Cybersecurity 2025: Navigating the Evolving Threat Landscape

Wissam Mallouli

CTO, Montimage

Online Conference, Organised by MECyS

10 April 2025

Co-funded by the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.

Agenda

01 Introduction: Some Figures

02 The Evolving Threat Landscape

03 AI-Powered Defenses

04 Conclusion and Q&A

Some Figures

Source : Global Threat Report 2025 – Crowdstrike

Micro and Small Enterprises (MSEs) represent 98.9% of the European enterprises.

43% of all data breaches involve small and medium-sized businesses.

61% of all MSEs have reported at least one cyber attack during the previous year.

40% of the small businesses that faced a severe cyber attack experienced at least 8 hours of downtime.

85% of MSPs consider ransomware one of the biggest threats to their SME clients.

30% of small businesses consider phishing attacks to be the biggest cyber threat

Some Figures

Source : Global Threat Report 2025 - Crowdstrike

83% of small and medium-sized businesses are not financially prepared to recover from a cyber attack.

91% of small businesses haven't purchased cyber liability insurance.

Only 14% of small businesses consider their cyber attack and risk mitigation ability as highly effective.

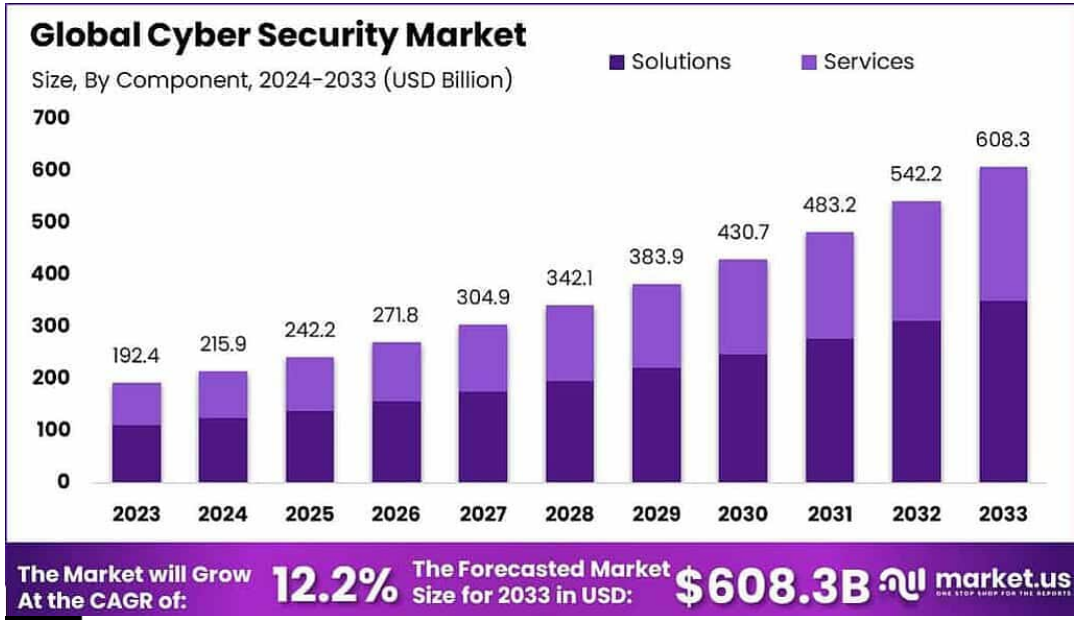
43% SMBs do not have any cybersecurity plan in place.

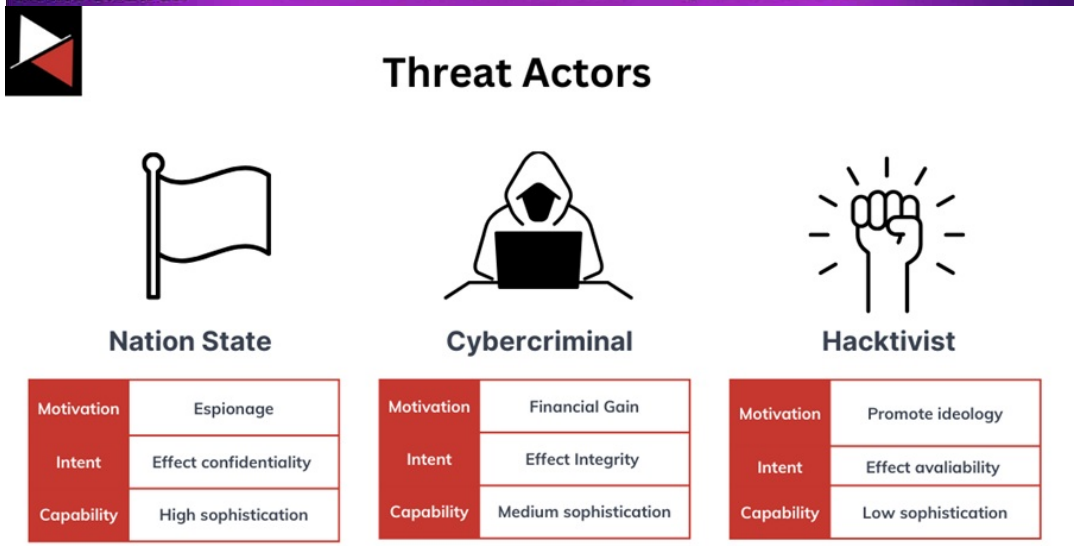
One in five small companies does not use endpoint security, and 52% SMEs do not have any IT security experts in-house.

87% of organizations reported experiencing AI-driven cyberattacks in the past year. 93% of businesses expect to face daily AI attacks over 2025.

The Evolving Threat Landscape

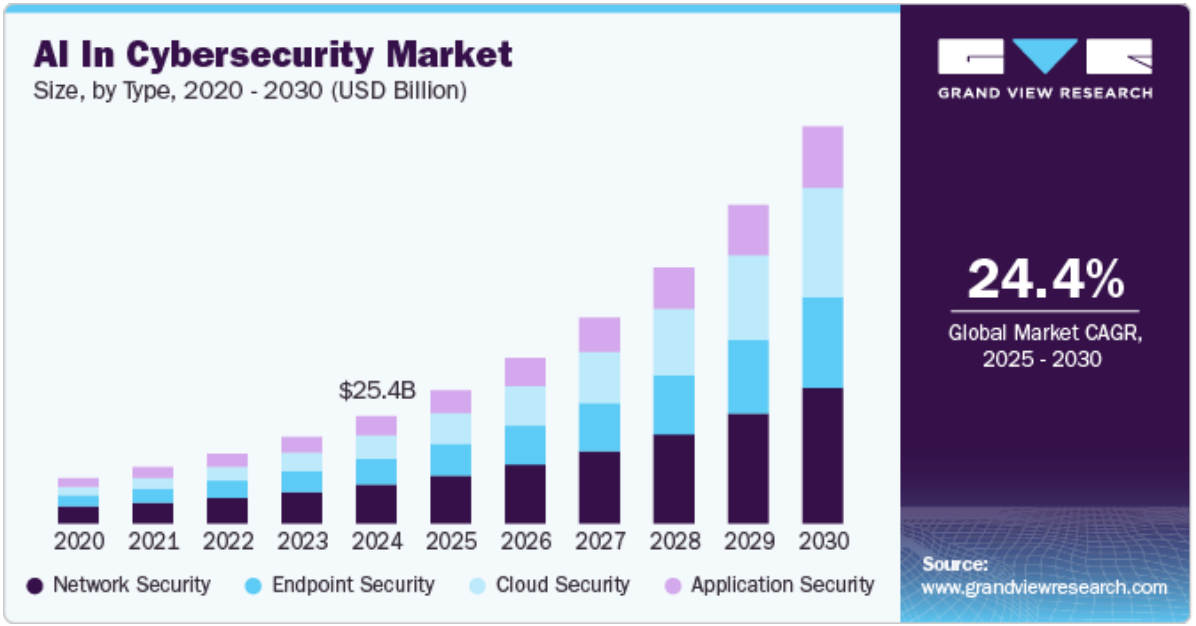
- Cybercrime is becoming more organized and industrialized (e.g., ransomware-as-a-service).
- Threat actors include state-sponsored groups, hacktivists, and cybercriminal syndicates.
- Increased attack surfaces due to IoT, remote work, and digital transformation.

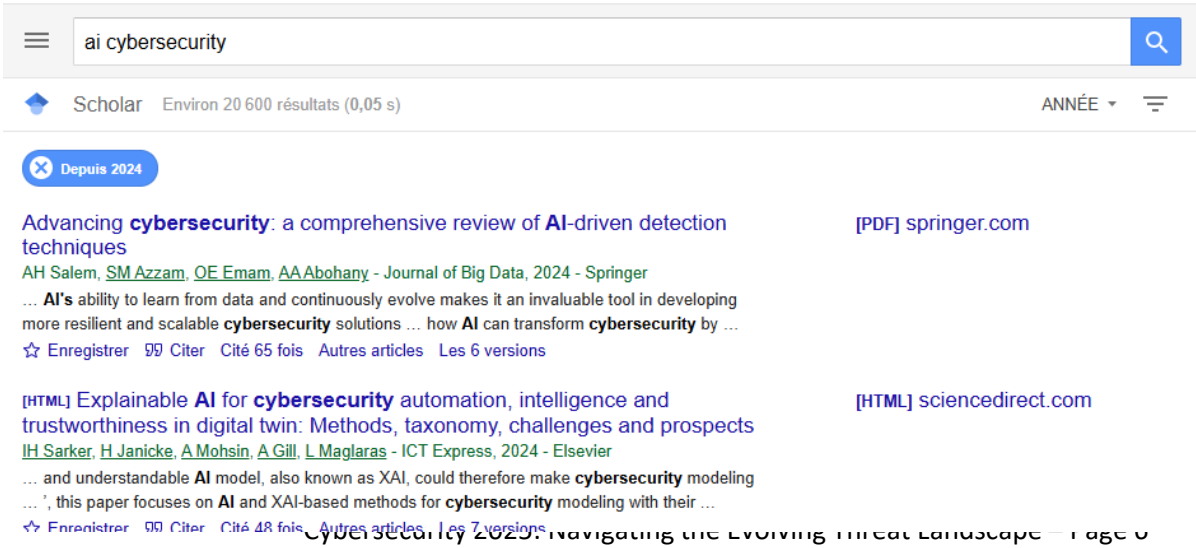




Rise of AI-Powered Attacks and Defenses

- Use of generative AI for phishing, deepfakes, and social engineering.
- AI models used to automate malware development and vulnerability discovery.
- LLM-based attack scripts generation
- Increased scale and sophistication of cyberattacks
- On the defense side: AI/ML for threat detection, anomaly detection, and behavior analysis etc.





AI-Driven Cyber Threats

Cyber threats are no longer manual and isolated…
They're increasingly automated and sophisticated, powered by AI.
Here are some examples:

AI-Powered Phishing

Mass-produced, highly personalised, realistic phishing emails at scale

AI Deepfake Scams

AI-generated videos/audio impersonating executives or trusted contacts

Adaptive Malware

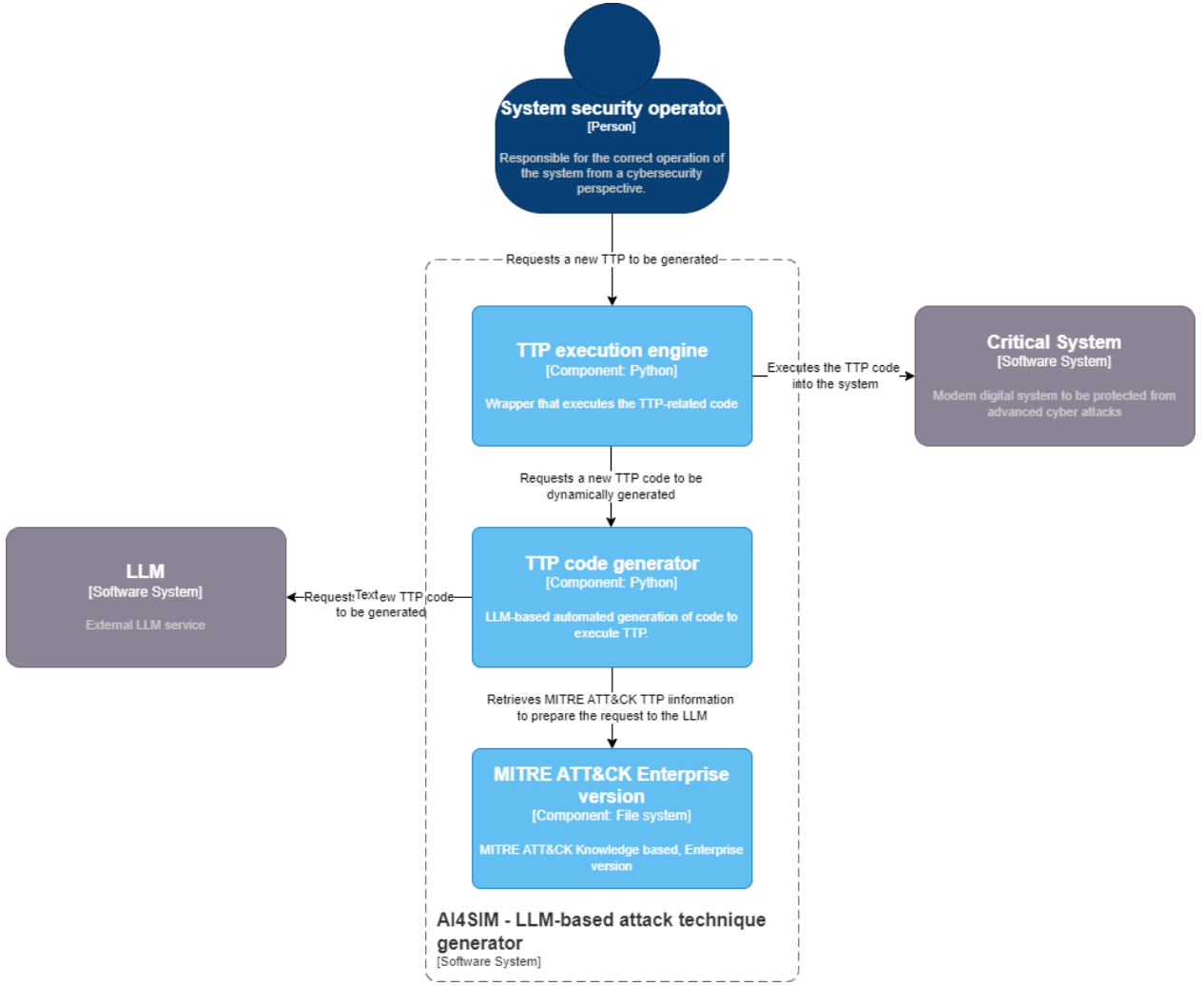
Malware that evolves autonomously, evading conventional detection and response mechanisms

LLM-based Attacks Scripts

Using Generative AI to generate attacks based on their description

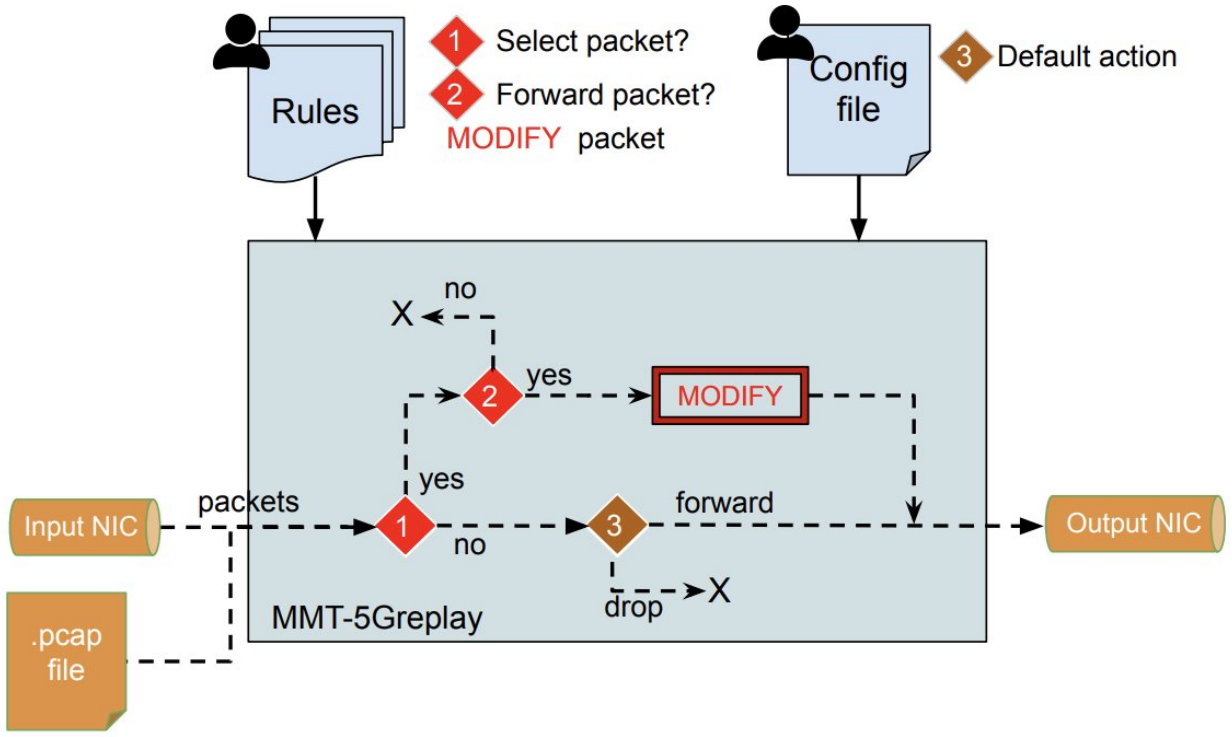
AI4CYBER – LLM based attack generation based on MITRE

- LLM-based automated generation of executable code of atomic TTPs from the MITRE ATT&CK model
- Implementation based on GPT 3.5
- Validation in AI4CYBER sandbox
  - A total of 565 distinct TTP codes have been automatically generated and executed
  - Windows and Linux OS
  - Success rate of 16%
    - Generated TTP codes that require major updates but still useful for a cyber security expert working on cyber security testing (35%)



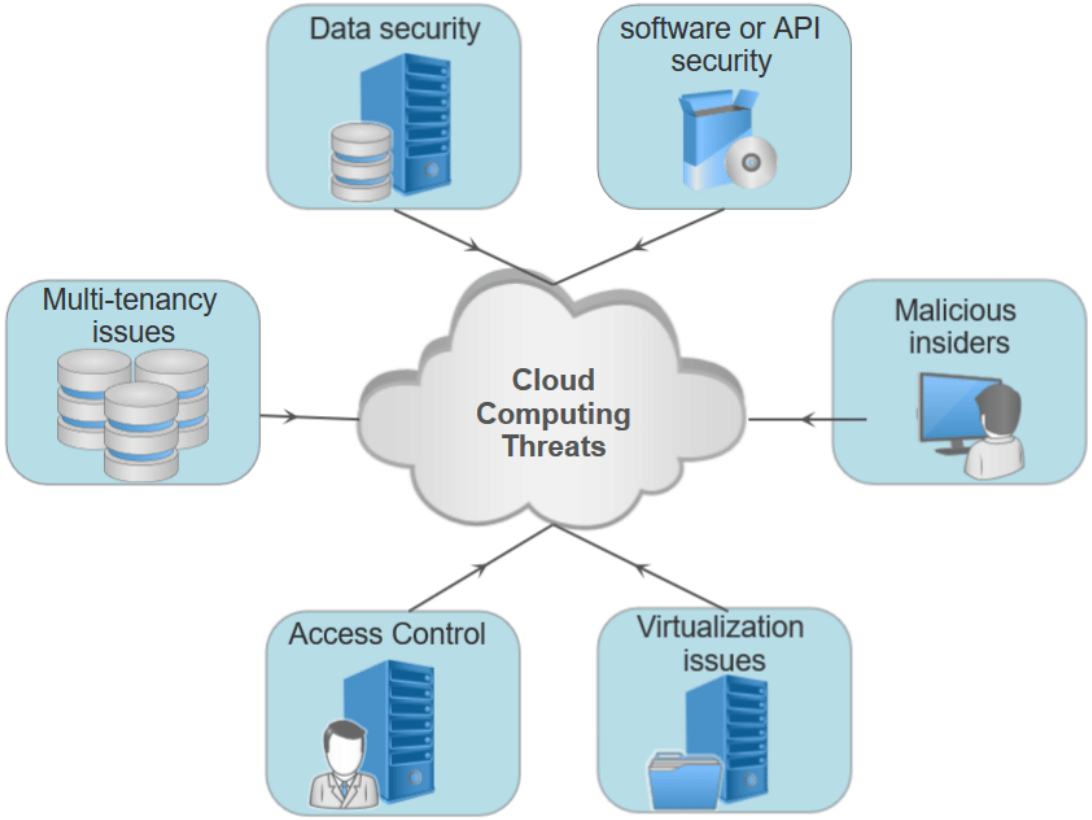
AI4CYBER – GAN-based Network Fuzzer

- Generative Adversarial Network
- The generator creates novel and potentially malicious input data
- the discriminator evaluates the responses of the target system to these inputs.
- The GAN learns to create inputs that are more likely to trigger vulnerabilities based on the feedback from the discriminator.
- If a novel vulnerability is discovered, it provides feedback to the GAN to refine the generation process further.



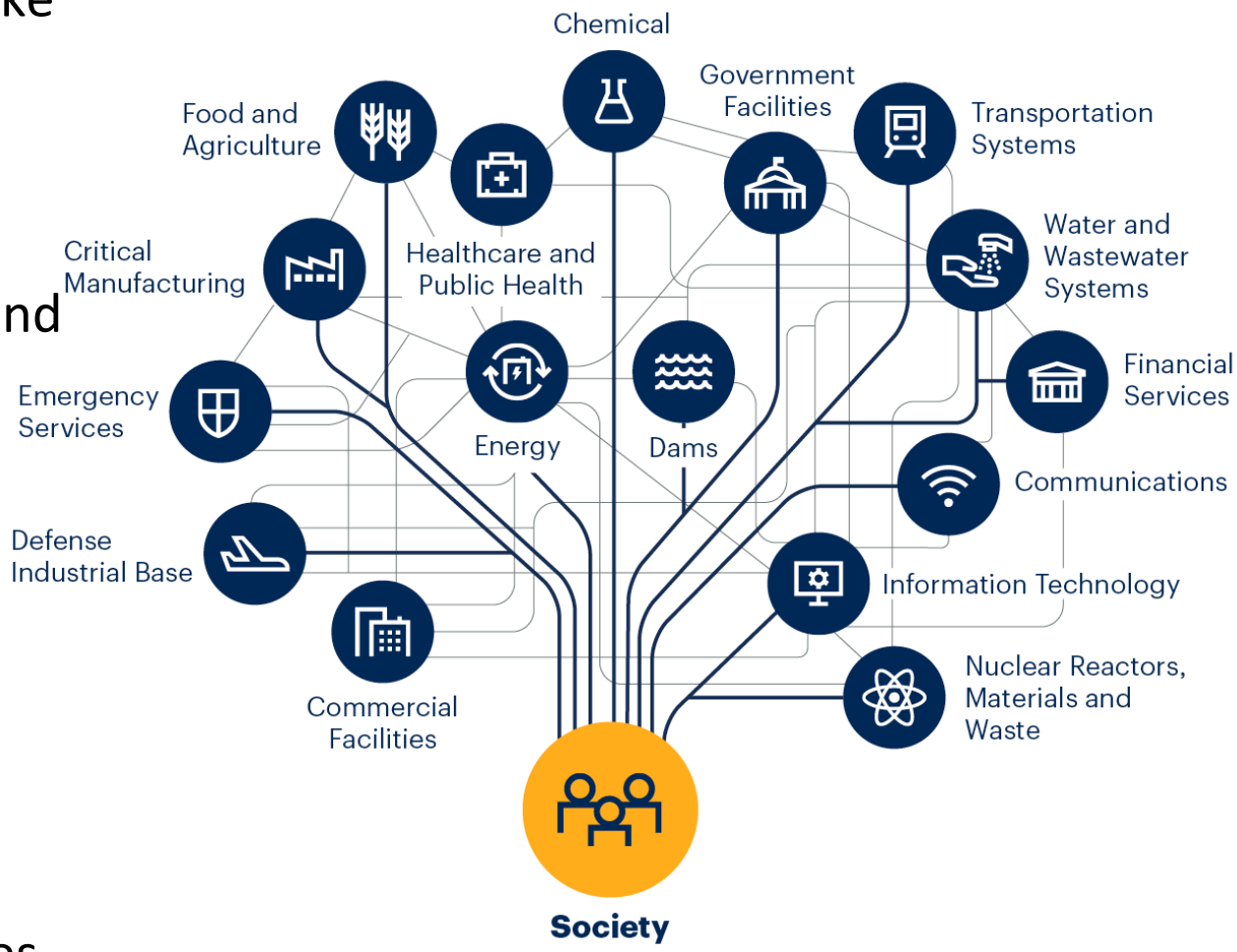
Cybersecurity in the Age of Cloud and Remote Work

- Cloud misconfigurations and shadow IT as major risks.
- Remote work blurs network perimeters, making endpoint security critical.
- Rise in insider threats and credential theft.



Critical Infrastructure and Supply Chain Under Threat

- Increased targeting of critical infrastructures like energy, transport, and healthcare sectors.
- Supply chain attacks (e.g., SolarWinds) show vulnerabilities beyond direct assets.
- Many industrial systems run legacy software and lack proper network isolation.
- The convergence of IT and OT increases the chance of cyber incidents having physical consequences.
- Nation-state actors: Well-funded, persistent threats are increasingly targeting strategic infrastructure.
- Frameworks like NIS2 push for stronger risk management and incident response capabilities.



Leveraging AI for SME Cybersecurity

“Best efforts are not enough, you have to know what to do.”

- **W. Edwards Deming**, American Economist, Statistician, and Quality Management Pioneer

SMEs

- ‼ Frequent cyber attack targets
- ‼ Limited Resources and Expertise
- ‼ Increasing threat levels from cyber threats leveraging AI

Enhance Defences

- ✓ Faster threat detection
- ✓ Proactive response automation
- ✓ Zero trust architectures
- ✓ Cybersecurity automation

With Efficient AI-Enhanced Tools

Build more resilient digital systems

Leveraging AI for SME Cybersecurity

- Threat Detection & Response
  - Re… …oring and anomaly detection.
  - Automat… …igate threats quickly.
- Endpoint Protection
  - AI-driven malware detection and pr…
  - Protects devices (laptops, mobiles, …s) from cyberattacks.
- Phishing & Fraud Preventi…
  - AI identifies an… …s and fraudulent activ…
  - Reduces human error in email security.
- Vulnerability Management
  - …I scans systems for vulnerabilities and prioritizes …s.
  - …elps SMEs f… …s.
- Managed S…
  - Outsourced AI-driven cybersecurity for SMEs with limited resources.
  - 24/7 monitoring and support.

Complexity

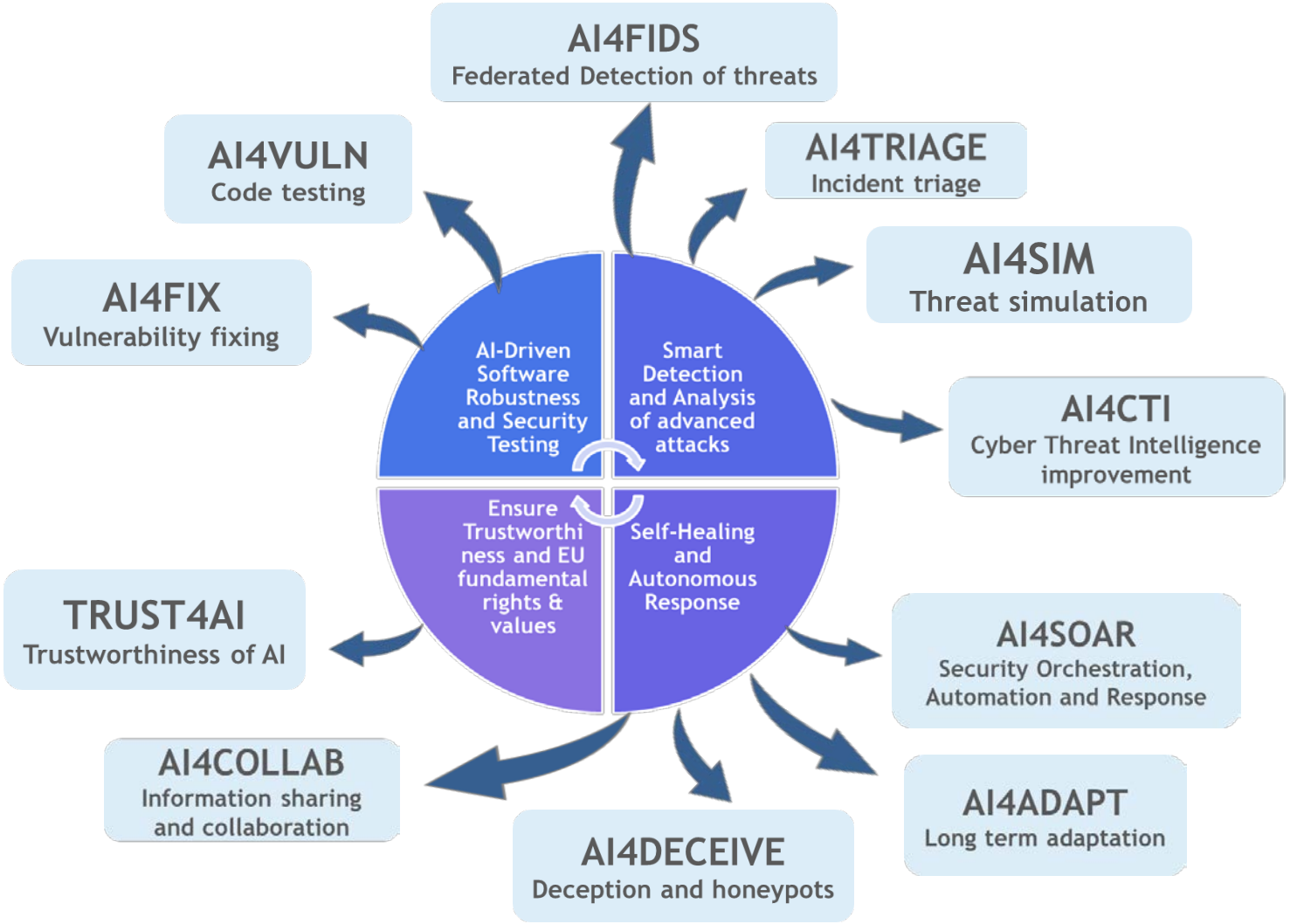
Budget, ressources

Data privacy

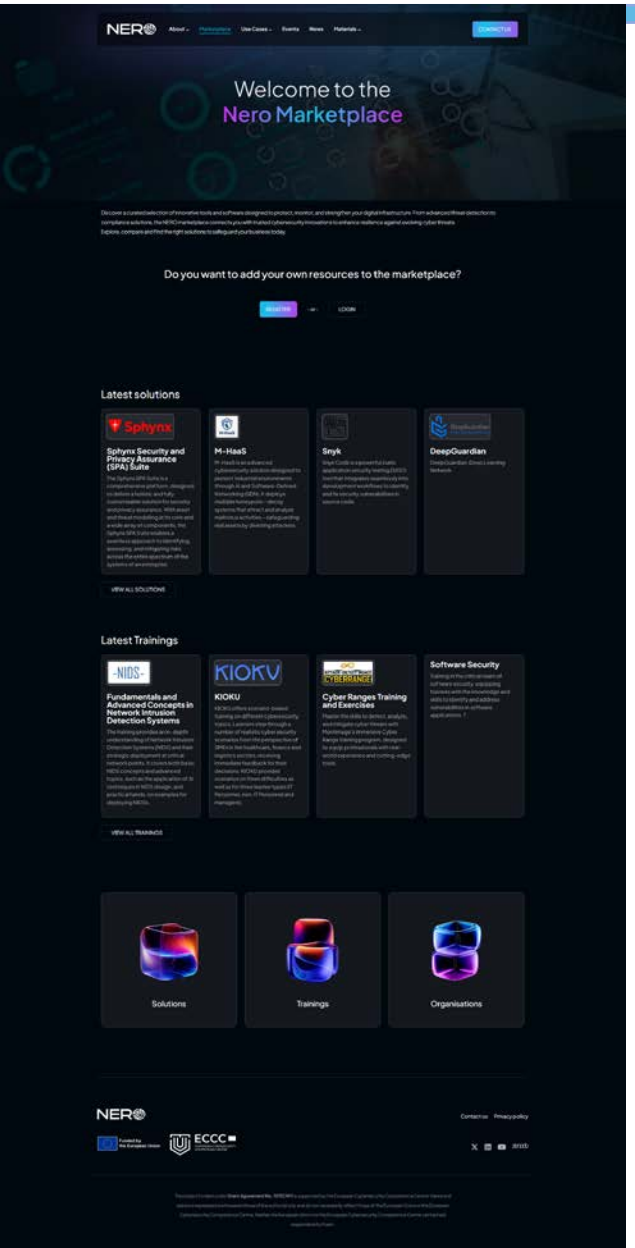
Skills

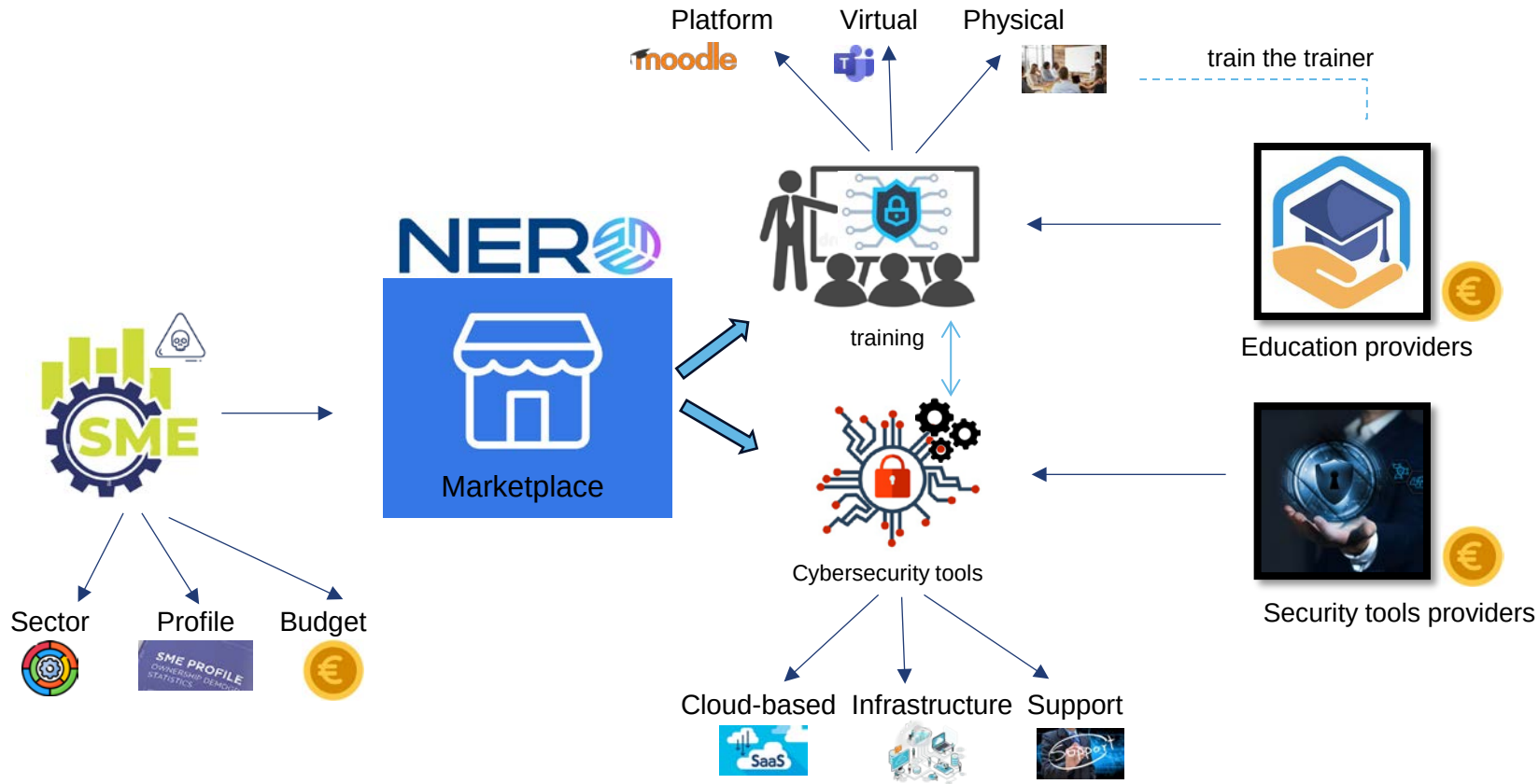
AI trustworthiness

Examples from AI4CYBER



The NERO marketplace





Conlusion

- Cyber threats are evolving rapidly, driven by AI, automation, and increasing digital interconnectivity.
- Ransomware and supply chain attacks remain among the top threats for all sectors.
- Critical infrastructure is highly vulnerable and must adopt resilience-by-design strategies.
- AI is both a threat and a defense tool — organizations must harness it wisely.
- Zero Trust and continuous monitoring are essential pillars of modern cybersecurity.
- Collaboration, awareness, and regulation are key to building a more secure digital future.

Thank you for your attention!

MONTIMAGE

Wissam Mallouli

wissam.Mallouli@montimage.eu

www.montimage.eu

Co-funded by the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.