DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

MI a házban, avagy egy kiberbiztonsági szakember találkozása egy felforgató technológiával

Dr. Krasznay Csaba
egyetemi docens
CrySyS Lab

Először is, mit tudok én most az MI-ről?

Mit mondanak a “nagyok” az MI-ről?

The Power and Promise of AI

AI is reshaping every industry, pushing the boundaries of what technology can achieve. These quotes highlight AI's vast potential and its promise to revolutionize both business and daily life.

"AI is the new electricity."
Andrew Ng

"Artificial intelligence is the future, and the future is here."
Fei-Fei Li

"Computers are able to see, hear and learn. Welcome to t
Dave Waters

"Artificial intelligence will reach human levels by around 2
we will have multiplied the intelligence, the human biologi
a billion-fold."
Ray Kurzweil

"AI is not just a tool for automation; it's an enabler for aug
Satya Nadella

AI and Humanity's Future

As AI technology advances, it raises significant questions about the future. These thinkers reflect on AI's potential to transform humanity—for better or worse.

"The development of full artificial intelligence could spell the end of the human race."
Stephen Hawking

"AI will be the best or worst thing ever for humanity."
Elon Musk

"The pace of progress in artificial intelligence is incre
exponential."
Elon Musk

"The question of whether machines can think is abou
submarines can swim."
Edsger Dijkstra

"The real risk with AI isn't malice but competence."
Elon Musk

Ethics, Responsibility, and Risks of AI

AI's influence brings ethical concerns and societal responsibilities. Here, leading voices address the moral questions we must consider as AI becomes more embedded in our lives.

"With artificial intelligence, we are summoning the demon."
Elon Musk

"Technology is a useful servant but a dangerous master."
Christian Lous Lange

"The key question isn't 'What can AI do?' but 'What should AI do?'"
John C. Havens

"We must address, individually and collectively, moral and ethical issues raised by cutting-edge research in artificial intelligence and biotechnology, which will enable significant life extension, designer babies, and memory extraction."
Klaus Schwab

"Artificial intelligence is only dangerous if we pretend it has intent."
Chris Messina

Forrás: https://jdmeier.com/ai-quotes/

Mit jelent számomra az MI?

Az biztos, hogy az MI már elfoglalta a

AI has also introduced a new dimension of risk: adversaries targeting the very AI systems underpinning the modern enterprise. As AI is embedded into development pipelines, SaaS platforms, and operational workflows, AI systems themselves become part of the attack surface. Adversaries exploited legitimate AI tools by injecting malicious prompts that generated unauthorized commands. As innovation accelerates, exploitation follows. Security must parallel the slope of innovation. In the agentic era, cybersecurity is the foundational infrastructure required to protect AI itself.

The data in this year's Global Threat Report makes clear that speed is now the defining characteristic of intrusion, and it has fundamentally reshaped how adversaries evade detection.

The average eCrime breakout time fell to **29 minutes** in 2025, a 65% increase in speed from the prior year. The fastest breakout took just **27 seconds**. In one intrusion, data exfiltration began within four minutes of initial access. The window to detect, decide, and respond has narrowed dramatically.

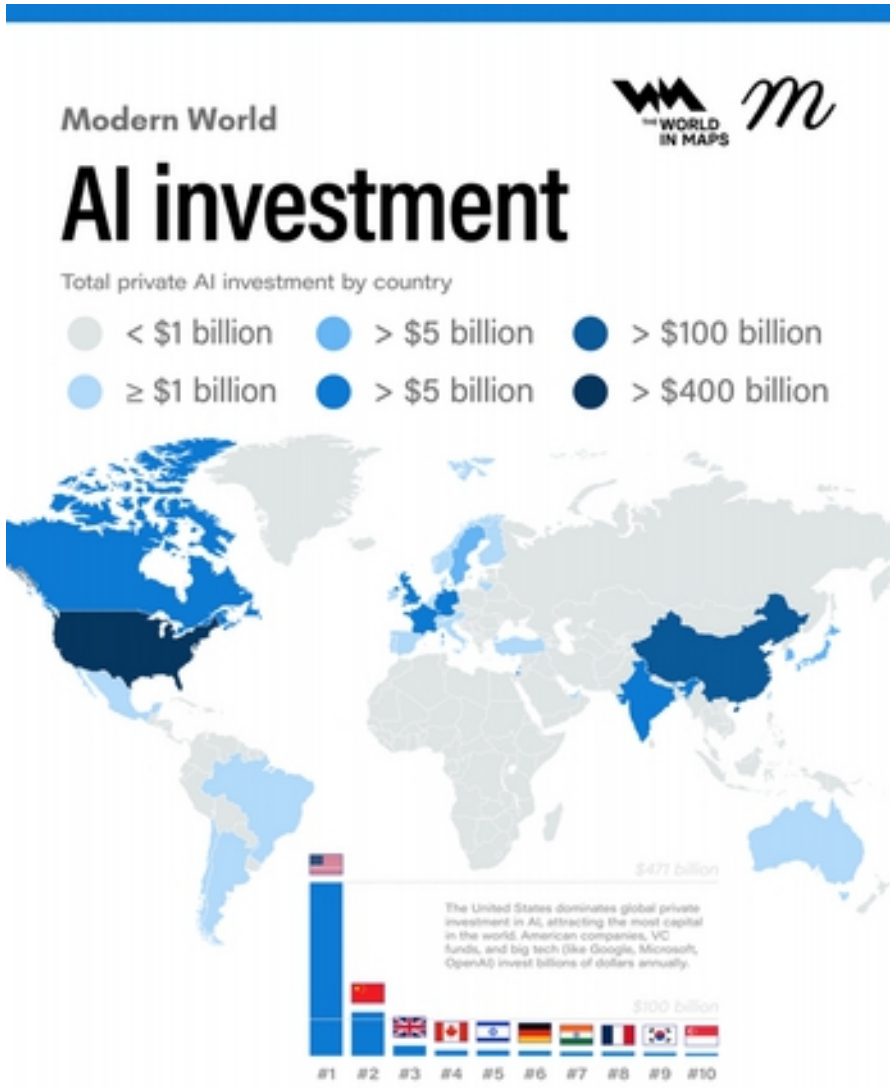
In 2025, evasion was defined by the speed at which adversaries exploit trust. Adversaries operated through valid credentials, trusted identity flows, approved SaaS integrations, and inherited software supply chains. Notably, **82%** of detections were malware-free. Intrusions moved through authorized pathways and trusted systems, blending into normal activity.

Forrás: CrowdStrike 2026 Global Threat Report

Mandiant has observed evidence indicative of closer collaboration between initial access partners and secondary groups. A key signal is the time delta between the earliest activity by an initial access partner and the hand-off to a secondary threat cluster, which has been steadily decreasing since 2023. In this context, the "earliest activity" is the earliest activity in the environment that can be attributed to an attacker. This includes non-interactive events, such as the distribution of malware, and represents the moment at which a group gains access to an environment, whether they utilize it or not. A hand-off occurs at the moment of earliest activity by a secondary group. In 2022, Mandiant identified the median time between initial access and subsequent hand-off was greater than 8 hours. However, in 2025, the median time between initial access and the time at which a second group had access to the environment was 22 *seconds*. In many cases, this reflects the often automated process through which initial access partners deliver malware directly on behalf of the secondary group instead of advertising access in an underground forum.

Forrás: Mandiant M-Trends 2026

De kié az MI? Geopolitikai kérdések



BUSINESS 2.0 | Events | Climate Tech | Robotics | Automation | Crypto | Space

RANK	COUNTRY	TOTAL INVESTMENT	PRIVATE (2024)	GOVERNMENT	KEY FOCUS
1	United States	$470.9B	$109.1B	$8.1B	Generative AI, enterprise, chips
2	China	$125B	$9.3B	$56B (39%)	Manufacturing, semiconductors
3	European Union	€110B	~$50B cumulative	Varies	InvestAI initiative
4	United Kingdom	$28B	$4.5B	Varies	Fintech, healthcare AI
5	Canada	$15.3B	$2.4B govt pledge	$2.4B	Supercomputers, SMB access
6	Israel	$15B	Strong VC	$130M	Defense, cybersecurity
7	Germany	$11.3B	Private-led	Varies	Manufacturing, automation
8	India	$11.1B	Growing	$1.25B	IndiaAI Mission
9	Singapore	$7.3B	Private-led	Strategic	Financial services, smart city
10	Japan	$5.9B	Corporate-led	National strategy	Robotics, manufacturing

Szóval, hogyan álljak hozzá CISO-ként?

Ugyan, mi baj lehet ebből?

Rövid kitérő: MI a hadviselésben

Pentagon says US military to be an 'AI-first' fighting force

2 days ago

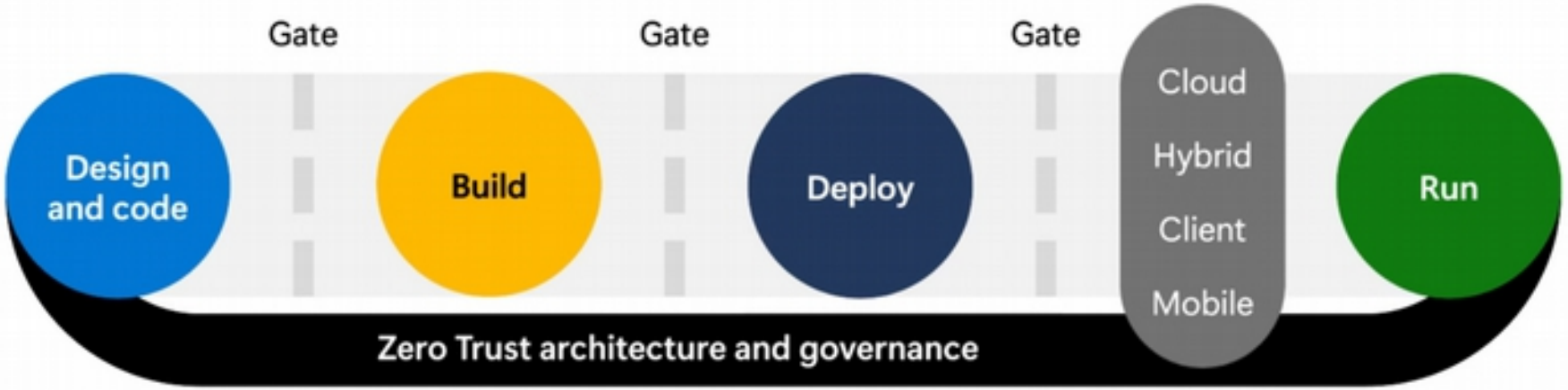
Kali HaysTechnology reporter

Reuters

US Defence Secretary Pete Hegseth has called for more AI use by the US military

The US military plans to increase its use of artificial intelligence (AI) further after the Pentagon agreed to new and expanded contracts with some of the biggest names in technology.

De legnagyobbak már biztosan tudják,



Security risks (and the need to mitigate them) can occur at any point in the development lifecycle:

- Design – ensure that the design doesn't naturally allow attackers to easily gain unauthorized access to the workload, its data, or other business assets in the organization.
- Code – ensure that writing (and re-use) of code doesn't allow attackers to easily take control of the application to perform unauthorized actions that harm customers, employees, systems, data, or other business assets. Developers should also work in a secure environment that doesn't allow attackers to do this without their knowledge.
- Build and Deploy – ensure that the continuous integration and continuous deployment (CI/CD) processes don't allow unauthorized users to alter the code and allow attackers to compromise it.
- Run – ensure that environment running the code (cloud, servers, mobile devices, others) follows security best practices across people, process, and technology to avoid attackers compromising and abusing the workload. This includes the adoption of well-established best practices, security baseline configurations, and more.
- Zero Trust architecture and governance – All of these stages should follow Zero Trust principles to assume breach (assume compromise), explicitly verify trust, and grant the least privilege required for each user account, machine/service identity, and application component.

… vagy mégsem?

Best practices • February 3 • 6 min read

Microsoft SDL: Evolving security practices for an AI-powered world

By Yonatan Zunger, Corporate Vice President and Deputy Chief Information Security Officer, AI

What's new in SDL for AI

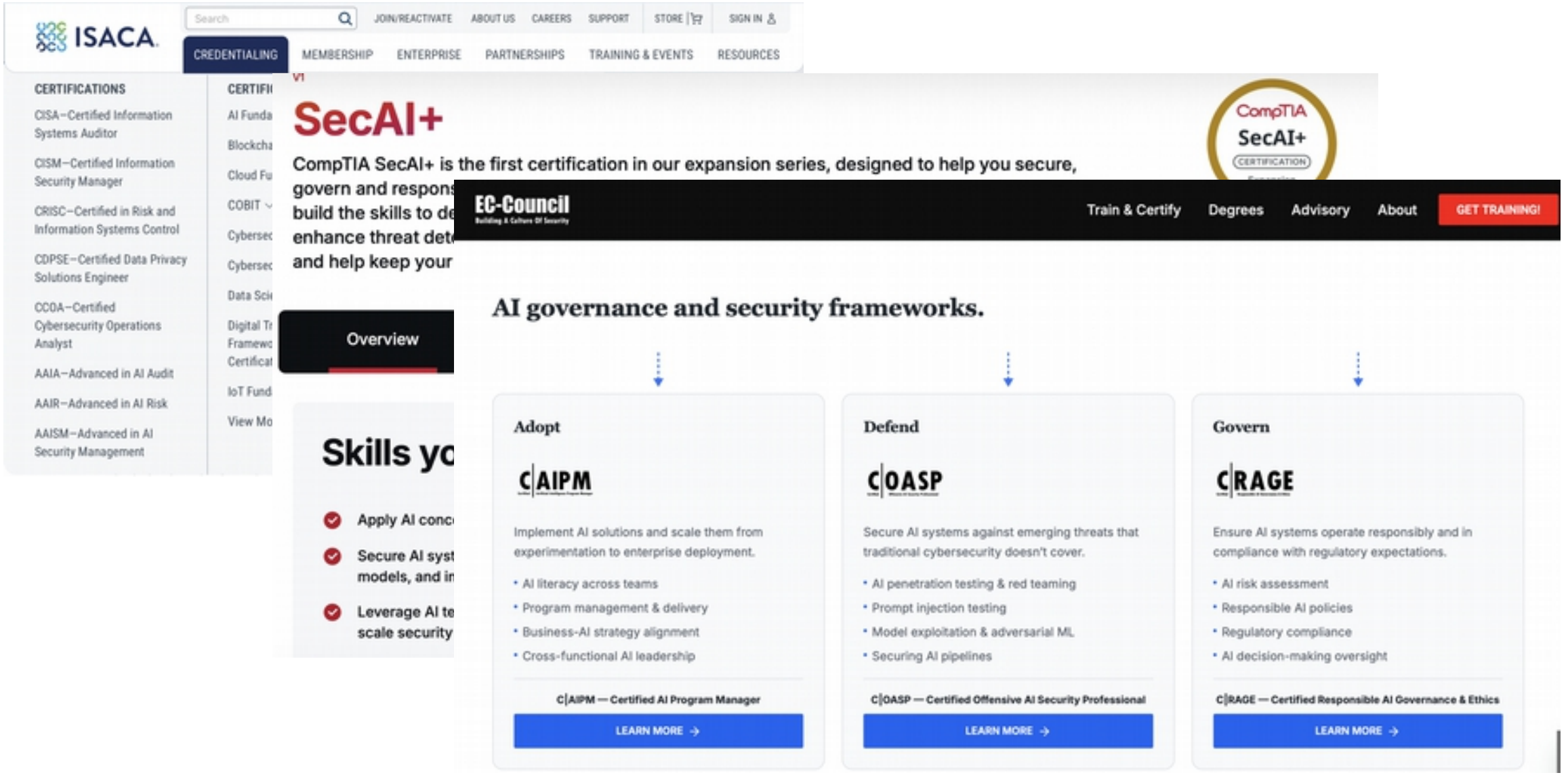
Microsoft's SDL for AI introduces specialized guidance and tooling to address the complexities of AI security. Here's a quick peek at some key AI security areas we're covering in our secure development practices:

- **Threat modeling for AI**: Identifying cyberthreats and mitigations unique to AI workflows.
- **AI system observability**: Strengthening visibility for proactive risk detection.
- **AI memory protections**: Safeguarding sensitive data in AI contexts.
- **Agent identity and RBAC enforcement**: Securing multiagent environments.
- **AI model publishing**: Creating processes for releasing and managing models.
- **AI shutdown mechanisms**: Ensuring safe termination under adverse conditions.

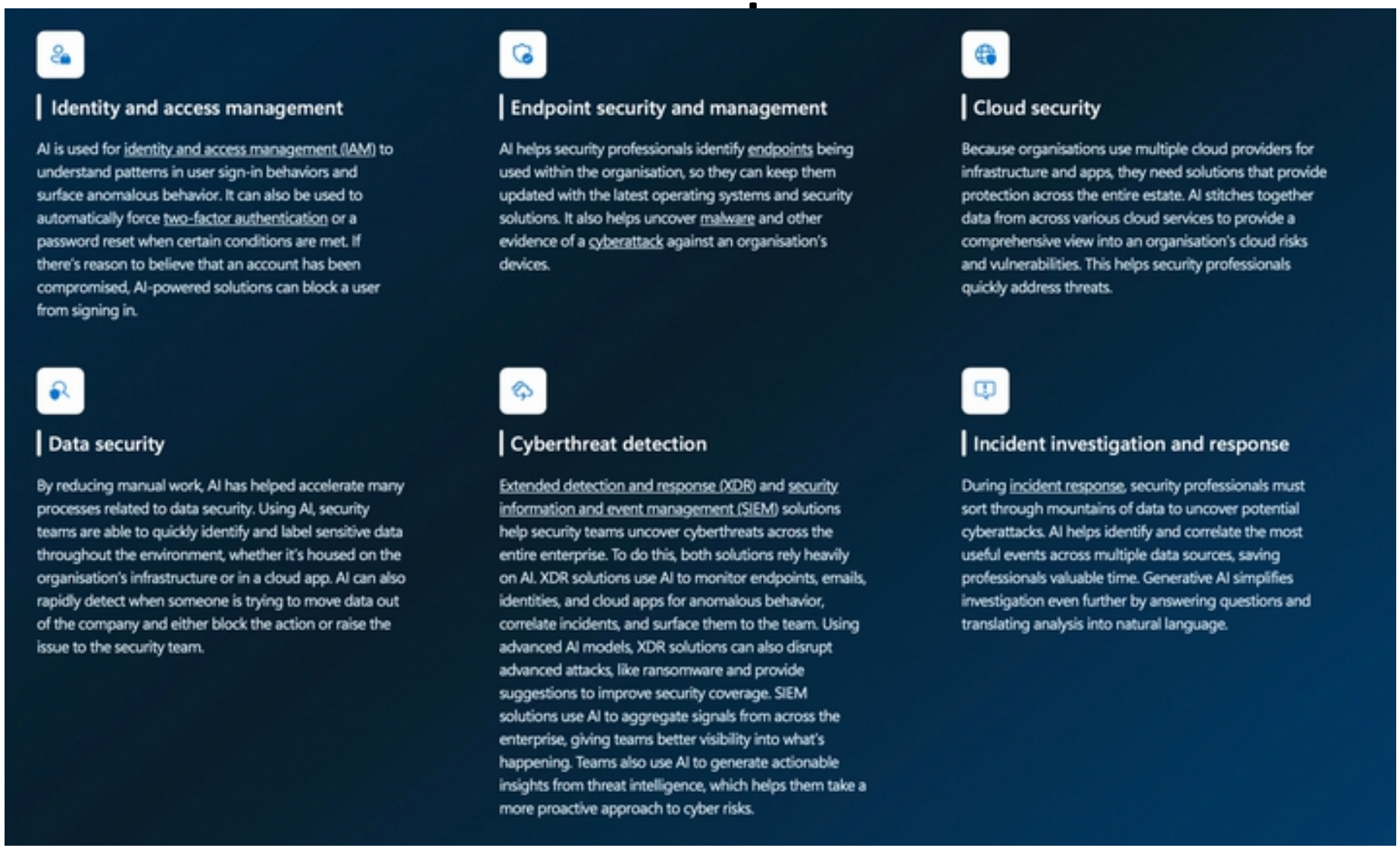
In the coming months, we'll share practical and actionable guidance on each of these topics.

De majd a szabványok megmutatják!

De legalább vizsgázni már tudunk!



Az eszközeink, amik jelenleg biztosan



Identity and access management

AI is used for identity and access management (IAM) to understand patterns in user sign-in behaviors and surface anomalous behavior. It can also be used to automatically force two-factor authentication or a password reset when certain conditions are met. If there's reason to believe that an account has been compromised, AI-powered solutions can block a user from signing in.

Endpoint security and management

AI helps security professionals identify endpoints being used within the organisation, so they can keep them updated with the latest operating systems and security solutions. It also helps uncover malware and other evidence of a cyberattack against an organisation's devices.

Cloud security

Because organisations use multiple cloud providers for infrastructure and apps, they need solutions that provide protection across the entire estate. AI stitches together data from across various cloud services to provide a comprehensive view into an organisation's cloud risks and vulnerabilities. This helps security professionals quickly address threats.

Data security

By reducing manual work, AI has helped accelerate many processes related to data security. Using AI, security teams are able to quickly identify and label sensitive data throughout the environment, whether it's housed on the organisation's infrastructure or in a cloud app. AI can also rapidly detect when someone is trying to move data out of the company and either block the action or raise the issue to the security team.

Cyberthreat detection

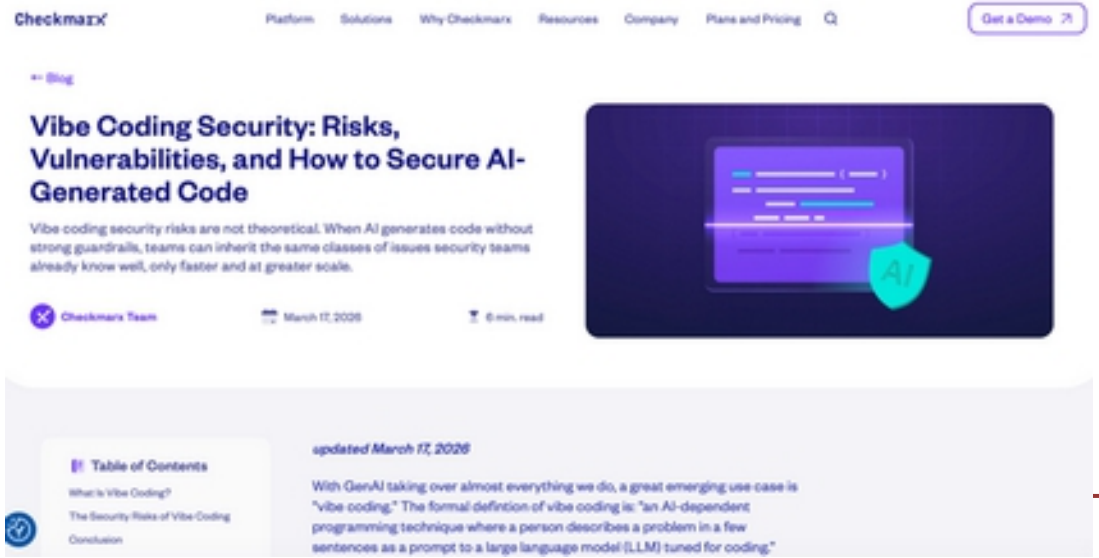
Extended detection and response (XDR) and security information and event management (SIEM) solutions help security teams uncover cyberthreats across the entire enterprise. To do this, both solutions rely heavily on AI. XDR solutions use AI to monitor endpoints, emails, identities, and cloud apps for anomalous behavior, correlate incidents, and surface them to the team. Using advanced AI models, XDR solutions can also disrupt advanced attacks, like ransomware and provide suggestions to improve security coverage. SIEM solutions use AI to aggregate signals from across the enterprise, giving teams better visibility into what's happening. Teams also use AI to generate actionable insights from threat intelligence, which helps them take a more proactive approach to cyber risks.

Incident investigation and response

During incident response, security professionals must sort through mountains of data to uncover potential cyberattacks. AI helps identify and correlate the most useful events across multiple data sources, saving professionals valuable time. Generative AI simplifies investigation even further by answering questions and translating analysis into natural language.

Forrás: Microsoft - What is AI for cybersecurity?

A meglepetések, melyekkel nap, mint nap esülü



Összefoglalás

- csabakrasznay
- www.crysys.hu 

Köszönöm a figyelmet!