# ETSI launches new specification to enhance AI cybersecurity worldwide



ETSI has introduced a new technical specification designed to bolster the cybersecurity of Artificial Intelligence (AI) systems in response to the rising tide of digital threats. Released by the European Telecommunications Standards Institute (ETSI), the document, titled 'ETSI TS 104 223 - Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems,' outlines a comprehensive set of requirements to safeguard end users and offer practical guidance for AI security.

The specification adopts a lifecycle approach to AI security, structured around 13 core principles that expand into 72 trackable requirements spanning five distinct lifecycle phases. This framework aims to elevate security practices across all participants involved in AI system development and deployment, including developers, vendors, integrators, and operators.

Among the advantages of this approach is the establishment of transparent, high-level security principles coupled with tangible measures to protect AI systems. The requirements are intended to serve as a foundational defence mechanism in the face of rapidly evolving cyber threats targeting AI.

ETSI highlights that AI technology presents security challenges distinct from those associated with traditional software. Specific risks addressed include data poisoning, model obfuscation, indirect prompt injection, and complex data management issues. In response, the specification blends established cybersecurity methodologies with contemporary AI security research and newly developed guidance tailored to these unique threats.

The development of the specification was undertaken by ETSI's Technical Committee on Securing Artificial Intelligence (SAI), comprised of representatives from international organisations, government bodies, and cybersecurity experts. ETSI emphasises that this interdisciplinary and collaborative process has produced globally pertinent requirements suitable for deployment in a variety of contexts.

Alongside the primary specification document, ETSI has committed to publishing an implementation guide intended to assist Small and Medium-sized Enterprises (SMEs) and other stakeholders. This supporting guide will include case studies from diverse deployment environments to facilitate adherence to the baseline security standards specified by TS 104 223.

Scott Cadzow, Chair of ETSI's Technical Committee for Securing Artificial Intelligence, said in an interview with SecurityBrief UK: "In an era where cyber threats are growing in both volume and sophistication and negatively impacting organisations of every kind, it is vital that the design, development, deployment, and operation and maintenance of AI models is protected from malicious and unwanted inference. Security must be a core requirement, not just in the development phase, but throughout the lifecycle of the system. This new specification will help do just that – not only in Europe, but around the world."

He further noted, "This publication is a global first in setting a clear baseline for securing AI and sets TC SAI on the path to giving trust in the security of AI for all its stakeholders."

ETSI's initiative seeks to raise AI security standards internationally while providing accessible and actionable guidance to organisations of varying sizes. The new specification and forthcoming implementation guide aim to act as reference points for the AI industry amid ongoing concerns about digital safety and trust.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.etsi.org/newsroom/press-releases/2521-etsi-technical-specification-sets-international-benchmark-for-securing-artificial-intelligence> - This page confirms the release of the ETSI TS 104 223 specification titled 'Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems,' describing its lifecycle approach with 13 core principles and 72 trackable requirements across five lifecycle phases to improve AI security. It also highlights the specification's focus on mitigating unique AI threats such as data poisoning and model obfuscation, developed by the ETSI Technical Committee on Securing Artificial Intelligence with international participation.
2. <https://www.etsi.org/deliver/etsi_ts/104200_104299/104223/01.01.01_60/ts_104223v010101p.pdf> - This PDF is the full ETSI TS 104 223 specification document itself, which provides detailed baseline cybersecurity requirements for AI models and systems, structured by five lifecycle phases (design, development, deployment, maintenance, and end of life) and defines the scope and principles referenced in the article.
3. <https://securitybrief.co.uk/story/etsi-sets-global-baseline-for-ai-cyber-security-with-new-standard> - This article reports on ETSI's new technical specification establishing a global baseline for AI cybersecurity, supporting claims about the specification's goal to protect users and guide stakeholders including developers, vendors, integrators, and operators with actionable AI security measures.
4. <https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice> - The UK Government's AI Cyber Security Code of Practice outlines baseline cybersecurity principles for AI systems, which served as a foundational input that influenced the ETSI TS 104 223 specification, corroborating the article's mention of collaborative and evolving AI security standards.
5. <https://www.hunton.com/privacy-and-information-security-law/uk-publishes-ai-cyber-security-code-of-practice-and-implementation-guide> - This page explains that the UK Code of Practice and Implementation Guide for AI cybersecurity is intended to support stakeholders including SMEs, underpinning the ETSI specification and its upcoming implementation guide, which aligns with the article's note about guidance to assist SMEs and diverse deployment environments.
6. <https://www.etsi.org/committee/1459-sai> - This webpage about ETSI's Technical Committee on Securing Artificial Intelligence (SAI) confirms the interdisciplinary composition of the committee, including international organizations, government bodies, and cybersecurity experts, supporting the article's assertion about the collaborative development process producing globally relevant AI security requirements.
7. <https://news.google.com/rss/articles/CBMioAFBVV95cUxQUE1RX3BRRThNelVrTTQwSG9mWG5Oc20wOGFKVmpKVkpkZXNPMXFFQ2FhdVkxaDVRcGVOLTlFcTBEbkhoMnZ0V21yOUtiWGlJV2Y2R2I0Wnh2UUF0OVZQaUhZYmp4Qk5mbU1qanVuWXNQWmhmaEd0emdsSmVhTlZVWkdJUVNXQ3VDTU10UFZfdTNjaHhvdi1SQUVSaU5zSGJD?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data