Why CISOs Cannot Rely on Artificial Intelligence for Threat Detection

Hybrid AI outperforms Unsupervised AI

- Human intelligence at machine scale
- Accurate data for effective AI learning
- Validation of predictive capability

AWN CyberSOC with Hybrid AI

- 10X better threat detection and 5X less false positives
- Human validated threat detection accuracy
- Concierge Security Engineer supervises AI learning

Advancements in machine learning, neural networks and cognitive computing have made artificial intelligence (AI) systems the next big thing in cybersecurity. Like any booming field, what AI is and is not can be sometimes unclear.

Marketers have not helped the situation by indiscriminately adopting the AI term to make their products sound more intelligent. Despite the many claims, what is abundantly clear is that cybersecurity has entered a new era. Cybercrimes are committed by sophisticated, technically adept criminals who are leveraging every attack vector available. Massive amounts of data from thousands of sources must be analyzed, and the analytics capacity required is far beyond the cognitive capabilities of humans. Leveraging the superior computing capabilities of machines Is required to help address this issue, thus driving the need for AI to become an essential component of every CISO's cybersecurity toolkit. However, AI has yet to reach the performance of human intelligence and intuition, and therefore CISOs must factor that in when considering AI as part of their security operations infrastructure.

The cybersecurity problems that CISOs face today are still best left for smart, experienced analysts. AI means many things, but fundamentally it is the science of enabling computers to do things that can be done by intelligent humans. Merely solving complex problems or solving problems faster is not AI but just computing.

To solve problems, AI needs to learn, which is done through machine learning, a field within AI focused on learning algorithms. These algorithms are designed to continuously improve by using the results from one set of data being used for the next iteration of learning. Over time, as more data is processed, the algorithm should get smarter and better at predicting what it was designed to do. In cybersecurity, it could be the identification of certain traffic patterns as being indicative of an attack, or profiling users to flag suspicious behavior.

Cybersecurity is Fundamentally a Data Problem

There are many problems in cybersecurity, but having accurate, comprehensive and timely data is where it all starts. One of the biggest problems in cybersecurity is alert fatigue due to false positives from system-generated alarms. Security analysts become desensitized to alerts, due to the sheer volume that are generated, and so they eventually end up ignoring them. This could have disastrous consequences since an ignored alert could be a breach which costs a company billions of dollars, as we saw in the recent Equifax case.

When AI is involved, filtering out false positives is even more critical, since the machine learning algorithms are using this data to refine their threat predictive capabilities. Even with the best algorithms, if the learning is done on bad data, then the algorithms will be useless. AI could be trained to identify false positives, but the learning needs to be done on data where the incidents have been accurately classified.

Data scientists commonly spend 80% of their time cleaning and organizing data for analysis. The task of cleansing data is such a big part of data analysis that data scientist Mike Driscoll coined the term “data munging” in 2009. It is the most undesirable part of developing algorithms for AI, though an undeniably critical step in the process of leveraging AI for cybersecurity.

It is easy to see how an analyst could spend up to 80% of their time on data munging. When an alert occurs, an analyst needs to view the alert in the context of what triggered it. This could require the gathering of a user’s behavioral data, network traffic flow data and logs from various servers and network equipment. In most cases, the data will not be available, and the analyst needs to go about the tedious process of collecting the data. This process can take minutes if the data has already been collected, or even days or weeks if the analyst needs to set up the data collection process. Once collected, all the data needs to be cleaned, parsed and merged with the other data for analysis.

Hybrid-AI: Harnessing the Potential of AI in Cybersecurity

Modern day cybersecurity operations require the processing of such vast amounts of data, AI must be a tool in a CISO’s portfolio of defenses. AI is great at automating routine tasks or situations where the data is known to be clean and accurate. What it does not do well is identifying what needs to be done to process an exception. There is no better way to handle a cybersecurity exception than having an experienced cybersecurity analyst examine it to assess what the correct action should be.

In the AI field, this is known as human in the loop (HITL) AI. Machine learning algorithms not only need accurate data to be effective, they also need to know when and how to incorporate new data. The end output of AI is to make some sort of prediction, and in many cases, this requires sound judgment. In cybersecurity, AI has yet to come close to being able to apply the appropriate judgment required, which is why HITL AI is the best model for a CISO to successfully leverage AI in their security operations.

AWN CyberSOC with Hybrid AI

Arctic Wolf recognizes the limitations of AI's application in cybersecurity, and leverages Hybrid AI to deliver the best of both worlds in its SOC-as-a-Service. Hybrid AI combines human intelligence with machine learning to provide ten times better threat detection, reduce false positives by five times, and speed up response times between detection and response. It applies the learnings from real life security incidents that may not be easily characterized with superfast data processing. Hybrid AI is able to incorporate new data and unexpected events, and can overcome poor data to provide the best protection in the industry.

The human in Arctic Wolf's Hybrid AI HITL system is a Concierge Security Engineer (CSE), who is a seasoned security analyst with industry certifications. They are elite professionals steeped in the art and science of cybersecurity and are well-versed in the industry's best practices. The combination of AI leveraging sophisticated machine learning algorithms and the CSE makes Hybrid AI the industry's most adaptive cybersecurity AI system available.

CSEs create custom rules that filter out false positives or other noise that may reduce the efficacy of AI predictions. They also review the threats identified by the AI system to validate whether they are actual threats or false positives. This provides a closed loop feedback mechanism that does not blindly depend on the data the AI system is using to learn how to identify a threat. The effect is a threat detection capability that combines human intuition with machine scale for ten times better threat detection and five times less false positives.

CSEs play a far larger role in AWN CyberSOC than just supervising machine learning. They are the customer's primary point of contact for all their cybersecurity needs. CSEs act as a trusted advisor to a CISO. Leveraging the broader Arctic Wolf team, they lead the execution of routine and non-routine tasks for the customer. These tasks can include threat hunting, forensic analysis of incidents, or assisting with reports for compliance or regulatory audits.

AWN CyberSOC with Hybrid AI: The Best of Both Worlds

Artificial Intelligence	Concierge Security Engineer
• Learns from Concierge Security Engineer • Predicts threats without bias • Has consistent speed and accuracy	• Helps AI learn by identifying inaccurate data or presenting new data • Provides feedback loop to validate predictions • Analyzes exceptions based on experience and intuition

AI is an essential tool for modern security, so every CISO must have a strategy for how to leverage it for their security operations. The sheer volume of data that needs to be processed ensures that a security strategy that does not include AI is destined to fail. But relying on AI alone is also a losing strategy, because AI's predictive accuracy is wholly dependent on the quality of data from which it learns. Without the cleansing of the data with an HITL learning system, that data is likely permeated with false positives.

Exceptions handling by cybersecurity experts can make the difference between security operations that provides robust threat detection, and one that is insufficient. If a company is experiencing an attack for the first time, the AI algorithm may encounter a scenario that it has never seen, and flag it as an exception. AI alone is not intelligent enough to then go find the necessary data, conduct the forensic analysis and make a determination of whether or not it is a threat. Today, assessing the potential of a threat and performing the thoughtful analysis can only be done by a human being.

AWN CyberSOC with Hybrid AI combines the best of AI with expert CSEs, so that our customers get the best of both worlds. Combining human intelligence with machine learning creates a winning combination that allows CISOs to leverage AI for world-class security operations.

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com