ETSI TR 104 030 V1.1.1 (2025-03)

Securing Artificial Intelligence (SAI);
Critical Security Controls for Effective Cyber Defence;
Artificial Intelligence Sector

Reference
DTR/SAI-002

Keywords
AI, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Securing Artificial Intelligence (SAI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The rapid, ubiquitous global proliferation of networked Artificial Intelligence (AI) systems and services gives rise to associated risks. The Critical Security Controls address the general practices that most enterprises should take to secure their systems. The present document guidance emerged from collaborations among experts in the AI sector and intended to apply the security best practices found in the latest version of the Critical Security Controls to AI environments. However, because networked AI systems have the same properties and functions as computational systems generally, a consensus has emerged that the existing Critical Security Controls and implementation tools apply in their present form.

Introduction

Artificial Intelligence systems are functionally indistinguishable from other networked computer-based systems. Although significant concerns exist as to computation models employed, trust in the veracity of ingested information, and societal use, the applicable Critical Security Controls and implementation tools appear to apply unchanged. Published AI guidelines and projects [i.1], [i.3], [i.4], [i.5] to [i.22] all focus on secure design, secure development, secure deployment, potential misuse, and secure operation and maintenance, but the basic security controls remain the same.

1 Scope

The present document applies the latest version of the Critical Security Controls [i.5] and risk measurement tools [i.6] for effective risk control and enhanced resilience of the AI sector together with other industry AI controls.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 104 223: "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".

NOTE: The following reference is not publicly available at the date of publication and may be unavailable for an extended period of time.

[i.2] European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).

[i.3] "AI Cyber Security Code of Practice", UK DSIT.

[i.4] "Guidelines for secure AI system development", UK NCSC.

[i.5] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.6] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.7] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.8] ETSI TR 103 959: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Cloud Sector".

[i.9] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.10] MITRE: "Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS™)".

[i.11] Massachusetts Institute of Technology (MIT): "AI Risk Repository".

[i.12] OpenSSF: "AI/ML Security WG".

[i.13] OWASP: "AI Exchange".

[i.14] Cloud Security Alliance®: "AI Controls Matrix".

[i.15] Cloud Security Alliance®: "AI Model Risk Management Framework".

[i.16] Cloud Security Alliance®: "Large Language Model (LLM) Threats Taxonomy".

[i.17] NIST AI 100-1: "Artificial Intelligence Risk Management Framework (AI RMF 1.0)".

[i.18] NIST: "Artificial Intelligence Risk Management Framework Playbook".

[i.19] NIST AI 600-1: "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile".

[i.20] NIST AI 800-1 2pd: "Managing Misuse Risk for Dual-Use Foundational Models".

[i.21] CEN/CLC/JTC 21, WI JT021029: "Artificial intelligence — Cybersecurity specifications for AI Systems".

[i.22] Google: "Secure AI Framework (SAIF)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
CSA	Cloud Security Alliance®
LLM	Large Language Model
SAIF	Secure AI Framework

4 Applying the Critical Security Controls for effective risk control and enhanced resilience of the AI sector

The rapid, ubiquitous global proliferation of networked Artificial Intelligence (AI) systems and services gives rise to associated risks. The Critical Security Controls address the general practices that most enterprises should take to secure their systems. The present document guidance emerged from collaborations among experts in the AI sector and intended to apply the security best practices found in the latest version of the Critical Security Controls to AI environments. However, because networked AI systems have the same properties and functions as computational systems generally, a consensus has emerged that the existing Critical Security Controls and implementation tools apply in their present form.

The Critical Security Controls, facilitation methods and implementation guidelines apply in total ([i.5], [i.6], [i.7], [i.8] and [i.9]).

Annex A: Bibliography

- Lukas Lange, et al, AnnoCTR: "A Dataset for Detecting and Linking Entities, Tactics, and Techniques in Cyber Threat Reports", 11 April 2024.
- Cloud Security Alliance®: "Confronting Shadow Access Risks: Considerations for Zero Trust and Artificial Intelligence Deployments", 6 May 2024.
- Cloud Security Alliance®: "AI Organizational Responsibilities - Core Security Responsibilities", 5 May 2024.
- Cloud Security Alliance®: "AI Resilience: A Revolutionary Benchmarking Model for AI Safety", 5 May 2024.
- Cloud Security Alliance®: "Principles to Practice: Responsible AI in a Dynamic Regulatory Environment", 5 May 2024.
- Cloud Security Alliance®: "The State of AI and Security Survey Report", 2 April 2024.
- Cloud Security Alliance®: "Security Implications of ChatGPT", 9 August 2023.
- Cloud Security Alliance®: "Artificial Intelligence in Healthcare", 6 January 2022.

History

Document history		
V1.1.1	March 2025	Publication