DISRUPTING MSP CYBERSECURITY

Embracing Innovation for a More Efficient Security Model

By: Ricardo Villadiego

Index

Executive Report

This white paper provides an analysis of the current state of cybersecurity within the Managed Service Provider (MSP) landscape. It underscores the urgent need for MSPs to innovate and adapt in the face of rapidly evolving cybersecurity best practices and a challenging business landscape. Our position is that many of the advances made in 'advanced' cybersecurity technologies have been incremental, not disruptive. These legacy tools lead to inefficient cybersecurity operations and services. Our proposed solution is to leverage key network infrastructure signals for real time detection, and through integrations leverage existing elements of the cybersecurity stack to empower operators.

Key Findings

- **Market Vulnerability:** MSPs, reliant primarily on a traditional security model (Email Security, EDR, Firewalls), face increasing inadequacy against advanced threats and innovative disruption.
- **Legacy technologies:** SIEMs and SOARs demand significant cybersecurity analyst time to manage and maintain. Their pricing model is ineffective and, more often than not, drives the creation of unintentional blindspots in the pursuit of optimizing the cost structure of these tools.
- **AI/ML Limitations:** While AI and ML technologies can address the failings of legacy technologies, without human oversight, this can lead to inefficiencies and security gaps. A balance needs to be maintained in Secops between people and technology.
- **Need for Integrated Solutions:** MSPs' siloed cybersecurity solutions require a shift towards an integrated cybersecurity models while balancing automation with human expertise.
- **Legal and Business Continuity Risks:** Neglecting to adapt to these evolving cybersecurity challenges exposes MSPs to potential legal actions and operational risks.

Recommendations

- **Leverage Network Telemetry:** The Adversary always needs to use the network to achieve their aims, so prioritize leveraging the signals coming from the network.
- **Integrate and Automate:** Seek solutions offering seamless integration and effective automation within the cybersecurity stack.
- **Balance Technology with Expertise:** Combine AI/ML tools with human decision-making.
- **Stay Agile and Informed:** Adapt strategies in response to emerging technologies and threats.
- **Focus on Continuous Training:** Equip teams for efficiently operating cybersecurity with AI/ML tools and in a landscape with rapidly evolving best practices.

Failing to innovate now means risking obsolescence and the direct threat of their customers getting compromised. Embracing integrated, advanced cybersecurity solutions and balancing technology with human insight is crucial for future success.

Introduction

MSPs' Current Model Is Ripe For Disruption

In 1997, Clayton Christensen published "The Innovator's Dilemma", popularizing the expression "Disruptive Technology" (later rebranded 'disruptive innovation'). Ever since, the tech scene—from Silicon Valley to China, and beyond—has pursued disruptive innovation. In that book, Christensen identified **6 factors that indicate that an incumbent market leader is ripe for disruption:**

Indicators of Impending Disruption	Considerations for MSPs
Overshooting Customer Needs: When a company's products or services surpass the needs of its customers, it becomes susceptible to disruption. This happens because established companies focus on improving their existing products to attract higher-paying customers, but in doing so, they often overlook the needs of their average customers.	Overshooting with complex solutions can alienate clients seeking simplicity. MSPs should enable clients' core operations, offering essential cybersecurity without excessive complexity. This strategy meets client needs and positions the MSP as a vital business partner, reducing disruption risks from competitors.
Sustaining Innovation Focus: Companies are often focused on sustaining innovations (incremental improvements to existing products) rather than disruptive innovations (completely new products that open new markets). These companies tend to ignore the opportunities for disruptive innovation, leaving an opening for disruptive companies.	It's easy to fall into the habit of doing "cybersecurity as usual" (and defending sunk costs) with tools like SIEMs and SOARs that have only evolved incrementally in the past few decades.
High Profit Margin Focus: Established firms usually prioritize higher-margin products to satisfy their stakeholders. Disruptive technologies, on the other hand, often start in low-margin markets, which established companies ignore until it's too late.	Prioritizing high-margin cybersecurity offerings risks missing out on innovative, lower-margin technologies that could later dominate the market and attract a wider range of clients.
Inability to See New Market Opportunities: Established firms often fail to see the potential of a disruptive product to open up a new market. They see only the loss of their existing market and not the larger potential of the new one. Alternatively, they are so caught up in day-to-day operations and maintaining the relationship on a month-to-month basis that they fail to think about retaining their customers for the longer term.	Staying up-to-date with the noisy cybersecurity market is challenging, but essential to recognize emerging disruptive technologies that could capture new market segments and offer long-term client value, beyond the immediate operational focus.

Value Networks: Companies are embedded in value networks (the context within which a firm identifies and responds to customers' needs, solves problems, procures input, reacts to competitors, and strives for profit) that constrain their ability to invest in disruptive technologies.	Your value networks (encompassing customer relations, vendor partnerships, industry standards, and market trends) are complex. It's crucial to not let this complexity impede adopting disruptive cybersecurity technologies.
Customer Dependence: Companies are often dependent on their existing customers for revenue, making it difficult for them to invest in disruptive technologies that their customers don't want. This is related to the concept of "listening to your customers", which, while generally a good business practice, can prevent a company from innovating in a disruptive way.	While customer feedback is invaluable, over-reliance on current client preferences can limit your willingness to invest in opportunities that might initially lack customer demand but have the potential to redefine the market and attract new business.

Examples of Innovative Disruption Led By Technology

As the speed of technology increases exponentially, the examples of enterprises left behind by the march of progress are rapidly multiplying.

Blockbuster vs Netflix

In the late 1990s and early 2000s, Blockbuster was the dominant player in the movie rental business. In 2008, Blockbuster CEO Jim Keyes said "Neither RedBox nor Netflix are even on the radar screen in terms of competition." Keyes even went so far as to compare Blockbuster to Walmart, and Netflix to Apple.

Blockbuster fell victim to many of the factors mentioned by Christensen in the Innovator's Dilemma:

- While they did not overshoot their customer needs, they failed to adapt to the greater convenience offered by their competitors. Consequently, their customers' needs adapted, but they did not.
- Blockbuster was focused on incremental improvements to their existing model, such as in-store enhancements and promotions. Meanwhile, Netflix introduced a disruptive innovation with its streaming service, which fundamentally changed how customers accessed and consumed media.
- Blockbuster was heavily invested in its high-revenue generating physical store model, while Netflix started with a lower-margin mail-based and later a streaming service, initially less profitable but with a much larger growth potential.
- Blockbuster failed to see the potential of online movie rentals and streaming, considering it a niche market not worth pursuing aggressively. This allowed Netflix to establish a dominant position in this new market.
- Blockbuster was embedded in a value network of physical stores, real estate leases, and DVD suppliers, making it difficult for them to switch to a completely online model.

- Blockbuster was highly dependent on its in-store customers. Despite having an online service, Blockbuster was reluctant to promote it heavily, as it would cannibalize its in-store sales.

Netflix, with its subscription-based, mail-order service, and later on-demand streaming, disrupted Blockbuster's business model. Blockbuster, failing to adapt to this digital transformation and unable to innovate its traditional brick-and-mortar business model, eventually went bankrupt.

Nokia & Blackberry vs iPhone & Android

Nokia and BlackBerry were once the leaders in the mobile phone market. However, their market positions were disrupted by the innovative touch-screen smartphones introduced by Apple (iPhone) and Google (Android).

While Nokia and BlackBerry focused on incremental improvements to their existing product lines, Apple and Google fundamentally reinvented the smartphone, combining a mobile phone with a powerful computing device and a platform for third-party apps. Nokia and BlackBerry were unable to adapt quickly enough to this disruptive innovation, and their market shares dramatically declined.

The iPhone didn't only supplant Nokias and Blackberries. When Apple launched the iPhone they also killed their biggest money maker at the time, the iPod. Steve Jobs recognized that if he did not disrupt his own technology, others would.

Winners and Losers in Disruption

The winners in disruption are the ones who are capable of identifying changes in market demands and technology trends and adapting their strategies accordingly. They are not afraid to challenge the status quo even if it means disrupting their existing services and products.

Winners recognize that innovation isn't just about refining existing offerings; it's about pioneering new products to tap into unexplored markets. Netflix and the smartphone revolution led by Apple and Android exemplify this.

The losers in disruption, on the other hand, are the ones who cling too tightly to their current models and sunk costs and fail to see the potential in new market opportunities. Losers focus too much on their existing customers, overlooking the emerging needs of potential new customer segments.

Losers in disruption are the ones who fail to recognize that buyers' behavior will change regardless. No company, no matter how large will be able to force consumer behavior. Companies can only adapt to the behaviors and patterns that are already happening. For example, Meta spent 36 billion USD on the Metaverse but wasn't able to attract more than a handful of users.

As we pivot our lens toward the MSP market, we see the same indicators of a market ripe for disruption. It is in a similar position to Blockbuster and Nokia before their declines. The landscape of cybersecurity threats is evolving rapidly, and the current MSP model shows signs of strain and limitation.

It is becoming apparent that **the future will belong to those who can leverage disruptive technologies to provide innovative, efficient, and effective cybersecurity solutions.** Providers of Cybersecurity services need to decide if they will entrench themselves in the status quo, or embrace disruptive innovation as Steve Jobs did when he launched the iPhone.

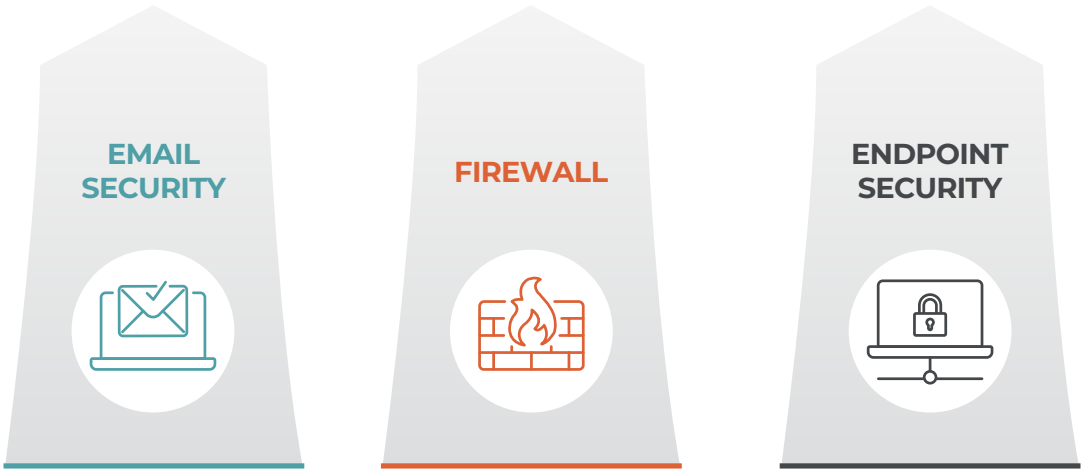
The Current MSP Cybersecurity Tripod

The Role of Cybersecurity within MSP Offerings

MSPs offer a wide range of services to their customers, and traditionally, cybersecurity lies far from the core of those services. MSPs already have to manage a large haystack of general IT services and tools, each requiring specialized knowledge. However, certain cybersecurity services have been standard for MSPs for a long time and customers now expect a certain level of security to be provided. MSPs must recognize that cybersecurity is now at the core of their offerings or risk being left behind by disruption.

The typical MSP cybersecurity tripod stands on three disconnected pillars within their wider IT offerings—Endpoint Detection and Response (EDR), email security, and firewalls. These foundational elements serve as the first line of defense against a multitude of cyber threats, from malware infiltrations to sophisticated phishing attacks and network breaches. However, three pillars don't form a stable base unless there's something to hold them together.

The Typical Cybersecurity Stack: a Closer Look



Email Security

In the realm of MSP offerings, email security forms a basic defense mechanism, acting as the digital equivalent of a moat around a castle. It's designed to shield organizations from a barrage of threats that arrive via email, such as phishing scams, malware attachments, and other forms of social engineering attacks. By employing advanced filtering algorithms and threat detection techniques, email security solutions aim to intercept these dangers before they ever reach the user's inbox.

Despite its critical role, email security alone is insufficient. Attackers continuously evolve their strategies, crafting more sophisticated and harder-to-detect threats. With the advent of widely accessible LLM and generative AI models, these threats will increase in sophistication and improve their success rate. Consequently, email security must be part of a larger, integrated cybersecurity strategy rather than a standalone solution.

Endpoint Detection and Response (EDR)

EDR and its latest iteration XDR extend beyond traditional antivirus solutions by continuously monitoring and analyzing endpoint data to detect and respond to cyber threats. EDR systems identify anomalies that suggest a security breach, thereby enabling rapid containment and remediation.

However, the effectiveness of EDR hinges on its integration with other cybersecurity components. Without proper correlation with signals from firewalls and email security, EDR can generate a high volume of alerts, many of which might be false positives, leading to alert fatigue among analysts. EDR is also subject to numerous evasion strategies.

Managed EDR services have emerged as a potential solution to the overwhelming alert management burden faced by MSPs. However, this approach has introduced its own set of issues. This "sustaining" solution often results in managing only a portion of the security stack, preventing MSPs from developing their in-house talent and potentially causing them to overlook the broader opportunities presented by disruptive innovations in the cybersecurity landscape.

Firewalls

Firewalls act as the gatekeepers, controlling the flow of inbound and outbound network traffic based on an applied rule set. They are a longstanding element of cybersecurity stacks, crucial for establishing a perimeter defense. Modern firewalls have evolved into next-generation firewalls (NGFWs), incorporating deeper inspection capabilities and integrating intrusion prevention systems to identify and block sophisticated attacks.

Yet, the challenge arises when firewalls operate in silos, disconnected from the rest of the cybersecurity framework. This separation can create blind spots and limit the potential for comprehensive threat intelligence.

The Challenge of Siloed Cybersecurity Solutions

While each of these solutions has its strengths and weaknesses, when they are implemented without any integrations or connections, their weaknesses are amplified more than their strengths.

Operational Strain and Resource Allocation

The operational strain of managing disparate cybersecurity tools can lead to inadequate resource allocation. MSPs often find themselves stretched thin, attempting to cover all bases without the necessary integration and automation that could streamline operations and optimize their security offerings.

The Burden of False Positives and Alert Fatigue

Another pressing challenge for MSPs is the deluge of alerts, many of which are false positives. This not only exhausts analysts but also detracts from their ability to identify and address legitimate threats, thereby weakening the overall security posture.

Compromised Incident Response

Siloed defenses can slow down the incident response times as the lack of integration requires manual intervention to piece together information from different sources during an attack.

Data Integration Bottlenecks

Sharing and correlating data including threat intelligence across siloed platforms is often a manual and error-prone process, which can lead to delays and inaccuracies in threat detection and analysis.

'Jack of All Trades' Vendor Pitfalls

Vendors marketing all-in-one cybersecurity solutions often deliver subpar capabilities, offering a "best-of-no-worlds" scenario where none of the features match the effectiveness of specialized, dedicated solutions. This can leave MSPs with a comprehensive tool that is mediocre at best in dealing with specific threats and their customers' needs, lacking the depth of protection needed in today's complex threat landscape.

The Need for Improvement in MSP Cybersecurity Models

Summarizing the Current State of MSP Cybersecurity

The current state of MSP cybersecurity is a patchwork of essential services that operate more in parallel than in concert. While each component of the cybersecurity tripod—email security, EDR, and firewalls—plays a vital role, the lack of integration and cohesive management results in a security posture that is less than the sum of its parts.

Developing Talent Efficiently

The traditional cybersecurity operations model is not sustainable. Cybersecurity analysts face steep learning curves for each new cybersecurity tool. The constant need to adapt to new technologies makes it challenging to train cybersecurity talent efficiently, leads to burnout, and often causes talent to move on soon after getting trained up.

The Imperative for Enhanced Solutions and Approaches

To counteract these shortcomings, MSPs must embrace a more stable base for cybersecurity. This includes adopting solutions that offer better integration capabilities, enhancing automation to reduce the workload on analysts, and employing advanced analytics to cut through the noise of false positives. By doing so, MSPs can transform their cybersecurity offerings from a tripod of isolated pillars into a robust, interconnected framework capable of withstanding the pressures of an ever-evolving threat landscape.

How Not to Level Up Your Cybersecurity Stack

Legacy Security Tools Dominate Cybersecurity Stacks

MSPs looking to update their security practices with the latest cybersecurity tools might be tempted to look at the best practices of SecOps teams at MSSPs and large enterprises. However, this would be a mistake.

The tools that make up the Security Operations Centers at MSSPs and large enterprises are largely the result of sustaining innovation, rather than disrupting innovation. These iterative improvements upon existing tools are geared to enhance their performance and lifespans within current frameworks. Ultimately they compel operation within outdated bloated frameworks when better, more efficient practices are attainable with modern technologies.

SIEMs

Security Information and Event Management systems (SIEMs) have long been the backbone of many organizations' cybersecurity strategies, yet they are arguably the biggest examples of sustaining innovation causing headaches. Originally designed as log collectors (at a time when networks were far simpler), SIEMs have incrementally integrated rule-based anomaly detection and expanded their capabilities to address emerging threats. While these improvements have undoubtedly enhanced their performance within existing frameworks, SIEMs still carry inherent limitations that cause frustration to cybersecurity operators.

SIEMs are increasingly inadequate due to several key failings: a high rate of false positives, alert fatigue from over-reliance on rule-based approaches, difficulty in adapting to rapidly evolving cyber threats, lack of context in event response, and extensive manual maintenance requirements.

As the cybersecurity landscape continues to evolve, the sustained innovation approach of SIEMs highlights the need for disruptive thinking to truly revolutionize how we detect and respond to modern-day threats.

EDRs/XDRs

EDR solutions were developed as a response to the limitations of traditional endpoint security, aiming to provide deeper insights into endpoint activities and enhance incident response capabilities. XDR, touted as an extension of EDR, aims to broaden the scope beyond endpoints by incorporating telemetry from various sources. While EDR and XDR solutions bring advancements to threat detection and response, they are, in essence, refinements and extensions of existing tools rather than disruptive innovations.

The reliance on historical data, signatures, and predefined patterns to detect threats hinders their ability to effectively identify sophisticated and emerging attack techniques, revealing a need for more agile and forward-thinking approaches in modern cybersecurity strategies.

EDRs also tend to generate a lot of alerts and false positives for cybersecurity operators to investigate and respond to. Often the required staff and skills to operate these tools become too much for smaller cybersecurity teams to handle.

MDRs

In response to the inherent limitations and challenges of operating SIEMs and EDRs, MDRs (Managed Detection and Response offerings) have emerged as an additional service, offering organizations the ability to outsource the management of detected anomalies, alerts, and incidents.

MDRs underscore a recurring issue in cybersecurity – the reliance on expensive human resources to compensate for technology shortcomings. Instead of tackling the core problems with tools like SIEMs and EDRs/XDRs, MDRs serve as costly workarounds.

With suboptimal cybersecurity tools, the prevailing approach involves expensive services that attempt to fill technological gaps with manual labor. This strategy is neither efficient nor sustainable, requiring substantial investments in human expertise without resolving the underlying cybersecurity challenges. The 'state of the art' label often masks the fact that these solutions are expensive stopgaps, rather than comprehensive answers to modern cyber threats.

How Have These Tools Fallen Behind?

While technology has been moving ahead at lightning speed, our cybersecurity tools and security practices have been slow to adapt. To transcend the current paradigm, it's necessary to recognize the needs faced by security operators as well as how technology better empowers these needs. The 3 technological advances they are not using to their fullest are AI, Cloud Computing, and cheaper data storage and processing power.

Artificial Intelligence

Modern artificial intelligence algorithms are far better suited to certain cybersecurity tasks than human minds. This frees up cybersecurity operators to apply themselves to tasks that better suit human intelligence.

- Analyzing vast amounts of data to identify patterns and anomalies
- User and entity behavior analysis
- Detecting malware
- Automating incident responses
- Hunting for threats based on intelligence such as hash values, IP addresses, domain names, and network/host signals.

Cloud Computing

The great cloud migration makes it far easier to deliver services to a wide range of customers. No longer does complex hardware have to be delivered and installed on-premises. Instead, cost-efficient services can be provided and perfected directly from the cloud. It is also now easier to integrate the various elements of the cybersecurity stack directly in the cloud.

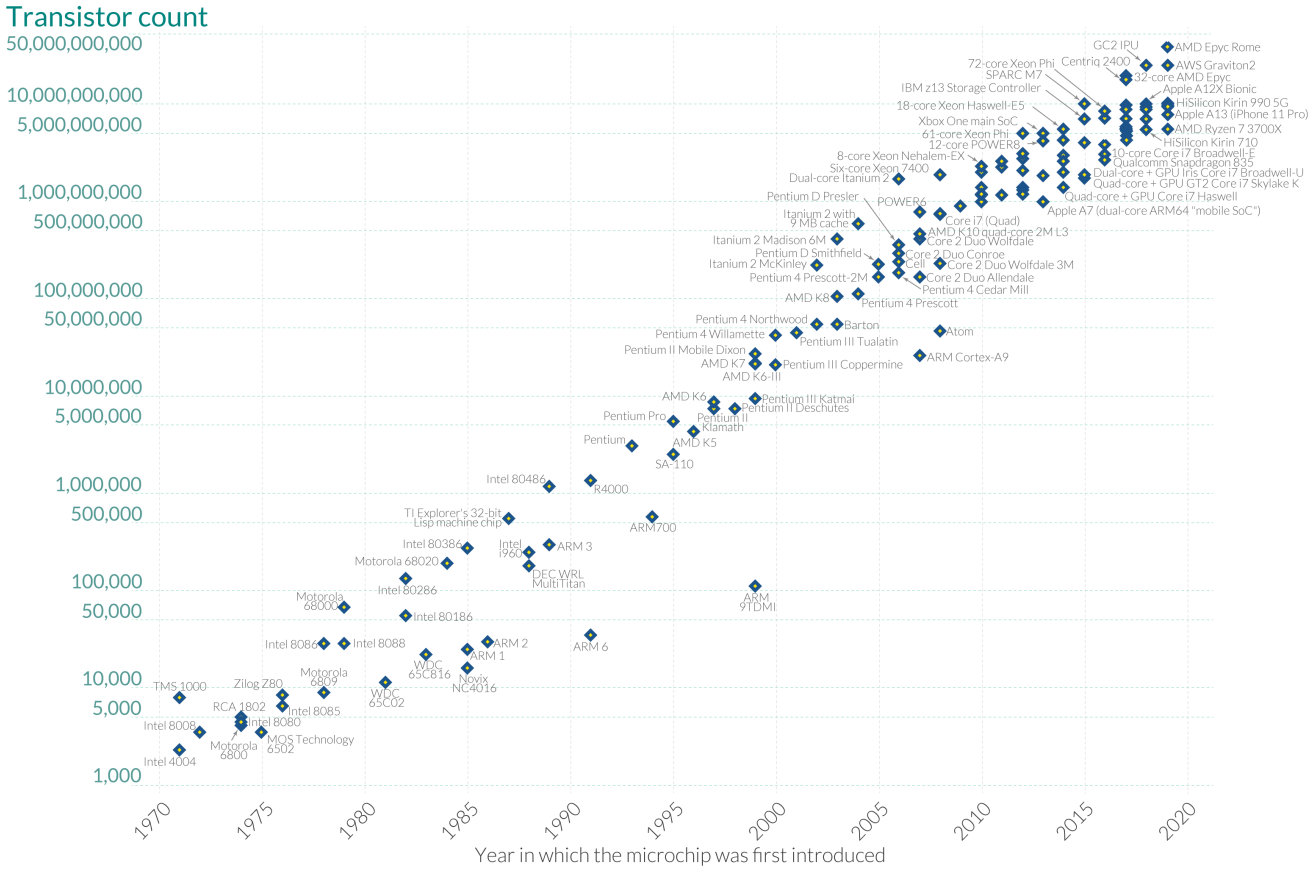
Data Storage and Computing Power

According to Moore's law, data storage and computing power decrease in cost exponentially. This allows us to apply more powerful analysis to cybersecurity tools rather than rules tinkered out by human minds.

It also creates challenges. We've seen similar increases in system complexity and the amount of data that is created and stored. Not all of that data is useful.

Moore's Law: The number of transistors on microchips has doubled every two years

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing - such as processing speed or the price of computers.



Source: https://ourworldindata.org/moores-law

As we mentioned earlier, not every stored piece of data is valuable. It might be tempting to think that with the affordability of modern processing power, you might as well analyze everything. However, if we were to analyze everything a system produces, we would need a system equal to the size of the one creating the data to do so. Instead, it behooves one to only select for analysis the data sources that offer the most threat signal for their size (information density).

You do not need every log. You do not need every alert. You don't need to decrypt the contents of every packet. You do not need hundreds of alerts. You do not need a haystack of tools to find one bad incident.

The Opportunities and Limitations of AI/ML for MSPs

Cybersecurity experts and commentators have long touted the integration of artificial intelligence (AI) and machine learning (ML) as a silver bullet. We've heard promises about its ability to predict, adapt, respond to threats in real time, and provide a significant leg up in an era where cyber-attacks grow in complexity and frequency. It's important to recognize that while we are starting to see AI and ML deliver on some of these promises, they come with their own set of challenges.

Benefits of AI/ML in Cybersecurity

Before diving into the limitations, it's important to acknowledge the substantial benefits AI and ML offer to the cybersecurity landscape:

- **Efficiency:** With the ability to process vast datasets at unprecedented speeds, AI systems can identify threats in real-time, ensuring immediate responses.
- **Predictive Analysis:** Through machine learning algorithms trained on historical data, these systems can foresee potential future threats, allowing for proactive measures.
- **Adaptability:** One of the primary strengths of ML is its ability to learn and adapt. Instead of being reliant on static algorithms, it can evolve to recognize new threats without manual intervention.
- **Automation:** Routine tasks, such as software patching or addressing recognized threats, are streamlined, reducing the time between threat detection and resolution.
- **Minimized Human Error:** With AI taking charge of routine tasks, there's a reduced margin for the errors that come with human oversight.

However, while these advantages paint a promising picture, the integration of AI/ML is not without its complications.

Limitations of AI/ML in Cybersecurity

The overarching concern arises when we start viewing cybersecurity solely as a 'big data problem'. The theory is that with enough data, AI will decipher all patterns and predict any anomalies that signify a threat. This perspective has its flaws.

Turning Cybersecurity into a 'Big Data Problem'

According to cryptologist, cybersecurity expert and author of 'Data and Goliath' Bruce Schneier, "Big data was supposed to give us certainty. The idea was that if you have enough data you can learn everything you need to know. It kind of is a harmful mindset." While this serves as its own example of sustaining disruption by adapting an existing technology rather than building disruptive tools from first principles, it can lead to some practical difficulties.

While it's true that AI requires vast amounts of data to operate efficiently, reducing cybersecurity to a mere data-crunching exercise oversimplifies the intricacies and nuances of cyber threats. As any data scientist will tell you, it's not always about how much data you have, but the relevance and quality of that data.

Creating Noise

AI systems, in their quest for anomaly detection, can produce a lot of alerts. Many of these can be false positives, leading to alert fatigue. This can desensitize security professionals to alerts, potentially causing them to overlook genuine threats.

Language Learning Models are Promising, but Immature

Large Language Models (LLMs) have rightly impressed with their ability to 'understand' a large body of data and extract relevant, well-composed information. Leveraging these strengths, we can envisage a SOC-of-the-Future where analysts are empowered by AI assistants that provide relevant, actionable intelligence.

As it stands, LLMs can potentially play some useful roles:

- **Source relevant contextual information:** The AI can scan existing operative knowledge bases (threat intelligence, playbooks, etc) for recommended actions relevant to the current threat. The role of the human counterpart will be 'sanity checking' and implementing the suggested measures.

- **Provide a brief on emerging threats:** The AI can scan new intelligence (X, blogs, publications, advisories, etc.) The human role will again be of sanity checking, incorporating, and expanding on the relevant intelligence.

However, LLMs still have an Achilles' heel in the form of their tendency to 'hallucinate' and create seemingly appropriate answers without any factual basis. Further research and development is needed before these AI agents can be implemented, especially in a sensitive environment. New human specialists will be needed to train (and retrain) the LLM, while cybersecurity analysts will need to learn new human skills in operating and interpreting AI-generated results.

Treating AI as the Hammer when the Problem is Not a Nail

In our rush to implement AI solutions everywhere, we often forget the adage that when all you have is a hammer, every problem looks like a nail. For some vendors, the academic interest in finding an application for AI overrides their interest in creating a fitting solution to the problems faced in cybersecurity.

There are nuances in threat detection and response where human intuition, experience, and contextual understanding outpace the most advanced algorithms. It's paramount to always remember the human who will be using AI-enabled tools and ensure that their needs are not over-shot or under-shot.

The Better Way: Optimize the Security Stack and Prioritize Cybersecurity Analyst Decision-Making

The solution doesn't lie in discarding AI/ML but in optimizing how we use it. Here's a more balanced approach:

- **Optimizing the Security Stack**: Rather than overwhelming the security infrastructure with numerous AI tools, it's essential to choose tools that integrate well and offer complementary functions. This creates a streamlined system that maximizes the strengths of AI without causing data overload.

- **Human-AI Collaboration:** While AI can handle vast datasets and detect patterns beyond human capabilities, human experts bring context, intuition, and experience to the table. It's important to distinguish which tasks are performed best by which party. Anomalies flagged by AI should be reviewed by cybersecurity professionals to determine their actual threat level. This collaborative approach ensures that the breadth of AI is complemented by the depth of human judgment.

- **AI-Empowered Humans:** The learning curve in cybersecurity needs to be severely reduced by AI tools. level-one cybersecurity analysts will be able to operate as effectively as expert analysts with the correlation, context, and insights provided by AI assistance. This empowers professionals at all levels to make informed decisions swiftly while servicing thousands of customers.

- **Continuous Training and Adaptation:** The cyber landscape is ever-evolving. As such, AI/ML tools need continuous training with the latest threat data to remain relevant. Additionally, feedback loops should be established where the findings of human experts (post-analysis) are fed back into the AI system for better future predictions.

- **Reduce Dependence on Volume:** Instead of relying solely on vast datasets, the focus should shift to the quality and relevance of data. This ensures that AI systems are trained on pertinent information, reducing noise and increasing accuracy.

In conclusion, while AI/ML holds immense promise in reshaping the cybersecurity domain, it's vital to approach its integration with caution and strategic foresight. By optimizing the security stack and fostering a collaborative environment between AI and human experts, we can harness the full potential of AI while navigating its limitations. The future of cybersecurity isn't just AI-driven; it's a harmonious blend of machine efficiency and human expertise.

Better MSP Cybersecurity Operations

MSPs' cybersecurity operations are ripe for disruption because the tools have not kept up with technological advances. The advances that have been made have been incremental, rather than disruptive, resulting in inefficient tools. So how can we disrupt MSP operations for the better?

The key lies in empowering cybersecurity operators and secops teams by leveraging the most important signals coming from customers' network infrastructure alongside existing tools in the cybersecurity tripod.

The Network Is the Ultimate Source of Truth

Across all attacks, we continue to see one truth, that attackers need to use the network to achieve their ends. This means that the threat actors leave behind the footprints of their movements in the network metadata of the organization.

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Source: https://www.iso.org/standard/20269.html

Specifically, we can focus on the telemetry of these layers:

Layer 3: The Network Layer

This layer is responsible for determining the best path to route data across the network. It deals with logical addressing, path selection, and packet forwarding. IP (Internet Protocol) addresses are used at this layer to route information to its destination.

Layer 4: The Transport Layer

The Transport Layer ensures the reliable arrival of messages and provides error-checking mechanisms and data flow controls. It is also responsible for end-to-end connection and segmentation of data for transmission. Protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) operate at this layer.

These signals provide a rich source of threat intelligence that can be correlated with Indicators of Compromise (IoCs). Using the technological advances we mentioned previously (affordable processing power, cloud connectivity, and artificial intelligence), the information on confirmed threats affecting the enterprise network can be rapidly analyzed and acted upon, enabling proactive rather than reactive security measures.

Eliminating the Need for Excessive Logs, Alerts, and Incidents

In today's hyper-connected world, the volume of logs and alerts generated can be overwhelming, leading to 'alert fatigue'. With countless signals clamoring for attention, the real threats often get drowned in the noise, leading to delayed or inadequate responses.

But what if we could streamline this? The goal should be to focus on quality over quantity. By prioritizing confirmed IOCs and leveraging refined data from network layers, organizations can drastically reduce the volume of logs and alerts. This means that security professionals spend less time sifting through a sea of alerts and more time taking decisive action against genuine threats.

Creating a Better Security Operations Platform

Sustainable Cybersecurity Through Seamless Orchestration

Sustainable cybersecurity requires long-term cost-effectiveness and the well-being of cybersecurity professionals. An effective solution should harmoniously integrate with an organization's existing security tools, fostering a cohesive defense strategy. Rather than introducing a new tool for every new threat, the ideal platform complements and enhances the existing ecosystem, aligning with budget constraints and mitigating the risk of burnout among cybersecurity experts. This approach ensures not only robust security but also long-term cost-effectiveness.

Acting as a Definitive Source of Truth

A cutting-edge detection and response platform leverages the network as the definitive 'source of truth.' Continuously monitoring and scrutinizing network data, it delivers real-time insights that ensure swift and precise threat responses, thereby narrowing the threat actor's window of opportunity.

Coordinating the Existing Security Stack for Automated Response

Automation is the future. A leading platform should be able to interface with the existing security tools, initiating automated responses as soon as threats are detected. This not only accelerates response time but also optimizes resources by acting without delay.

Employing Human Intelligence Only Where It Is Needed

AI-driven processes are incredibly powerful, but there are nuances in threat detection and response where human intuition is unparalleled. Thus, while a platform might handle the vast majority of tasks, it should be designed to pull in human expertise only for those situations that demand intricate judgment.

Hybrid Deployment

The flexibility of deployment is paramount. The best platforms should cater to diverse organizational needs, whether it's on-premises, cloud, or a hybrid of both. Such adaptability ensures that regardless of an enterprise's unique structure or needs, the solution remains effective and robust while maximizing the value of existing technology investments.

Conclusion

The cybersecurity landscape does not stand at the precipice of some revolutionary shift. Instead, we are caught in a race with rapidly advancing technologies, and threats. Unfortunately, cybersecurity practitioners like those at MSPs have been falling behind. Embracing innovative disruption is how these practitioners continue to deliver services that provide value to their clients and remain competitive in cybersecurity.

The Consequences of Not Embracing Disruption in the MSP Cybersecurity Stack

- **Financial Impact:** Failure to evolve with the market could mean that MSPs fail to capitalize on potential income streams, operate cybersecurity sub-optimally, and incur greater insurance costs.
- **Operational Inefficiency:** Relying on outdated security methods can slow down operations, reducing the ability to respond to threats swiftly and effectively.
- **Legal Exposure:** Outdated cybersecurity practices expose MSPs to the risk of legal action from government entities, regulators, and client-victims, particularly if they operate under the assumption of reasonable care and protection.
- **Reputational Damage:** Ineffective security measures can lead to a loss of trust from clients and partners, impacting long-term business relationships and market standing.
- **Business Failure:** In extreme cases of not adapting to innovation in the market, companies like Blockbuster have been forced to close their doors.

Benefits of Adopting Innovative Tools and Strategies

Innovation, when applied thoughtfully, can be the cure for many of the challenges that plague the cybersecurity landscape.

- **Efficiency:** Innovative tools powered by AI and ML can drastically reduce response times, ensuring threats are neutralized before they can inflict significant damage.
- **Cost-Effectiveness:** While the initial investment in cutting-edge tools might seem steep, the long-term cost savings – both in terms of financial outlay and potential breach prevention – can be significant.
- **Adaptability:** As cyber threats evolve, so too should our defenses. Newer tools and strategies are designed to be more adaptable, ensuring they can counteract a wider array of threats.
- **Reduced Alert Fatigue:** Modern tools, when employed correctly, can significantly reduce false positives, ensuring that security professionals can focus their attention where it's most needed.

We've seen how companies like Blackberry and Nokia failed to act when innovation beckoned. In the ever-changing arena of cybersecurity, the choice is clear: innovate or face obsolescence. The stakes are high, and the time to act is now.

www.lumu.io

Lumu Technologies Inc. | 8600 NW 36th Street, Suite 150 Doral, FL 33166 | info@lumu.io | +1 (877) 909-5868