CyberMaxx

AI FOR CYBER DEFENSE

COMMITTING TO A SECURE DIGITAL FUTURE

Table of Contents

Committing to a Secure Digital Future

INTRODUCTION

In todays digital age, the rapid advancement of Artificial Intelligence (AI) presents both opportunities and challenges, specifically in the cybersecurity field. This series delves into the intricate relationship between AI and cyber defense, deeply exploring how this cutting-edge technology can be harnessed to protect the assets of CyberMaxx clients.

This series seeks to strike a balance between technological innovation and human ingenuity. We emphasize the importance of context, content, and correlation in developing modern Managed Detection and Response (MDR) strategy. CyberMaxx remains steadfast in its mission to utilize AI not as a mere novelty, but as a powerful ally in safeguarding our clients against cyber adversaries.

CyberMaxx statement on the application of AI

CyberMaxx will apply Artificial Intelligence for cyber-defense to the exclusive purpose in fulfilling our mission, of protecting client's business assets, guarding against those committed to wide-scale societal disruption through cyberattacks.

AUTHORED BY:

GARY MONTI

SVP OF SECURITY OPERATIONS

Gary Monti is a cybersecurity executive with 20+ years of experience. As Senior VP of Security Operations at CyberMaxx, he oversees advanced security solutions using the MaxxMDR framework. Previously, at Avertium, he improved security with the MITRE ATT&CK framework and managed service delivery. His background includes roles at Secureworks, BT Global Services, and International Network Services. Gary holds a Bachelor's in Computer Engineering and an MBA, with certifications as an XDR Certified Administrator and Analyst.

PART I
How AI Became Cyber Defense

Emerging technologies bring with them a measure of excitement, and none in recent memory has garnered as much attention as AI. In this first of a multi-part series, we will explore the application of Artificial Intelligence (AI) for protection of CyberMaxx clients. Ultimately the ability to secure the business assets of our customers is the standard of care any technology must be evaluated too, less it becomes a means unto itself, quickly fading as rapidly as it arrives.

During part 1, we will evaluate AI across the Intelligence Amplification continuum. We make this evaluation from the position of Security Operations, including the benefits and detriments of applying AI to threat detections and security incident investigations.

It's imperative we consider the source of truth AI claims to offer and whether CyberMaxx clients benefit from the professed presentation of facts absent confirmation bias or are drawn into a false sense of confidence.

Novel threats, dealing with the unknown, presents inherent challenges for AI, where fundamentally past results are utilized in making future predictions.

User and Entity Behavioral Analytics (UEBA), wrapped within the term machine learning, brought promise to remediating this faulty characteristic. We will evaluate whether the promise was fulfilled, determining if there is order in chaos. And if yes, how best to apply this knowledge in service to our clients.

Novel threats, dealing with the unknown, presents inherent challenges for AI, where fundamentally past results are utilized in making future predictions."

On May 11, 1997, Gary Kasparov, considered one of the greatest chess players of all time, lost in Game 6 of a chess match to IBM Supercomputer Deep Blue. AI innovation, in the form of chess engine development, accelerated the creation of the Stockfish engine in 2008, considered the best in the world. Currently at v16 each iteration has been defeated by human ingenuity and innovation.

Unconventional sacrifices of strategic pieces, use of chess board boundaries, time-pressure blitz games, all allowed for human creativity to gain an upper hand upon a platform with an arguably finite set of conditions.

What of the infinite possibilities in cyberthreats targeting our clients? Does it not stand to reason, the human inventiveness and resourcefulness that utilizes the application of AI in attack, is best repelled by the same imagination for the unconventional that human beings inspire. Human cleverness in prevention of cyberattacks will be the focus of the final segment in our series.

The CyberMaxx position on the use of Artificial Intelligence begins with consideration for its benefits in protecting the estate of our clients and ends when no longer capable in serving this purpose. Said differently, CyberMaxx is not in pursuit of AI as a technology for pure novelty.

It must serve the common purpose of shielding our clients from cyber threats, to which we are jointly committed. With this we share our CyberMaxx statement on the application of AI.

PART II
Offense Fuels Defense

Diving into part two, we will focus on evaluating AI enablement for Cyber Defense. Through this process we will come to appreciate the Tactics, Techniques, and Procedures (TTPs), universally unique to AI for development and execution of cyber-attacks. So, yes – we take up our defensive position by immersing ourselves in the offensive.

On February 20, 2024, the U.S. Department of Justice (Office of Public Affairs, U.S. Department of Justice), announced a joint effort with UK National Crime Agency (National Crime Agency), causing disruption of the LockBit cybercrime group. Most of the publicity since announcing, has been focused on the outcome, with the international task force assuming ownership of the LockBit infrastructure. However, what is only now starting to be revealed is the approach in nonrepudiation, the methods taken in identifying tradecraft exclusive to LockBit.

The underground is abuzz, with belief the fatal flaw was LockBit's use of AI in augmenting their attacks, while unknowingly revealing themselves."

The underground is abuzz, with belief the fatal flaw was LockBit's use of AI in augmenting their attacks, while unknowingly revealing themselves, by use and community sharing of these novel techniques, to government intelligence agencies who were actively monitoring.

As early as 2016, a research group from ZeroFox presented the application of AI (well, ML was more in fashion at that time), in creating personalized phishing emails through analysis of social media posts. For instance, we are all familiar with the Facebook quizzes to gather personal information. Research and Reconnaissance becomes our most notable application in the use of AI by Threat Groups for the purpose of creating personalized attacks. Furthering this approach, we evaluate Methods of Luring where generative AI seeks to establish more authentic decoys, to gain confidence with the high-value target, in providing prized information.

AI-enhanced, Research and Reconnaissance along with Methods of Luring are foundational in crafting threat vectors for delivering malicious payloads. The means may seem familiar, but it's the level of authenticity that improves the likelihood of compromise.

So – how to defend?

Context Content Correlation

Cyber Defense pre-millennium was all about speed to detection, where static, identifying signatures for malware, coupled with limited points of entry to fixed network architectures, gave rise to Threat Detection Operations (TDO) aka Alert, Identify, Notify. The post-millennium brings with it a softening of the edges to our network. Endpoint, Detection and Response is born of Mobile networking and Handhelds requiring flexibility in detection and a means of containment and isolation. Enter Managed Detection and Response (MDR).

Back to our telling of the LockBit Threat Group takedown. The mode of Defense was first tied to Contextual understanding of Ransomware as the arena for combat. AI-Correlation (Defense) to AI-Enabled Attack Vectors (Offense), with identifying characteristics of LockBit revealing vulnerabilities in the threat group's infrastructure. At that point it was simply a matter of the international coalition to execute on the age-old adage that best Defense is a strong Offense.

PART III
Think Like An Adversary, Defend Like A Guardian

This segment we present the necessity to move out of the MDR Black Box to an AI Defensive 3c model (Context, Content and Correlation). By this approach we think like an adversary and defend like a guardian as the Modern MDR standard in Defensive Cyber Security Operations.

In contemporary warefare a cyber attack is the first strike of offensive operations. On January 13, 2022, the government of the Ukraine experienced wide-scale defacement of its public websites. This attack was later identified as a reconnaissance mission, soon to be followed by a massive campaign on February 24, 2022 – approximately 2hrs before the Russian military crossed into the Ukraine. Denial of Service and Wiper attacks, intended to eliminate access, and destroy critical data, were launched against Ukrainian government and commercial agencies, disrupting satellite communications, restricting access to financial institutions, and disabling public communications.

We must consider where AI could have aided in defense of this cyber-frontal assault.

Doing so requires we evaluate for Large Language Modules (LLMs) inherent to advanced AI systems, which by their nature are designed to produce logical responses when queried.

LLMs consume massive data sets (think petabytes), for their training, primarily sourced within the public domain in the form of books, articles and websites.

Therein lies the challenge, where AI, (particularly generative AI), attempts to provide precise response to modern-day queries, utilizing historical data. In our 3c Model, Correlation is risked by the potential for bias, whether societal or cognitive.

For purposes of our discussion, Conformity Bias is the greatest inhibitor to establishing a defensive posture in cybersecurity, utilizing AI.

> **Modern MDR breaks us out of the Black Box, and reduces the influence of bias, in the investigation of cyber threats."**

As we discussed in Part II, many of today's MDR providers, have their roots in Threat Detection Operations (TDO). They function as established MSSPs leveraging proprietary platforms, creating an MDR Black Box from their TDO Black Box legacy. Solely through inclusion of endpoint telemetry they rebrand as MDR. All the while, the operating standards are based on MSSP workflows.

Alert investigations follow a conventional MSSP path of:

(1) signature and profile mapping to identify the alert

(2) historical records search for the identified alert

(3) evaluation of prior incident handling procedures

(4) third-party validation (Ex then: VirusTotal, Ex now: AI)

These 4 steps of incident handling are the legacy of MSSPs, ultimately influencing many MDR providers in determining the likelihood of a cyber - attack The fatal flaw is we exclude broader context of the alert, as it is evaluated in isolation. We restrict the second of our 3c Model, Context. Years of conventional MSSP analysis creates a conformity bias in Step 3 (evaluate for prior incident handling).

The Incident Handler will examine for what someone did before them and be inclined to take the same steps. Even with Step 4, as augmented through AI, the attributes of bias within the LLMs will lean toward conventional MSSP event handling, producing the same results.

PART IV
Human Ingenuity for Modern MDR Operations

In this final part, we will explore the application of human ingenuity to Modern MDR operations as we fulfill on our mission to Think Like an Adversary and Defend Like a Guardian. Let's pick up with our homework from Part III, referring to Chapter 1, The Nature of War, and Chapter 4, the Conduct of War from the U.S. Marine Corps manual, MCDP1, titled Warfighting (U.S. Marine Corps).

Universal Principles of War

Cyberwarfare as with Conventional warfare is a clash of opposing wills, compounded with multi-variables, referred to as Friction. We consider the boundless landscape of Cyberwarfare, impending obstacles, or random chaos. Friction can be self-induced through lack of clearly defined goals or overly complicated protocols. All of these are amplified with Uncertainty, Fluidity, Disorder, and Complexity as facets of war.

Augmented Intelligence

Artificial Intelligence can aid our cause, respective to the Nature of War, if we pay mind to 2 critical factors, beginning with, Waging war takes a moral, mental, and physical toll on the combatants (Chapter 4, U.S. Marine Corp). Principles of integrity particularly come into play, during incident handling.

I recall an episode in my career when encountering the transmission of illicit materials, where the standards of operations restricted notification through the ticketing system to the named client contacts, as appearing in the contract. There were indicators that one of the client practitioners may have been involved in this criminal act. Therefore, sending a ticket to this individual would only reveal the findings and not address the crime. Applying a moral code to our standards of operations, a notification was sent to 'all' those identified as client contacts, from which the organization was able to isolate the perpetrator, bringing this person to justice. From this, we acknowledge AI was able to deliver the data, while human morality dictated the response.

The second critical factor is avoidance of the fallacy, Appeal to Authority. Anyone experimenting with AI for Cyber Defense is quick to realize there is a wealth of false positives generated as LLMs bring both foundational and private learnings to response, not often orchestrated and quite often non-correlated. The result is Alert Apathy or Alert Fatigue, which speaks to the mental and physical exhaustion, suffered by security operators, from handling excessive and duplicative false positives. Consequences from exhaustion lead to a tendency to default to a third party for decision-making, at risk of Appealing to Authority.

When VirusTotal launched in 2004 it became the default authority for many MSSPs. However, with cases of rare malware, it becomes a less reliable source. We must consider that we don't position AI similarly; where it is the guru, the authority, the tiebreaker. As we've already learned, AI's dependency on prior learnings to make future predictions doesn't account for all conditions. Therefore, we need to evaluate AI for use as augmented intelligence with human oversight, for security investigations, but not the final authority. The test AI must pass is whether we are confident our clients are better protected through its application, and that we don't subject ourselves to Appeal of Authority, as a fallacy in our decision making.

Balancing AI and Human Ingenuity

Let's take the MDR workflow of Detect, Investigate Respond. AI we discussed in the form of augmented intelligence suits us well, in the detection and investigation stage. However Human Ingenuity wins when it comes to Response, the Big R. Here's what I mean – In the Detect stage there is this path of research, development, deployment, tuning, and affirmation. What's all too common with many MDR providers is the exclusive use of platform response (Little r), where the same exact sequence of research, development, deployment, tuning, and affirmation, occurs…repeatedly in attempts to automate response.

This is the reason we must put our attention on Response as the primary element of Modern MDR, leveraging Human Ingenuity for the scope of compromise evaluation, when conducting threat response.

By this approach, we gain the benefit of 3 separate but interconnected human characteristics:

1. Questioning Assumptions
The ability to step back and recursively evaluate, particularly for motive, fits squarely in the realm of Human Ingenuity. We are challenging convention (the domain of AI) and seeking alternatives to what's in front of us.

2. Scope of Compromise Evaluation
This is both a Depth and Breadth exercise, conducted recursively and simultaneously, well suited to Human Ingenuity. Root Cause Analysis (Depth) of the attack and Environmental Spread (Breadth) of the attack.

3. Consequences of Determination
Formulating outcomes of the chosen path, particularly in the long term, is well suited to Human Ingenuity. This includes the ability to balance for aspects of urgency with other responsibilities to the business, such as the ethics of the choices that are made.

One of the best examples of Big R, and the application of Human Ingenuity, is the decision to contain a threat actor to non-critical business systems for observation while evaluating and learning novel techniques over a period. Compare this approach to the AI-driven little-r technique of instant isolation and containment, requiring continual repeats of the incident to establish a behavioral algorithm.

I'll take the former of contain and evaluate, with human observation; over multiple attacks, eventually correlated through machine learning.

> **Human Ingenuity wins when it comes to Response, the Big R.**

Final Words and Take-Aways

In Part I we introduced the application of AI to the aid of Cyber Defense. With this, we set the stage for the evaluation of AI along an Intelligence Amplification continuum. A structure for prescriptive use, with clear expectations for results, as a complement to human ingenuity.

With Part II we presented the importance of Context, Content, and Correlation moving past the legacy Black-Box of MSSPs and pseudo-MDR providers where superficial speed-to-detect is the standard.

Instead, we champion Modern MDR with a Contextual understanding of the attack, federated Content, (beyond what is being ingested as client security-control telemetry) and Correlation of all Telemetry with federated-threat-intelligence, as blended Content, is the surest means of Cyber Defense.

Take-Away #1

Establish a Modern MDR Strategy, where Offense Fuels Defense by utilizing Federated Threat Intelligence and content, supplemental to the telemetry provided by your security controls. This approach will fulfill the 3 C's of Context, Content and Correlation.

For Part III we came to appreciate that conventional MSSP analysis; typical to pseudo-MDR providers, creates conformity bias either by groupthink or application of LLMs with historical learning by historical MSSP incident handling. The result is convention can restrict those searching for a Modern MDR solution, which emphasizes Response as primary.

Take Away #2

Many of today's MDR providers are operating by convention, in an echo chamber, with AI bringing the addition of a Confirmation Bias to the pre-established Conformity Bias of the LLM. Apply Critical Thinking, avoiding the pitfalls of bias during incident investigation.

Take Away #3

Human Ingenuity wins when it comes to Response (Big R), as the new standard for Modern MDR operations. Shifting the Detect Black Box of legacy MSSPs to the response (little-r) Black Box of platform-tuned isolation and containment foregoes Human Oversight and requires duplication in research, development, deployment, tuning, and affirmation. Skill up and seek out those who apply Human Ingenuity to threat research, response, and hunting.

CyberMaxx's Position on the Use of Artificial Intelligence

Lastly, we conclude our series as we began, stating CyberMaxx's position on the use of Artificial Intelligence begins with consideration for its benefits in protecting the estate of our clients and ends when no longer capable in serving this purpose. Said differently, CyberMaxx is not in pursuit of AI as a technology for pure novelty. It must serve the common purpose of shielding our clients from cyber threats, to which we are jointly committed. With this, we share our CyberMaxx statement on the application of AI.

CyberMaxx will apply Artificial Intelligence for Cyber Defense for the exclusive purpose of fulfilling our mission, of protecting clients' business assets and guarding against those committed to wide-scale societal disruption through cyberattacks.

About CyberMaxx

CyberMaxx, founded in 2002, is the leading provider of managed detection and response (MDR) services. We help customers reduce risk by tightly integrating MDR with offensive security, threat hunting, security research, digital forensics, and incident response (DFIR) to continually adapt to new and evolving threats. Our modern MDR approach is tailored to the unique characteristics and risk factors of each customer, enabling us to take full ownership of the response process and, optionally, manage key security controls. By thinking like an adversary and defending like a guardian, we help our customers stay a step ahead of threat actors.