eSENTIRE

eBOOK

XDR: The Secret to Highly Effective Managed Detection and Response (MDR) Services

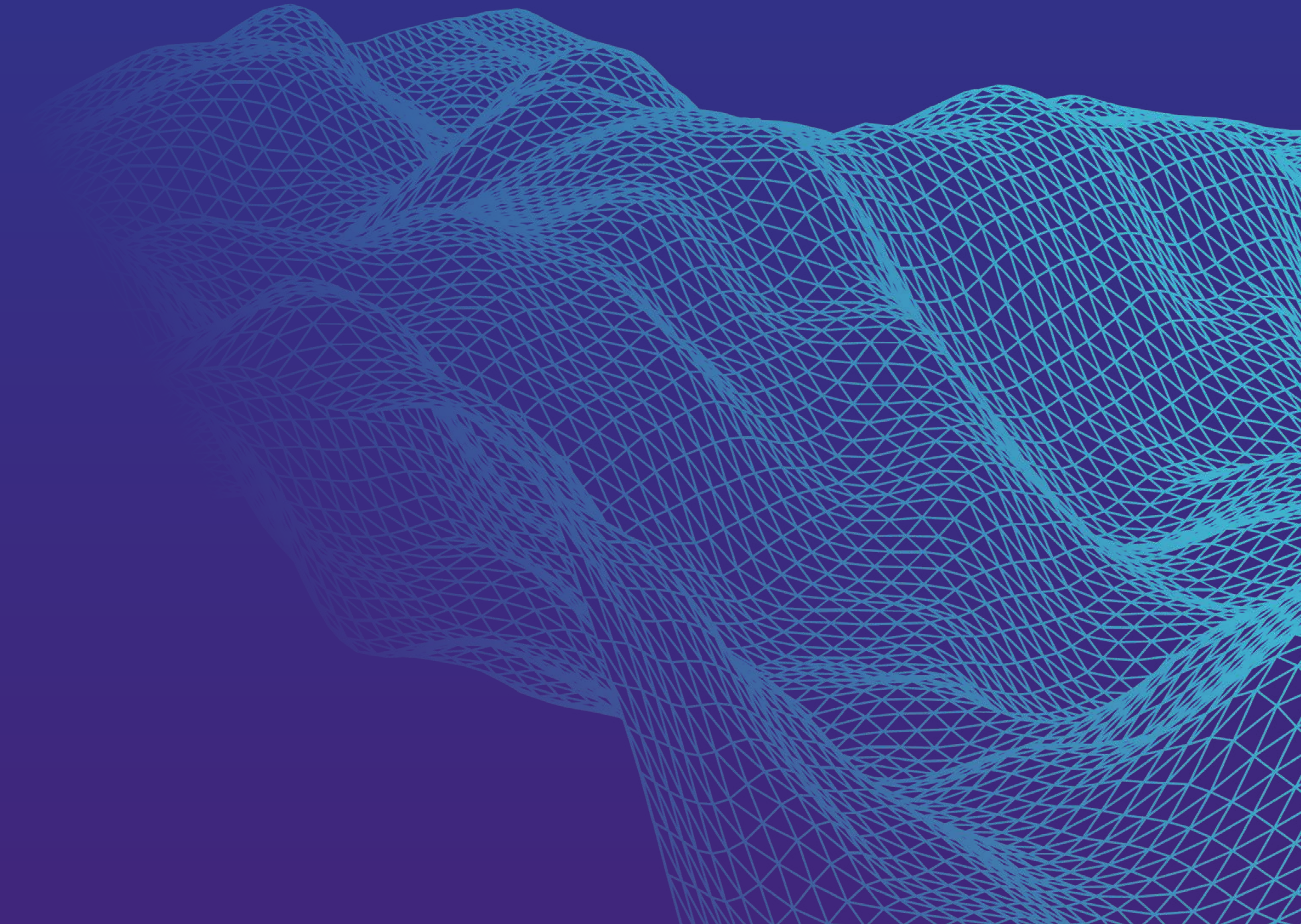


Table of Contents

I. Introduction: Today's Cyber Threat Landscape Demands Rapid Response

The job of a cybersecurity professional has never been easy, but the events of the past two years have tested the defenders' resolve in new ways. With easier access to ever-more sophisticated tools, attackers have launched an escalating wave of attacks based on familiar threat actions.

Cyber by the Numbers

$4.24M

average cost of a data breach

$847K

average payment demanded by cyber criminals in 2020

51%

security professionals reporting their team's performance was negatively impacted by remote work

3.1M

unfilled positions for skilled cybersecurity professionals globally in 2020

Phishing attacks, the exploitation of stolen credentials and social engineering are continuing to result in large-scale data breaches,[1] with the average breach now costing its victim $4.24 million — the largest single-year data breach cost increase in nearly a decade.[2] Meanwhile, ransomware attack volumes reached an all-time high, with the average payment demand also skyrocketing to a historical peak of $847,344 in 2020.[3]

With costs and risks on the rise, security teams are being stretched thinner than ever. The shift to work-from-home wasn't easy for many security operations teams to navigate, with 51% of security professionals reporting that their team's performance was negatively impacted by remote work in a recent survey conducted by FireEye.[4] In that same survey, more than 80% of security analysts described their jobs as "painful" or "very painful" due to workload increases that are driving them to the brink of burnout.[5]

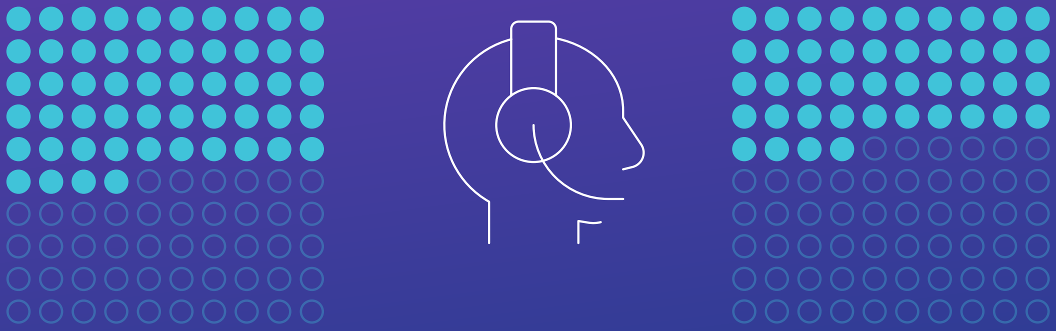
Despite these challenges, rapid response capabilities are essential. Data breaches that take more than 200 days to identify and contain cost an average of $1.26 million more than those that are identified and fully contained in less than 200 days.[6] Organizations that want to mitigate this significant financial risk must be able to contain malicious activities within their environment in far less time, and do so consistently.

To achieve this end, it's essential to maintain threat detection, investigation and response capabilities that are highly effective, and that are in place 24/7.

Growing numbers of organizations are looking to Managed Detection and Response (MDR) providers offering outsourced cybersecurity services to help them meet this need. Only 54% of organizations currently have access to their own Security Operations Center (SOC) – and a mere 44% of those with fewer than 10,000 employees do.[7] This is the case despite the fact that SOC capabilities are the key to building a mature cybersecurity program. Many companies are outsourcing these activities so that they can gain access to expertise and reduce risks without having to turn their focus away from their core business competencies.

[1] https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf, [2] https://www.ibm.com/downloads/cas/OJDVQGRY, [3] https://start.paloaltonetworks.com/unit-42-ransomware-threat-report, [4] https://www.fireeye.com/content/dam/collateral/en/rpt-ponemon-institute-second-annual-study-economics-of-the-soc-2021.pdf, [5] https://www.fireeye.com/content/dam/collateral/en/rpt-ponemon-institute-second-annual-study-economics-of-the-soc-2021.pdf, [6] https://www.ibm.com/downloads/cas/OJDVQGRY, [7] 451 Research. Voice of the Enterprise: Information, Security, Organizational Dynamics 2020. [8]

Organizations with Access to an In-House SOC



54%

organizations have access to an in-house SOC

44%

organizations with fewer than 10,000 employees have access to an in-house SOC

As a result, the market for Managed Security Services (MSS) is fast-growing and competitive. Gartner reports that there's been 44% growth in prospective buyers' inquiries over the past year.[8] But with more than a thousand companies around the globe now offering some form of MSS, it's more difficult than ever to figure out what makes a service offering "highly effective." There's no standardized results reporting across the industry, nor are there transparent quantitative measures that can be applied universally to evaluate performance.

In fact, every MDR provider faces the same array of challenges that an in-house security operations (SecOps) program does. Skilled cybersecurity professionals remain in short supply, with an estimated 3.1 million unfilled positions around the globe in 2020.[9] And the quality of an MDR provider's services is dependent upon the effectiveness of its people — the security analysts, threat hunters, incident responders and content and automation engineers that do the detective, investigative and operational work of containing threats.

Their jobs are difficult, especially when performed at scale across multiple clients' environments. This makes it absolutely critical that SecOps teams are supported and enabled in their work. To furnish the top-notch support that makes highly effective MDR service possible, a provider must invest in the right technology foundation, one that enhances operational effectiveness and makes it easier to find and remediate threats at speed.

XDR is this technology foundation. In the remainder of this report, we'll explore what XDR is, how it works and why it enables security professionals to do the best possible work.

[7] 451 Research. Voice of the Enterprise: Information, Security, Organizational Dynamics 2020. [8] https://www.gartner.com/doc/reprints?id=1-27JN2ORS&ct=210928&st=sb, [9] https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

II. What Is Extended Detection and Response (XDR)?

Even before the events of 2020, many organizations struggled to maintain effective security operations programs. With growing numbers of workloads moving to the cloud, IT ecosystems were becoming increasingly complex and distributed. At the same time, widespread adoption of DevOps practices led software release cycles to become shorter and shorter. In conjunction with the cloud's ephemerality, this meant that organizational computing environments were increasingly dynamic and ever-changing.

Not only had attack surfaces grown, but business-critical operations had become increasingly reliant upon digital technologies, making the potential consequences of an incident or breach more serious. With the expansion of the attack surface came a corresponding increase in the number of logs and telemetry sources from the environment that SecOps teams were tasked with monitoring.

Today, digital business processes are more critical to the bottom line than ever, while sweeping adoption of hybrid and work-from-home policies is further expanding the attack surface. In the face of this constellation of challenges, legacy security architectures built from an expansive array of point solutions operating in siloed fashion can no longer keep up. Security Information and Event Management (SIEM) platforms tend to be inefficient & clunky and weren't designed to provide analysts with highly relevant background or the contextual information needed to make good decisions in real time.

The Limitations of SIEM in the Modern Threat Landscape

SIEM technology evolved largely in order to meet compliance requirements, which mandated that organizations store and retain log data in a single, centralized location. The technology's usefulness for threat hunting or post-incident investigations quickly became apparent, but SIEM was never designed — or intended — to serve as a correlation engine in real time. Making it possible to answer complex questions across correlated data was never among SIEM's strengths, and platforms typically require extensive tuning, rules-writing or programming before they can be used to help real-world analysts understand what's going on in the environment.

XDR was developed to solve these problems.

Though multiple definitions of the term exist, we favor the one advanced by 451 Research. According to this definition, extended detection and response is a technology approach that involves combining a pre-built integration of multiple security telemetry sources with analytics and response capabilities.[10]

In many security programs, SIEM solutions were brought in to house event logs from a broad array of security tools, operating systems, applications and network appliances. SIEM enabled analysts to correlate and search this log data, but often didn't provide analysts with adequate real-time visibility into activities taking place on endpoints, where a majority of threat actors make their initial foray into the environment. Hence, SecOps programs began adopting purpose-build endpoint detection and response (EDR) tools. EDR gave them the ability to gather data directly from endpoint devices to support threat detection and investigation, as well as to execute certain response actions. EDR's limitation, however, is that its detection and response capabilities are confined exclusively to the endpoint.

[10] 451 Research. Technology & Business Insight: The Rise of Extended Detection and Response

XDR provides next generation detection and response capabilities, extending the enhanced visibility and threat containment functionality that NDR and EDR offer across the entirety of the IT ecosystem. XDR brings context to external threat intelligence and to the internal business environment by synthesizing data from synthesizing security telemetry including network, endpoint, cloud, email, identity, the Internet of Things (IoT) and more.

Born of the need for complete attack surface visibility in today's distributed and heterogeneous computing ecosystems, XDR finds patterns within the data ingested to aid threat detection, reduce false positives and automate threat response & remediation. This makes it a powerful source of efficiency and value for high-performing security teams. With the best approaches to XDR, there's enough contextual information from the customer's environment – and adequate understanding – to be able to contain threats confidently. This containment can be automated, knowing that the process won't interrupt critical business operations unnecessarily.

Business Leaders Must Drive Security Efficiency

94%

of workloads are forecasted to be running in the cloud by the end of 2021.[11]

80%

of organizations will continue to allow users to work from home after the pandemic's end.[12]

84%

DevOps teams are releasing new features faster than ever before.[13]

87%

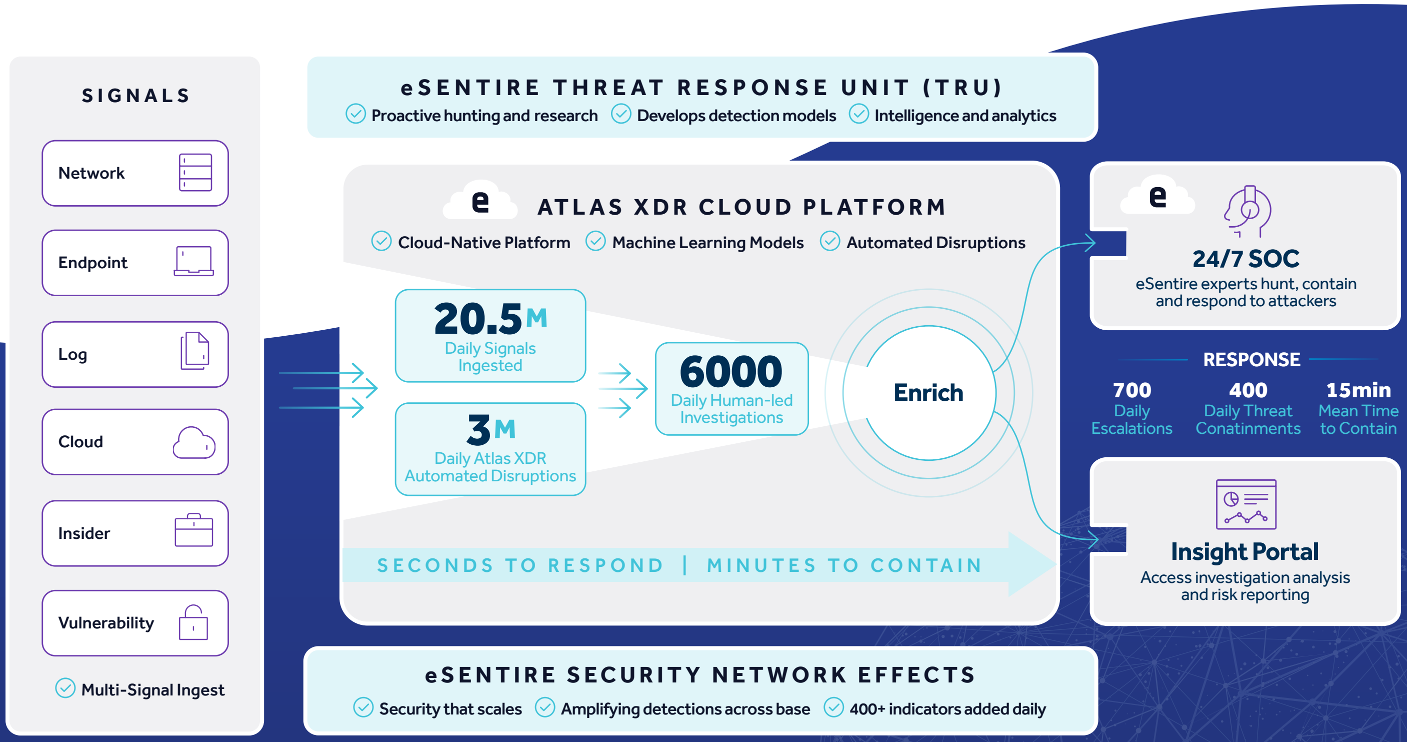
of organizations report not having enough cybersecurity resources.[14]

[11] https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, [12]https://www.gartner.com/en/newsroom/press-releases/2020-10-13-gartner-identifies-three-dimensions-that-define-the-new-employer-employee-relationship,[13]https://learn.gitlab.com/c/2021-devsecops-report?x=u5RjB_,[14]451 Research. Technology & Business Insight: The Rise of Extended Detection and Response.

III. How It Works: A Deep Dive into XDR

Though we've described XDR as the technology foundation that enables highly effective MDR providers to find and remediate threats at speed, XDR is more than just a single technology. Instead, it's an approach that strives to integrate security tools, control points, telemetries and analytics into a comprehensive enterprise-wide system to cut through the noise and enable analysts to focus on the security events that most warrant attention.

XDR gathers signals from across the whole of today's cloud-native and hybrid architectures. It normalizes, enriches and contextualizes this data, initiating automated responses in seconds for high fidelity security detections. Powerful machine learning (ML) models are applied to XDR platforms to provide human experts with the right information at the right time. SOC analysts and threat hunters are empowered to hunt, contain and respond to attacks exponentially faster - with less fatigue and frustration, when an automated response is not possible. XDR also delivers reliable insights to accelerate investigation analysis and streamline risk reporting.



SIGNALS

Network

Endpoint

Log

Cloud

Insider

Vulnerability

✓ Multi-Signal Ingest

eSENTIRE THREAT RESPONSE UNIT (TRU)

✓ Proactive hunting and research ✓ Develops detection models ✓ Intelligence and analytics

ATLAS XDR CLOUD PLATFORM

✓ Cloud-Native Platform ✓ Machine Learning Models ✓ Automated Disruptions

20.5M Daily Signals Ingested

3M Daily Atlas XDR Automated Disruptions

6000 Daily Human-led Investigations

Enrich

SECONDS TO RESPOND | MINUTES TO CONTAIN

24/7 SOC

eSentire experts hunt, contain and respond to attackers

RESPONSE

700 Daily Escalations

400 Daily Threat Conatinments

15min Mean Time to Contain

Insight Portal

Access investigation analysis and risk reporting

eSENTIRE SECURITY NETWORK EFFECTS

✓ Security that scales ✓ Amplifying detections across base ✓ 400+ indicators added daily

Here are some key facts about XDR's core capabilities:

- **XDR ingests multiple signal sources.** What makes XDR powerful is that it's able to gather and normalize data from across the enitre environment. This enables high-fidelity detection because it gives security teams true and comprehensive visibility from endpoint to cloud and beyond. Ideally, there should be no limits on what the security team can see or how much information can be incorporated into analyses. This means included technologies shouldn't be limited to a single vendor's product portfolio or solution suite.

- **Intelligent analytics eliminate noise and greatly reduce false positive rates.** In traditional SIEM-centric security architectures, high false positive rates are a perennial problem, as well as the primary contributor to burnout among security analysts. Excessive noise can also lead to alert fatigue, which can ultimately result in failures to detect if analysts end up dismissing alerts because they simply don't have enough time to investigate all events. In XDR, machine learning (ML) models and artificial intelligence (AI) algorithms aid analysts in recognizing patterns. The technology does so by automatically bringing in contextual data and taking investigative steps that a human would otherwise have to take. The end result is time savings and far fewer false positives.

- **Enriched data and contextual information enables threat hunting.** Because multiple different types of signals are ingested by the XDR platform, it's possible to see relationships within this rich data when it's the object of human investigation in threat hunting. If there's evidence of attack techniques that were used in the past, of relationships between the various parts of an attack sequence, or of activity patterns that are clearly malicious, this becomes readily apparent to security researchers. When the models have high confidence, automated response actions can be initiated.

- **Automated response capabilities dramatically accelerate threat containment.** When an XDR platform incorporates automated response capabilities, it's possible to initiate containment activities in mere seconds if there's a high degree of confidence that an observed activity is risky or malicious. A top-performing XDR platform that leverages proprietary decision-making technology to facilitate automated disruptions can execute effective, safe and appropriate containment protocols whenever there's clear evidence that they're warranted, reducing threat actor dwell time.

- **XDR platforms can learn from current threat intelligence, observed investigations and response actions taken across the platform.** Top-performing XDR platforms can make use of large volumes of data on current and emerging threats to improve detection accuracy. In particular, an XDR platform that sees detections, investigations and response actions across a large number of customer environments will be able to learn from that information. It can generalize from those learnings to the benefit of all customers. The investigation steps learned in one customer's environment can be automated in another's, and response and containment activities that were successful in one environment can be extended to all customers. It's a rapid feedback cycle that's constantly improving and hardening the security postures of the provider's global customer base.

- **XDR supplies proactive security that scales.** In traditional security architectures built around the capabilities of a SIEM, each additional signal source that the security team adds has the potential to increase the false positive rate and contribute to security analyst overload. Not so with XDR: increasing the number of signals ingested actually enhances detection fidelity. What's more, because ingesting more data leads to better-quality investigations and responses, this is an effect that's amplified when more customers leverage the platform. This network effect is the reason that expanding the size of an MDR provider's global customer should only improve its capabilities.

IV. A Peek Under the Hood: How Machine Learning Enables Highly Effective MDR

How, exactly, can an XDR platform help security teams solve some of the most pressing and longstanding challenges that have plagued SecOps since the dawn of the modern computing era? To answer this question, we'll need to take a closer look at the advanced algorithms that lie at its heart.

When security analysts are responsible for manually monitoring and triaging events, limited time and resources are the enemy. It's not easy to pay the right amount of attention to each alert when you're confronting hundreds of alerts daily and facing an enormous volume of unstructured data to analyze. In fact, as many as 79% of alerts go uninvestigated in some security programs due to a lack of analyst time.[15]

Machine learning (ML) excels at pattern recognition. Finding subtle patterns in large volumes of data isn't a task that's a good match for how humans think, but it's where ML shines. The machine learning models that investigate events in an industry-leading XDR platform are capable of detecting relationships within the different types of data and signals that flow through the platform.

[15] https://www.enterprisemanagement.com/research/asset.php/3441/InfoBrief:-A-Day-in-the-Life-of-a-Cyber-Security-Pro

In many ways, ML models "think" according to a pattern that's the exact opposite of how human cognition works. When it comes to people's attention, the more information and distractions there are, the harder it is to see and remember what's most important. For ML, the converse is true: the more data there is in the training set, the more examples there are to learn from. The more examples there are to learn from, the better the model can predict the solution for a new example. This is why data is like gold for AI-powered systems. And, in fact, data that's annotated so that it can be used as a learning example is the real gold. This is also why AI-powered systems are so well-suited to automate actions that tend to be fatiguing and overwhelming for humans.

XDR acts as a force multiplier for the human security analysts within a SOC environment because it draws their attention to what matters most. The technology learns from previous investigations, so it's able to suggest the best actions to take in each novel investigation situation.

The "Brains" of the SOC: How XDR Aids Detection, Investigation and Automated Response

An industry-leading XDR platform will automate high-confidence threat responses, and where such a response isn't possible, present the security analysts supporting it with a rich data object for investigation. This data object will be enriched with contextual information and stripped of vendor-specific detail that might otherwise made it hard to understand.

The platform makes it easy to answer questions like these:

- Which of these pieces of information are relevant?
- Which of these events are related?
- Which activities are obviously, clearly and demonstrably malicious?
- When it is appropriate to initiate an automated response workflow?
- What requires further analysis and human attention?

When there are very high-confidence answers to all of these questions, investigation and response can be fully automated. This entirely removes human effort from the process.

In cases where there's some ambiguity, the platform gives analysts ready access to the sort of in-depth information that makes their jobs easier. It also allows them to be more creative, have more confidence in their effectiveness, and stop more threats. This may explain why integrating security technologies is not only associated with a 10.5% increase in a security program's effectiveness, but is strongly correlated with improvements in the recruitment and retention of talent.[16]

XDR Use Case: Threat Hunting for Malicious PowerShell Activity

PowerShell has been part of Windows for over a decade. It's popular among IT administrators because it gives them extensive access to the operating system's internals. But it's also widely exploited by attackers.

Threat hunters often focus on searching for PowerShell exploits because they're so prevalent.

However, examining every single PowerShell script that runs in an enterprise IT environment manually would consume an enormous amount of time and energy.

Running an ML model makes it effortless to monitor all PowerShell executions. Each can be automatically scored according to how likely it is to be associated with malicious activity. Those that trigger alerts do so with a high degree of confidence. The reason such a high degree of confidence is possible is that the platform had access to a large number of examples of previous PowerShell executions – all labeled "benign" or "malicious" when they were investigated.

This transforms threat hunting from a "needle in the haystack" search to a hypothesis-driven activity that has a high probability of finding real and present threats.

[16] https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-outcomes-study-main-report.pdf

V. Better Together: MDR + XDR

Given the realities of today's challenging threat landscape, it's no surprise that growing numbers of business leaders are choosing Managed Detection and Response over traditional Managed Security Services. A primary benefit of MDR is that it prioritizes rapid response, threat containment, and remediation actions, alongside the alerting and monitoring capabilities that comprised the standard MSS offering.

When a provider is fully invested in managing incidents all the way through to resolution, they have a strong incentive to deliver superior overall security outcomes. They can't act as a mere alert factory — delivering high volumes of false positives without an actionable response component to their services.

Though the abbreviations are similar enough to confuse the uninitiated, MDR and XDR aren't the same thing.

MDR is a comprehensive service offering that's built upon this technology foundation, but it also includes access to human experts, taking intuitive, manual actions to respond & remediate threats, and optimize security operations, when an automated action is not possible.

XDR is a technological approach that enables high-fidelity detection, faster and more accurate investigations and automated responses.

More than a tool: XDR is a technology, but it's also a living artifact

When cybersecurity vendors sell XDR solutions, they're providing tools. These may be powerful and full-featured tool sets, but they're static. What an MDR provider instead offers includes all the programming and engineering work that's necessary to transform these tools into a potent enabler of effective security operations and rapid threat containment. An enormous amount of expertise is involved in operating an XDR platform effectively — creating runbooks, curating content, leveraging threat intelligence, learning from historical investigations — that few in-house security programs have ready access to.

Consider, for example, detection engineering. This is a critical support function for security operations teams and XDR platforms, but it's one that we don't often discuss. Detection engineering is what enables the XDR platform to perform accurate and comprehensive detection. Together with automation engineering, detection engineering provides the content that powers the platform. But it requires constant curation – by a team of experts – to stay ahead of dynamic attacker behaviors.

In addition, security network effects are critical to XDR's success: the more threat data and investigation & response actions that the ML models can be trained on, the more accurately they'll detect, investigate and respond to malicious activity. Thus, an XDR platform that's able to incorporate a large amount of investigation data from a diverse set of MDR client environments into its ML training data set will be more successful and effective than one with access to fewer and less diverse investigations. An MDR provider's collective history of investigations gives the platform a source of wisdom that's larger than the sum total of any individual enterprise's cybersecurity threat and incident history.

An industry-leading multi-signal MDR service provider will offer far more than mere access to XDR technologies, including:

- ✓ Capable and full-featured security monitoring coverage
- ✓ 24/7 expert-level SOC support
- ✓ Advanced detection engineering driving automated threat disruptions
- ✓ Elite, hypothesis-driven threat hunting
- ✓ Correlated Alerting, triage capabilities, threat investigations & tactical threat containments
- ✓ Remediation recommendations, actions and verification that have been learned from and validated across a large number of customer environments

VI. What to Look for in an MDR Provider

In today's complex and ever-evolving threat landscape, speed is of the essence. A majority of attackers (54%) are able to breach a target environment in under 15 hours,[17] and most ransomware strains can spread across a victim's network in three to four hours, encrypting files on each individual endpoint in just seconds. The most virulent can achieve this in less than 45 minutes.[18]

There are several factors that are critical to keep in mind as you evaluate MDR providers:

Consider the Mean Time to Contain

The best strategy for mitigating risks and protecting your organization from the potential devastation that such attacks can cause is to cultivate rapid response capabilities. So, first and foremost, look for an MDR provider willing to commit to a Mean Time to Contain malicious activity. In addition, you should understand the length of time it takes to limit a threat to a single host within your environment and ensure the provider can follow through with the commitment.

Size of customer base matters

Because an MDR provider's clients serve as the source for the data set that's used to train the ML models that power the XDR platform's detection and rapid response capabilities, it's important to choose a well-established company. After all, the more clients the provider has, the richer their data set. The richer the data set, the more accurate the detections, the quicker the investigations and the faster the containment will be.

Look for an MDR provider that customers trust

One of the primary benefits of leveraging MDR services is that the provider can take containment and remediation actions on your behalf. However, you'll have to give them permission to do this, which may mean ceding control over business-critical systems and processes. A provider that's well-versed in performing remediation activities on behalf of multiple other clients in your industry will have the contextual awareness and experience to earn your trust.

In addition, an MDR provider who does a great deal of end-to-end containment and remediation will be able to incorporate information on those activities into its XDR ML training data. This means that its models will be able to operate on the basis of information that's much richer and more extensive — encompassing the whole of the incident lifecycle — than those belonging to companies that primarily perform monitoring only.

Don't underestimate the value of integrations

It's obvious, but still bears mentioning. You'll save money if you don't need to rip and replace everything in your existing security technology stack. Even more importantly, however, operating across multiple vendors' tools and solutions can enable complete attack surface visibility and actually improve detection accuracy. This further increases the diversity of that all-important model training data set, making it that much more representative of real-world conditions. With that said, deep integration with a few key tools is more important than broad integration with every tool. It's most important to obtain full EDR telemetry and response integration than to integrate with every security toolset in existence.

> “ Better outcomes from AI-driven systems are all about access to the right data set to train the models. Ultimately, the predictions are the source of value, but in order to get accurate predictions, you need a large set of high-quality examples to learn from. As an MDR provider, we generate an ever-growing set of high-quality investigation and response examples each day in our SOC. That gives us an advantage when it comes to finding the right learning models to power our XDR platform.
>
> - Dustin Hillard, Chief Technology Officer at eSentire

[17]https://www.nuix.com/sites/default/files/downloads/marketo/report_nuix_black_report_2018_web_us.pdf, [18]https://www.zdnet.com/article/microsoft-some-ransomware-attacks-take-less-than-45-minutes/

VII. Not All MDR Is Created Equal: What Sets eSentire Apart

eSentire's complete, multi-signal Managed Detection and Response service provides 24/7 protection against the most sophisticated attacks, including those capable of bypassing conventional security controls.

Built upon the eSentire Atlas XDR Cloud Platform, our MDR services leverage the efficiencies it creates for threat detection, investigation, and complete incident response. Atlas XDR relies on machine learning models to eliminate noise, enable real-time threat detection and automatically block threats. Atlas ingests over 20 million security signals daily, automatically blocking 3 million threats per day without involving our SOC — or your security team. If an orchestrated response isn't possible, Atlas XDR equips our cyber experts with the insights and tools they need to perform deep investigations and execute manual containment, with a Mean Time to Contain of 15 minutes.

eSentire MDR doesn't just deliver alerts. Instead, we focus on delivering superior security outcomes. The eSentire Atlas XDR Cloud Platform combats emerging threats by ensuring that every new detection in one customer's environment is immediately transformed into protection across our global customer base. We accomplish this through the use of patented ML-powered algorithms that are constantly improving their performance to enhance our detection, investigation, threat hunting and remediation capabilities.

OUR DIFFERENCE:

Cloud-native architecture	**Patented Machine Learning Models**	**Multi-Signal Coverage**	**Network Security Effects**	**Extensive Response Capability**
A cloud-based, scalable, distributed platform provides security and redundancy	Adaptive ML and AI models eliminate noise	Ingestion, normalization and correlation of data across network, endpoint, email, identity, log, cloud and other sources	One of the industry's largest sets of full end-to-end incident management data	Automated defenses block known threats, while human-led investigations facilitate rapid containment of novel attack tactics
YOUR RESULTS:				
You get reliability at scale and on demand, and services that can grow with your business	You get accurate real-time threat detection and rapid containment, even of entirely novel threats	You get comprehensive, holistic monitoring and protection of the entire attack surface.	You get access to highly accurate machine learning models that are constantly improving.	You get a mean time-to-contain of 15 minutes or less.

> Every time we call the eSentire SOC, we get a true security analyst on the first touch to walk us through our incidents clearly and efficiently. No other provider delivers such personalized service and expertise. Leveraging the eSentire Atlas platform, in conjunction with access to their sophisticated threat intelligence team, we have been able to cut our incident time to resolution in half.
>
> \- Michael Smith, Vice President, Director of Information Technology at HKS

Not all MDR is created equal

	eSentire	The Other Guys
24/7 Always-On Monitoring	✓	Limited
24/7 Live SOC Cyber Analyst Support	✓	Limited
24/7 Threat Hunting	✓	✗
24/7 Threat Disruption and Containment Support	✓	✗
Mean Time to Contain 15 Mins	✓	✗
Powerful Machine Learning XDR Cloud Platform	✓	✗
Multi-Signal Visibility & Coverage (Endpoint, Network, Log, Cloud, Email, Identity, Vulnerability, Insider)	✓	✗
Automated Detections with Signatures, IOCs and IPs	✓	Limited
Detections Mapped to MITRE ATT&CK Framework	✓	Limited
Detection of unknown attacks leveraging patterns and behavioral analytics	✓	Limited
Alerting of Suspicious Behavior	✓	Limited
Confirmation of True Positives	✓	Limited
Rapid Human-Led Investigations	✓	Limited
Threat Isolation and Containment	✓	Limited
Remediation Support & Verification	✓	Limited
Real-time Portal Visualizations	✓	Limited
Threat Advisories, Research and Thought Leadership	✓	Limited
Cyber Risk Advisor	✓	✗
Additional Security Services including Managed Phishing and Security Awareness Training, Security Incident Response Planning, Emergency Incident Response and more	✓	Limited

> We have been leveraging the Atlas platform for some time now and were pleased to see how easy it was to add endpoint protection to the suite of services we receive through the platform. It required very little work from our IT team and provides an additional layer of peace of mind in today's uncertain environment.
>
> - Neil Waugh, Chief Information Officer at M&C Saatchi

VIII. Conclusion

The current trends won't reverse themselves anytime soon. Cloud and remote work adoption will continue to increase, enterprise computing environments will continue to grow in complexity and attackers will continue their tireless search for the weakest link in your defenses. Traditional security controls and Managed Security Services were once effective, but they're no match for today's threats.

With eSentire, you're protected by an industry-leading pioneer backed by a cloud-native XDR platform. This means we have the visibility to see – and the capability to block – what other MDR providers will miss.

eSentire is recognized globally as the Authority in Managed Detection and Response because we support your cyber program with a combination of cutting-edge machine learning XDR technology, 24/7 threat hunting expertise, and security operations leadership to mitigate your business risk, and drive your cyber program forward.

Ready to get started?

Connect with an eSentire Security Specialist to learn more about how eSentire Multi-Signal MDR, powered by our Atlas XDR Cloud Platform, can deliver security that scales across your organization.

Contact Us

If you're experiencing a security incident or breach contact us ☎ 1-866-579-2200

eSENTIRE