REPORT ANALYSIS

Advanced AI models increase cyber risks for institutions

In short – New, advanced AI models increase the likelihood of cyber-attacks. Small and medium-sized enterprises in particular are vulnerable. This technology makes it easier and faster to identify and exploit vulnerabilities, resulting in less time to intervene. This report outlines what this means for institutions under AFM supervision. The focus lies on strengthening cyber resilience, for example by applying timely security updates, maintaining robust monitoring, facilitating rapid incident response, and ensuring baseline security measures are in place.

JUNE | 2026

AFM

1. Background

Recent publications[1] and evaluations[2] show that advanced AI models (General Purpose AI, as referred to in the EU AI Act) with increasing cyber capabilities are becoming increasingly adept at identifying vulnerabilities, combining attack steps, and independently executing complex cyber tasks. As a result, the time between the emergence or discovery of a vulnerability and its potential exploitation is becoming ever shorter[3].

Developments surrounding these models illustrate the acceleration within the threat landscape. Advanced AI models can automatically detect and exploit vulnerabilities and execute advanced attacks in controlled environments. At the same time, other AI models, including open-source models, are developing similar capabilities, making this development more broadly relevant. Although these models cannot yet always be fully independently tested by institutions and supervisors[4], independent research shows that they are increasingly capable of executing complex attack steps in controlled environments.

The AFM notes that the same AI is used for both offensive and defensive purposes. Moreover, technology companies deploy this same technology for defensive purposes, such as protecting vital infrastructure. This emphasizes that AI offers both opportunities to strengthen cyber resilience and entails risks due to potential misuse[5].

The capabilities of AI-driven cyber-attacks are increasing rapidly[6]. Attacks are becoming more complex, can operate autonomously for longer periods, and are more easily scalable[7]. This may give attackers an advantage in the short term[8]. The Dutch National Cyber Security Centre (NCSC-NL) also warns[9] that this development is significantly accelerating cyber-attacks.

Against this background, the pressure on the cyber resilience of institutions is increasing[10]. Institutions are expected to ensure their baseline security is in order, strengthen vulnerability management, and implement security updates more quickly. It is also important that they improve their monitoring and incident response and shorten reaction times. The AFM draws the attention of all institutions to this development, particularly mid-sized and smaller entities.

The AFM is monitoring these developments closely and expects institutions to assess which additional measures are necessary within their own organizations. At the same time, the AFM encourages institutions to explore how AI can be deployed to strengthen their own cyber resilience and that within the supply chain.

[1] Anthropic – Claude Mythos Preview / Red Team analysis
[2] Our evaluation of Claude Mythos Preview's cyber capabilities | AISI Work
[3] Anthropic – Project Glasswing
[4] Anthropic – Project Glasswing
[5] Generative AI: a transformative impact on cybersecurity | Netherlands Authority for Digital Infrastructure (RDI)
[6] UK AI Security Institute – autonomous AI cyber capabilities
[7] Our evaluation of Claude Mythos Preview's cyber capabilities | AISI Work
[8] SANS Critical Advisory: BugBusters - AI Vulnerability Discovery Hype vs. Reality | SANS Institute
[9] Anthropic's frontier model Mythos calls for immediate action | NCSC
[10] CERT-EU - AI is changing the economics of vulnerability discovery. Defenders should adapt now

2. What does this require of institutions

This development increases the pressure on institutions to respond more quickly to vulnerabilities and incidents. For you, this means that the time to react is becoming shorter. Attackers can strike faster after a vulnerability becomes known. As a result, you have less time to identify and resolve problems.

Why is this important for you?

Mid-sized and smaller institutions in particular face additional risks. For example, because their security is less developed or because legacy systems are still in use. At the same time, the impact of cyber incidents can be substantial, including within the supply chain in which you operate.

The AFM monitors these developments closely and expects institutions to assess what this means for their own organization. Do not adopt a wait-and-see approach.

What can you do now?

1. Accelerate security updates

The window of opportunity to exploit vulnerabilities is continuously shortening. It is therefore important to implement critical security updates as quickly as possible, preferably in an automated manner. Waiting is no longer advised in the current situation.

2. Ensure visibility and rapid action

Ensure that you know what is happening within your systems, so that you can detect anomalies in a timely manner. You do not immediately need advanced solutions for this. Even with basic logging and monitoring, potentially through your IT service provider, you can take important steps.

Furthermore, ensure that you can act swiftly in the event of incidents. Limit damage, for example, by segregating systems, mapping the attack surface, and ensuring reliable backups. Additionally, regularly test whether your internet-facing systems are adequately secured.

3. Explore the use of AI

AI not only presents risks, but also opportunities. You can deploy this technology to recognize and prioritize vulnerabilities more quickly. Initiate this in a controlled manner and collaborate with your suppliers where possible, establishing clear agreements regarding security and oversight. Even when ICT or security services are outsourced, the management board remains responsible for the cyber resilience of those services and for a controlled approach to risks within the supply chain.

4. Continue to strengthen baseline security

Even in a changing threat landscape, baseline security measures remain essential, such as:

- utilizing multi-factor authentication
- managing access rights carefully
- ensuring oversight of internet-facing systems

Baseline measures in particular make the difference when attacks are executed more rapidly and easily. For further guidance, we refer to the AFM Principles for Information Security and the 5 basic principles[11] of secure digital business from the NCSC-NL. For institutions subject to DORA, the Regulatory Technical Standards on the ICT risk management framework[12] additionally provide relevant guidance, including for vulnerability and patch management.

[11] NCSC – 5 basic principles of digital resilience

[12] EUR-Lex – Delegated Regulation (EU) 2024/1774 / DORA RTS