AI In Threat Detection and Proactive Security

Ekin Yilmaz

June 2025

In today's interconnected world, cyber threats are evolving at an unprecedented pace. IBM estimates that a cyberattack costs a business $4.33 million, nearly double the cost in the United States. Furthermore, the annual cost of Cybercrime is projected to exceed $10.5 trillion by 2025. The need for effective, efficient, and automated cybersecurity methods has never been more critical.

This is where Artificial Intelligence steps in. With the rise in cybercrime, numerous complex threats have also emerged. Some notable examples include AI-powered ransomware, advanced social engineering, phishing attacks, and even supply chain attacks targeting smaller vendors to get access to multiple larger companies. These emerging threats often bypass conventional security solutions, leaving a unique gap for AI to fill.

Proactive Security with AI

The true potential of AI in security lies in its ability to achieve proactive defense. This is far beyond mere threat detection to foretelling and countering threats before they can become active. Agentic AI, in particular, can revolutionize proactive defense. Agentic AI systems are capable of making decisions independently and learning how to respond to novel situations.

AI can eliminate a detected threat, understand its context, and automatically contain or remediate it, such as quarantining infected systems or blocking threatening IP addresses. Autonomous Threat Response provides a real-time, adaptive response, significantly reducing the window of opportunity that attackers typically enjoy.

By constantly learning from global threat intelligence and observed attack trends, AI has the potential to forecast impending attack vectors and vulnerabilities. Companies can enhance their defenses, implement patches, and change security policies before they are exploited.

AI systems can continually refine their detection models and response procedures using new data and feedback on attack outcomes, thereby enhancing their long-term security posture.

Reorienting Threat Detection from Reactive to Predictive

AI is transforming threat detection from a reactive to a proactive and predictive function. Unlike static defenses, AI-based systems are capable of processing vast volumes of data. AI-powered applications can process and correlate massive volumes of security data, including network traffic, endpoint logs, user activity, and threat intelligence feeds, in real-time. They can do so to detect faint patterns and indicators of compromise that humans would be unable to discover.

Through monitoring overall behavior trends, AI has been able to effectively flag anomalies as potential threats, including even previously unknown zero-day attacks. It is a critical feature in the war against AI-driven attacks and APTs, which are designed to evade traditional detection methods.

AI executes the initial stages of threat assessment, alleviating the burden on security teams and response time. Security teams are left to do what they do best — more complex and strategic work, rather than sifting through a deluge of alarms by automating these processes.

Predictive AI For Threat Detection

The addition of AI into threat detection and active security has several significant advantages. AI can significantly decrease the time between a threat's appearance and its removal, which is crucial when running a company of any scale. Furthermore, it reduces both false positives and negatives, keeping actual threats in check with minimal effort. Kevin Mitnick, a cybersecurity expert, once stated that, "The human element is the weakest link in security." AI helps combat this by automating mundane tasks, allowing human security personnel to focus on high-level activities and reducing the likelihood of errors. It handles increased volumes and qualities of security data without corresponding increases in personnel.

Furthermore, as cyberattacks continue to evolve, AI provides a crucial edge in developing more resilient and proactive security defenses. For example, the NVD (National Vulnerability Database) catalogs over 10,000 new vulnerabilities every year. This gives AI another unique role since it can adapt to threats and vulnerabilities much faster than a human or a traditional counterpart. Companies, on average, took 3 days to respond to cyberattacks, according to Statista. They also took over 33 days to complete their investigation of the attack. This further highlights the edge of AI-powered security that could have avoided those attacks entirely and adjusted to them in a fraction of the time.

Let's Incorporate AI into Your Security

The total cost of cybercrime year over year is rising at an unprecedented rate. The cost of a cyberattack on a company with AI-based security is nearly half that of a company with traditional security. This large gap highlights the future threat detection that AI has. Auxin Security will be able to provide professional guidance and support during this transition. This enables companies to be better equipped for the cyber challenges of 2025 with AI-powered security, making their shield from attackers predictive and proactive instead of reactive.