EUROPEAN UNION AGENCY
FOR CYBERSECURITY

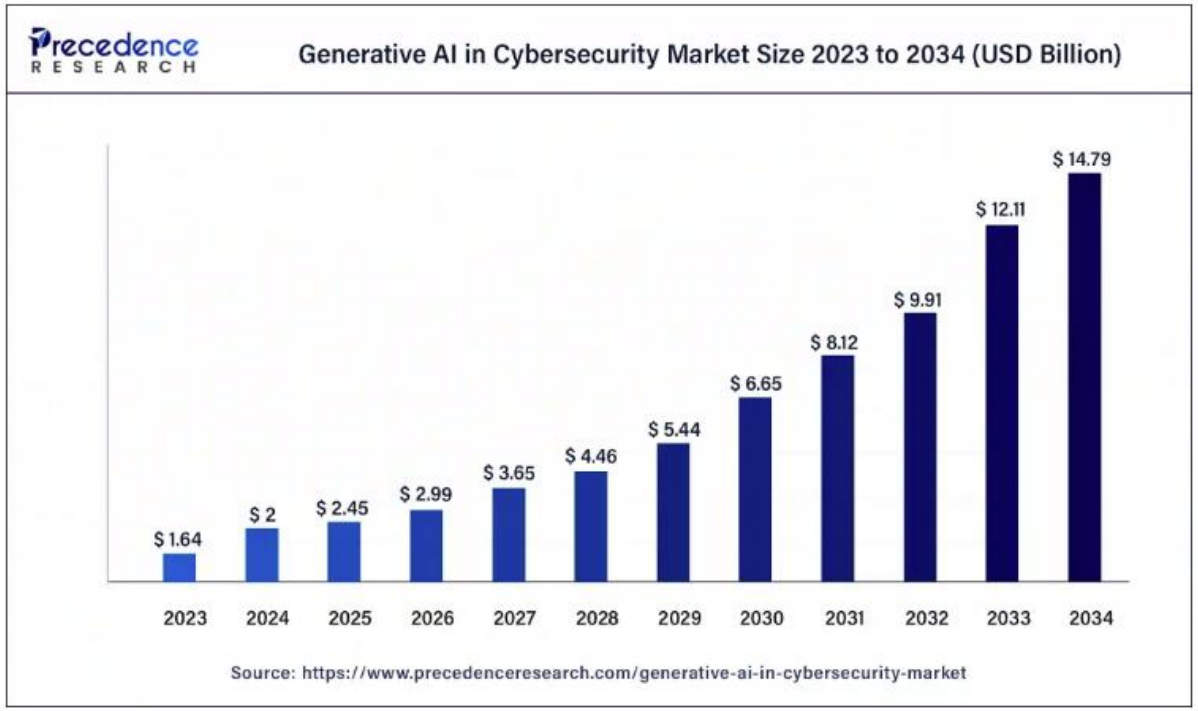
# CYBERSECURITY SKILLS IN THE AGE OF AI

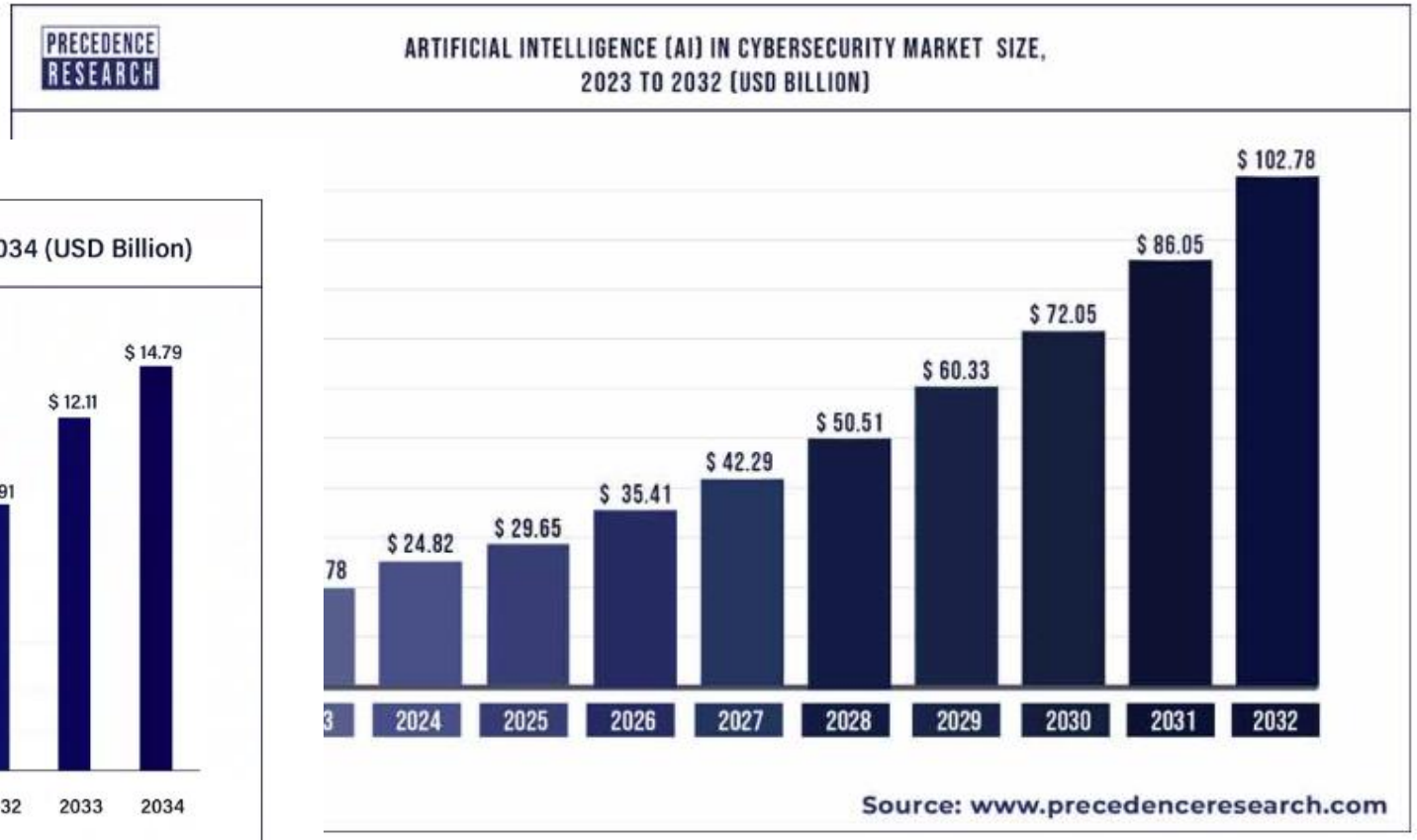
Isabel Praça, Etienne Capgras - presenters
Jutta Breyer, Sarka Pekarova, Athanasios Vasileios Grammatopoulos,
Edmundas Piesarskas, Jon France, Fabio Di Franco

28 09 2024

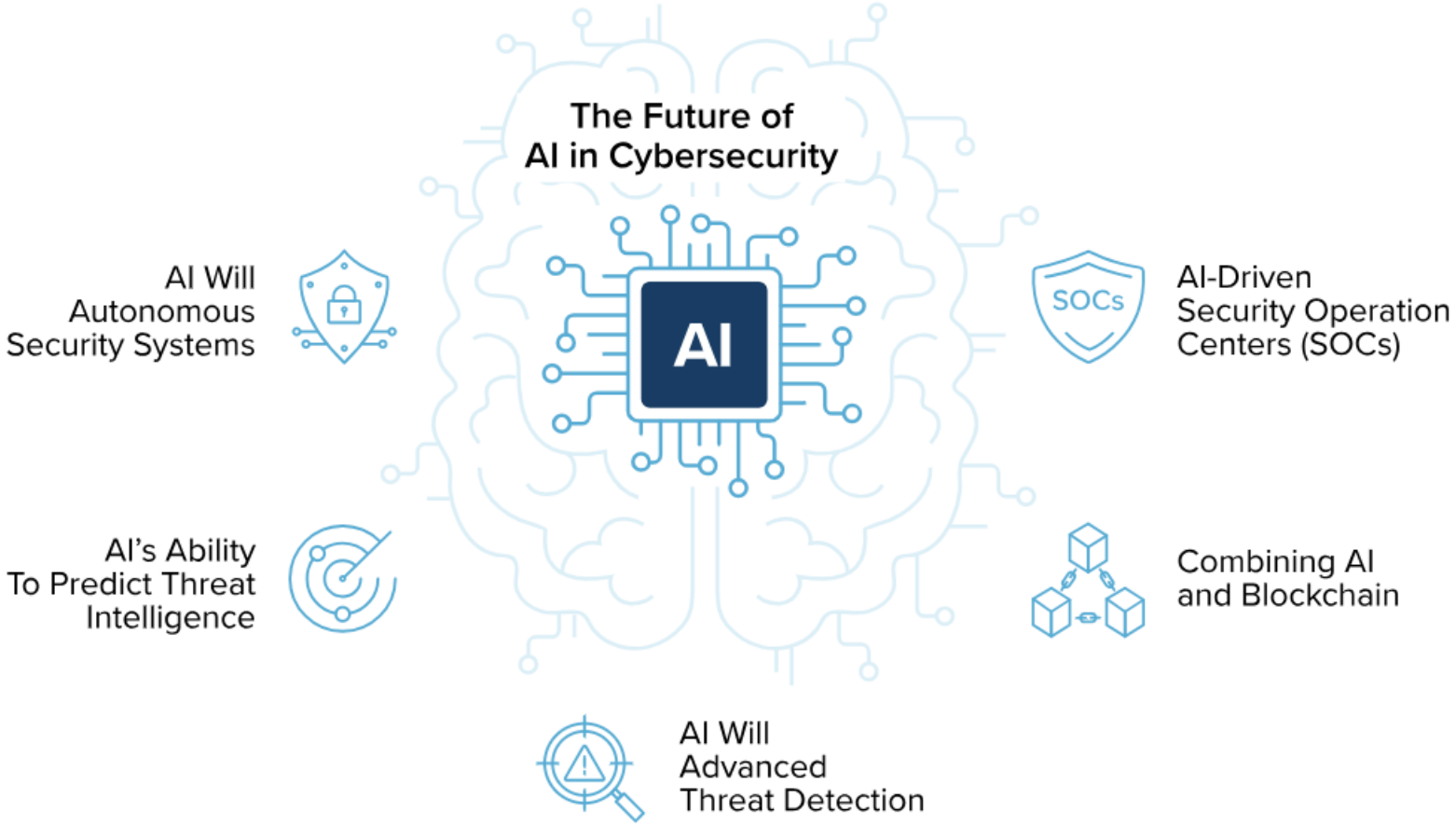
EUROPEAN
**CYBERSECURITY**
**SKILLS** FRAMEWORK

# AI GROWTH...


Precedence RESEARCH
Generative AI in Cybersecurity Market Size 2023 to 2034 (USD Billion)
$ 1.64
$ 2
$ 2.45
$ 2.99
$ 3.65
$ 4.46
$ 5.44
$ 6.65
$ 8.12
$ 9.91
$ 12.11
$ 14.79
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
Source: https://www.precedenceresearch.com/generative-ai-in-cybersecurity-market

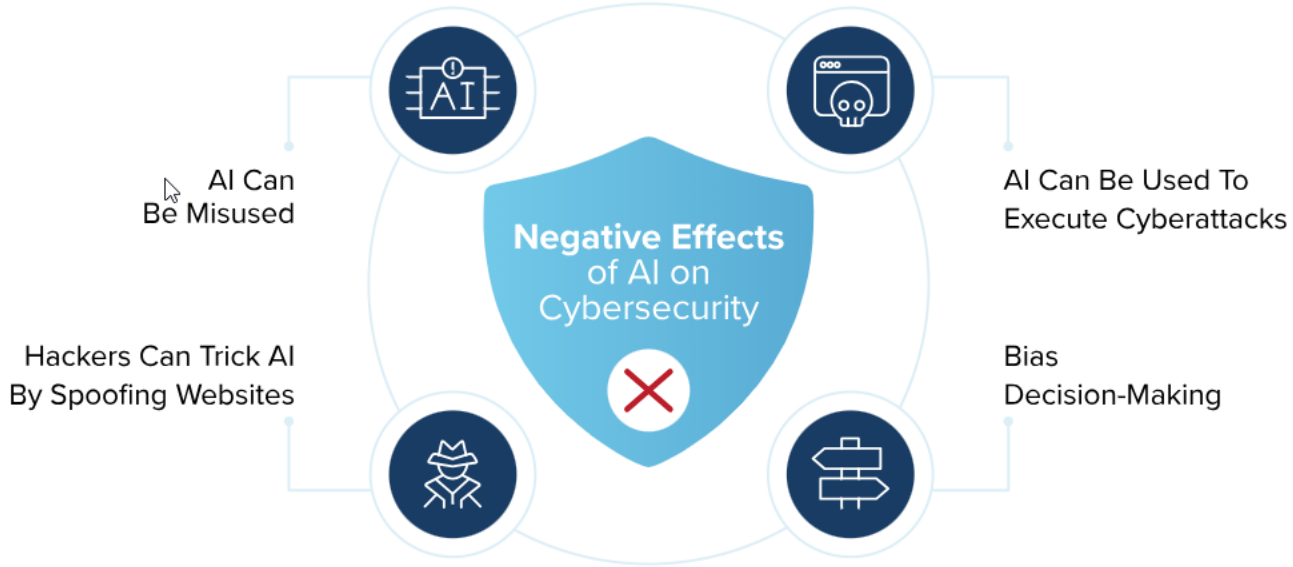

PRECEDENCE RESEARCH
ARTIFICIAL INTELLIGENCE (AI) IN CYBERSECURITY MARKET SIZE, 2023 TO 2032 (USD BILLION)
78
$ 24.82
$ 29.65
$ 35.41
$ 42.29
$ 50.51
$ 60.33
$ 72.05
$ 86.05
$ 102.78
3
2024
2025
2026
2027
2028
2029
2030
2031
2032
Source: www.precedenceresearch.com

# AI4CYBER...

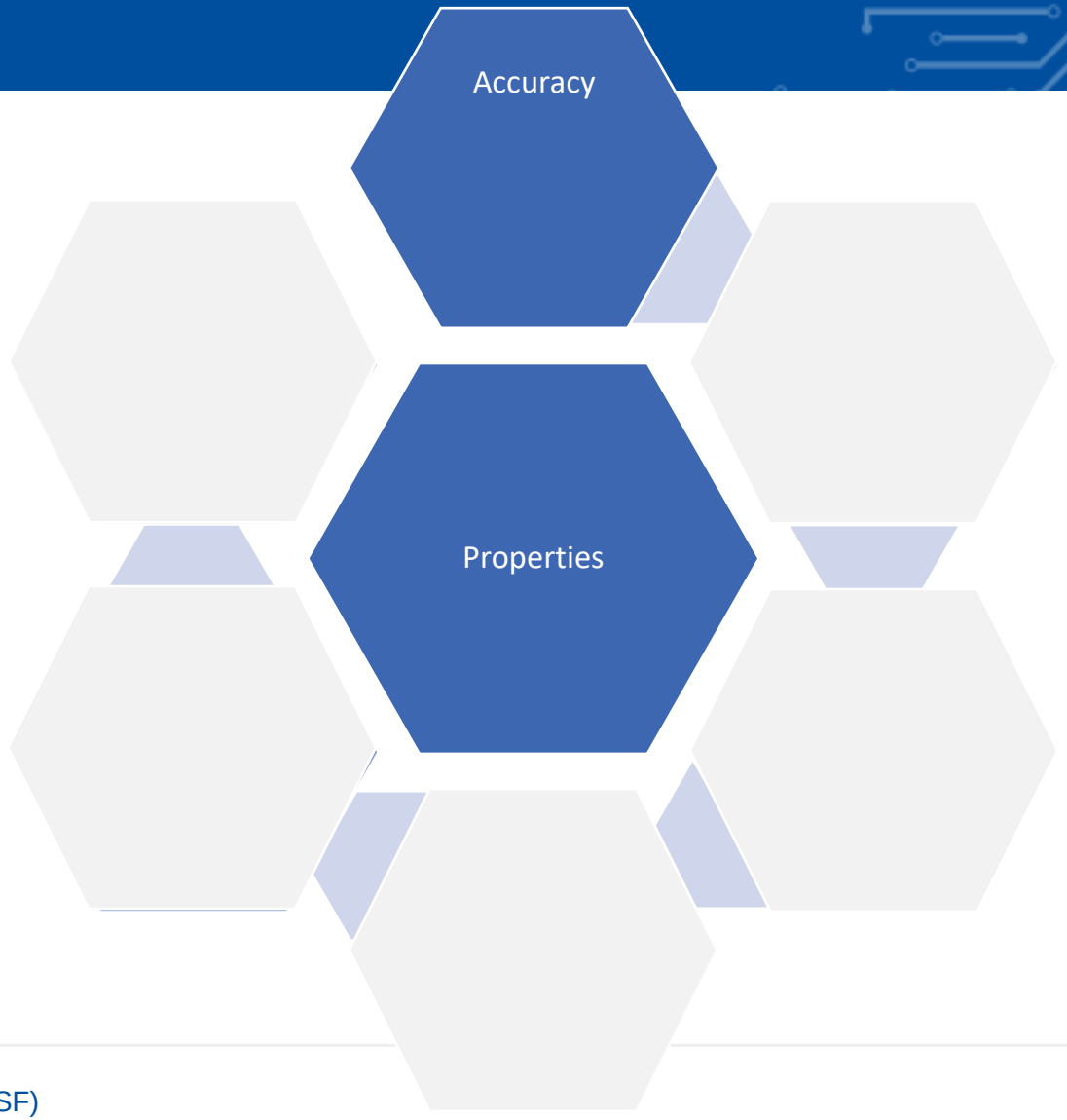

The Future of
AI in Cybersecurity
AI
AI Will
Autonomous
Security Systems
SOCs
AI-Driven
Security Operation
Centers (SOCs)
AI's Ability
To Predict Threat
Intelligence
Combining AI
and Blockchain
AI Will
Advanced
Threat Detection

# A NEW WEAPON...

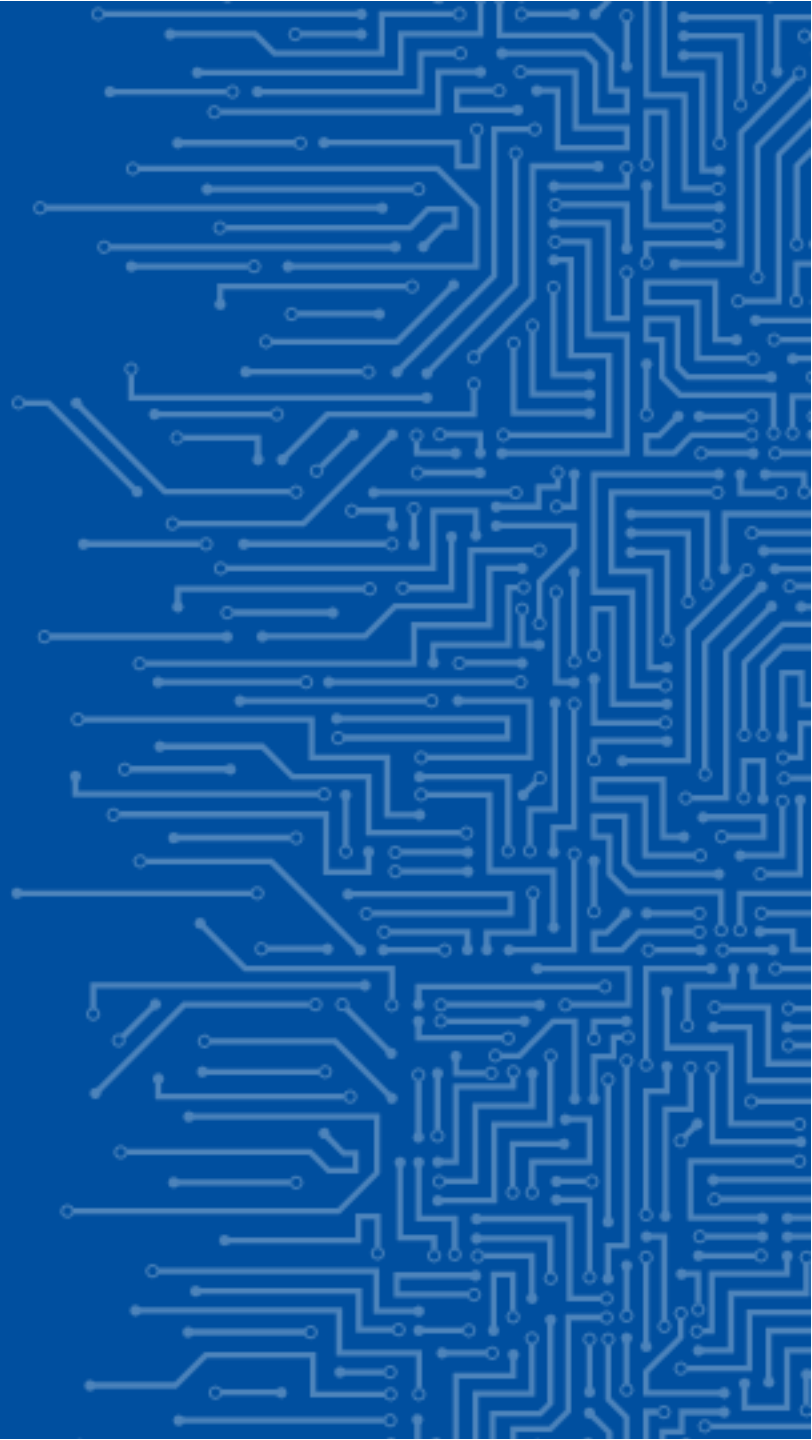
## Negative Effects of AI on Cybersecurity



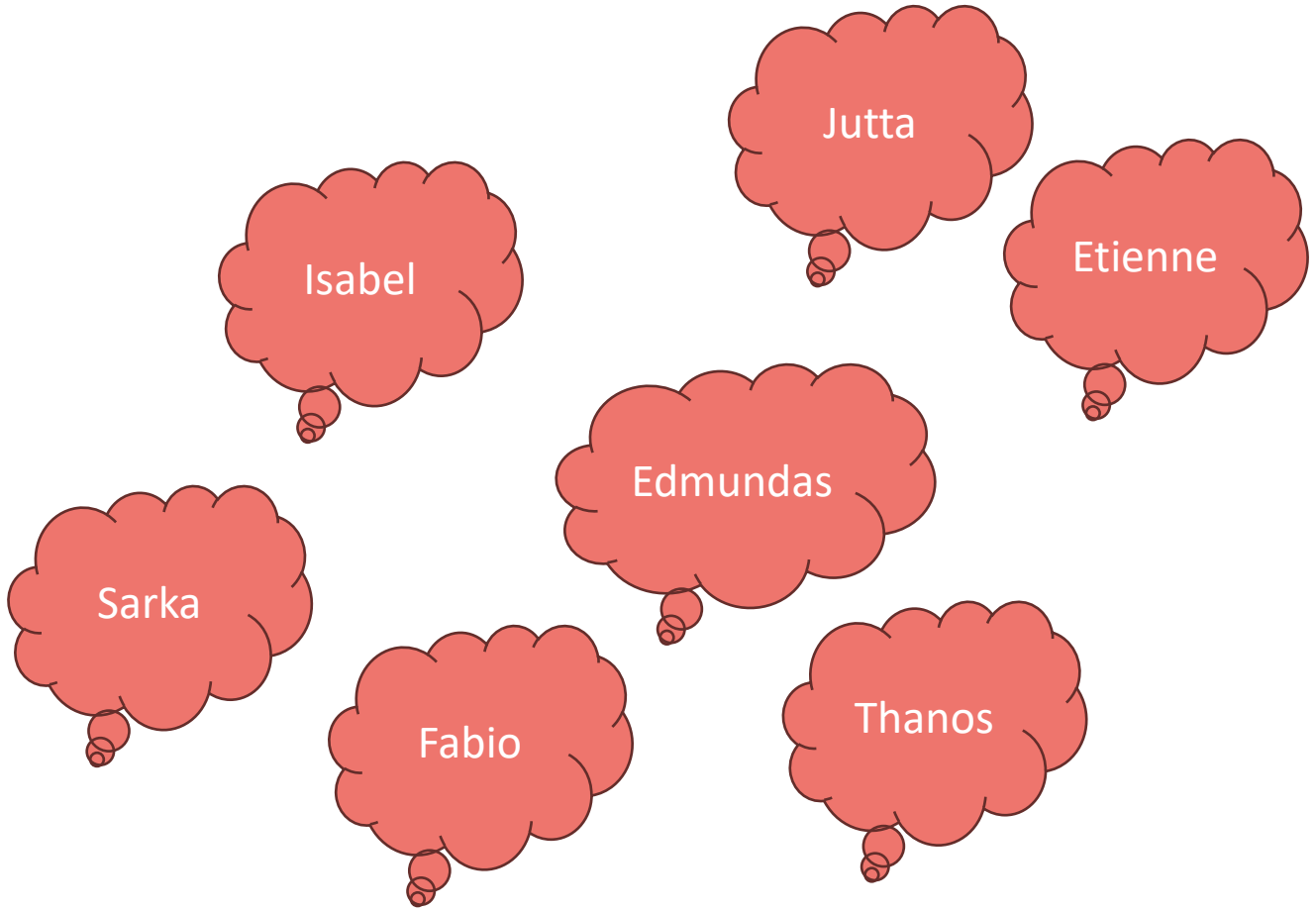
# AI PROPERTIES



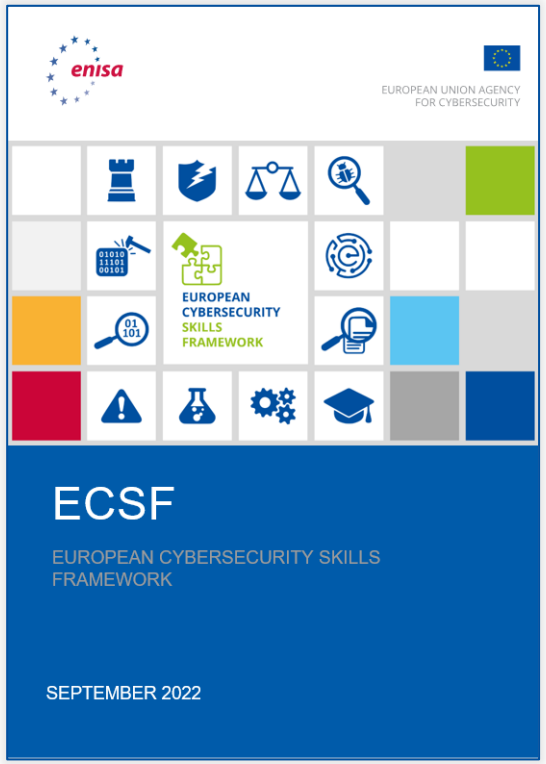
# HOW TO CONTEXTUALISE AND UTILISE THE ECSF'S FRAMEWORK TO THE AI FIELD?



# HARD BRAINSTORMING...



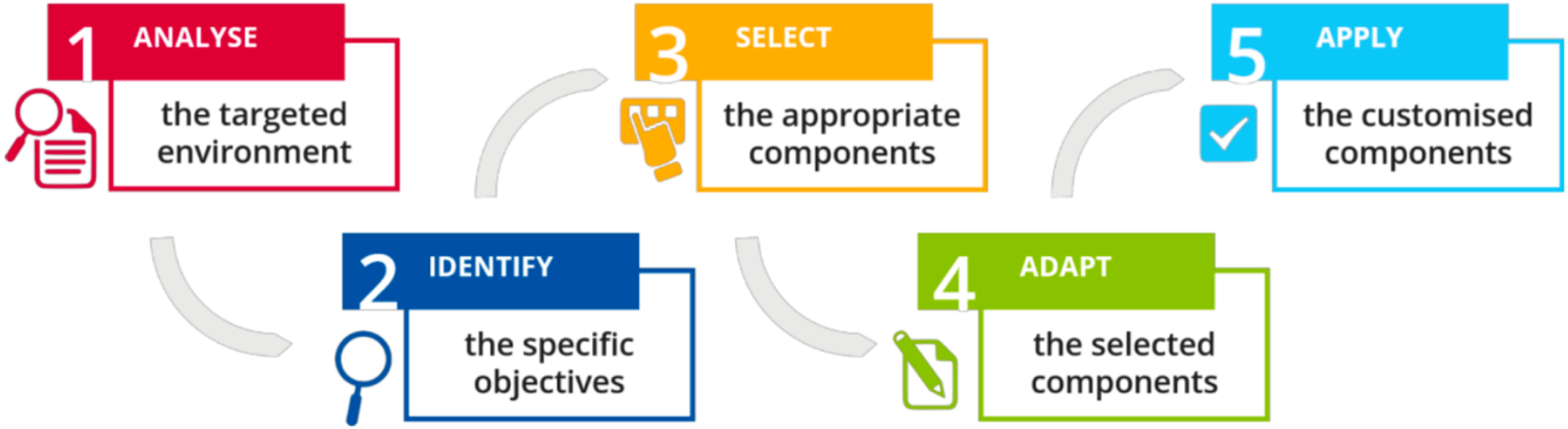
# CONSIDERING





# METHODOLOGY

## APPLYING THE ECSF 5-STEP GUIDE

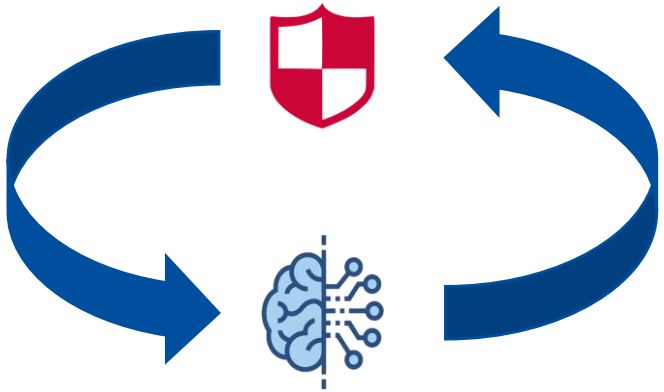


# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


Considering cybersecurity and AI in both ways

Every ECSF profile is concerned by AI, in one way or another

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK



AI impacts cybersecurity professions:

- As a subject of study
- As a rising threat vector
- As an opportunity for enhancement

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


**Every ECSF profile is concerned by AI, in one way or another**


Cyber Threat Intelligence Specialist


Cybersecurity Risk Manager


Cybersecurity Researcher

They analyse AI-related risks, monitor emerging AI threats, and research AI vulnerabilities to stay ahead of potential security challenges.

Penetration Tester

Digital Forensics Investigator


Cyber Incident Responder

By integrating AI, they can identify vulnerabilities more effectively, analyse forensic data with greater efficiency, and respond to incidents faster and more accurately, significantly improving their overall capabilities and performance.

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


**Every ECSF profile is concerned by AI, in one way or another**

Cybersecurity Architect

Cybersecurity Implementer

Cybersecurity Educator

Need a solid understanding of how to design, implement, and teach AI-integrated systems securely.

Chief Information Security Officer (CISO)

Cybersecurity Auditor

Cyber Legal, Policy and Compliance Officer

Are called upon to take a stance on AI, developing policies, auditing AI systems for compliance and security, and ensuring that AI deployments align with legal and ethical standards.

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


Splitting the problem into two main questions:

1) How do we contextualise the ECSF for AI?

2) Are the ECSF profiles influenced by AI-related technologies, and if so, how?

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


Focusing on one profile before extending:

1) On the ECSF side: focus on the Penetration tester profile

2) On the AI side: use of the ENISA's Multilayer framework

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


## The landscape of available resources is vast and rapidly evolving

*Model inversion and extraction*

*Application of AI/ML algorithms*

*AI regulation and ethics*

*TrustedAI ART*

*MLSecOps Top 10*

*Foolbox*

*Adversarial Machine Learning*

*AI/ML fundamentals*

*AI-based automation*

*AI vulnerabilities and testing*

*AI-related certifications*

*EU AI Act*

*MITRE ATLAS*

*Pralab secml*

*Data poisoning*

*Application of AI-based tools*

*OWASP Top 10 for LLM*

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


## ENISA's Multilayer Framework for Good Cybersecurity Practices for AI


- **Legal aspect** – defining the cybersecurity legal and regulatory needs of a specific sector/domain
- **Security aspect** – analysing the various sectors or domain-specific assets that need to be protected
- **Risk aspect** – covering the specific types of risks associated with the analysed domain
- **Tools aspect** – ensuring the inclusion of tools used in the sector/domain in question
- **Threat aspect** – taking into account sector or domain-specific threats and threat actors

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN


## Contextualized version for the Penetration Tester profile

| | Description |
|---|---|
| **Legal aspect** | **Compliance Checks**<br>Ensure AI systems comply with AI-related laws like the EU AI Act and GDPR. Document compliance issues and provide detailed reports on legal vulnerabilities. |
| **Security aspect** | **Vulnerability Assessment**<br>Secure AI assets and systems, identifying and mitigating vulnerabilities in datasets, algorithms, and models throughout their lifecycle. |
| **Risk aspect** | **Risk Evaluation**<br>Contribute to risk evaluation for audited AI-related systems, develop mitigation recommendations, and continuously monitor attack opportunities. |
| **Tools aspect** | **Tool Proficiency**<br>Use AI-specific tools like Foolbox, A2PM and ART to test AI models. Ensure tool usage aligns with organizational policies and contributes to the development of custom tools. |
| **Threat aspect** | **Threat Mitigation**<br>Identify AI-specific threats such as adversarial attacks, model inversion, and data poisoning. Implement defensive measures and conduct realistic threat scenarios to test AI robustness. |

# METHODOLOGY
# ECSF FIVE-STEP GUIDE APPLIED TO THE AI DOMAIN

**4 ADAPT**

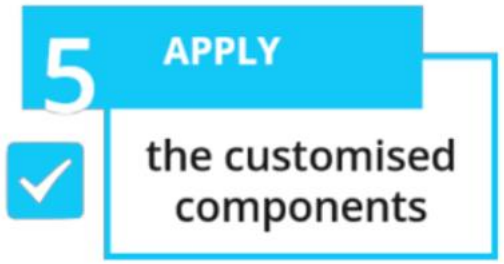
the selected components

| ECSF Penetration Tester | | Penetration Tester specialising in AI |
|---|---|---|
| [Summary statement] Assesses the effectiveness of security controls, reveals and utilises cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors. | → | Assesses the effectiveness of security controls ***protecting AI-related systems***, reveals and utilises cybersecurity ***AI-related* vulnerabilities**, assessing their criticality if exploited by threat actors ***and uses AI-enabled tools or methodologies for penetration testing engagements***. |
| [Skill] Perform social engineering | → | Perform social engineering *using* ***generative AI*** |
| [Knowledge] Cybersecurity recommendations and best practices | → | ***AI-related systems security and trustworthiness*** recommendations and best practices |

**Providing clarity regarding which tasks, skills, and knowledge areas are impacted by AI, and to what degree: AI-related systems, AI-enabled tools, as a subject of study, as a potential opportunity**

# HOW TO MAKE USE OF THE REPORT?

# EXAMPLE USE CASES




**For recruitment team in organisations**
Clearly outline job requirements and select candidates who not only have ML/AI expertise but are also equipped with relevant cybersecurity skills

**For learning programme providers**
Pinpoint exactly where AI-specific content is needed and how to adapt the curriculum accordingly

**For Policy makers**
Critical guide to understanding the cybersecurity needs related to AI adoption across various sectors

**Research**
ECSF systematizes in a thorough way the tasks, knowledge, and skills a researcher in the field of cybersecurity needs to have.

# Stay tuned!

# THANK YOU FOR YOUR ATTENTION

**Stay tuned! A cookbook will be launched soon**

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

**European Union Agency for Cybersecurity**
Agamemnonos 14, Chalandri 15231,
Attiki, Greece

- EuSkills@enisa.europa.eu
- www.enisa.europa.eu