ANOMALI

AI IN CYBERSECURITY

Building Smart Defenses and Outsmarting Threats

If there was such a thing as a cybersecurity Swiss Army Knife, it would definitely be AI. AI can provide more robust protection against dangerous threats, enhance threat hunting, and streamline security analysts' efforts. When implemented effectively, AI serves as a robust defense against sophisticated AI-powered attacks.

Why AI makes the best security "shield"

There are myriad reasons why AI-powered security defenses are a significant upgrade over previous security stacks. First, AI processes data at a speed far beyond human capabilities, enabling the detection of subtle patterns that can easily be overlooked in vast data sets that most enterprises struggle to manage.

AI also transforms threat hunting by enabling security analysts and researchers to search through massive data volumes in a fraction of the time (think petabytes in seconds) required by older technologies. Generative/conversational AI tools facilitate quicker threat detection by allowing natural language queries, saving time typically spent crafting complex queries while enabling T1 analysts to perform at the level of a T3.

Some ways AI can boost cybersecurity defenses include:

- **Ongoing monitoring:**
  AI algorithms can analyze vast amounts of data in real time to identify patterns, anomalies, and potential threats. By continuously monitoring network traffic, system logs, and user behavior, AI can detect suspicious activities and potential security breaches.
- **User authentication:**
  AI-powered authentication systems can analyze vast amounts of biometric data and user behavior in real time, verifying identities more accurately and detecting unauthorized access or anomalous user behavior.
- **Prioritized vulnerability management:**
  One of the most vexing problems in security operations is alert fatigue. It's no easy matter to detect potential vulnerabilities and then sort the wheat from the chaff, triggering alerts only for the highest priority incidents. This is an area where AI really shines. By analyzing vulnerability scans and triaging their findings, AI lets security teams focus on the most critical issues that need immediate attention.
- **Automation:**
  AI can automate incident-response processes, triggering sequences of pre-defined actions in response to detected threats. This may include blocking suspicious network traffic, isolating compromised systems, sending alerts, etc.

- **Security orchestration:**
  Whereas the term “automation” usually refers to automating individual tasks or processes, orchestration is a “meta automator,” creating and streamlining automated workflows across security tools, applications, and environments. This allows collaboration and correlation across multiple systems — previously a nearly impossible undertaking — exponentially improving overall incident-response capabilities.
- **Beating hackers at their own game:**
  AI has helped hackers maliciously elevate their attacks by making them more sophisticated and harder to detect. For example, phishing attacks from five years ago were easier to spot, since they often contained bad grammar, unrealistic scenarios, or other obvious “tells.” But generative AI can help anyone write like a Harvard graduate or “sanity check” their emails to help them evade notice. AI can help you identify and neutralize these threats.

Anomali’s AI-Powered Security Operations Platform does all of the above, and more. With its ability to query and correlate current and historical data from every source in your ecosystem, it can add context to events that might otherwise escape notice.

AI threats require an AI defense

There’s an interesting irony when it comes to AI-powered security solutions: the solution’s AI is itself a significant attack surface. The following are some ways that an attacker might use AI to compromise a target’s AI:

Adversarial attacks:

Manipulating input data to deceive AI systems into making incorrect predictions or classifications, creating potential vulnerabilities

Data poisoning:

Unlike other adversarial attacks that target the model during inference, data poisoning attacks strike at the training phase, injecting malicious data into datasets to manipulate the behavior of AI systems and compromising integrity

Model inversion:

Exploiting the information leakage from AI models to infer sensitive information about the training data, potentially putting user privacy at risk

Evasion attacks:

Feeding manipulated input data to AI systems to evade detection or classification, such as malware designed to bypass AI-based security systems

Anomali's AI is particularly effective at dealing with these types of attacks because it uses its own, closed AI "universe." There's no need to worry about bad actors corrupting its models because it essentially resides in its own locked room. They cannot inject malicious data models into its training dataset and it doesn't leak data that hackers can exploit.

How Anomali leverages AI to elevate your security posture

When you use Anomali, you get the best AI-Powered technology to strengthen your defenses against any type of attack. Anomali's intelligent Copilot queries your data (including historical data) in real time and matches it against the industry's most robust repository of threat intelligence to mitigate hallucinations. And because every moment during an attack counts, it is designed to correlate petabytes of relevant telemetry with intelligence to deliver meaningful insights in mere seconds.

For example, imagine that Anomali detects a suspicious file in your system. In real time, it will quickly search your data from every source — past and present — to discover whether the same IOC has shown up before (and how many times). This context is tremendously helpful in uncovering the origin of the threat and the timeframe of when it entered your environment. It limits risk by enabling you to respond immediately (such as isolating an endpoint or blocking malicious traffic).

Another benefit of using Anomali is its ease of use. Whereas most security platforms require users to construct elaborate queries, Anomali lets you ask questions in natural language. Its AI-Powered Copilot searches your data — from any source or over any time period — and provides answers almost instantaneously.

Schedule a live product demo and learn how Anomali can help you harness the potential of the leading AI-Powered Security Operations Platform.