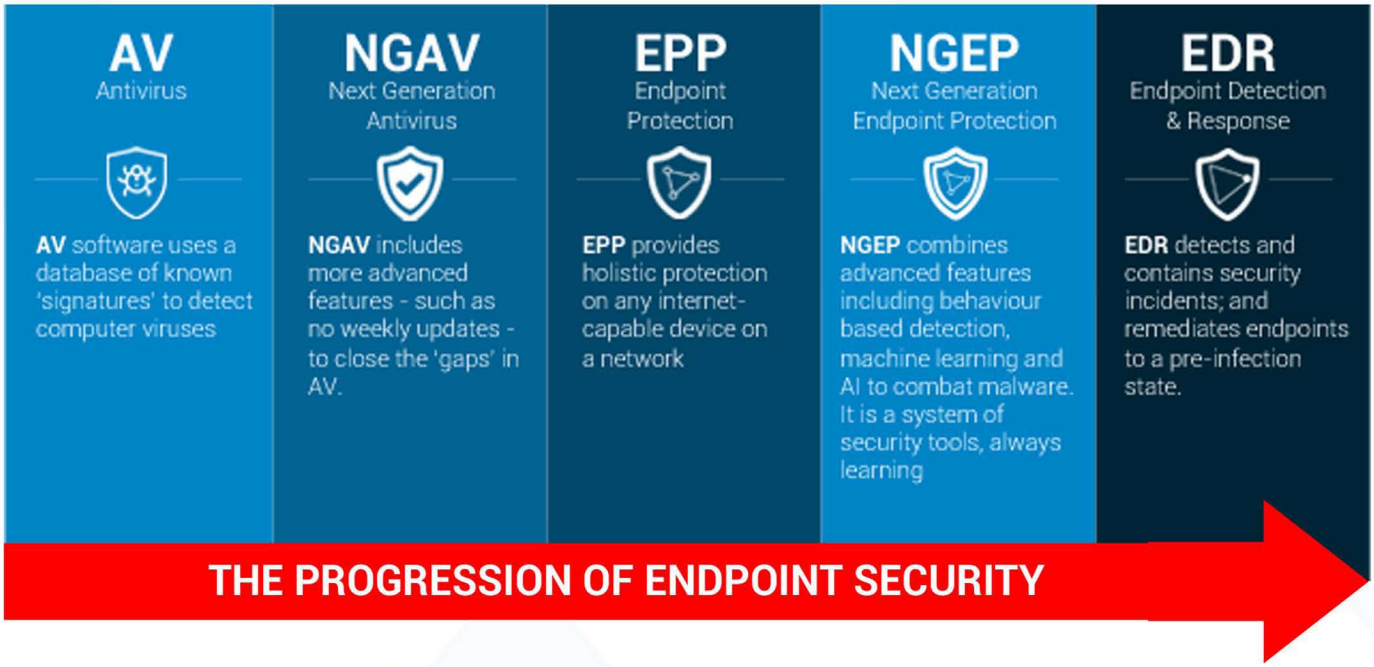

Figure 4 - The Progression of Endpoint Security

Traditional AV Features

To build a more complete understanding of the difference between these two security tools, the first step is to consider how a modern antivirus solution identifies malware on a computer system. Here, these solutions might implement one or more of the following types of scans to identify malicious software:

Signature scans. During these scans, antivirus software will scan any new applications on a machine, read, and compare their hashes or signatures against a database of known malware signatures. Once the antivirus solution matches the signatures, the application will be identified as malware and remedial steps can then be taken.

Heuristic scans. In contrast to signature scans, heuristic scans don't rely on signatures to identify possible malware. As such, these scans might identify applications as malware even though their signature does not match any of the signatures in the database of known malware. To do this, the antivirus solution will launch the application in a sandbox to determine if it exhibits any malicious activity such as launching excessive processes, deleting, or encrypting files.

Integrity scans. During these scans, an antivirus solution will scan a system and detect any changes to files on the system. This is because changes to files might indicate a malicious process. Once these changes are detected, the antivirus solution will identify possible malware and prompt a response and remedial action.

Behavioral analysis. Advanced antivirus solutions might also implement behavioral analysis, which analyzes process behavior. These systems identify processes with abnormal behaviors compared to other processes on the computer system. This capability is especially helpful to identify unknown or evasive malware.

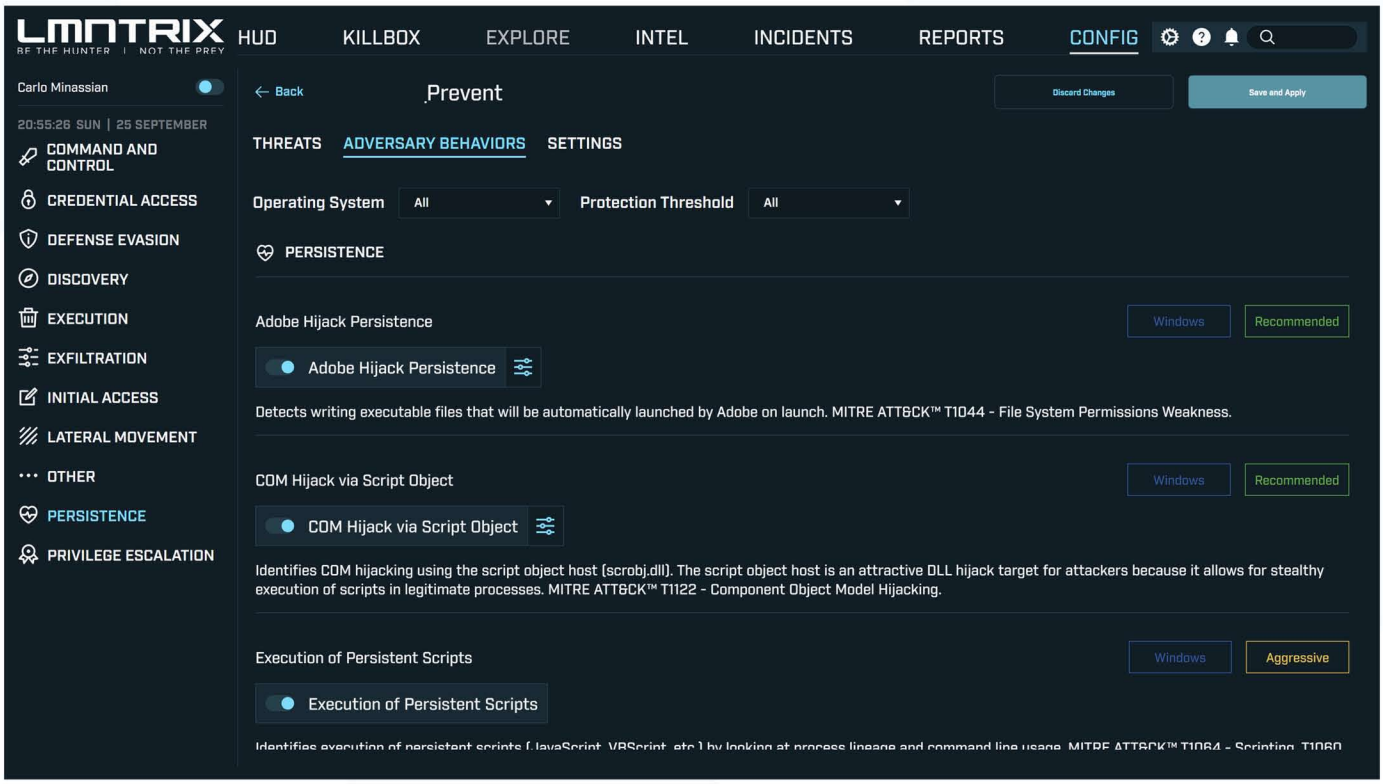

Figure 5 - LMNTRIX XDR Endpoint Security Adversary Behaviors

Traditional AV Shortcomings

Despite the features mentioned above, traditional antivirus still exhibits several limitations. In turn, these limitations prevent traditional antivirus solutions from effectively dealing with a wide range of security risks, including:

- **Modern, advanced threats.** Because traditional antivirus solutions, to a large extent, rely on a signature database to identify possible malware, they can only identify security threats that have been identified before. As a result, as attack techniques and methods evolve and new threats are launched, traditional antivirus solutions are simply unable to detect advanced threats. Attackers can thus easily circumvent these defenses.

- **Polymorphic malware.** Polymorphic malware consistently changes its identifiable features like file names, file types, or signatures. This feature allows these types of malware to avoid known signatures. The result is that polymorphic malware can avoid detection by traditional antivirus solutions which are an especially relevant limitation, considering that up to 97% of modern malware uses polymorphic techniques to avoid detection.

- **Malicious documents.** As mentioned earlier, attackers can use documents to deliver malicious code to a computer system. Once such a document is opened, it either runs software hidden in the file or a script contained in the file that downloads the software from a remote website. And because there is no malicious code contained in the file when it's downloaded, it is able to avoid detection by antivirus software solutions. Considering this, it is understandable why document-based malware is so popular with attackers. In fact, according to a 2019 report, more than half of all malicious files detected between January and April 2019 were in the form of document-based malware.

- **Fileless malware.** Unlike document-based malware, fileless malware doesn't rely on the installation of files onto a system, but are rather memory-based. This means they can successfully avoid detection by antivirus applications that only scan installed files. Moreover, because they have no signature, antivirus solutions that detect malware based on signatures cannot detect them.

- **Encrypted traffic.** Another tactic employed by attackers is to use encrypted traffic to send malware or malicious code to a computer system. This is because encrypted files rely on encryption keys to be opened, and antivirus software typically does not have these encryption keys. As such, these solutions can read the contents of the file and, by implication, its signature. As a result, these files are then able to avoid detection.

The Differences Between Traditional AV and EDR

Now that we have highlighted the basic features and limitations of traditional antivirus in more detail, it is time we consider the differences between traditional antivirus software and EDR closer.

Based on the above limitations, it is clear that traditional antivirus solutions are far less capable than EDR. Traditional AV provides only a single security tool and it is more simplistic which, limits its scope and capabilities. In contrast, EDR provides more context and data regarding more devices which makes it far better at detecting and identifying threats.

Another significant difference between traditional antivirus and EDR is that, while enterprise-grade antivirus solutions can be deployed to an organization's endpoints, EDR is capable of being deployed to a wider range of endpoints. This is an important difference, as organizations have ever-expanding network systems and only EDR is capable of providing centralized, organization-wide security that continuously monitors for threats.

One of the most significant differences between these tools, however, lies in the way they detect threats. As mentioned earlier, antivirus solutions scan a system and identify any threats based on one of the methods outlined above. As such, it more often than not identifies threats after the infection. And attackers have devised ways to bypass these security solutions.

EDR, implements real-time monitoring for threat detection. Apart from this, EDR records vast amounts of data which helps organizations understand the complete context of an attack which, in turn, creates an understanding of not only why the attack happened but also how to prevent similar attacks in the future.

Ultimately, EDR presents a more effective security solution compared to antivirus software because it allows organizations to take a proactive approach to security and risk management instead of a reactive approach.

How LMNTRIX Benefits From EDR Telemetry

We now have a broad overview of what EDR is, how it works, what benefits it offers, and how it differs from traditional antivirus. Let's consider how LMNTRIX XDR benefits from EDR telemetry.

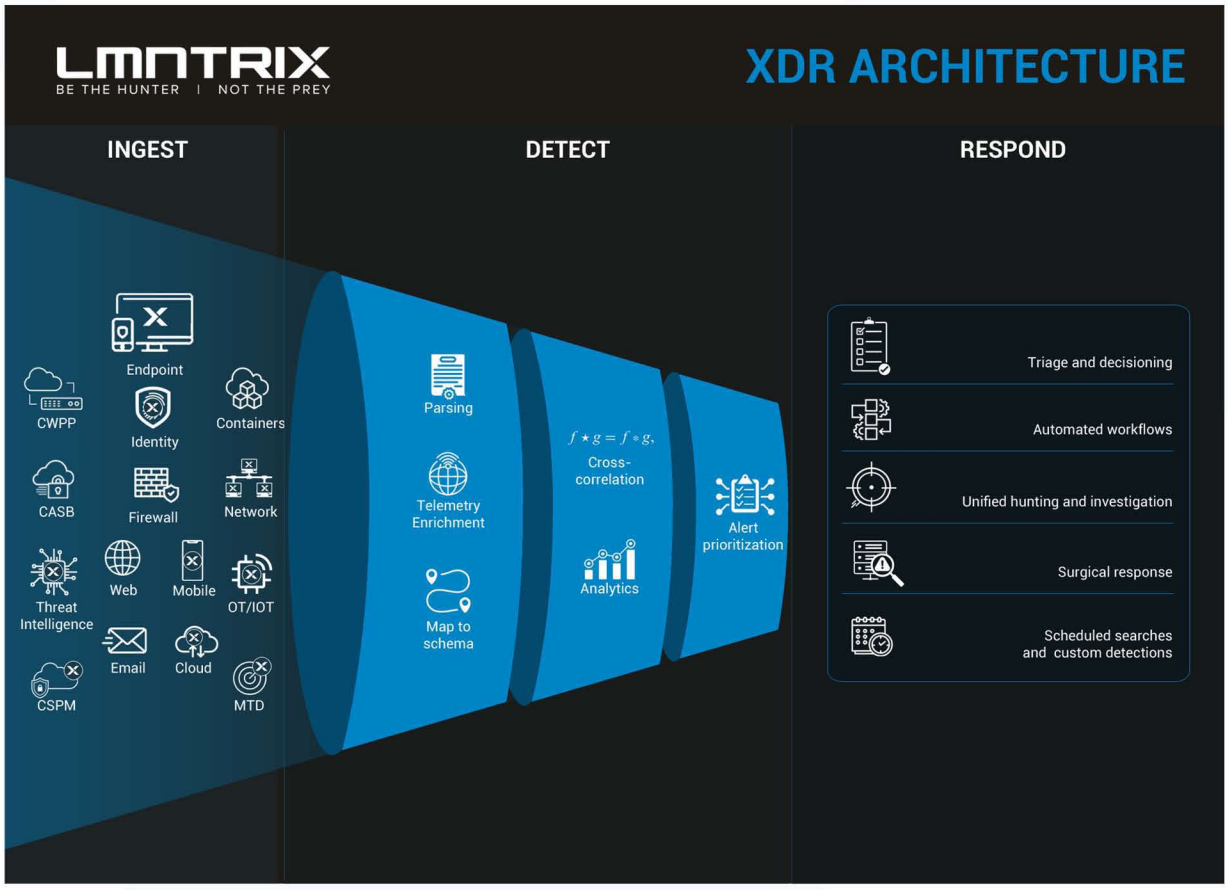

Figure 6 - LMNTRIX XDR Architecture

As a Native XDR vendor and with added ability to ingest data from any source, LMNTRIX is one of few vendors that offers all components of an XDR solution and provides 24/7 MDR including adversary hunting at no extra cost. This means that the buyer will not need to purchase and integrate additional technology solutions into the XDR platform to enjoy the benefits nor do they need to worry about building and operating a 24/7 SOC. Native XDR platform is fully integrated and operational out of the box. Everything works seamlessly no signal normalization and integration is required, no complex application and integration testing is required every time a platform component is updated, no training and operating multiple solutions, and no extra expense. A Native XDR will allow organizations to replace one or more existing security tools (such as EDR, NGAV, NDR, Network Forensics, UEBA, Machine and Underground Intelligence, Deceptions, CSPM, etc.) to make the purchase more cost efficient. It also allows organizations to benefit from additional protections that they otherwise could not afford to purchase and/or operate.

LMNTRIX XDR is a Cloud SaaS cyber defense platform that provides a unique utility model for enterprise security and provides insights into threats on enterprise, cloud, mobile, hybrid, and industrial control systems (ICS) networks. LMNTRIX XDR provides pervasive visibility, threat hunting, validation, investigation, containment, remediation, unlimited forensic exploration features and capabilities in a single cloud platform on demand.

With these features and capabilities, LMNTRIX XDR is capable of offering several unique advantages over other EDR, XDR or SIEM solutions on the market today. For example, LMNTRIX XDR is based on multiple detective, responsive, and predictive capabilities that integrate and share information to build a security protection system that is more adaptive and intelligent than any one element. The constant exchange of intelligence, between the XDR components and the wider cybersecurity community enables LMNTRIX to keep abreast of the tactics techniques and procedures (TTP's) of the most persistent, well-resourced, and skilled attack groups. Furthermore, LMNTRIX XDR provides a holistic and multi-vector platform that has an unlimited retention window of full-fidelity network and endpoint traffic, and it provides innovative security visualizations while still offering the ease and cost savings of an on-demand deployment model.

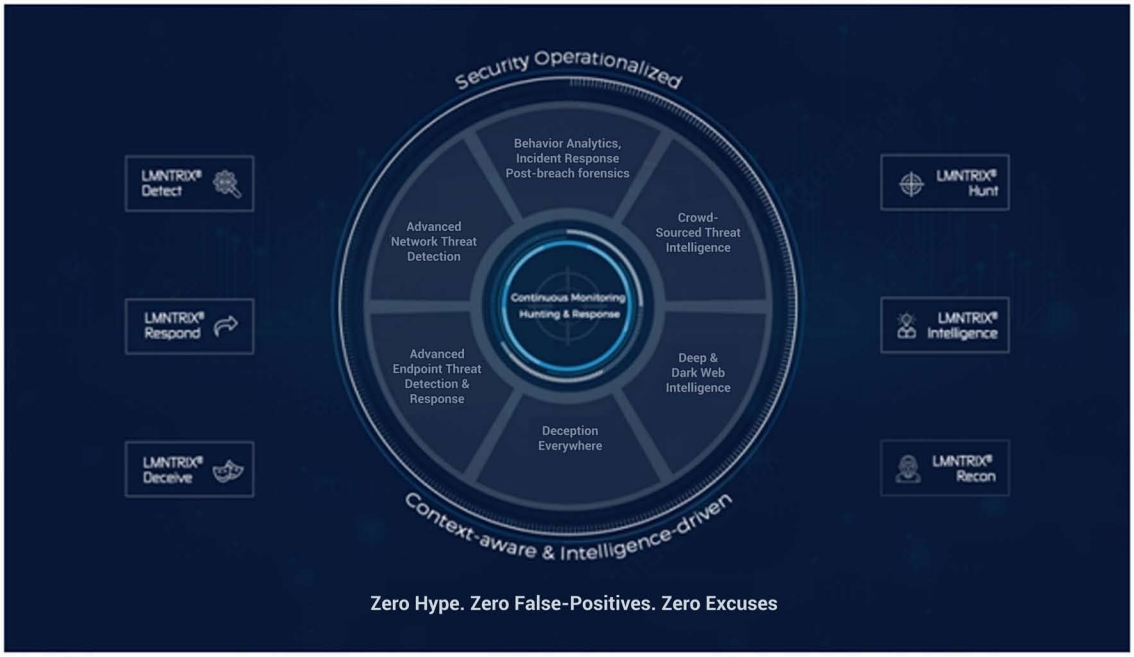

Figure 7 - LMNTRIX XDR Benefits from EDR telemetry

As part of its XDR offering, LMNTRIX provides LMNTRIX XDR Endpoint Security, a proprietary endpoint agent with enhanced NGAV and Endpoint Threat Detection and Response capabilities in a lightweight custom built agent that can be deployed to all endpoints within the organization. LMNTRIX XDR Endpoint Security offers the following features:

- Protects systems and networks against known malware and variants thereof, including malware such as ransomware. In addition, it also protects systems and networks against obfuscated malware, unknown malware, zero-day attacks, memory-resident attacks, and other fileless attacks.

- LMNTRIX XDR Endpoint Security also has the ability to detect and analyze the lateral movement of an advanced threat and provides protection from in-memory movement.

- Provides the ability to identify and alert on known-good applications that are compromised or behaving maliciously.

- Provides automatic prevention of threats based on behavioral indicators.

- Provides effective protection against document-based attacks, flash exploits, browser exploits, and a variety of other techniques that attackers use, including malicious scripts that use Python, PowerShell, Perl, and more.

- Provides pre-execution protection from known threats and provides full post-execution visibility into what is occurring within a system or network.

- Provides visibility to see threats through attack analysis and improves attack prevention by closing security gaps.

- Provides multiple mechanisms of protection, including terminating processes and it offers the ability to one-click delete a file, add a program to a blacklist, or request an upload of a binary.

- It ensures a low false-positive rate and provides multiple mechanisms for dealing with false positives.

- It is able to detect events that match Tactics, Techniques, and Procedures (TPP), uses machine learning for malware analysis, and is able to adapt quickly to new attack tools, tactics, techniques, and procedures.

- It is able to provide visibility into the root cause of an attack and the machine location on the network whether it's on-premise or off-premise and makes investigation possible even when the computer is off-line or reformatted. In addition, it can also isolate a host from a network but still retain communication. As such, it is also able to determine the scope and spread of an attack after detection.

- Provides extensive configuration options that allow different protection policies for different groups of endpoints and configurable detection to prioritize important events and reduce unnecessary alerts.

In addition, to this functionality, LMNTRIX XDR Endpoint Security provides data that is used by LMNTRIX Cyber Defense Center to continuously monitor all endpoint activity, perform adversary hunting, validate breaches, investigate, contain, remediate, and detect encrypted attacks automatically.

By providing this information, the service enables intrusion analysts to find similarly infected endpoints and broaden their visibility to the entire scope of a compromise. And once LMNTRIX CDC has confirmed an intrusion, they disrupt malware-driven tactics, techniques, and procedures, limit the lateral movement of the attack by quarantining and blocking the threat.

Ultimately, by using this form of EDR, LMNTRIX XDR Endpoint Security provides the following benefits:

- **Lightweight endpoint sensor.** LMNTRIX XDR Endpoint Security's proprietary, lightweight, custom agent is easy to deploy quickly and requires no pre-configuration, while still being able to capture detailed state information that facilitates protection against a variety of exploits, malware, and attacks.

- **Real-time detection.** LMNTRIX XDR Endpoint Security enables organizations to identify, analyze, and respond to advanced threats against their network systems in real-time. This forms the foundation of a proactive approach, which is more effective at identifying and responding to threats compared to a reactive approach.

- **Reduced response time.** Being able to detect threats in real-time means that organizations have the ability to discover every infected machine on the network and the location of the infected files on the machine. In turn, this reduces incident response times drastically from days to mere minutes.

- **Incident response.** In the event of an attack, LMNTRIX's analysts respond immediately, which means they limit the fallout of the attack and have an organization's systems and network up and running as soon as possible.

- **Adversary hunting.** Adversary hunting is the stealthy and surgical detection and eviction of adversaries within your network without prior adversary knowledge or known indicators of compromise.

The goal of hunting is to detect and evict adversaries that have bypassed defenses before damage and loss can occur. To do so, a hunter must be able to enter the network undetected, identify the adversary at any stage of the kill chain, and evict them without disrupting running systems. MDR including adversary hunting is included at no extra cost with the LMNTRIX XDR Endpoint Security.

- **Breach validation.** Because threats are properly analyzed and validated before the organization is alerted, organizations won't fall victim to alert fatigue. Moreover, this strategy reduces escalations and false positives by up to 95%.

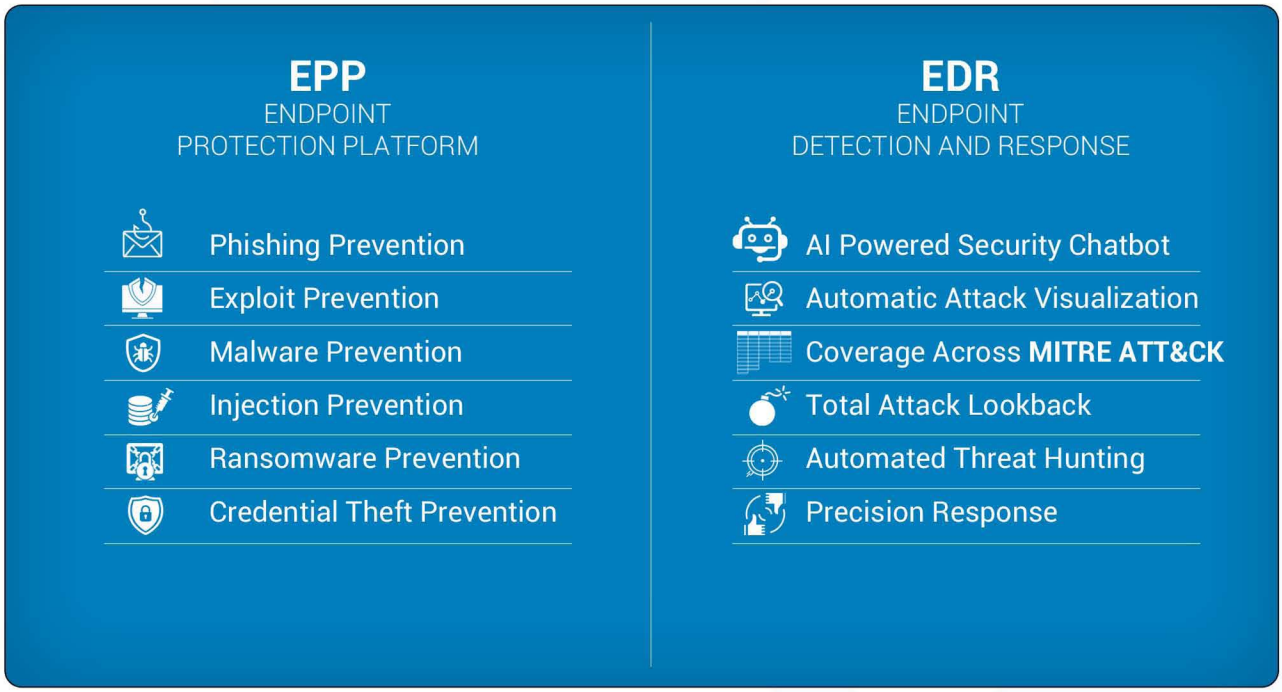

Figure 8 - LMNTRIX works through the full **MITRE ATT&CK** Chain stopping malicious code at every stage from pre-execution, lateral movement and post-execution including data exfiltration.

Use Cases

Now that we've seen what EDR is, how it compares to traditional antivirus solutions, and how a platform like LMNTRIX benefits from EDR telemetry, it is important to consider some of the use cases for EDR.

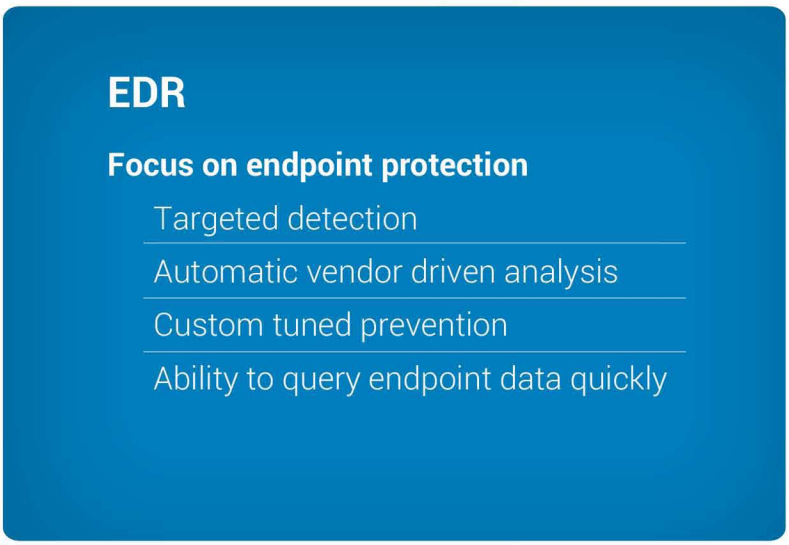

Figure 9 - Use Case for EDR/EPP Solution

Gaining Context Within the Organization

With the sheer number of malware discovered every day, it's simply not possible to investigate every suspicious or possibly malicious event within a network or system. This is where context comes in, as it aids in understanding the surrounding circumstances around an event and, in the process, can mean the difference between identifying an actual threat or, reacting to a false alarm.

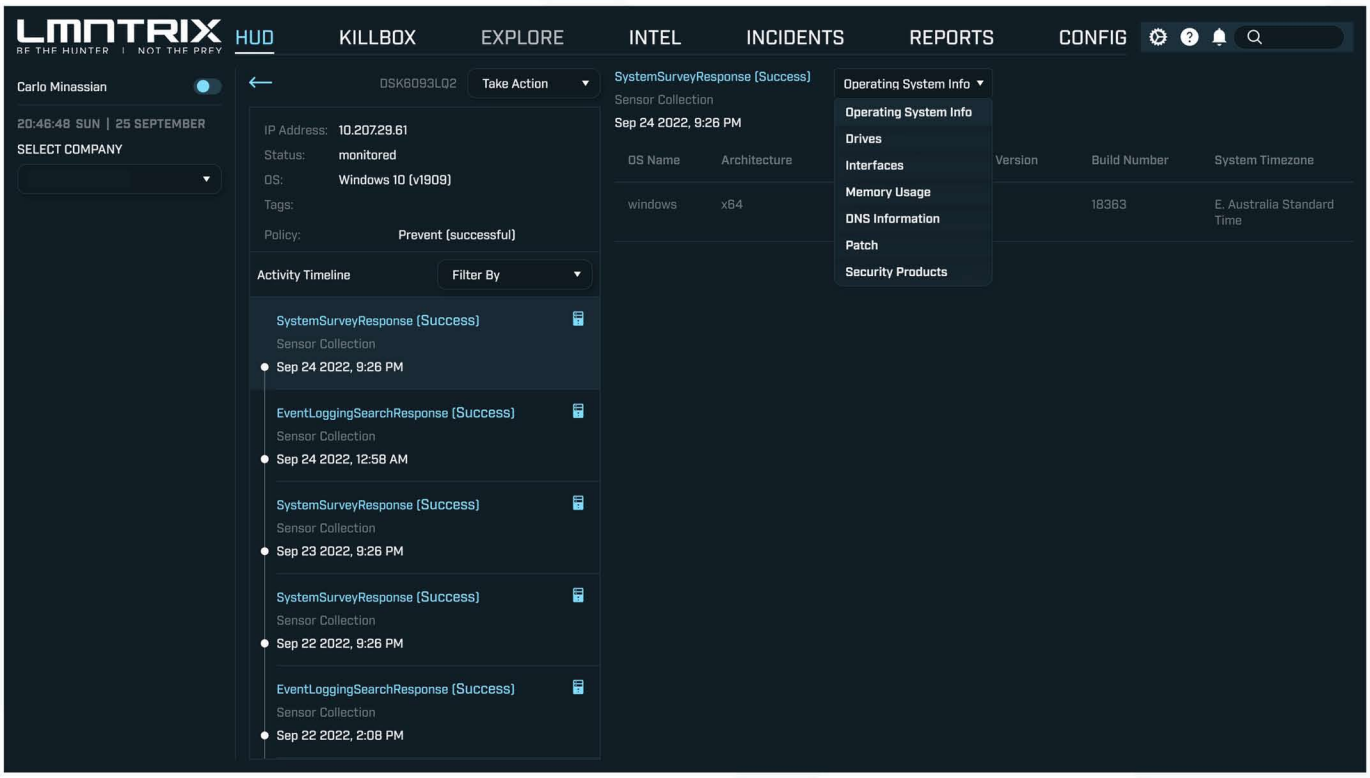

Figure 10 - LMNTRIX XDR Endpoint Security provides Context using Machine and System details

But what exactly is context? To explain the concept, let's look at a simple example. Assume that a bakery uses an automated baking machine to bake 50 cakes per day during the course of a weekend. During the week, however, demand is lower, and the bakery only needs to bake 15 cakes per day. However, the machine does not know this and if the right adjustments are not made it will continue baking 50 cakes, no matter what day of the week it is. This does not mean that the machine has malfunctioned, only that it lacks context.

When it comes to cyber security, the position is no different. When organizations have many endpoints they need to monitor, they will soon become overwhelmed by alerts that lack context, especially when these endpoints are monitored based on a rules-based system. Without the necessary context, these systems will continue to provide alerts, no matter how benign an activity it is. With the necessary context, however, these organizations will be alerted to real threats while threats that pose no danger will be avoided. As a result, the number of alerts will decrease and security teams will have more time to respond to actual threats more effectively and efficiently.

Yet, despite this, any effective security strategy relies on data and security personnel having access to comprehensive and contextual data about all activities within its network or systems. And this is where EDR solves the problem referred to above by providing valuable context within the organization.

EDR systems continuously monitor all endpoints, they gather vast amounts of data regardless of whether they detect a threat or not. This data can then be used to provide context around events and help security teams better understand what is happening within a network or system. The data can also be converted into visualizations that make it easier to make more sense of the data, correlate events with context, and formulate effective and efficient security strategies.

For example, assume a security team receives an alert about a specific activity, investigates it, finds it to be benign, but doesn't store the data relevant to the activity or event. When the same activity occurs in the future, the team will once again receive an alert and will have to investigate to determine whether it is a malicious activity.

Conversely, armed with the historical data surrounding the event, the team will correlate this data with the current event and know the activity is benign even before they investigate. Ultimately, this not only prevents alert fatigue but also makes security teams more effective and efficient.

Accelerating Investigation Workflows

The next use case for EDR is to accelerate investigation workflows in the event that an incident occurs. The entire EDR process goes through four stages to protect an organization against cyber threats, and one of these is the investigation workflow. Thus, to understand how EDR is able to accelerate the investigation workflow, it is important to consider how EDR works for a moment.

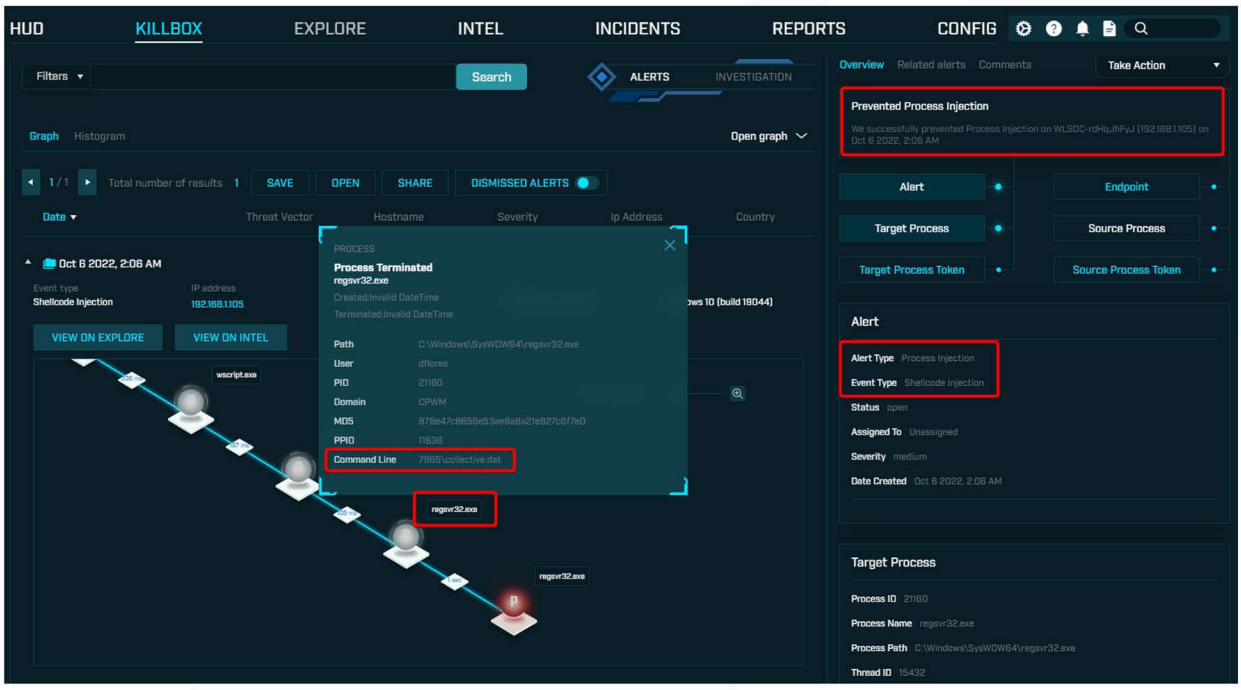

Figure 11 - Threat Detection using LMNTRIX XDR Endpoint Security

The first stage in the process is the detection stage. During this stage, agents installed on all of an organization's endpoints will continuously monitor the endpoint and collect telemetry data. This data is then analyzed by machine learning algorithms and compared to threat intelligence databases. Combined, this capability allows EDR to monitor billions of events across an entire network in order to identify possible malicious activity. Moreover, EDR has the ability to remove known threats when they are detected.

Once an anomaly is detected, an alert will be sent to prompt security teams to investigate the issue further. When this happens, the team will move to the triage stage. During this stage, they will study the data provided by the EDR solution to not only eliminate false positives, but also classify any of the alerts as possible malicious activity. To do this, they will look at several aspects relating to the activity. We deal with malware triage in more detail later.

When the team flags an activity as malicious, it will trigger the investigation process. During this stage, the team will attempt to confirm that the activity is malicious. As such, they will look at all the data surrounding the activity. It is this data that shows them what happened and why it happened. This means the more data they have at their disposal; the faster they will be able to investigate the activity. And because, as mentioned earlier, EDR provides a wealth of data, it provides a full context and better understanding of the activity.

In addition, because modern attacks employ lateral movement to spread the attack and infect other endpoints, EDR can detect these infections, confirm malicious activity, and help teams to contain the lateral spread of the threat. Combined, access to more data and the ability to monitor the spread of an infection to other endpoints, allow teams to investigate activities far faster, which, in turn, leads to faster response and recovery times.

Throughout the stages mentioned above, an EDR solution will gather data whether it detects any anomalies or not. By using this data, it can then also accelerate the investigation workflow for future investigations.

Once the investigation stage is complete, teams will move to recovery. This can involve several strategies, depending on the specific activity or threat. We look at incident response in more detail later in this white paper.

Malware Containment Process

Containment is a critical component of every cyber-attack. Not only does it give security teams the opportunity to contain a threat before it overwhelms them or causes more damage, but it also gives them the ability to gather information and evidence surrounding the threat. It also sets the stage for the threat's eradication. As a result, it's crucial that teams have the necessary malware containment processes in place to effectively deal with incidents and events. In turn, this relies on an effective containment strategy that allows teams to make better decisions.

Effective containment strategies differ based on the type of attack. For example, strategies used to contain malware where attack can include:

- Blocking all incoming network traffic.
- Blocking networks, incoming traffic, and services on firewalls.

- Disconnecting infected systems from the network
- Shutting down infected systems.
- Locking compromised accounts or changing passwords.

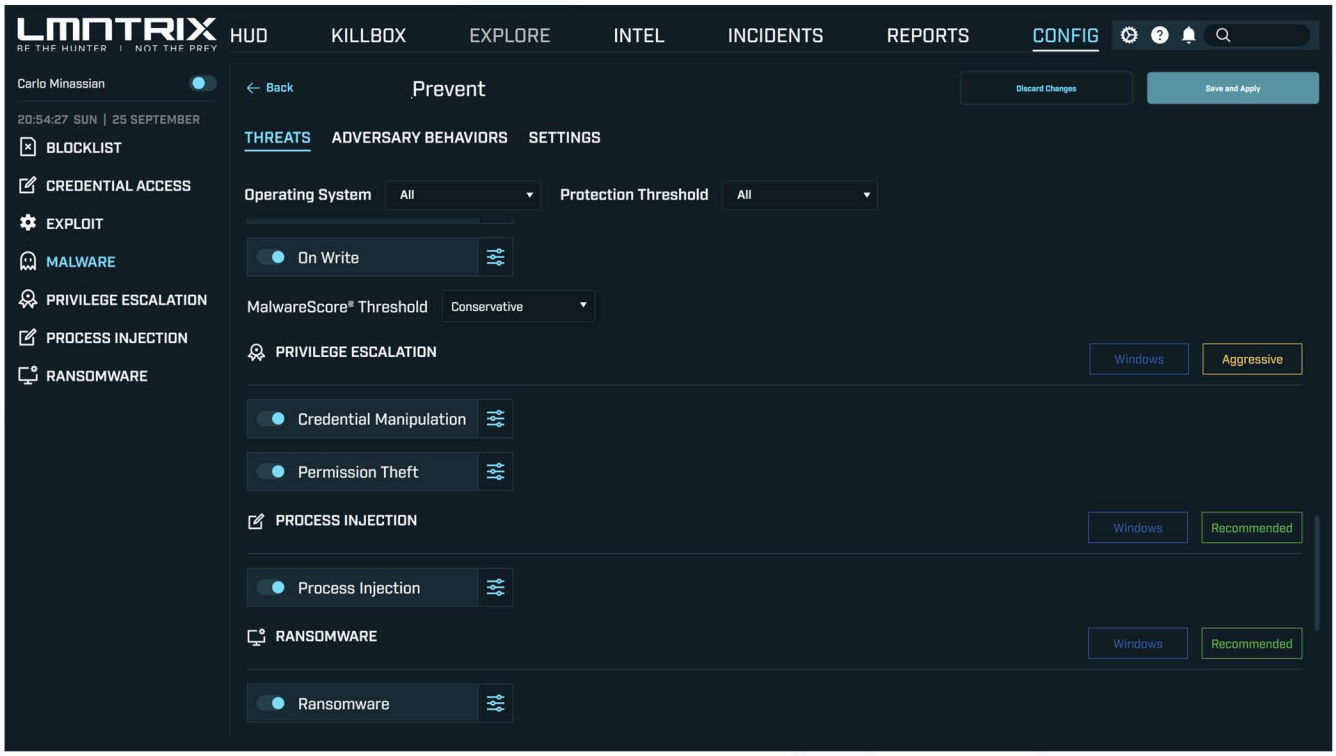

Figure 12 - Advanced Threat Prevention Capability with the LMNTRIX XDR Endpoint Security

From an endpoint perspective, containment takes place by isolating the endpoint from the rest of the network. This gives security teams the opportunity to identify the threat, investigate the threat in more detail, and, ultimately, eradicate the threat while preventing any lateral movement of the threat on the network. During this process, EDR plays a critical role because, as it is confined to the endpoint, it can provide information on the files, processes, and data flow of the threat.

Once the malware has been contained, security teams can investigate or analyze it. This can be done in one of three ways. Firstly, security teams can use malware triage, a type of static malware analysis, to learn more about the threat. During triage, teams will need to answer these basic questions:

- **How was the sample acquired?** Firstly, it needs to be established how the sample was obtained. In some cases, teams will be able to answer this question reasonably easily where, for example, the sample was obtained through an email or executable. In some cases, however, it could be more complicated and teams would have to investigate where the malware came from.

- **What is the name of the sample?** Next, the team will need to get the file name of the sample. Fortunately, this is also a relatively simple process.

- **What is the file size and extension?** It's also important to obtain, apart from the file name, also the file size, extension, and other metadata regarding the file. Like the file name, this information is also relatively simple to obtain.

- **What are the file hashes for the file?** Next, it's important to obtain the file hash of the file in order to identify the file. This can be done using a variety of cryptographic functions including MD5, SHA1, SHA256, SHA384, SHA512, and others. There are also a variety of tools for all major operating systems that can extract this information.

- **Is the sample packed or obfuscated?** The next step is determining whether the sample is packed or obfuscated. When obfuscated, attackers try to hide the execution of the file. When packed, the file is compressed and cannot be analyzed. Either way, these methods hamper a team's ability to statically analyze a file. Fortunately, there are tools and strategies to overcome this.

- **Is the malware binary, and if so, what functionality does it have?** Next, teams should determine whether a file is binary. If it is binary, teams should determine what capabilities the files have or, in other words, how it uses the operating system's shared libraries to perform different tasks.

- **Has the sample been seen before?** The final question to be answered is whether the file has been seen before. The most common way to answer this question is to consult threat intelligence sources.

While malware triage can reveal basic information about a threat, it does have some limitations. For example, it does not allow for the in-depth investigation of obfuscated or packed malware or binaries. This is where other forms of malware analysis come in.

Firstly, advanced static analysis, also known as code analysis, allows teams to study every component of a binary file without executing it. This is done by using a disassembler like IDA Pro, which allows security teams to reverse engineer the machine code into assembly code. During this process, they will get insights into the file's headers, functions, and strings. Simply put, advanced static analysis allows teams to read and understand the file's code, and it shows them what the binary or program is supposed to do.

However, despite the advanced nature of this method, modern hackers can still evade advanced static analysis by using several techniques. This is when dynamic malware analysis comes in. As the name implies, it allows security teams to run the malware application to investigate its behavior. Because this process poses severe risks, it is performed within a segregated or sandbox environment which, in turn, is a virtual environment that is isolated from the rest of the network. By running the application in a sandbox, security teams can avoid the risk to the remainder of the network and other production systems.

When performing dynamic analysis, security teams can see how the malware behaves and how it modifies the sandbox system including creating new file paths, IP addresses, registry keys, and so on. It also shows them if the malware is communicating with an attacker's server. Ultimately, dynamic analysis provides threat hunters with increased visibility into a threat, which allows them to understand the true nature of the threat better.

Attackers today can evade sandboxes also. As a result, and a final option, security teams can also choose to combine all the methods above into a hybrid approach. When they do, they will avoid the limitations of basic static analysis, while still being able to detect sophisticated malware that's intended to hide from sandboxing technology. Security teams can get the best of both worlds by using a hybrid approach, and can detect more sophisticated threats to protect their organization more effectively.

Decisive Response Process

An effective security strategy relies on, in part, detecting and protecting organizations against cybersecurity threats. However, this is simply not enough, as the volume of cybersecurity incidents are increasing significantly. In addition, these incidents and attacks are, as mentioned earlier, getting more advanced and capable of evading detection and identification. As a result, security teams also need to have a decisive response process in place to respond to incidents when they happen. Considering this, it is important that we consider how organizations can develop a decisive response process.

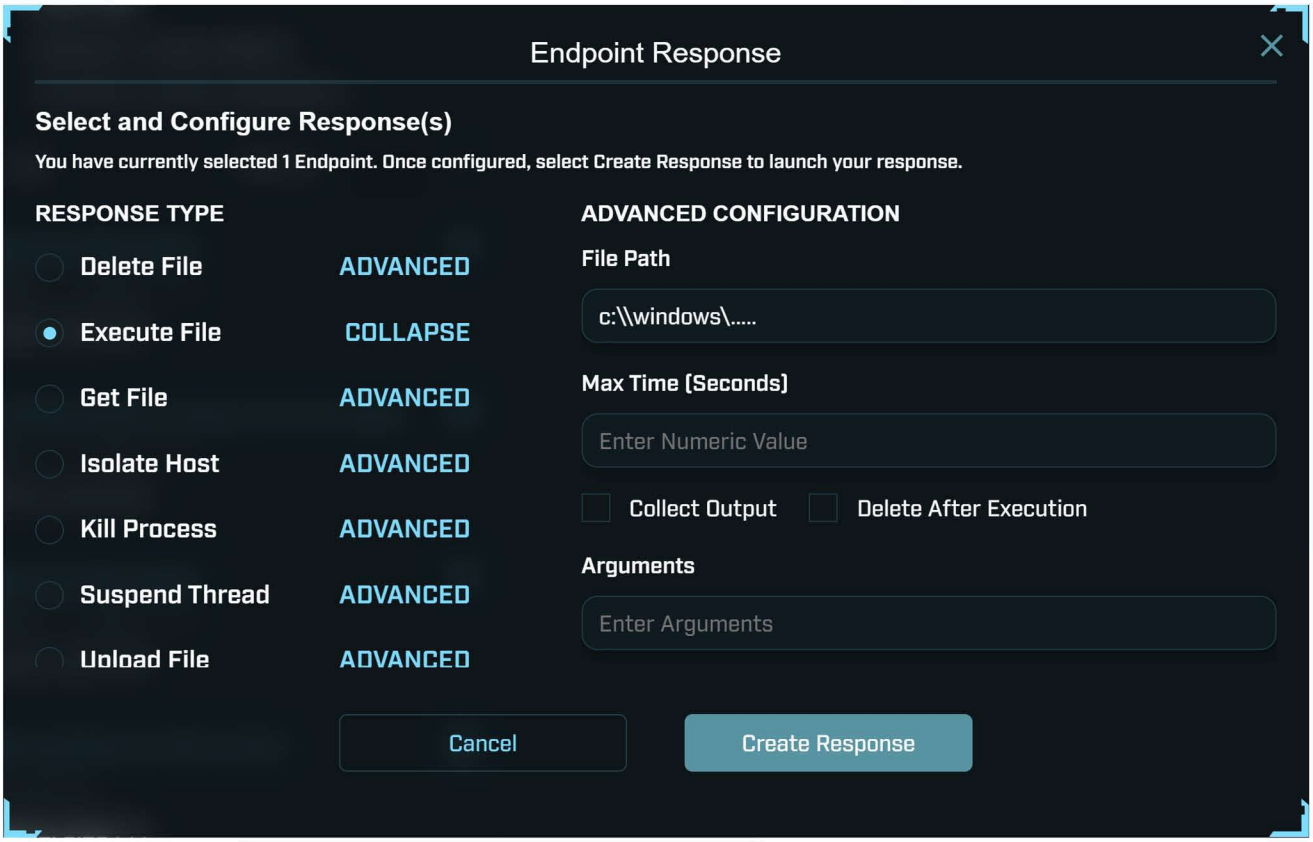

Figure 13 - Surgical Response LMNTRIX XDR Endpoint Security

The first step in the process is that every organization understands the threats they face, both internally and externally. This understanding will help organizations prepare for the cyberattacks they are most likely to encounter. As such, and to achieve this understanding, organizations should, inter alia, consider what types of attacks, incidents, or malware infections they have experienced in the past, whether their employees were victims of targeted attacks, and how severe those incidents or attacks were. They should also consider the types and severity of attacks that their competitors, business partners, and other companies in their industry have experienced.

Once organizations have an understanding of the threats they face, the next step in the process is to develop an effective incident response plan. This is a critical component of a decisive response process, and the lack of an incident response plan severely hampers an organization's ability to recover from an attack. In turn, this leads to more severe damage.

Fortunately, there are many resources available that allow organizations to develop effective incident response plans. In fact, we will deal with developing an incident response framework in more detail later in this white paper. It is important to remember, however, that while these resources might be helpful, an incident response plan will need to be specific to an organization's unique needs and requirements.

When organizations have developed an incident response plan, they should also endeavor to test and improve their plan and processes consistently. This is because, as mentioned earlier, the cyber security landscape is continuously evolving and threats are getting more advanced and capable of evading detection and eradication. One of the best ways to ensure improvement is to consistently conduct attack simulations that will show organizations how well their incident response plans are performing at responding to incidents. Through these simulations, organizations will also learn where did strategies might need more work and then implement the necessary measures to make improvements.

When making improvements, it's also critical that organizations streamline their incident response processes. The simple reason for this is when they streamline the processes, they will be able to identify any threats and respond to them a lot faster. This is especially relevant considering that incidents can go undetected for weeks or even months before organizations respond to them. All the while, they are able to induce significant operational, financial, and even reputational damage.

One of the most significant reasons for this is that many organizations rely on ad hoc investigations to detect and identify threats and incidents. Unfortunately, this is often not enough to prevent even the most basic attacks. We will deal with more suitable threat hunting methodologies in more detail later in this whitepaper.

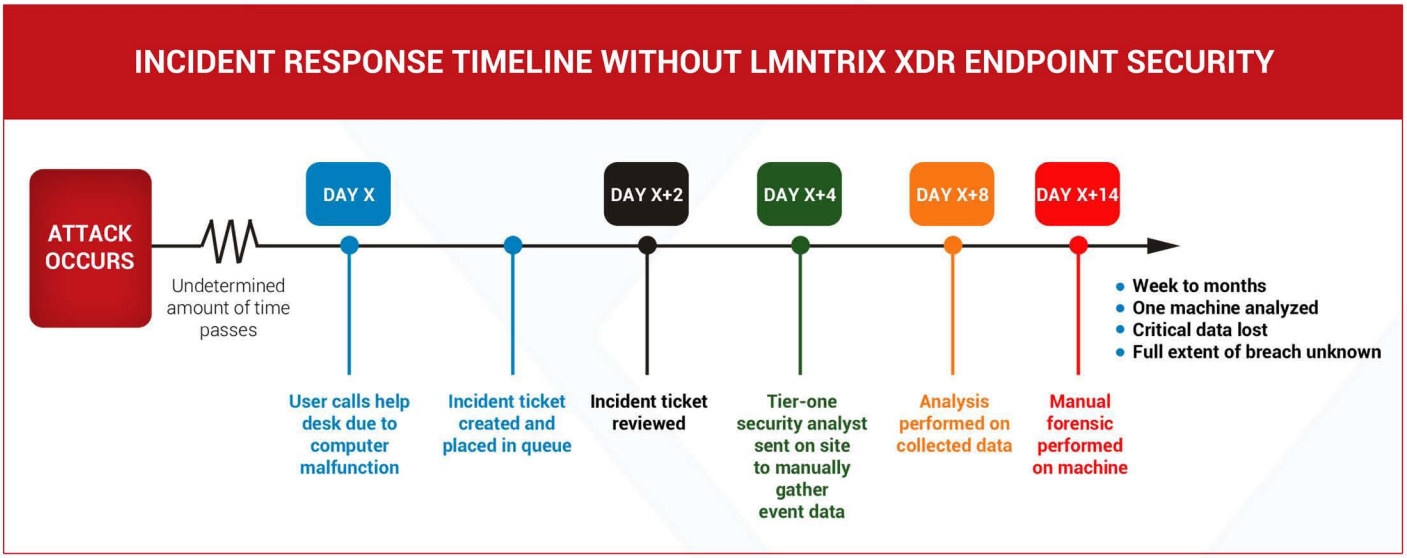

Figure 14 - Streamline Incident Response without LMNTRIX XDR Endpoint Security

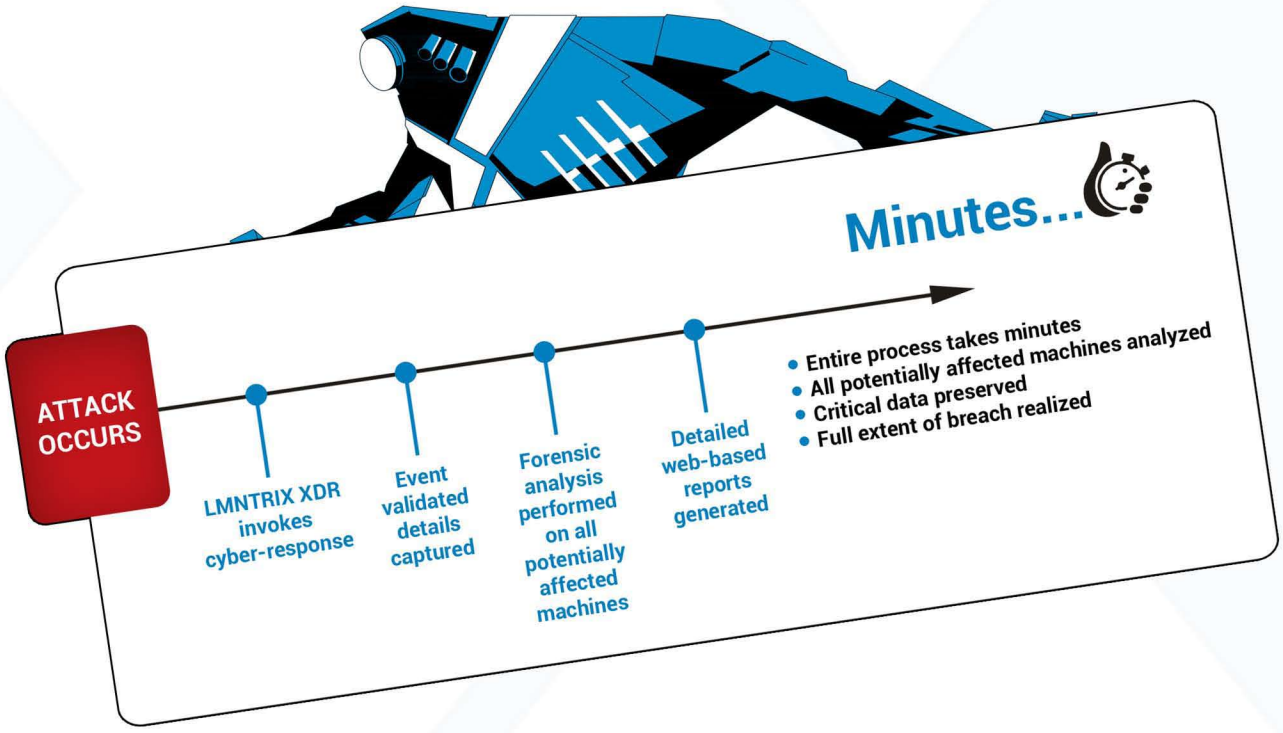

Figure 15 - Streamline Incident Response with LMNTRIX XDR Endpoint Security

Other ways to streamline incident response are to integrate data across all incident response processes and use automation to make detection and identification of threats quicker and easier. For example, in the case of a malware attack, an EDR solution can detect a suspicious sample and then isolate it automatically for investigation. In addition, once the sample has been analyzed as malicious, further automated processes can identify other endpoints that are infected and isolate them as well. When this happens, the solution can then also identify vulnerabilities in the network and inform security teams to take corrective action to remedy these vulnerabilities while, at the same time, storing the data relating to the incident for future reference.

While streamlining incident response and taking the other actions mentioned above are critical in a decisive response process, organizations should also focus on their overall incident response function. A better way to think of a decisive response process is to think of the aspects mentioned above as the building blocks of the process, and the overall incident response function as the foundation of it.

As a result, organizations need to build their response strategy on the right:

- **People.** It is crucial that organizations have the right incident response teams for their strategies to be most effective. As such, these teams have to be well coordinated and well-trained while having the appropriate skills and expertise to effectively address and deal with all aspects of an incident's lifecycle.

- **Processes.** As mentioned earlier, organizations need a consistent and well-defined incident response plan that will help them respond to cyber security incidents and attacks. It is also vital that these plans are continuously and consistently updated and refined to make sure they evolve as the cyber security landscape evolves.

- **Technology.** Apart from the right people and processes, organizations also need the right technology. In fact, it could be argued that it is the technology that binds the entire process together and enable the people to execute their functions in terms of the incident response plan. As a result, the technology an organization uses not only makes its incident response processes more effective and efficient, but it also gives its teams insights into events and incidents which, allows them to make better decisions and act on those decisions.

Ultimately, when all these fundamentals are in place, an organization's incident response function will be effective. If not, however, and organization focus on these aspects in isolation, the incident response process will only deliver marginal benefits, if any.

EDR Deployment Strategies

The next important aspect to understand is the different deployment strategies that can be used when implementing an EDR solution. In this respect, there are two ways organizations can consider when deploying an EDR solution, depending on their specific needs and requirements.

The first is an on-premise deployment, which could take the form of a software solution or a physical network security appliance that blocks unwanted traffic. Organizations that choose on-premise deployments are typically protective of their data and, as such, prefer to keep all their data on-site. In turn, this then involves implementing an on-site EDR solution.

While this deployment strategy can be effective for smaller organizations with offices located in the same geography, it does have some significant drawbacks. For instance, on-site EDR deployments typically don't support real-time behavioral analysis and often require longer response times. This lessens their impact and reduces their effectiveness in protecting the organization against threats.

Apart from these drawbacks, on-site EDR deployments also lack flexibility, and they're time-consuming to update. This inhibits their scalability and impacts the organization's agility negatively. More importantly, on-site deployments are more expensive than their cloud counterparts on most occasions. This is a relevant consideration for organizations that want to limit their expenses.

Cloud deployments are the ideal option for organizations that seek scalability, flexibility, and improved management. For this reason, they are more commonly used compared to on-site deployments. Apart from this, cloud deployments offer several other benefits.

For instance, cloud deployments offer faster response time and more effective protection. This is partly due to the fact that, with cloud deployments, remote response is possible. In addition, cloud deployments always offer the most updated protection, and it eliminates the constant updating and maintenance cycle encountered with on-premise deployments.

More importantly, because of the benefits mentioned above, cloud deployments don't require the management overhead, which, in turn, reduces the costs involved for organizations, and with their improved flexibility, these solutions are almost infinitely scalable.

For some organizations, depending on their unique needs and requirements, a hybrid deployment could also be a suitable approach. In this way, they're able to eliminate, to a large extent, the disadvantages of both approaches while incorporating the benefits of both in one solution.

Pre-Planning a Deployment

Irrespective of the deployment strategy an organization chooses, there are certain crucial steps the organization should follow before an EDR solution can be deployed. These steps can also inform the organization about which deployment might be most appropriate in its circumstances.

These steps include buy in from the management, assessing the infrastructure requirements, formulating a security policy, discover & profile endpoints, implement secure configurations, user security awareness, team collaboration and integrating security controls to provide complete visibility across the enterprise.

- **Assessing and understanding the infrastructure requirements.** The first step in the process is assessing and understanding the specific infrastructure requirements involved in deploying the EDR solution. In this regard, it is important to understand both the requirements and costs of hardware, software, upgrades, maintenance, and management. For example, depending on the amount of data the solution records, it could be resource-intensive or require significant bandwidth. These all impact the strategy to deploy the solution most effectively. The organization should also ensure that the solution is compatible with its operating systems, platforms, systems, and aligns with its scalability goals. Ultimately, the goal of this step is to ensure that the specific solution meets all the organization's needs and requirements.

- **Formulating an overall security policy.** No matter what deployment strategy an organization chooses, EDR will be ineffective if used on its own. As such, EDR is only effective if used as a component of an overall security policy. For this reason, organizations should develop this security policy before deploying an EDR solution. This involves conducting risk assessments, developing intrusion policies, and determining administrator responsibilities. This is the only for organizations to not only know what they need to protect, but also the best way to protect it.

- **Taking the process based approach.** Developing the security policies mentioned above is only one piece of the puzzle, though. As such, EDR can only be an effective tool for assessing, monitoring, and protecting endpoints if the security policy is implemented properly. As a result, the processes and procedures as provided in the security policy should be implemented with proper governance and compliance. If not, the security policy and the benefits offered by EDR will not amount to much and will be wholly ineffective.

- **Discovering and profiling endpoints.** It is crucially important to discover and profile all endpoints that need to be protected. This process of categorization and risk assessment plays a vital role in determining the risk posture for all endpoints and selecting the appropriate approach for monitoring and protecting them. In addition, once an EDR solution is successfully implemented, new endpoints that join the network should be consistently identified and assessed. Fortunately most, EDR solutions have this capability and if they don't, they should be integrated with monitoring solutions in order to identify these endpoints.

- **Implementing secure configurations for protection.** When doing the risk assessment mentioned in the step above, organizations will also learn how endpoints should be protected. These risk assessments will also help organizations reduce risk by minimizing the attack surface by configuring secure configurations for endpoints. And implementing these secure configurations for an organization's endpoints ensure that EDR works most effectively.

- **Fostering user security awareness.** Up to now, we've mostly dealt with technology-related aspects that should be considered before choosing and deploying an EDR solution. In addition, organizations should ensure that they create and foster security awareness under their users. As such, users must consistently be informed about security fundamentals, security issues related to their jobs and responsibilities, and safe computing. When this is done, the people within an organization will support the EDR by lowering the true positives, which, in turn, increases its effectiveness of the EDR investment.

- **Establishing management support and team collaboration.** For an EDR solution to be most effective, it's crucial that there be complete buy in across an entire organization. And this involves taking a top-down approach where leadership plays a significant role. In addition, to get complete buy in it's also necessary that there is an alignment and efficient collaboration across the enterprise, specifically between IT and security teams. When there is, teams will be better able to detect, analyze, and respond to incidents and breaches. For this reason, it's important to consider an EDR solution that facilitates integration and collaboration.

- **Deploying integrated intelligence.** We have already mentioned that the threat landscape is continuously evolving. As a result, it is essential to have threat intelligence to ensure that an EDR solution is as effective as possible. For example, LMNTRIX Intelligence aggregates over 300 threat intelligence sources and the proprietary technology behind it allows LMNTRIX to provide early detection and identification of adversaries in any organization's network. This is achieved by making it possible to correlate over 650 million threat indicators against real-time network data. Organizations will be better placed to protect themselves against both current and emerging threats, with context relevant threat intelligence provided by the likes of LMNTRIX.

Choosing an EDR Solution

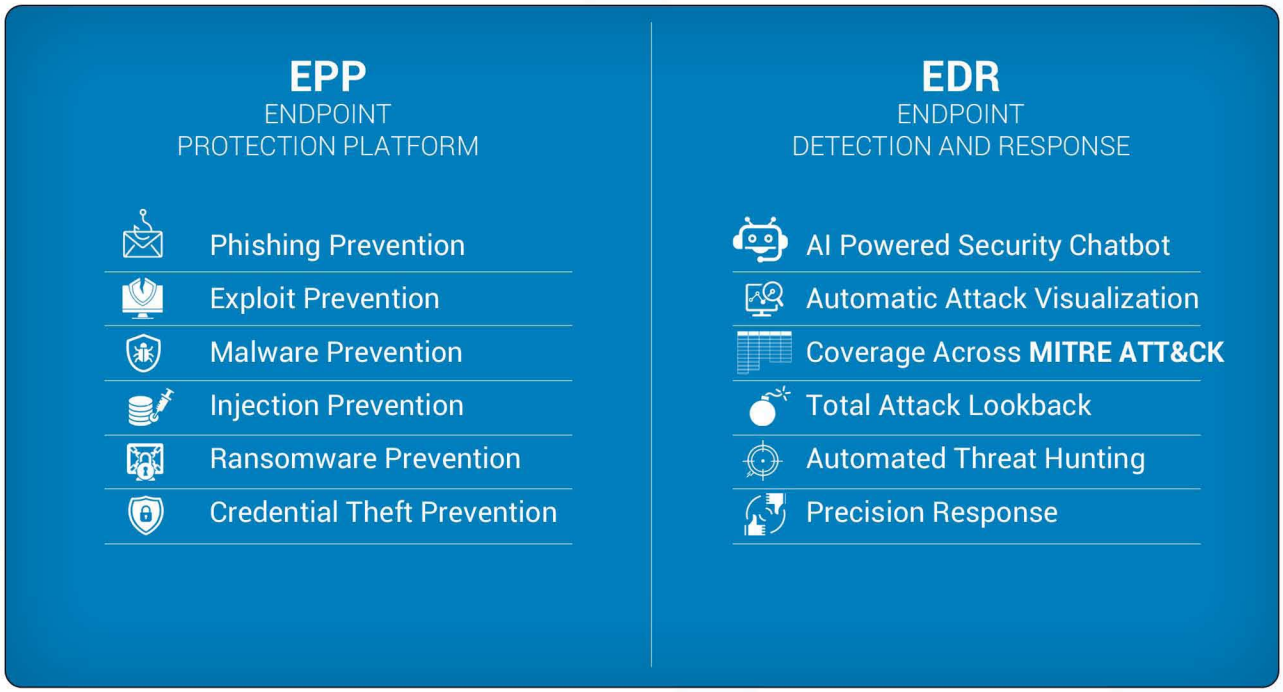

Figure 16 - LMNTRIX EDR / EPP Features

The next step before deploying an EDR solution is choosing the appropriate one based on an organization's specific requirements. When choosing the right solution, organizations must ensure that it complies with these requirements:

- First and foremost, the EDR solution should be able to provide protection based on the organization's needs and requirements and reduce the organization's risk. If it does not provide adequate protection, it is not worth the investment. You can use the above LMNTRIX XDR Endpoint Security solution features as a guide of what to look for.

- The solution must offer support for all the endpoints on the organization's network and provide in-depth visibility into all endpoint security, activity, communication, and configuration. In addition, it should also offer detailed monitoring of all endpoints on the network. At minimum there should be support for most common operating systems such as Windows, Mac and Linux.

- The solution should offer automated prevention, detection, and response capabilities and, as mentioned above, integrate with threat intelligence services. These capabilities, ultimately, enhance the effectiveness of the solution in dealing with threats. At LMNTRIX we rely on this Intelligence extensively and it represents a significant portion of threats we detect for our clients on a daily basis.

- The solution should also integrate with the other components of the organization's security infrastructure. Simply put, the EDR solution should form part of an effective, overall security strategy instead of standing on its own. As part of an overall strategy, the EDR will be able to provide valuable insights into endpoint activity and improve communication and collaboration, which, in turn, facilitates better detection and response capabilities. At LMNTRIX for example we have unified our tech stack onto a single XDR platform that allows our platform to share context and intelligence while our analysts single click investigation from any alert into logs, packets, endpoint, deceptions, machine or underground intelligence.

- The cost of the solution should fall within the organization's budget. Simply put, if the organization cannot afford to pay for the solution and operate it professionally, it will not provide any protection. Most importantly, the operating cost of an EDR may in many cases exceed the initial procurement cost, especially if the organization hires dedicated analysts and/or tries to setup a 24/7 operation. As such, if the cost exceeds the budget, it is better to steer clear. In addition, the EDR solution should also provide extensive product support including support for installation, set-up, and onboarding as the case may be. It's important to remember that this might be an additional cost item, so organizations should factor this into their budgets.

Deploying an EDR Solution

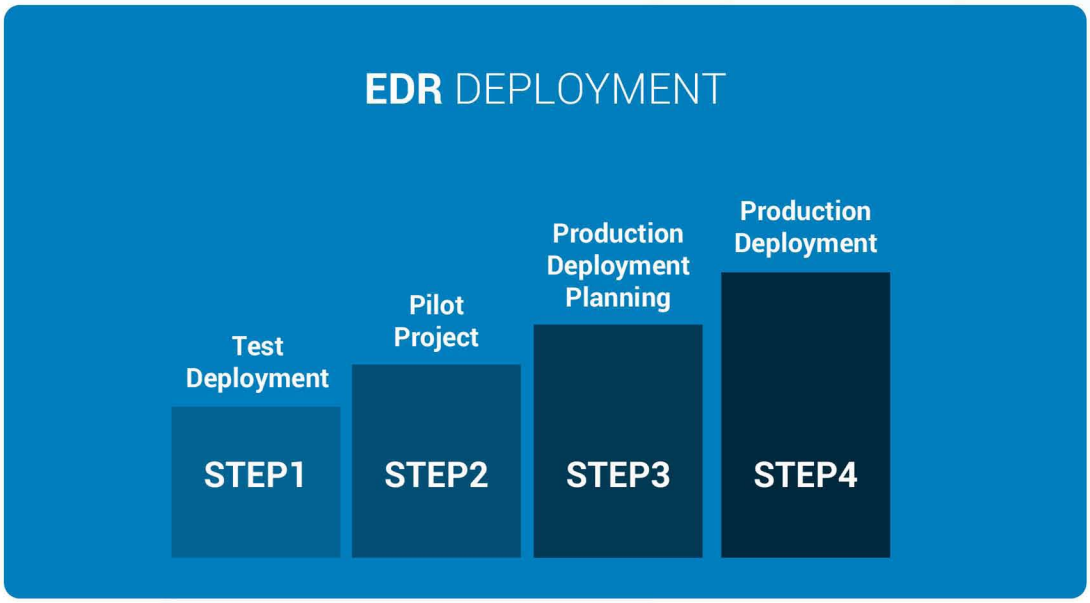

Figure 17 - A Phased Approach for EDR Deployment

Once the preparatory steps mentioned above have been taken, organizations can deploy the solution based on their chosen strategy. However, deployment is not as easy as flipping a switch and can be complicated. For this reason, and to ensure the best results, deployment should be undertaken using a phased approach.

Step 1: Test Deployment

The first step is to implement a test deployment that is, at its core, experimental and shows how the EDR deployment works, how it is installed and configured, and how it is used. As such, this deployment should not be implemented on an organization's main network, but rather on a test network. It should also have access to the remainder of the organization's security infrastructure, a sample of endpoints found on the main network, and other equipment present on the main network.

This test deployment gives organizations the opportunity to integrate the EDR solution into their security infrastructure, get support from the vendor, and, ultimately, get everything working as it should. It also gives organizations the ability to start testing threat detection processes and response capabilities. The test deployment also helps organizations identify and eliminate any issues or challenges in its deployment before being deployed on the main network.

Step 2: Pilot Project

When performing a test deployment, organizations will gather a wealth of insights into how the EDR performs, how it should be configured to be most effective, and how it integrates with the rest of the organization's security infrastructure. The organization can then use these insights and data to deploy the EDR on a selected subset of the organization's main network. During this stage, it's also important to involve employees in the process, who can test how the solution works and provide feedback.

Such a pilot project has one major benefit over a test deployment, in that it provides insights into typical user behavior and how the EDR solution performs in real-world circumstances. In turn, this shows organizations how well they will be able to deal with unexpected surprises and challenges they might not have encountered in the test environment.

It's important to remember that the pilot project might be an iterative process. As such, the process will repeat as the organization tests different configurations of the deployment and makes changes or improvements to make it more effective. Ultimately, the goal of the process is to cycle through different configurations to find the implementation that is more suitable based on the organization's needs and requirements, and working through each iteration of the pilot project will inform the most suitable implementation for the final deployment.

Step 3: Production Deployment Planning

After the pilot project is complete, the solution is almost ready to deploy. However, before deploying the EDR solution to production, it is crucial to plan properly. This typically involves coordinating with the organization's IT department and, if necessary, external service providers on when the deployment will be scheduled.

This schedule is also important to ensure that both on-site and external support teams are on hand to ensure that the deployment runs smoothly.

During this planning process, it is also important to gain an understanding of how the deployment will be configured and what effect it will have on the organization's network and systems. Ultimately, the goal with production deployment planning is to ensure that the EDR solution is deployed with as little disruption as possible and that the deployment is successful.

Step 4: Production Deployment

With planning complete, the solution can be deployed. To limit operation disruptions, it should be done on the schedule as planned, which will typically involve that the solution be deployed over a weekend, depending on the organization, of course. Depending on the specific solution, it might also be necessary to, in anticipation of the deployment, train the necessary personnel who will work with the solution. This will typically include the team who will handle events, detections, and responses. Once the full deployment is completed successfully, the organization will start to enjoy the benefits offered by the EDR solution.

Keep in mind, however, that the steps outlined above only serve as a broad outline of what the deployment process might look like, and it could differ based on the specific solution or the organization's requirements. In addition, the process can also vary depending on the type of deployment the organization uses.

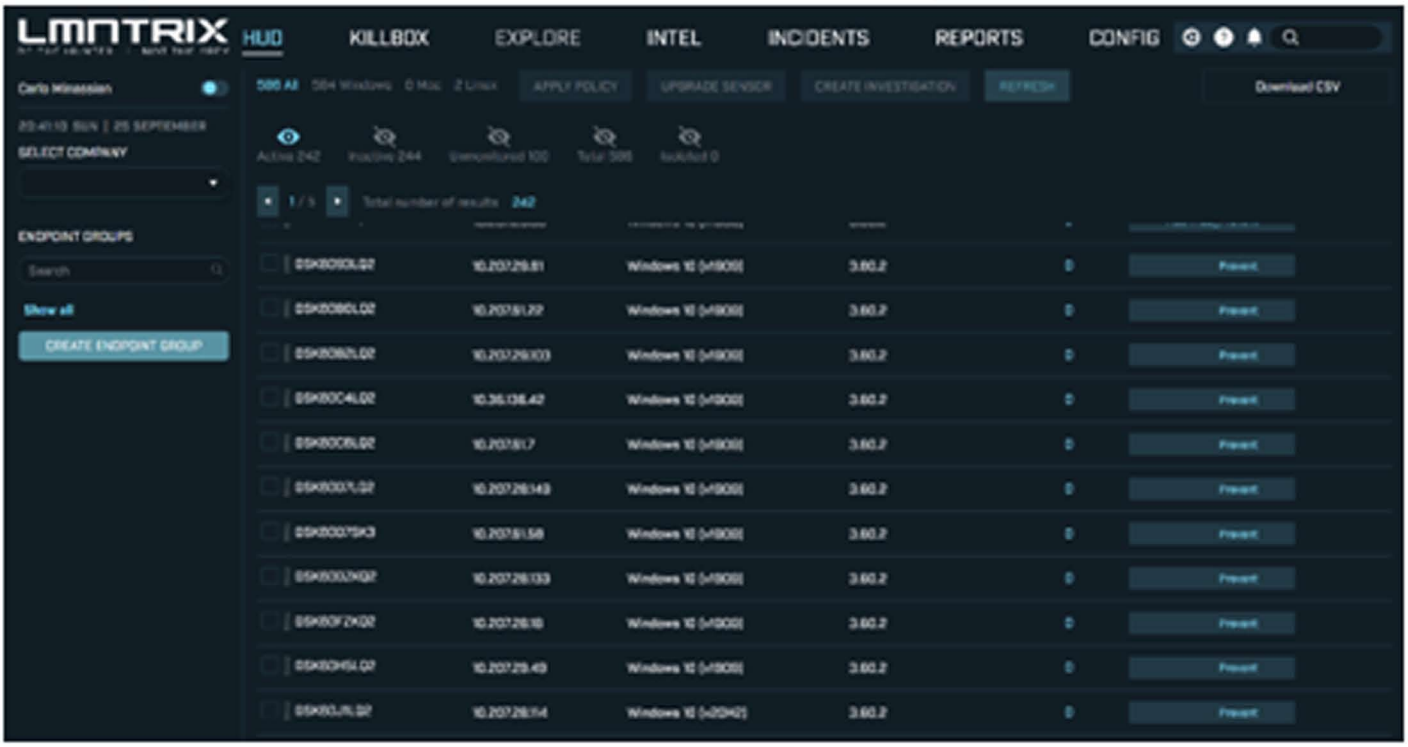

Figure 18 - Managing a Deployment using the LMNTRIX XDR Endpoint Security

Framework for Threat Hunting With EDR

We have now provided an overview of EDR, how it differs from traditional antivirus solutions, and how organizations would go about deploying an EDR solution. One question that remains open, however, is how these organizations can use EDR for threat hunting. Before answering this question, it's important to first discuss what threat hunting is and why organizations need it.

But first a quick definition of what is adversary hunting?

Adversary hunting is the stealthy and surgical detection and eviction of adversaries within your network without prior adversary knowledge or known indicators of compromise. The goal of hunting is to detect and evict adversaries that have bypassed defenses before damage and loss can occur. To do so, a hunter must be able to enter the network undetected, identify the adversary at any stage of the kill chain, and evict them without disrupting running systems. There are three key components of adversary hunting: stealth, early detection, and surgical response.

Stealth

Adversaries are looking for you as much you are looking for them. They hide and adapt their behavior upon detection of any traditional security tools. Enterprises must be stealthy and hide their presence from these advanced and adaptive adversaries.

Early Detection

Enterprises are often informed by a third party about a compromise on their networks, about 53% of breaches are detected by third parties, by then the damage has already occurred. Adversaries need to be rapidly detected at all phases of the kill chain to stop them from gaining un authorized access to critical systems and reduce the damage they can to inflict on the enterprise.

Surgical Response

Most adversaries target mission critical systems within enterprises, which are crucial to daily business operations.Once the source of compromise has been identified, these adversaries must be stopped. It is key to remove them surgically without any business disruption.

Why Organizations Need Adversary Hunting?

At its core, adversary hunting is the process of proactively searching for threats across a network. This proactive approach allows organizations to identify any threats that might have succeeded in avoiding detection by the organization's initial detection solutions. In a modern, technology-driven world, this is a vital capability because, as mentioned above, the time between an initial breach by the attacker and when an organization finds out about the breach can be up to 287 days.

During this window, also known as the dwell time of an attack, attackers can steal valuable information and compromise an organization's data. Simply put, the longer the dwell time, the more severe the damage. By way of reasoning, the faster the organization can identify a breach, the faster they can respond to any incidents, and the better they can limit the risk and severity of the damage.

Developing a Framework for Threat Hunting

When developing a threat hunting framework, it's important that organizations build their capabilities around a set of processes and tools that allow them to effectively identify and respond to cyber threats. EDR provides a valuable tool that allows these organizations to gather valuable insights and data relating to the suspicious endpoint activity on their networks.

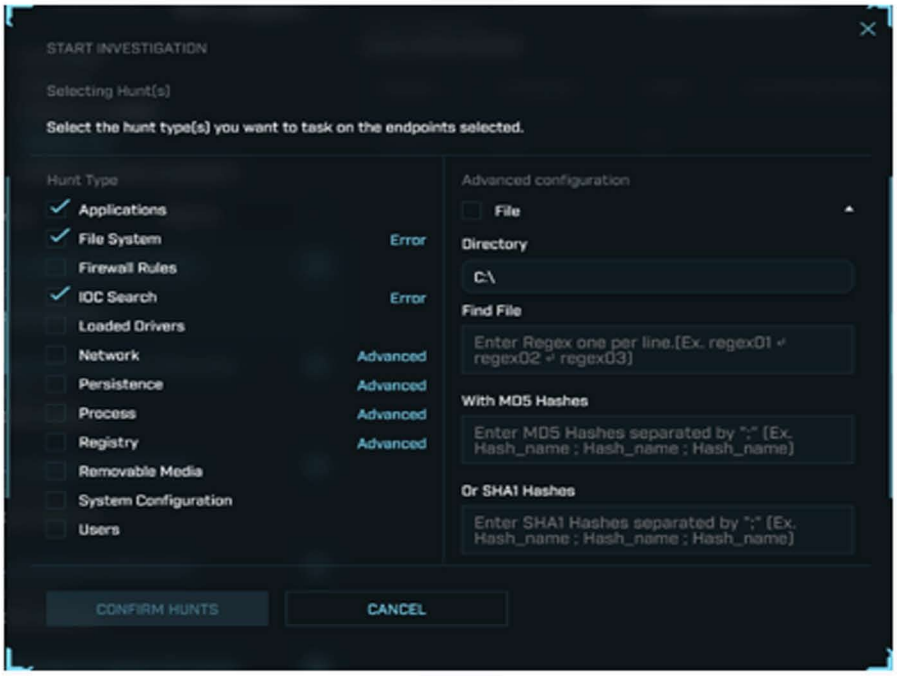

Figure 19 - Extensive Hunting Capability with the LMNTRIX XDR Endpoint Security

Threat Hunting Methodologies

Developing a framework for threat hunting firstly relies on choosing the right threat hunting methodology. Here, there are, generally, four different threat hunting methodologies:

- **Intelligence-based threat hunting.** This methodology relies on using sources of intelligence to prevent and respond to attacks. There are several sources of intelligence including indicators of compromise (IOCs), hash values, domain names, IP addresses, and more. Based on this intelligence, threat hunters will then define triggers that they will use to identify and uncover possible attacks and malicious activity.

- **Hypothesis-based threat hunting.** This methodology involves developing hypothesis about attacks and these investigations often result when a new threat has been identified and threat hunters investigate whether the attackers' tactics, techniques, and procedures (TPP) can be identified within their own network. This process typically involves testing three different types of hypothesis. Firstly, hypothesis can be formulated by making use of data analytics, machine learning, and behavior analytics, which allows threat hunters to analyze vast amounts of data to detect and identify any irregularities that might suggest malicious activity. Hypothesis can also be formulated and tested by using intelligence like malware analysis, vulnerability scans, and intelligence reports and feeds. Finally, hypothesis can also be formulated through situational awareness that allows threat hunters to assess enterprise risk and identify the digital assets that are critical to the organization. Since the process of Hypothesis-based threat hunting requires the analysis of vast amounts of data, it requires that large parts of the process should be automated.

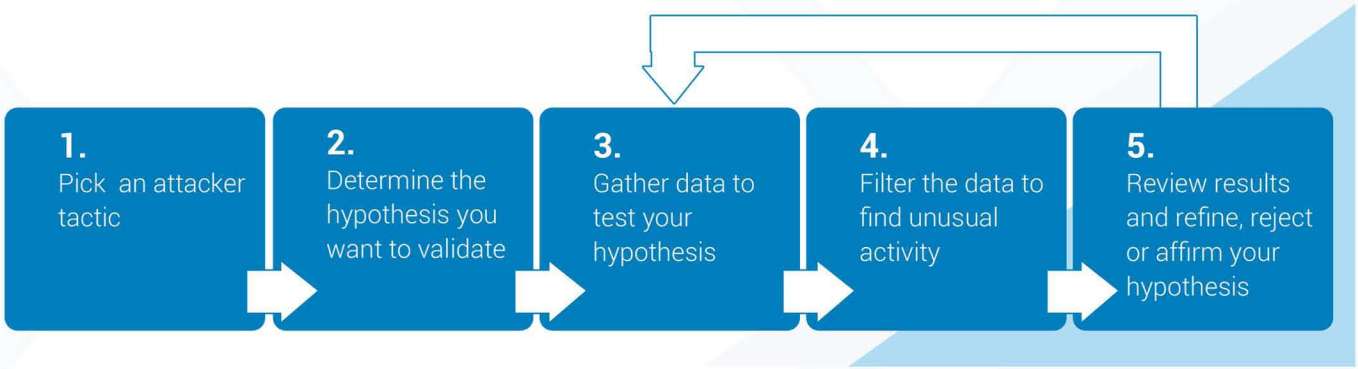

Figure 20 - Hypothesis-based threat hunting

- **Indicators of attack (IoA) investigations.** This methodology relies on identifying advanced persistent threat groups and malware attacks by using global detection frameworks or play books. As such, these types of investigations are often aligned with well-known threat frameworks such as **MITRE ATT&CK**. When implementing this methodology, threat hunters will use these indicators of attack and TTP's to identify possible threats. They will then develop a hypothesis that aligns with the threat framework and, after identifying a suspicious behavior, they will monitor suspicious activities to locate patterns and identify threats.

- **Hybrid approaches.** With hybrid approaches, organizations will use a combination of the mentioned investigation methodologies to locate, identify, and isolate threats. This gives organizations the flexibility they need to customize their threat hunting approach based on their specific requirements.

THREAT HUNTING FRAMEWORK

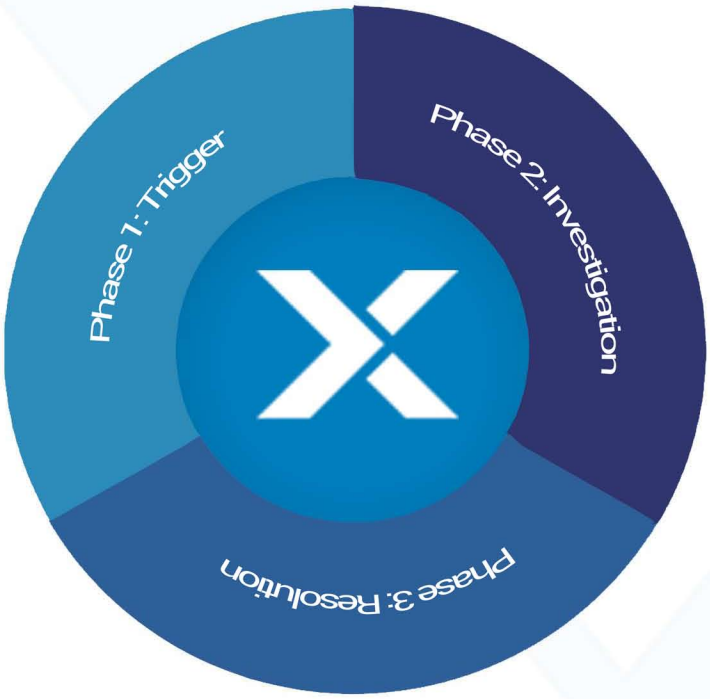

Figure 21 - Threat Hunting Framework

Irrespective of the methodology chosen, an effective, proactive threat hunting process has three phases. The first phase is when the threat hunter collects information about their network environment and formulates hypothesis of potential threats. Based on the hypothesis, they will then define a trigger that will result in further investigation. Apart from using hypothesis, threat hunters can also define triggers based on particular systems, platforms, network areas, and more.

During the next phase of the threat hunting process, and after a trigger is defined, the threat hunter will focus on proactively searching for anomalies or patterns that can prove or disprove the hypothesis developed earlier. This phase of the process relies on a wide range of technologies and tools that enable threat hunters to investigate these anomalies to, ultimately, determine whether they are malicious or not. During this phase of the process, EDR plays a vital role and gives threat hunters access to in-depth, detailed information about potential threats.

During the resolution phase, threat hunters will also use tools that can analyze and store information about potential threats. Irrespective of whether a suspicious activity was malicious or not, this information can be helpful for future investigations and analysis. As such, it can assist security teams to identify and predict trends and patterns, remedy vulnerabilities, and improve an organization's overall security measures.

THREAT HUNTING BEST PRACTICES

Figure 22 - Threat Hunting Best Practices

Now that we've seen what a typical threat hunting framework looks like, it's important to remember that this process should be as effective as possible. If it is, organizations will be able to better detect and eliminate threats. What follows are some best practices organizations should implement when developing and implementing their threat hunting frameworks. These best practices will improve the overall security measures of an organization.

Use the Right Data in the Right Context

Any effective threat hunting framework should be based on the right data. And here, EDR plays a vital role. It allows organizations to gather detailed endpoint information, activity, and behavior most likely including several operating systems, network traffic patterns, user activity, file hashes, network activity, file operations, connections, peripheral device activity, activity and event logs, and more.

Comprehensive endpoint data, however, is only one piece of the puzzle, and it doesn't mean much without the necessary context. This context, as mentioned earlier, is gained through the correlation of system activity to events, which, in turn, allows threat hunters to better detect and understand malicious behavior or attacks.

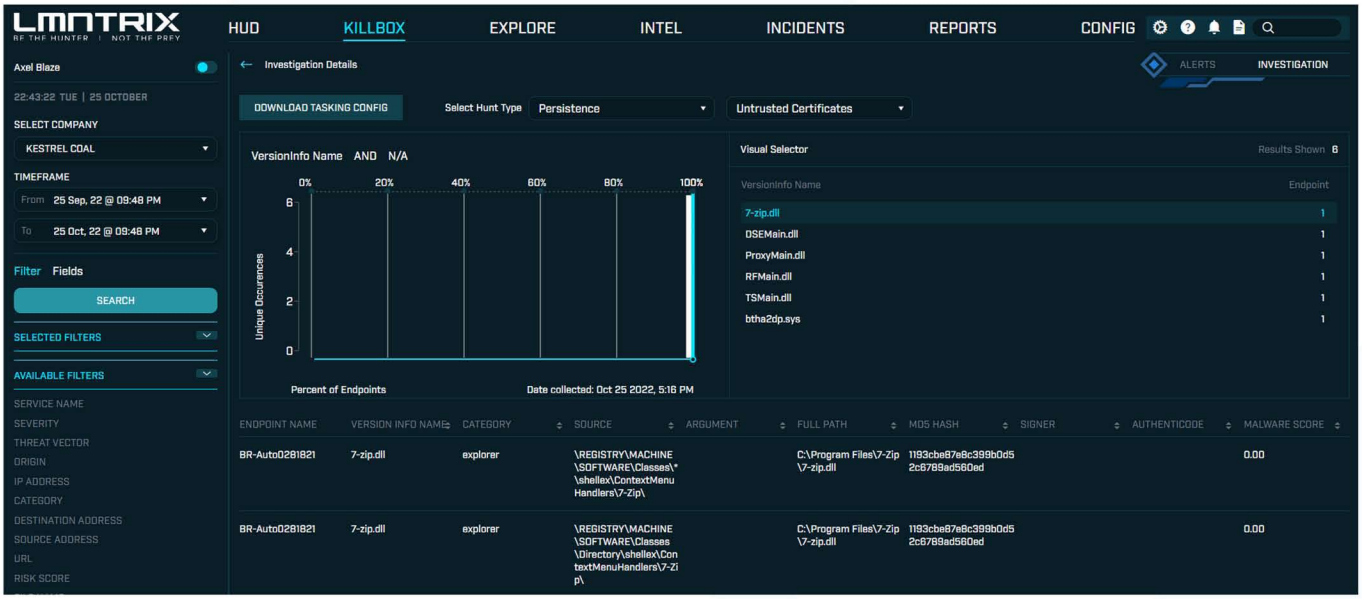

Figure 23 - LMNTRIX XDR Hunting for Untrusted Certificates

In this respect, EDR also plays a vital role because it constantly monitors all endpoints, irrespective of whether it detects an anomaly or not. These volumes of data allow EDR solutions to provide real-time, contextual information about events. As a result, when utilizing this information, threat hunters can make sense of the data and understand the complete picture around an event.

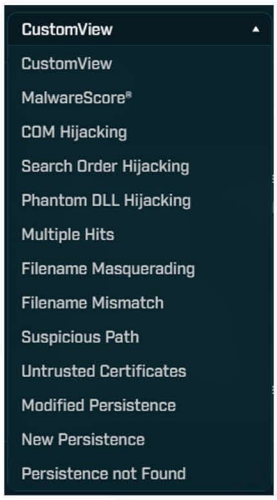

Figure 24 - LMNTRIX XDR Pre-defined Hunting Options

Understand What is Normal in the Network Environment

Apart from having access to the right data in the right context, it's also important organizations understand what is normal in their network environments. When they do, they will be better able to identify and detect malicious and adversity behavior. As a result, organizations need to understand their profiles, employee behavior, their valuable data, and their business activities. Understanding these aspects could help them establish a baseline of their"normal" and inform them what attackers could possibly target.

Once again, in this respect, EDR plays a crucial role. This is because modern EDR solutions use advanced user behavior monitoring and machine learning algorithms to distinguish between normal processes and behavior and possible malicious behavior. Once it identifies such an instance, it will trigger an alert, which would then necessitate an investigation. Ultimately, this makes the threat identification and detection process a lot faster and more accurate, which means faster response times and reduced risk.

Develop Hypothesis on Threats

Once organizations are armed with the right data in the right context and a baseline of what is normal, the next step in the process is to start hunting for threats. Here, the process differs based on whether a threat is known or unknown.

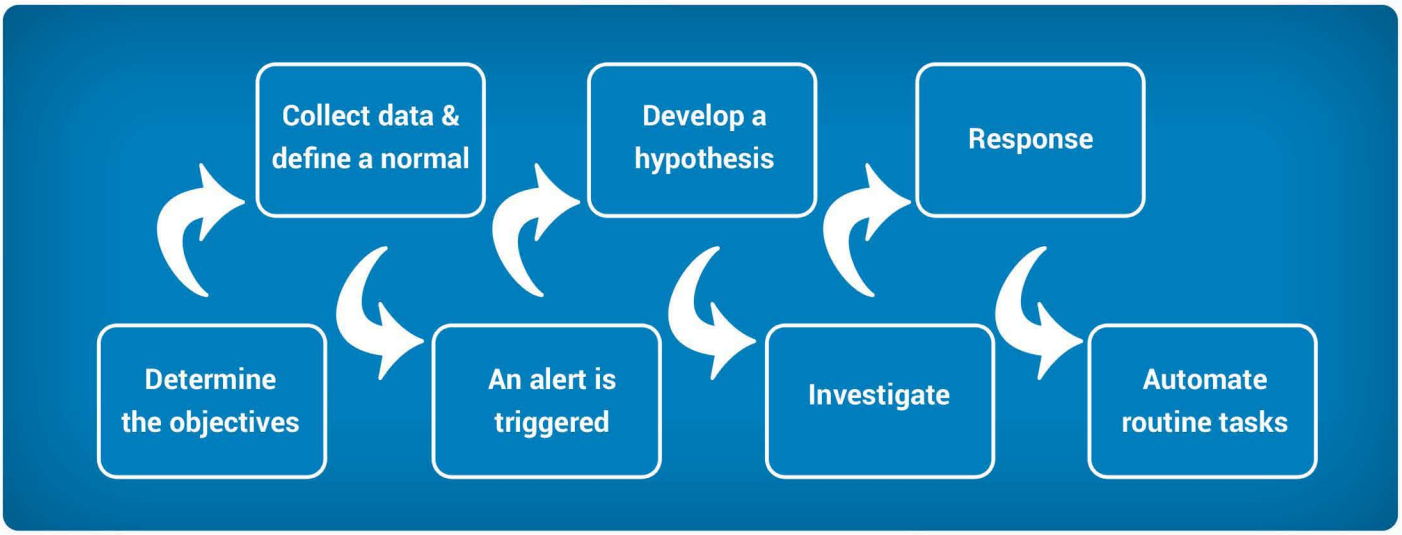

Figure 25 - Hunting for Threats

If the threat is known, threat hunting will be based on intelligence sources like hash values, IP addresses, domain names, and IOCs. In other words, the intelligence-based threat hunting methodology mentioned earlier will be implemented. When such a treat is identified, a trigger will alert threat hunters of its presence and prompt them to take further action.

For unknown threats, the hypothesis-based threat hunting methodology referred to above will be implemented. As such, organizations will formulate hypothesis about the activities that are taking place within their network environment and then test these hypothesis with a variety of tools.

For example, an organization might develop a hypothesis of where an attacker would attempt to gain access to their network environment. Once this hypothesis is developed, the organization would then test the hypothesis to validate if it poses a real threat. To test the hypothesis, organizations can use everything from behavioral monitoring, endpoint state assessment, network traffic analysis, physical disc inspections, and memory analysis. Once again, EDR plays a vital role in these processes as it provides valuable endpoint data.

Investigate any Possible Threats

When a hypothesis appears to be correct, and the threat hunter finds evidence of possible malicious activity, the next step is to investigate these possible threats further. During this investigation process, it is critical to determine the nature of the threat, the extent of the threat, and the possible impact of the threat. This not only involves identifying the threat based on one of the indicators above, but also finding similarly infected endpoints on the network. In other words, during the investigation, it is important to determine the full scope of the compromise.

In this respect, EDR provides real-time data and behavior analytics that help threat hunters establish the scope of the incident and identify any other infected endpoints. As a result, threat hunters can obtain all the facts and the full picture of an event, which, in turn, shortens investigation time and, ultimately, speeds up the response.

Respond Effectively and Efficiently

Once the investigation into a threat is complete, threat hunters need to respond effectively and efficiently. This means they first have to contain and eradicate the threat so that it does not cause any further damage to the system or network. Containing and eradicating the threat can take a variety of forms, including blocking all network traffic, shutting off the affected system, isolating endpoints, disrupting the TTP, and more, depending on the specific threat.

Once eradicated, they also have to implement measures to prevent similar attacks in the future. Fortunately, as mentioned earlier, EDR collects a wealth of data about every event that gives threat hunters a complete understanding of what happened, why it happened, and what they can do to prevent it from happening again in the future. Based on these insights, security teams will then be able to develop and implement measures and strategies to better detect and prevent similar attacks.

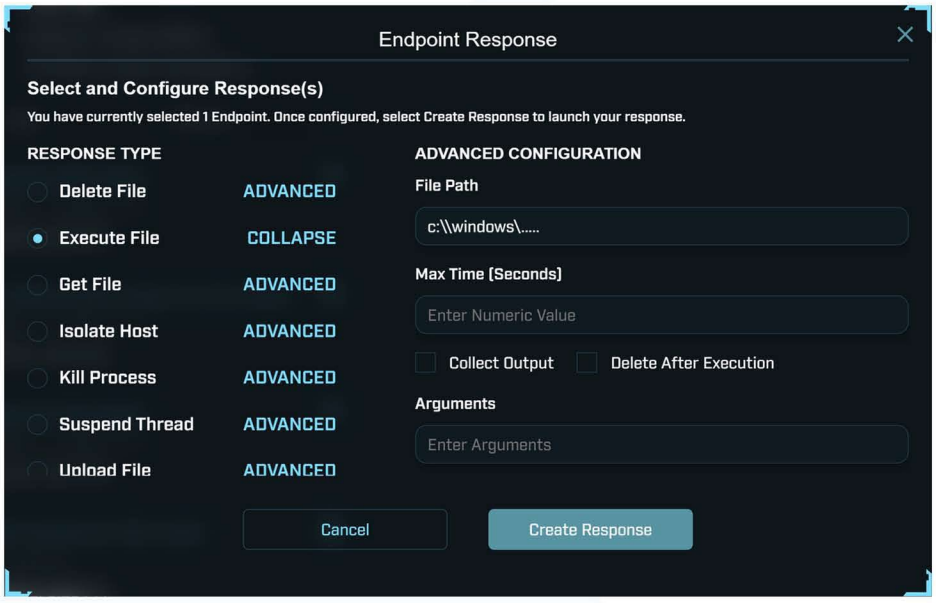

Figure 26 - LMNTRIX XDR Response Actions

Enhance Organization-Wide Security

The final step in the framework is to enhance organization-wide security with the insights obtained from the hunting, detecting, and remediating threats. During this process, security teams will use the data obtained from previous threats to improve an EDR solution's capability, which, in turn, improves security across all an organization's endpoints.

This is also where a solution like the LMNTRIX Active Defense comes into play. It is a validated and integrated threat detection and response architecture that hunts down and eliminates the most advanced and unknown threats that routinely bypass organizations' security measures. It includes a combination of cutting-edge technology, leading intelligence, and advanced analytics which, when used by professionals with unparalleled expertise, provides the ability to detect and investigate the threats other solutions fail to identify. In addition, it is also able to identify these threats with great speed and accuracy.

What A Threat Hunting Schedule Should Look Like?

The next aspect to consider when developing a threat hunting framework is to decide on a threat hunting schedule. In other words, the question that should be answered is how often threat hunting should take place. In this respect, it's important to distinguish between an organization's needs, requirements, and budget and what the ideal schedule should look like.

	LEVEL 0 TRADITIONAL Not considered Threat Hunting	LEVEL 1 EXPERIMENTAL Experimenting with Threat Hunting	LEVEL 2 INTERMITTENT Part-Time Threat Hunting	LEVEL 3 PROACTIVE Partial Use Case Generation / Execution	LEVEL 4 LEADING Complete Use Case Generation / Execution
PEOPLE	SOC Analysts Alert Driven mind set Basic alert triaging	SOC Analysts Basic understanding of forensics Good Endpoint / Network knowledge	Part time Threat Hunter Intermediate forensics knowledge Strong Endpoint / Network knowledge	Dedicated hunt team Strong Forensics / Malware Knowledge Strong Offensive Knowledge	Dedicated Hunt Team Level 3 capabilities plus research capability
PROCESS	24/7 Passive Monitoring	Ad Hoc Threat Hunting IOC Search	"Hunt Sprints" e.g. 1 Week per month Regular Threat Hunting	24/7 Proactive Threat Hunting Partial Use Case Generation	24/7 Proactive Threat Hunting Complete Use Case Generation Use Case Verification Use Case Automation
TECHNOLOGY	Traditional tooling e.g. SIEM Network IDS Network IPS Anti-Virus Alternative Automated Technology (i.e. Sandboxing) Based on "Known Bad" e.g. Signature-based Threat Intel Feeds	Endpoint Detection & Response (EDR) Partial Network Data Coverage Partial Deployment	Endpoint Detection & Response (EDR) Full Deployment Full-Time Automated EDR Usage (IOC Matching , Threat Feeds, etc.) Part-Time Advanced EDR usage (During Hunt Sprints)	Ability to Execute "HUNTING USE CASES" (Partial) Full-Time Advanced EDR usage Full Coverage of Network / Log Data Bespoke Configuration	Ability to execute "HUNTING USE CASES" (Complete) Level 3 Technology, plus: Tight Integration Between Data Sources Bespoke Development and Custom Use of APIs

Figure 27 - Threat Hunting Maturity Model

For example, some organizations might choose to perform threat hunting only on an ad hoc basis. This means they will typically hunt for threats when a specific event is triggered, such as, for example, the unauthorized access of a specific resource. They might also choose to threat hunt when they have staff available who are not busy with other duties or talks. This gives organizations that have limited budgets and staff an extra layer of protection. However, this is the least effective strategy to use when threat hunting.

For this reason, many organizations prefer to schedule threat hunting. This strategy involves setting aside specific times, at regular intervals, when staff will perform threat hunting. While this is an improvement on the ad hoc strategy mentioned above, it does have some drawbacks. For instance, when scheduled hunts are too far apart, it can increase the dwell time for attacks. And the longer the time between the attack and its discovery, the more damage it can create. As a result, when organizations implement this strategy, it is important that they keep the intervals between hunt as short as possible and that they prioritize searches at different time to make the process more efficient and effective.

Ideally, however, organizations with the necessary budgets and work forces, should engage in continuous, consistent threat hunting. Remember, attackers don't work on a schedule and, for the most effective protection, organizations shouldn't either. And the most effective protection is only achieved when an organization's network and endpoints are proactively monitored in order to detect and identify any attacks.

Who Should Perform Threat Hunting?

The final question to be answered when developing a threat hunting framework is: Who should perform threat hunting? This question has two aspects that need to be considered. Firstly, many organizations might be under the misguided apprehension that threat hunting can be performed, to a large extent, by automated systems using technologies such as machine learning and artificial intelligence.

Unfortunately, this is not the case. Despite advances in artificial intelligence, it's important to remember that cyber attackers are human. They are extremely skilled, and they understand the inner workings and processes of traditional defense solutions. In addition, they are also persistent and constantly develop advanced strategies, tactics, and techniques to bypass the security of even the most modern security systems.

LMNTRIX firmly believes the best way to counter such a human attacker is with a human defender. This is simply because when these attackers attack an organization's systems, only humans can understand the actions they take and detect the trail they leave. In fact, it's the only way organizations can detect modern threats and protect their networks effectively and efficiently.

Now, the next part of the question is: If the process of threat hunting can't be automated, who should perform it? From reading this white paper, it is probably clear that threat hunting is a specialist task that requires highly specialized skills. As such, it will typically involve security specialists like penetration testers, red teamers, forensic analysts, incident analysts and responders, malware analysts, threat hunters, and intelligence analysts. These specialists possess offensive security skills and understand the risks organizations face, the techniques and tools used by advanced attackers, and who can use a variety of tools to detect threats, effectively respond to them, and reduce an organization's risks.

This presents other problems. For one, these experts are hard to find and identify, especially for organizations that lack security skills or expertise. This makes it challenging to recruit the right experts. Moreover, hiring these experts in-house involves a significant expense and many organizations might not have the budget to retain them. Considering the above, establishing a security team and hiring these experts in-house might not be a viable solution for many organizations.

A more effective and affordable solution is thus to use a Managed Detection and Response (MDR) service such as the LMNTRIX Active Defense, that provides a comprehensive security solution. These MDRs employ experts with extensive skills and expertise, use the most up-to-date intelligence, and monitor networks and endpoints around the clock to ensure to identify and confirm any threats or compromises and, in the process, protect organizations and their data against threats and breaches.

Figure 28 - LMNTRIX Active Defense

Framework for Detecting Adversary Behavior with EDR

We now have a broad overview of how organizations can develop a framework for threat hunting with EDR. Similarly, we will now consider a framework for detecting adversary behavior. A core foundation of the effectiveness of such a framework is to understand the tools, techniques and tactics adversaries use to breach networks or systems. Fortunately, there are many frameworks available that help organization to gain understanding, and one of the most popular is the MITRE ATT&CK framework.

MITRE ATT&CK

Created in 2013, the MITRE Adversarial Tactics, Techniques, and Common Knowledge framework is a curated knowledge base and model for adversary behavior that shows the various stages of the attack lifecycle and the vectors attackers are known to target. Depending on the specific operating system or platform, ATT&CK is available in three iterations.

Firstly, ATT&CK for Enterprise focuses on adversarial behavior on Windows, Linux, Mac, and cloud environments. As its name suggests, ATT&CK for Mobile focuses on adversarial behavior on iOS and Android devices. Finally, ATT&CK for ICS focuses on adversarial behavior within ICS networks.

Irrespective of the iteration, one of the framework's main aims is to provide a categorization of the set of techniques adversaries use to reach their objectives and the ways organizations can defend themselves against these actions. As a result, the framework is used by organizations globally for threat intelligence, intrusion detection, threat hunting, risk management, and more.

MITRE ATT&CK Matrix

This categorization of techniques and tactics in terms of the framework are done using the ATT&CK Matrix that sets out the objectives of attackers in a logical order from the first stages of an attack to the very last. So, with every objective completed, attackers would be one step closer to their overall objective.

For the broadest iteration of MITRE ATT&CK, ATT&CK for Enterprise, the Matrix contains the following categorization of adversary behavior:

- **Reconnaissance.** The adversary attempts to gather information about their target that they will use for future attacks. This information can include detailed information about an organization, its employees, and its infrastructure and can be used by adversaries in future stages of the adversary lifecycle, like when planning and executing initial access, the next phase in the lifecycle.

- **Resource Development.** The adversary obtains the resources they will use to target an organization. Adversaries typically obtain these resources by creating or purchasing resources like domain names and equipment or by compromising or stealing resources like code and can also include accounts, capabilities, and infrastructure.

- **Initial Access.** Initial access includes the techniques and tactics used by adversaries to gain initial access to an organization's network or systems. These techniques can include everything from obtaining access details through targeted phishing attacks to exploiting vulnerabilities in the organization's network. More importantly, the initial access gained by an attacker can be used for continued access and the execution of their other objectives.

- **Collection.** Collection consists of techniques adversaries will use to gather information and the sources of information necessary to achieve their objectives. Here, these sources include everything from storage drives to email and browsers, and techniques used to gather information include capturing screenshots and other inputs.

- **Command and Control.** For this objective, adversaries will use techniques that allow them to control compromised systems within their target's network. These techniques differ based on the specific network, and adversaries commonly attempt to mimic usual network behavior in order to evade detection.

- **Exfiltration.** Exfiltration includes the range of techniques adversaries might use to steal data from their target's network and to avoid detection while removing the data from the network. The techniques include data compression, encryption, and putting size limits on data.

- **Impact.** For this objective, adversaries will use techniques to disrupt the availability or compromise the integrity of systems or networks by manipulating or interrupting business processes. These techniques include manipulating or destroying data.

Now, the immediate question is:
How does the MITRE ATT&CK framework align with EDR?

The framework can serve a vital purpose when developing behavioral analytics. Here, it can help in correlating suspicious activity with malicious activity. As such, it can help security teams simplify the process of distinguishing between malicious and benign activity.

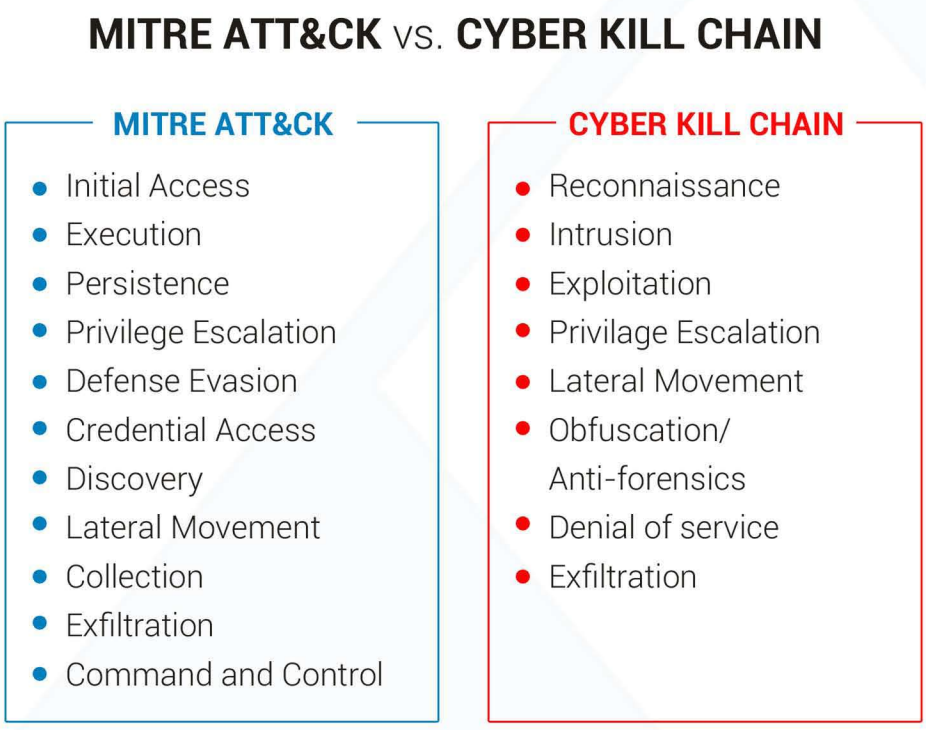

Figure 29 - MITRE ATT&CK vs. CYBER KILL CHAIN

In addition, the ATT&CK framework can also help security teams to enhance their threat intelligence. In other words, they can use the framework to obtain more detailed information about threats and threat actors. In turn, this allows security teams to determine if they can defend an organization's systems and networks against specific Advanced Persistent Threats (APT) and other common behaviors by multiple threat actors.

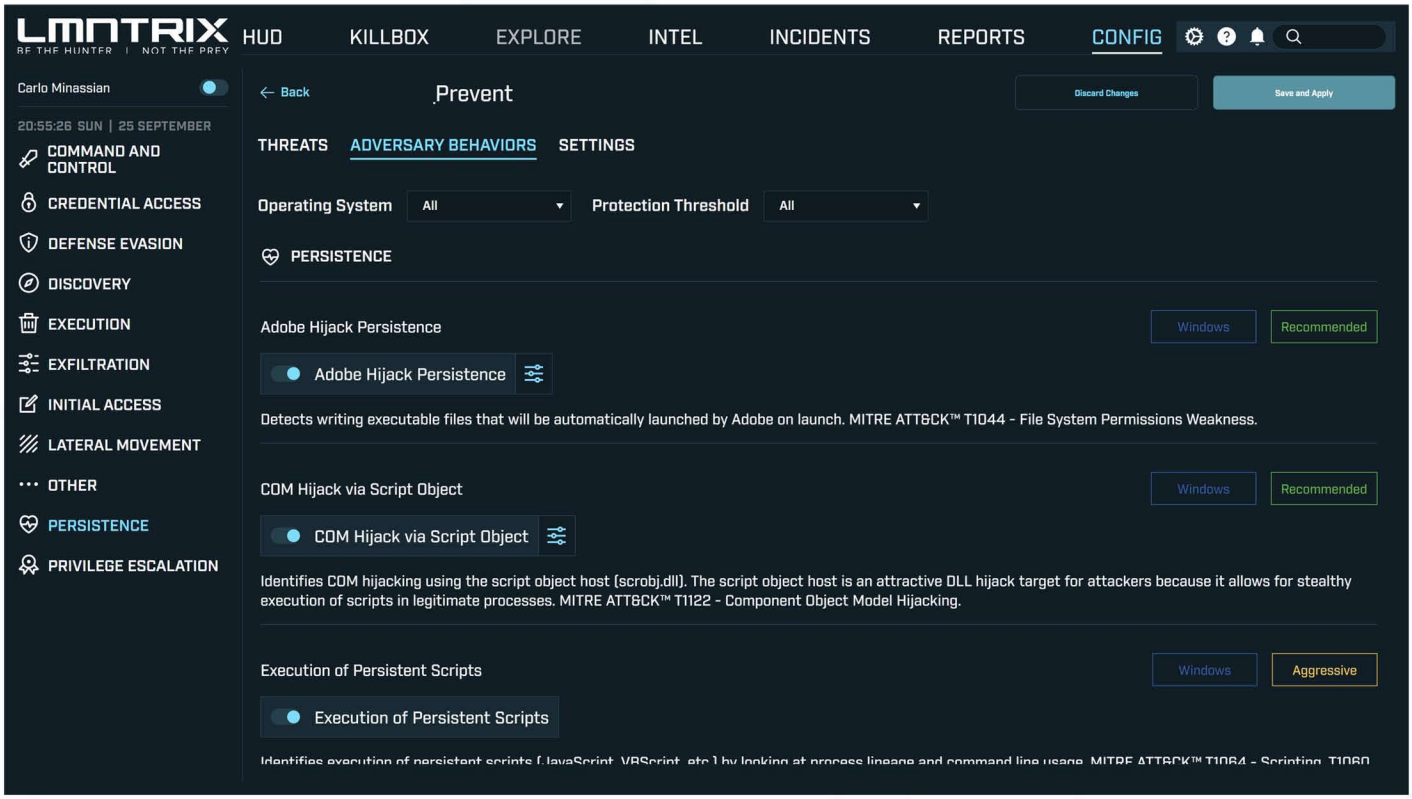

Figure 30 - Detection of Adversary Behaviors with LMNTRIX XDR Endpoint Security

Conversely, security teams can use EDR to detect and triage cyber threats at the endpoint level. To do this, they will typically use the following indicators:

- **Hash Values.** Has values like MD5 or SHA1 can indicate an attack if they correspond to specific suspicious or malicious files.
- **IP Addresses.** IP addresses might be an indication of a possible malicious attack.
- **Domain Names.** A domain name, or even a subdomain name, can be an indicator of possible malicious activity.
- **Network Artifacts.** All network activity leaves artifacts, and every piece of data that flows over a network as a result of adversary behavior can be considered an artifact. Most commonly, however, those artifacts that distinguish malicious activity from benign activity are considered to be indicators of malicious activity.

- **Host Artifacts.** These indicators are those caused by adversary behavior on an organization's hosts. Once again, only those that allow teams to distinguish between malicious and benign behavior are considered to be indicators.

- **Tools.** The tools or software used by adversaries to accomplish their goals can also serve as indicators.

- **TTPs.** The techniques and tactics used by an adversary as they gain access to a system or network to stealing or compromising data and every step in between can also serve as an indicator. It is here where the MITRE framework can play an especially critical role in helping identify adversary behavior.

Now, the connection between EDR and the MITRE ATT&CK framework can take one of two forms.

Firstly, because the MITRE framework is the industry standard for classifying adversary behavior, it can be helpful in assessing and testing EDR solutions. By testing a solution against the framework, organizations will learn how well the EDR solution performs at providing visibility, coverage, and detection. In other words, organizations will learn how effective an EDR solution will be at protecting the organization against cyber threats. This, ultimately, assists organizations in finding an EDR solution most suited to their unique needs, requirements, and network environment.

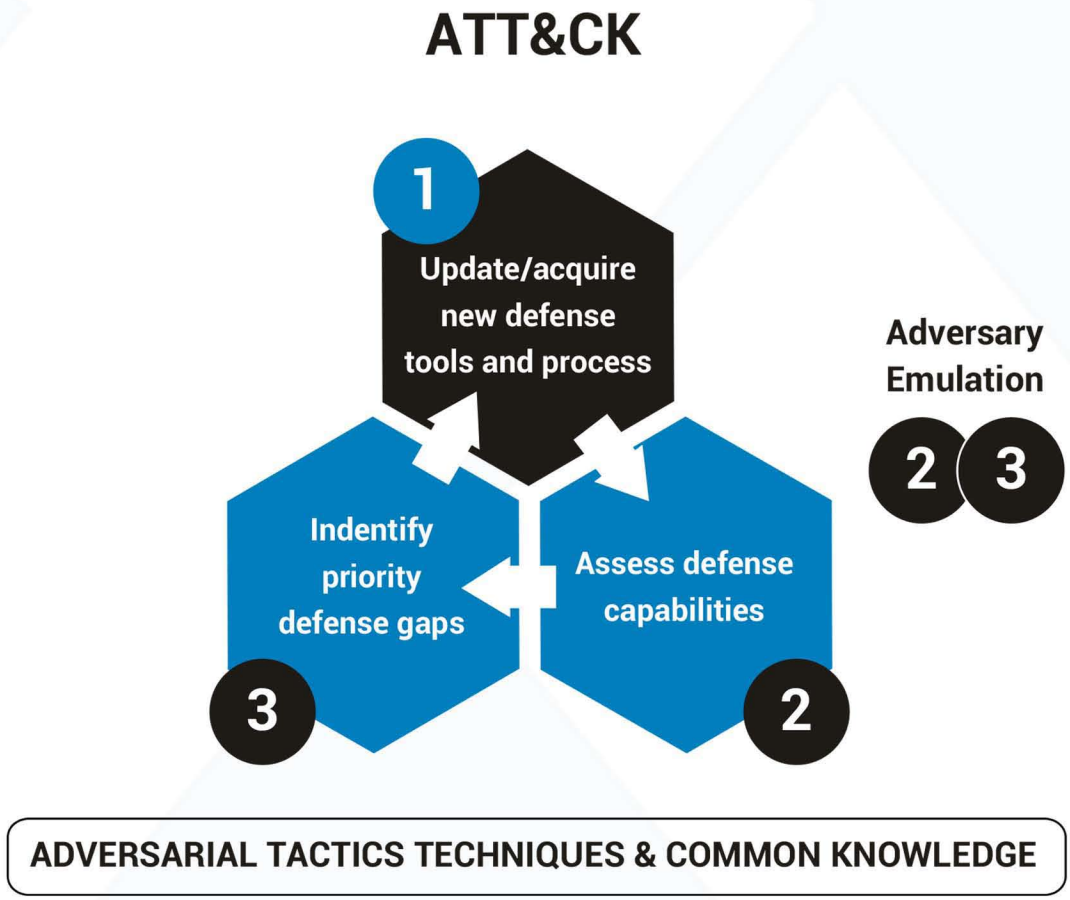

Figure 31 - Leveraging the ATT&CK matrix

More importantly, the MITRE ATT&CK framework can improve the effectiveness of an EDR solution. In this instance, organizations will map events recorded by the EDR solution to the framework. As such, it will then correlate the indicators mentioned above with the categorizations contained in the framework.

This results in the ability to not only detect possible malicious behavior, but also to determine the phases of the attack, assess the risk to the organization, and improve response prioritization.

Framework for Incident Response

As is the case with threat hunting mentioned earlier, incident response is a vital component of any successful and effective security strategy. This is simply because it allows organizations to detect, contain, and recover from any data breaches or intrusions. According to the National Institute of Standards and Technology (NIST), incident response involves four distinct phases.

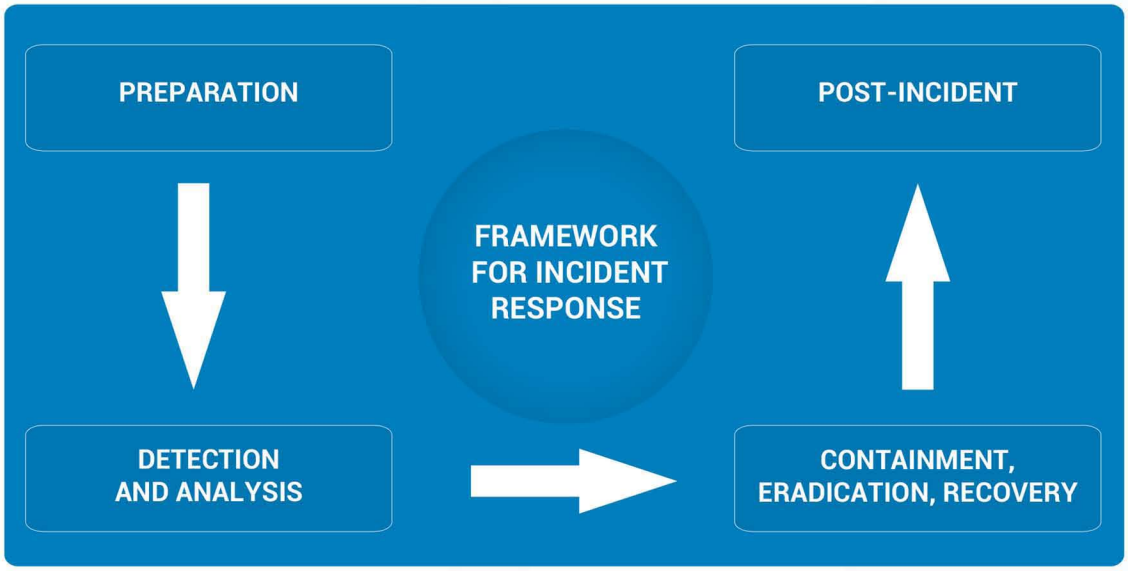

Figure 32 - Framework for Incident Response

Let us consider these four phases in more detail.

Preparation

The first phase in incident response is preparation, which, in turn, involves two aspects:

- **Preparing to deal with incidents.** The first phase, preparing to deal with incidents, involves providing all the tools and resources that might be necessary to effectively deal with incidents. As such, it involves compiling the relevant stakeholders' communication details, setting up incident analysis hardware and software, preparing other incident analysis resources like documentation and network diagrams, and ensuring access to mitigation software. In this respect, there are a few things to be mindful of. Firstly, the tools and resources an organization uses to deal with incidents will vary based on the organization's unique needs and requirements. Secondly, when providing and compiling these tools and resources, organizations should have multiple tools available to ensure redundancy when one tool fails.

- **Preventing incidents.** During the preparation phase it's also critical to ensure that the necessary systems and practices are in place to protect networks, applications, and systems, by implication, prevent incidents. This is because if incidents are not prevented, their volume will increase, which will then overwhelm the incident response team. In other words, the effect of not preventing incidents with the rights practices and tools is that the incident response team will not be able to deal with any real concerns effectively and efficiently. This can then result in slower response times, more data loss, service unavailability, and more severe damage. For this reason, to prevent incidents, it is necessary that organizations implement practices and systems such as risk assessments, network security measures, malware monitoring, and more. It is here where EDR starts to play a role in the incident response framework, as it is able to prevent a significant number of known and unknown threats.

Detection and Analysis

The next phase in incident response is when teams detect and analyze incidents. During this phase, it is important to remember that, in respect of attacks, they can occur in almost limitless ways. As a result, it doesn't make sense for organizations to attempt to prepare to deal with every conceivable incident. However, organizations should generally be able to deal with most incidents and focus on those that use common attack vectors. For example, organizations should focus on attacks that use the Internet, email, impersonation, attrition, and other common attack vectors. It's important to remember that this is just a small sample of common attack vectors, and there are many others. As such, organizations should focus on those that are most applicable to their circumstances.

When organizations are prepared to deal with these attacks, their response strategies will go into effect at the first signs of an incident. Generally, the signs of an incident can come in two forms; either a precursor or an indicator. A precursor is a sign that an incident might happen in the future, while an indicator is a sign that an incident has occurred or might be occurring at a specific moment. Either way, these precursors or indicators may be detected with a variety of tools or solutions, and it is here where EDR plays a significant role in helping security teams identify the signs of an intrusion or attack. For example, as mentioned earlier, LMNTRIX's Respond not only provides protection against known, unknown, and obfuscated malware, but also provides pre-execution protection from known threats.

This phase of the incident response framework does not stop with detection, however. It also involves incident analysis. It is here where security analysts will evaluate every sign of an incident, irrespective of whether it's a precursor or indicator, to determine whether the threat is legitimate. And once a threat is identified, it's important that security teams record all the event's surrounding facts, including a summary of the event, the status of the event, incidents related to the event, impact assessments, and more. As mentioned earlier, this can be a daunting task considering the sheer number of signs or alerts that the team will receive.

ENDPOINT DETECTION AND RESPONSE (EDR)	
Endpoint Data Recording	**Investigation of Data & Recording**
Network, event, process, files. commands, operation, etc.	**Sweep** (search) for indicators of compromise to understand the impact of detections
Many telemetry data points	**Find** the root cause of a detection and remediate/prevent/invastigate again
Stored on endpoints or in server, or a hybrid approach	**Hunt** for indicators of Attack based on behavior rules or threat intelligence. Automatic (detection) or manual

Figure 33 - EDR features used during Incident Response

Fortunately, because EDR provides context around an event, it's able to reduce the number of alerts, enhances analysis, and makes it easier for security teams to distinguish between those events that are benign and those that pose real danger.

Once an incident has been identified and its data has been recorded, the team needs to prioritize which incidents they will deal with first. This is because different incidents have differing impacts on an organization's data, workflows, operations, and processes. As such, incidents should not be dealt with on a first-come, first serves basis. Typically, teams will prioritize incidents based on the following factors:

- **The incident's impact on the organization's operations.** Depending on the systems that the incident impacts, it could have a severe effect on those who use those systems and, by implication, on the organization's operations. In this respect, teams should not only consider the current impact of the incident on the operations of the organization, but also the future impact if the incident is not dealt with.

- **The incident's impact on the organization's data.** Incidents can also impact an organization's data in that it can have an effect on the integrity, availability, and confidentiality of the data. As such, teams should prioritize incidents based on the severity of the impact on the data.

- **The resources required to recover from the incident.** Finally, teams should also prioritize incidents based on the resources that will be required to recover from the incident. Generally, the higher the incident's impact on the organization's operations and data, the more resources will be required to recover from the incident. It is important to remember, however, that in some cases, recovery might not be possible. This will, for instance, be the case where sensitive data has been compromised. In these cases, it makes little sense to spend resources on recovery, and a better option would then be to spend those resources on improving security and preventing similar incidents in the future.

When the security team has identified an incident, analyzed it, and prioritized their response to it, they also need to notify all relevant stakeholders that will play a role during the later phases of the incident response framework. Who these stakeholders are will depend on every organization's unique makeup and can include management, security officers, legal departments, human resources departments, law enforcement, and others.

Containment, Eradication, and Recovery

The next phase in the incident response framework is containment, eradication, and recovery. Containment is a critical component of this phase and serves to reduce the severity of the damage caused by the incident. It also gives teams the time to eradicate a threat and recover from it, gather evidence relating to the incident, and, as such, it forms the foundation of this phase. Effective containment relies on a well-developed containment strategies based on the type of incident and the risks it poses to the organization. We've dealt with malware containment processes in greater detail earlier.

Once an incident has been contained, the team will take the necessary steps to eradicate the incident and recover from it. Eradication can take different forms depending on the type of incident. For example, if the incident was a malware attack, eradication might involve deleting the malware and disabling any user accounts that were compromised. Eradication also involves finding similar vulnerabilities within the networks or systems and implementing strategies to mitigate these vulnerabilities to prevent future attacks. Here, EDR can also play a significant role. For example, with the information provided by LMNTRIX Respond, intrusion analysts can find all similarly infected endpoints to eradicate the threat completely.

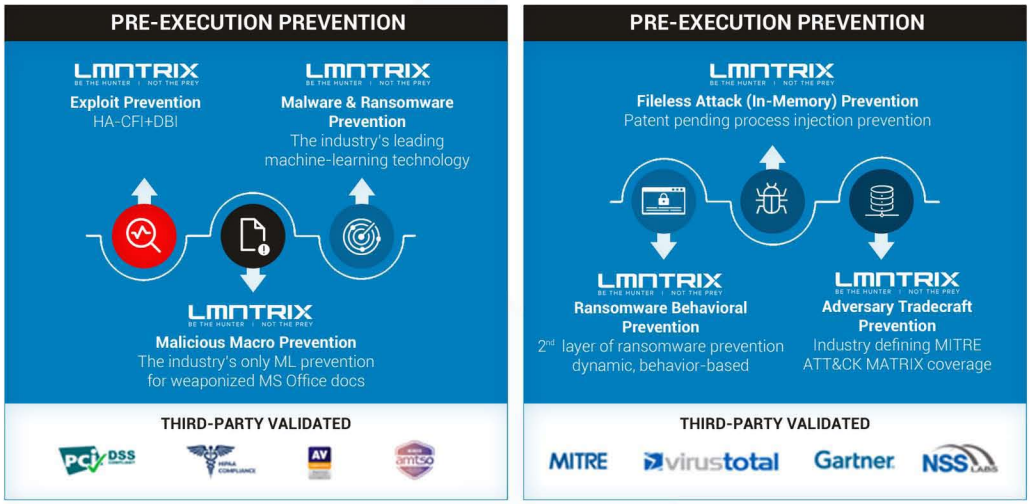

Figure 34 - LMNTRIX XDR Endpoint Security Pre & Post Execution Capability

When the threat has been eradicated, recovery takes place. This is when system administrators restore the organization's systems and networks to the normal operation and confirm that all these systems function normally. Typically, during recovery, teams will also implement strategies to illuminate or reduce other vulnerabilities in the system to prevent similar incidents.

Post-Incident

The final phase in the incident response framework is the post-incident processes that security teams will follow after a threat has been eradicated and recovery has taken place. It is during this phase that security teams will do a complete assessment of the incident, what happened, what they've learned, and what they can do to prevent similar incidents from occurring again. During this phase, data is extremely important, as it allows teams together valuable insights not only into the incident but also the strategies to prevent similar incidents. Based on these insights, they can then improve their strategies and eliminate vulnerabilities, which make it easier to handle or prevent similar incidents in the future.

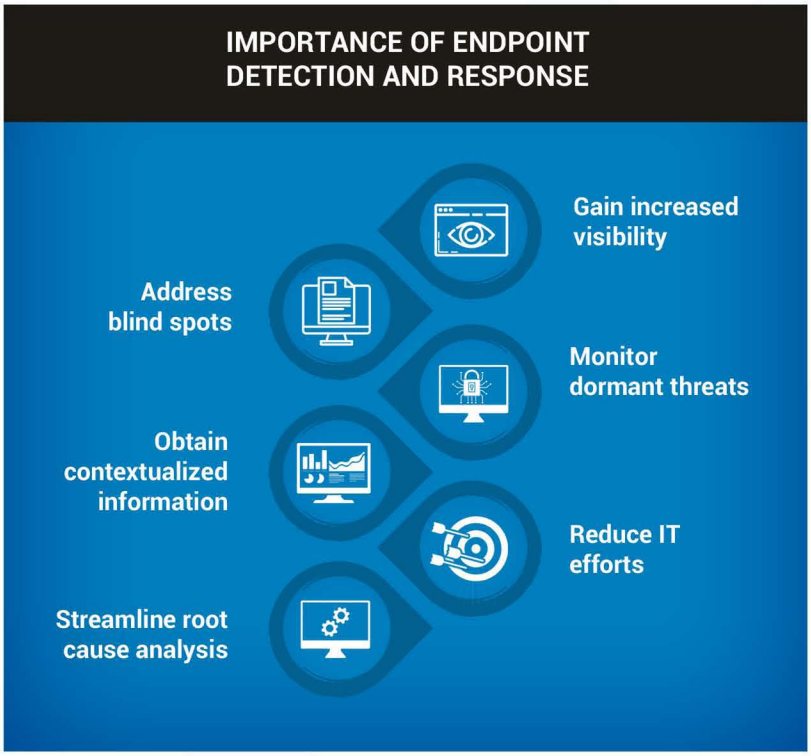

Figure 35 - Significance of EDR / Endpoint Detection & Response

Based on what we mentioned earlier, EDR plays a significant role in the post incident processes. Since EDR continuously records data, whether it detects an incident or not, it provides a wealth of information that teams can use to gather the entire context surrounding any security incident. This, in turn, not only allows them to streamline their detection processes but also allows them to improve security and formulate more effective and efficient incident response strategies.

ABOUT **LMNTRIX**

Often times, the difference between preventing a cyber-attack or suffering a crippling loss is simply knowing where to look for the signs of a compromise. Even the most advanced attackers leave traces of their presence so an effective defense must not only be vigilant, but also ever-adaptive in response to changes in attacker tactics. A critical element in this age of constantly evolving threats is a detailed view of an organization's entire potential attack surface. Log collection solutions are simply outgunned against today's advanced threat actors as they either lack the data, or the ability to analyze their data in a manner that allows rapid attack detection.

LMNTRIX has reimagined cyber security, turning the tables in favor of the defenders once again. We have cut out the bloat of SIEM, log analysis, false positives and associated alert fatigue and we created new methods for confounding even the most advanced attackers. We combine deep expertise with cutting-edge technology, leading intelligence, and advanced analytics to detect and investigate threats with great speed, accuracy, and focus. We believe that in a time of continuous compromise you need continuous response not incident response. Our approach turns inward and assumes that you're already breached and that you're continually going to be breached, so we take a pro-active, offensive, hunting, adversarial pursuit stance as opposed to a reactive, defensive, legacy stance with analysts staring at a SIEM console wishing they could detect an APT. As a company we stand in defiance of the unwanted human presence within corporate networks by attacking the root of the problem the adversary's ability to gain entry and remain undetected. Our real-time hunt operations identify signs of planned and active attacks and take action to neutralize them, forming the basis of our comprehensive Active Defense approach to limiting security exposure.

LMNTRIX Active Defense is a best in class Managed Detection & Response (MDR) service that detects and responds to advanced threats that bypass perimeter controls. The outcomes we deliver clients are validated breaches that are investigated, contained and remediated. All incidents are aligned to the kill chain and MITRE ATT&CK framework containing detailed investigative actions and recommendations that your organisation follows to protect against the unknown, insider threat and malicious attacker.

LMNTRIX becomes an extension of your internal team, we can augment your MSSP, or be a full-service SOC as a service security solution.

LMNTRIX Active Defense is a three-tier outcome-based solution (Gartner refers to it as Managed Detection & Response (MDR) and our platform Extended Detection & Response (XDR).

(1) LMNTRIX XDR (AWS Data Lake and Platform)
(2) LMNTRIX TECHNOLOGY STACK (Deployed deep within Customer Networks)
(3) LMNTRIX CYBER DEFENSE CENTRE (Security Analyst Driven).

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, UEBA and Deception Everywhere with completely automated attack validation, investigation, containment and remediation on a single, intuitive platform. Backed by a 24/7 Managed Detection and Response service at no extra cost LMNTRIX provides comprehensive protection of the environment for even the smallest security teams. It is a single investigative platform for insights into threats on enterprise, cloud, hybrid, and industrial control systems (ICS) networks. The LMNTRIX XDR delivers unique advantages over current network security solutions. It is a holistic and multi-vector platform with unlimited retention window of full-fidelity network traffic, innovative security visualizations, and the ease and cost-savings of an on-demand deployment model.

LMNTRIX XDR is based on multiple detective, responsive, and predictive capabilities that integrate and share information to build a security protection system that is more adaptive and intelligent than any one element. The constant exchange of intelligence, between the Active Defense components and the wider cybersecurity community enables LMNTRIX to keep abreast of the tactics techniques and procedures (TTP's) of the most persistent, well-resourced, and skilled attack groups.

Figure 36 - LMNTRIX XDR

LMNTRIX TECH STACK is a powerful, proprietary threat detection stack embedded within the client environment, behind existing controls. TECHNOLOGY STACK comprises multiple detective systems, combining threat intelligence application and correlation, static-file analysis, user and entity behavior analytics (UEBA) and anomaly detection techniques to find threats in real-time. It eliminates 'alert-fatigue' determining which alerts to escalate through multi-platform consensus.

Figure 37 - LMNTRIX XDR A Comprehensive Threat Prevention, Detection & Response Platform

LMNTRIX CYBER DEFENSE CENTER (CDC) A global network of Cyber Defense Centers comprising trained and certified hunters and intrusion analysts, provides constant vigilance and on-demand analysis of your digital assets and networks. Our intrusion analysts actively probe and monitor your networks and endpoints 24x7, using the latest intelligence and proprietary methodologies to look for signs of compromise. When a suspected breach is detected, the team performs an in-depth analysis of potentially affected systems to confirm the breach. When data theft or lateral movement is imminent, our endpoint containment feature makes immediate action possible by quarantining affected hosts, whether they are on or off your corporate network. This significantly reduces or eliminates the consequences of a breach.

Figure 38 - LMNTRIX Cyber Defense Centre

LMNTRIX XDR
Endpoint Security Supported Platforms

LMNTRIX XDR Endpoint Security agents are only supported on the following operating systems:

Windows OS Support

- Windows Server2008R2, 2012R2, 2016-2022(32 & 64-bit)
- Windows 7 SP1 (32 & 64-bit)
- Windows 8.1 (32 & 64-bit)
- Windows 10 (32 & 64-bit)
- Windows 10 Anniversary (32 & 64-bit)

Linux OS Support

- CentOS 6.x, 7.x and 8.x
- Red Hat Linux 6.x, 7.x(64bit)and 8.x (64bit)
- Ubuntu 14.04 (64bit), 16.04(64bit), 18.04(64bit) and 20.04(64bit)
- SUSE Linux Enterprise Server 15
- Amazon Linux 2

Mac OS Support

- Mac: 10.11 (El Capitan)
- 10.12 (Sierra)
- 10.13 (High Sierra)
- 10.14 (Mojave)
- 10.15 (Catalina)
- MacOS 11 (Big Sur)
- MacOS 12 (Monterey)

Solaris OS Support

- Solaris 10(5.10) x86 (SPARC)

Note: ARM processors are not supported for Windows and Linux OS. The Apple M1 chipset is supported.

Virtual environments:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- VMWare
- Xen Server

LMNTRIX
BE THE HUNTER | NOT THE PREY

SENSOR RESOURCE CONSUMPTION

Lightweight dissolvable agent that deploys in minutes with no end user impact or reboot required:

- Average CPU Usage: <2%
- Memory Utilization: < 200 MB (Trimmed down policy like *_TMP)
  = 600 MB for all the detections enabled (including aggressive custom detections)
- Sensor footprint on disk < 5 MB
- Optional Sensor event datastore on disk = 10 GB by Default (configurable as low as 500MB)

MINIMUM ENDPOINT HARDWARE REQUIREMENTS

- 2 CPU Cores
- 2 GB Memory
- 10 GB of available storage (For lower storage requirements, consult with the LMNTRIX CDC)

Proxy Support

For enterprise networks that do not allow direct Internet access, the LMNTRIX XDR Endpoint Security agent provides support for enterprise proxies.

TO LEARN MORE
ABOUT **LMNTRIX** VISIT

https://lmntrix.com/

LMNTRIX USA.
333 City Blvd West, 17th Floor,
Suite 1700, 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 INDIA.
VR Bengaluru, Level 5, ITPL Main Rd,
Devasandra Industrial Estate,
Bengaluru, Karnataka 560048,
+91-22-49712788

LMNTRIX Australia.
Level 25, 100 Mount Street,
North Sydney NSW 2060
+61.288.805.198