



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for Security information and event
management (SIEM) systems**

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-0010

KeywordsCRA, Cybersecurity, SIEM

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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	11
Foreword.....	11
Modal verbs terminology.....	12
Introduction	12
1 Scope	13
2 References	13
2.1 Normative references	13
2.2 Informative references.....	13
3 Definition of terms, symbols and abbreviations.....	14
3.1 Terms.....	14
3.2 Symbols.....	15
3.3 Abbreviations	15
4 Product context.....	15
4.0 Introduction	15
4.1 Product Functions.....	16
4.2 Product Architecture.....	16
4.3 Operational Environment	16
4.3.1 General description.....	16
4.3.2 Physical/Hardware environment.....	17
4.3.3 Logical/Software environment.....	17
4.3.4 Connectivity aspects	17
4.4 Distribution of Security Functions	17
4.4.1 General.....	17
4.4.2 Security functions provided by the product	17
4.4.3 Security functions provided to the product.....	18
4.5 Users.....	18
4.6 Use Cases	18
4.6.1 Overview	18
4.6.2 Guidance.....	18
4.6.3 UC-1-RESEARCH: Research SIEM	18
4.6.4 UC-2-HOME: Home SIEM	19
4.6.5 UC-3-FLEET: Fleet monitoring	19
4.6.6 UC-4-IOT: IoT monitoring.....	19
5 Technical requirements for products.....	20
5.1 Introduction	20
5.1.1 Applicability of the requirements	20
5.1.2 Applicability of Annex K	20
5.1.3 Applicability of Annex R.....	20
5.2 Appropriate level of cybersecurity	20
5.2.1 Overview	20
5.2.2 REQ-ALC-01.....	20
5.2.2.1 Requirement	20
5.2.2.2 Applicability.....	20
5.2.3 REQ-ALC-02.....	21
5.2.3.1 Requirement	21
5.2.3.2 Applicability.....	21
5.2.4 Mapping of requirements to use cases	21
5.3 No known exploitable vulnerabilities.....	21
5.3.1 Overview	21
5.3.2 REQ-KEV-01	21
5.3.2.1 Requirement	21
5.3.2.2 Applicability.....	21
5.3.2.3 Use-case applicability	21

5.3.3	Mapping of requirements to use cases	22
5.4	Secure by default configuration.....	22
5.4.1	Overview	22
5.4.2	Requirements	22
5.5	Security updates	22
5.5.1	Overview	22
5.5.2	REQ-SU-01.....	22
5.5.2.1	Requirement	22
5.5.2.2	Applicability.....	22
5.5.3	Mapping of requirements to use cases	23
5.6	Authentication and access control	23
5.6.1	Overview	23
5.6.2	REQ-AAC-01	23
5.6.2.1	Requirement	23
5.6.2.2	Applicability.....	23
5.6.3	Mapping of requirements to use cases	23
5.7	Confidentiality protection.....	23
5.7.1	Overview	23
5.7.2	REQ-CON-01	23
5.7.2.1	Requirement	23
5.7.2.2	Applicability.....	23
5.7.3	REQ-CON-02	24
5.7.3.1	Requirement	24
5.7.3.2	Applicability.....	24
5.7.4	REQ-CON-03	24
5.7.4.1	Requirement	24
5.7.4.2	Applicability.....	24
5.7.5	Mapping of requirements to use cases	24
5.8	Integrity protection	24
5.8.1	Overview	24
5.8.2	REQ-INT-01	24
5.8.2.1	Requirement	24
5.8.2.2	Applicability.....	25
5.8.3	REQ-INT-02	25
5.8.3.1	Requirement	25
5.8.3.2	Applicability.....	25
5.8.4	REQ-INT-03	25
5.8.4.1	Requirement	25
5.8.4.2	Applicability.....	25
5.8.5	Mapping of requirements to use cases	25
5.9	Data minimisation	25
5.9.1	Overview	25
5.9.2	REQ-DM-01	26
5.9.2.1	Requirement	26
5.9.2.2	Applicability.....	26
5.9.3	Mapping of requirements to use cases	26
5.10	Availability protection.....	26
5.10.1	Overview	26
5.10.2	REQ-AP-01.....	26
5.10.2.1	Requirement	26
5.10.2.2	Applicability.....	26
5.10.3	REQ-AP-02.....	26
5.10.3.1	Requirement	26
5.10.3.2	Applicability.....	26
5.10.4	REQ-AP-03.....	27
5.10.4.1	Requirement	27
5.10.4.2	Applicability.....	27
5.10.5	REQ-AP-04.....	27
5.10.5.1	Requirement	27
5.10.5.2	Applicability.....	27
5.10.6	Mapping of requirements to use cases	27
5.11	Non-interference.....	27

5.11.1	Overview	27
5.11.2	REQ-NI-01	28
5.11.2.1	Requirement	28
5.11.2.2	Applicability.....	28
5.11.3	REQ-NI-02	28
5.11.3.1	Requirement	28
5.11.3.2	Applicability.....	28
5.11.4	Mapping of requirements to use cases	28
5.12	Attack surface minimisation	28
5.12.1	Overview	28
5.12.2	REQ-ASM-01	28
5.12.2.1	Requirement	28
5.12.2.2	Applicability.....	28
5.12.3	Mapping of requirements to use cases	29
5.13	Exploit mitigation.....	29
5.13.1	Overview	29
5.13.2	REQ-EM-01.....	29
5.13.2.1	Requirement	29
5.13.2.2	Applicability.....	29
5.13.3	Other requirements	29
5.13.4	Mapping of requirements to use cases	30
5.14	Monitoring.....	30
5.14.1	Overview	30
5.14.2	REQ-MON-01	30
5.14.2.1	Requirement	30
5.14.2.2	Applicability.....	30
5.14.3	REQ-MON-02	30
5.14.3.1	Requirement	30
5.14.3.2	Applicability.....	30
5.14.4	REQ-MON-03	30
5.14.4.1	Requirement	30
5.14.4.2	Applicability.....	30
5.14.5	Mapping of requirements to use cases	31
5.15	Factory reset and data portability	31
5.15.1	Overview	31
5.15.2	REQ-DRT-01.....	31
5.15.2.1	Requirement	31
5.15.2.2	Applicability.....	31
5.15.3	REQ-DRT-02.....	31
5.15.3.1	Requirement	31
5.15.3.2	Applicability.....	31
5.15.4	Mapping of requirements to use cases	32
6	Assessment criteria for compliance with technical requirements	32
6.1	Introduction	32
6.1.1	General.....	32
6.1.2	Guidance for identifying interfaces or data processing.....	33
6.2	Appropriate level of cybersecurity	33
6.2.1	Overview	33
6.2.2	REQ-ALC-01.....	33
6.2.2.1	Objective	33
6.2.2.2	Preparation	34
6.2.2.3	Activities	34
6.2.2.4	Verdict.....	34
6.2.2.5	Evidence.....	34
6.2.2.6	Guidance	35
6.2.3	REQ-ALC-02.....	35
6.2.3.1	Objective	35
6.2.3.2	Preparation	35
6.2.3.3	Activities	35
6.2.3.4	Verdict.....	36
6.2.3.5	Evidence.....	36

6.3	No known exploitable vulnerabilities.....	36
6.3.1	Overview	36
6.3.2	REQ-KEV-01	36
6.3.2.1	Objective	36
6.3.2.2	Preparation	36
6.3.2.3	Activities	36
6.3.2.4	Verdict.....	36
6.3.2.5	Evidence.....	36
6.4	Secure by default configuration.....	37
6.4.1	Overview	37
6.5	Security updates	37
6.5.1	Overview	37
6.5.2	REQ-SU-01.....	37
6.5.2.1	Objective	37
6.5.2.2	Preparation	37
6.5.2.3	Activities	37
6.5.2.4	Verdict.....	37
6.5.2.5	Evidence.....	37
6.5.2.6	Guidance	37
6.6	Authentication and access control	38
6.6.1	Overview	38
6.6.2	REQ-AAC-01	38
6.6.2.1	Objective	38
6.6.2.2	Preparation	38
6.6.2.3	Activities	38
6.6.2.4	Verdict.....	38
6.6.2.5	Evidence.....	38
6.7	Confidentiality protection.....	38
6.7.1	Overview	38
6.7.2	REQ-CON-01	38
6.7.2.1	Objective	38
6.7.2.2	Preparation	38
6.7.2.3	Activities	39
6.7.2.4	Verdict.....	39
6.7.2.5	Evidence.....	39
6.7.3	REQ-CON-02	39
6.7.3.1	Objective	39
6.7.3.2	Preparation	39
6.7.3.3	Activities	39
6.7.3.4	Verdict.....	39
6.7.3.5	Evidence.....	39
6.7.3.6	Guidance	39
6.7.4	REQ-CON-03	40
6.7.4.1	Objective	40
6.7.4.2	Preparation	40
6.7.4.3	Activities	40
6.7.4.4	Verdict.....	40
6.7.4.5	Evidence.....	40
6.8	Integrity protection	40
6.8.1	Overview	40
6.8.2	REQ-INT-01	40
6.8.2.1	Objective	40
6.8.2.2	Preparation	40
6.8.2.3	Activities	40
6.8.2.4	Verdict.....	41
6.8.2.5	Evidence.....	41
6.8.3	REQ-INT-02	41
6.8.3.1	Objective	41
6.8.3.2	Preparation	41
6.8.3.3	Activities	41
6.8.3.4	Verdict.....	41
6.8.3.5	Evidence.....	41

6.8.3.6	Guidance	41
6.8.4	REQ-INT-03	42
6.8.4.1	Objective	42
6.8.4.2	Preparation	42
6.8.4.3	Activities	42
6.8.4.4	Verdict.....	42
6.8.4.5	Evidence.....	42
6.9	Data minimisation	42
6.9.1	Overview	42
6.9.2	REQ-DM-01	42
6.9.2.1	Objective	42
6.9.2.2	Preparation	42
6.9.2.3	Activities	43
6.9.2.4	Verdict.....	43
6.9.2.5	Evidence.....	43
6.9.2.6	Guidance	43
6.10	Availability protection.....	43
6.10.1	Overview	43
6.10.2	REQ-AP-01.....	43
6.10.2.1	Objective	43
6.10.2.2	Preparation	43
6.10.2.3	Activities	43
6.10.2.4	Verdict.....	43
6.10.2.5	Evidence.....	44
6.10.3	REQ-AP-02.....	44
6.10.3.1	Objective	44
6.10.3.2	Preparation	44
6.10.3.3	Activities	44
6.10.3.4	Verdict.....	44
6.10.3.5	Evidence.....	44
6.10.4	REQ-AP-03.....	44
6.10.4.1	Objective	44
6.10.4.2	Preparation	44
6.10.4.3	Activities	44
6.10.4.4	Verdict.....	44
6.10.4.5	Evidence.....	45
6.10.5	REQ-AP-04.....	45
6.10.5.1	Objective	45
6.10.5.2	Preparation	45
6.10.5.3	Activities	45
6.10.5.4	Verdict.....	45
6.10.5.5	Evidence.....	45
6.11	Non-interference.....	46
6.11.1	Overview	46
6.11.2	REQ-NI-01	46
6.11.2.1	Objective	46
6.11.2.2	Preparation	46
6.11.2.3	Activities	46
6.11.2.4	Verdict.....	46
6.11.2.5	Evidence.....	46
6.12	Attack surface minimisation.....	46
6.12.1	Overview	46
6.12.2	REQ-ASM-01	46
6.12.2.1	Objective	46
6.12.2.2	Preparation	47
6.12.2.3	Activities	47
6.12.2.4	Verdict.....	47
6.12.2.5	Evidence.....	47
6.12.2.6	Guidance	47
6.13	Exploit mitigation.....	47
6.13.1	Overview	47
6.13.2	REQ-EM-01.....	47

6.13.2.1	Objective	47
6.13.2.2	Preparation	47
6.13.2.3	Activities	47
6.13.2.4	Verdict.....	48
6.13.2.5	Evidence.....	48
6.14	Monitoring.....	48
6.14.1	Overview	48
6.14.2	REQ-MON-01	48
6.14.2.1	Objective	48
6.14.2.2	Preparation	48
6.14.2.3	Activities	48
6.14.2.4	Verdict.....	48
6.14.2.5	Evidence.....	48
6.14.3	REQ-MON-02	48
6.14.3.1	Objective	48
6.14.3.2	Preparation	49
6.14.3.3	Activities	49
6.14.3.4	Verdict.....	49
6.14.3.5	Evidence.....	49
6.14.4	REQ-MON-03	49
6.14.4.1	Objective	49
6.14.4.2	Preparation	49
6.14.4.3	Activities	49
6.14.4.4	Verdict.....	49
6.14.4.5	Evidence.....	49
6.15	Factory reset and data portability	49
6.15.1	Overview	49
6.15.2	REQ-DRT-01.....	50
6.15.2.1	Objective	50
6.15.2.2	Preparation	50
6.15.2.3	Activities	50
6.15.2.4	Verdict.....	50
6.15.2.5	Evidence.....	50
6.15.2.6	Guidance	50
6.15.3	REQ-DRT-02.....	50
6.15.3.1	Objective	50
6.15.3.2	Preparation	51
6.15.3.3	Activities	51
6.15.3.4	Verdict.....	51
6.15.3.5	Evidence.....	51

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847.....	52
-------------------------------	--	-----------

Annex B (informative):	Security analysis.....	55
B.0	Overview	55
B.1	Assets	55
B.1.1	Data.....	55
B.1.2	Hardware	55
B.1.3	Product and monitored element functions	55
B.2	Risk factors.....	56
B.2.1	Overview	56
B.2.2	[RF-NET] Accessibility of the network connected to product assets	56
B.2.3	[RF-FUN] Sensitivity of product function.....	56
B.2.4	[RF-NUM] Number of monitored elements	56
B.2.5	[RF-ADM] Availability and skill of administration	56
B.3	Assumptions.....	57
B.3.1	Overview	57
B.3.2	Proper platform.....	57
B.3.3	Proper administrator	57
B.3.4	Attacker expends resources proportionate to product assets.....	57
B.4	Threats and security analysis of threats.....	57

B.4.1	General.....	57
B.4.2	Security analysis methodology	57
B.4.3	List of threats, risk assessments, and mitigations	57
B.4.3.1	TH-UEVU: Unknown exploitable vulnerabilities.....	57
B.4.3.2	TH-KEVU: Known exploitable vulnerabilities.....	59
B.4.3.3	TH-CACC: Circumvention of access control	60
B.4.3.4	TH-DSTP: Unauthorised access to data stored via used product	60
B.4.3.5	TH-UADT: Unauthorised access to data transmitted or stored.....	61
B.4.3.6	TH-CONF: Access to assets via configuration errors	62
B.4.3.7	TH-AVAI: Denial of service attack on product	63
B.4.3.8	TH-DDOS: Interference with other devices.....	64
B.5	Mapping of risk factors to use cases.....	65

Annexes C to J:	Void	66
------------------------	-------------------	-----------

Annex K (normative):	Generic cryptographic requirements and assessment.....	67
-----------------------------	---	-----------

K.1	Cryptography	67
K.1.1	Requirement.....	67
K.1.2	Assessment of product cryptographic configuration.....	68
K.1.2.0	General	68
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms	68
K.1.2.1.1	Assessment objective.....	68
K.1.2.1.2	Assessment preparation	68
K.1.2.1.3	Assessment activities	68
K.1.2.1.4	Assessment evidence	68
K.1.2.1.5	Assessment verdict	69
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms	69
K.1.2.2.1	Assessment objective.....	69
K.1.2.2.2	Assessment preparation.....	69
K.1.2.2.3	Assessment activities.....	69
K.1.2.2.4	Assessment evidence	70
K.1.2.2.5	Assessment verdict	70
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms	70
K.1.2.3.1	Assessment objective.....	70
K.1.2.3.2	Assessment preparation	70
K.1.2.3.3	Assessment activities	70
K.1.2.3.4	Assessment evidence	71
K.1.2.3.5	Assessment verdict	71
K.2	Crypto agility.....	71
K.2.1	Requirement.....	71
K.2.2	Assessment of crypto-agility.....	72
K.2.2.1	Assessment objective	72
K.2.2.2	Assessment preparation.....	72
K.2.2.3	Assessment activities	72
K.2.2.4	Assessment evidence.....	73
K.2.2.5	Assessment verdict.....	73
K.3	ACM-extended cryptographic mechanisms	73
K.3.1	Requirement.....	73
K.3.2	List of ACM-extended cryptographic mechanisms	73
K.3.3	Assessment	73
K.4	Interoperability-based cryptographic mechanisms	74
K.4.1	Requirement.....	74
K.4.2	List of interoperability-based cryptographic mechanisms	74
K.4.3	Assessment	74

Annexes L to Q:	Void	75
------------------------	-------------------	-----------

Annex R (normative):	Additional provisions for products relying on Remote Data Processing Solutions (RDPS)	76
-----------------------------	--	-----------

R.1	Scope and applicability	76
R.2	RDPS as a product-boundary extension	76
R.3	Threat model	77

R.3.1	Assets.....	77
R.3.2	Threat catalogue.....	78
R.3.3	Mapping of assets to threats.....	79
R.4	Security requirements.....	79
R.4.1	General and guidance for requirement structure	79
R.4.2	Applicability of Annex R requirements	79
R.4.3	Local product side requirements	80
R.4.3.1	Data authenticity of interactions received from the RDPS side	80
R.4.3.2	Integrity of interactions received from the RDPS side.....	80
R.4.3.3	Confidentiality of data exchanged with the RDPS side	80
R.4.3.4	Availability.....	81
R.4.4	RDPS side requirements	82
R.4.4.1	Data authenticity of interactions received from the local product side	82
R.4.4.2	Integrity of interactions received from the local product side	82
R.4.4.3	Confidentiality of data exchanged with the local product side.....	82
R.4.4.4	Availability.....	83
R.4.5	Mapping of threats to requirements	84
R.5	Conformity assessment.....	84
R.5.1	Local product side requirements	84
R.5.1.1	Assessment case for REQ-RDPS-L-AUTH-001.....	84
R.5.1.2	Assessment case for REQ-RDPS-L-AUTH-002.....	85
R.5.1.3	Assessment case for REQ-RDPS-L-AUTH-003.....	86
R.5.1.4	Assessment case for REQ-RDPS-L-INTEG-001.....	87
R.5.1.5	Assessment case for REQ-RDPS-L-INTEG-002.....	88
R.5.1.6	Assessment case for REQ-RDPS-L-INTEG-003.....	88
R.5.1.7	Assessment case for REQ-RDPS-L-CONF-001	89
R.5.1.8	Assessment case for REQ-RDPS-L-CONF-002	90
R.5.1.9	Assessment case for REQ-RDPS-L-CONF-003	91
R.5.1.10	Assessment case for REQ-RDPS-L-AVAIL-001	92
R.5.1.11	Assessment case for REQ-RDPS-L-AVAIL-002	93
R.5.1.12	Assessment case for REQ-RDPS-L-AVAIL-003	93
R.5.2	RDPS side requirements	94
R.5.2.1	Assessment case for REQ-RDPS-R-AUTH-001.....	94
R.5.2.2	Assessment case for REQ-RDPS-R-AUTH-002.....	95
R.5.2.3	Assessment case for REQ-RDPS-R-AUTH-003.....	96
R.5.2.4	Assessment case for REQ-RDPS-R-INTEG-001.....	97
R.5.2.5	Assessment case for REQ-RDPS-R-INTEG-002.....	98
R.5.2.6	Assessment case for REQ-RDPS-R-INTEG-003.....	98
R.5.2.7	Assessment case for REQ-RDPS-R-CONF-001	99
R.5.2.8	Assessment case for REQ-RDPS-R-CONF-002.....	100
R.5.2.9	Assessment case for REQ-RDPS-R-CONF-003.....	101
R.5.2.10	Assessment case for REQ-RDPS-R-AVAIL-001	102
R.5.2.11	Assessment case for REQ-RDPS-R-AVAIL-002	103
R.5.2.12	Assessment case for REQ-RDPS-R-AVAIL-003	103
R.6	Mapping of CRA Annex I to Annex R requirements	104
Annex S (informative): Change history		106
History		107

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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 draft Harmonised European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI Standardisation Request deliverable Approval Procedure (SRdAP).

The present document has been prepared under the Commission's standardisation request C(2025) 618 final [i.3] to provide one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) [i.1].

Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the present document, a presumption of conformity with the corresponding requirements of that Regulation and associated EFTA regulations.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

Introduction

The present document provides the technical cybersecurity requirements for the products in scope, following a risk-based approach in support of the Cyber Resilience Act (CRA) [i.1]. The technical cybersecurity requirements are therefore proportionate to the intended purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

Clause 4 does not contain technical requirements; it describes the product context that is considered for the application of this standard.

Clause 4 also defines Use Cases (UCs) that represent the main deployment scenarios reflecting the intended purpose and reasonably foreseeable use of the product, which serve as the basis for identifying relevant cybersecurity risks.

Clause 5 specifies technical cybersecurity requirements for the product to mitigate the identified risks, including their applicability conditions.

Clause 6 specifies the assessment criteria and procedures for verifying compliance with the requirements of clause 5.

Annex A maps the technical requirements of the present document to the essential requirements of the CRA [i.1].

Annex B describes the methodology used to assess the security risks of the products in their context.

Annex K supports the definition of the cryptographic requirements and assessment criteria used by the present document.

Annex R provides supplementary requirements and assessment provisions where a product relies on remote data processing solutions (RDPS) for the provision or support of one or more product functions.

1 Scope

The present document specifies technical requirements and corresponding assessment criteria for Security Information and Event Management related to cybersecurity.

The products with digital elements in scope, hereinafter "SIEM" or "SIEM systems":

- are specified within the "technical description" of the "category of product" number 7 by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as: Products with digital elements that collect data from multiple sources, analyse and correlate that data and present it as actionable information for security-related purposes, such as threat and incident detection, forensic analysis or compliance purposes.
- are covered only within the product context described in clause 4.

The present document covers those products for the purpose of demonstrating compliance with the essential cybersecurity requirements of Regulation (EU) 2024/2847 [i.1] Annex I, Part I under the conditions identified in Annex A.

SIEM systems intended for use in the industrial operational technology (OT) domain are excluded from the scope of the present document, see prEN 50770 series [i.5].

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the [ETSI docbox](#).

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 necessary for the application of the present document.

- [1] [ENISA](#) European Cybersecurity Certification Group Sub-group on Cryptography: "[Agreed Cryptographic Mechanisms](#)", Version 2.0, April 2025.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

- [i.1] [Regulation \(EU\) 2024/2847](#) of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

- [i.2] [Commission Implementing Regulation \(EU\) 2025/2392](#) of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council.
- [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
- [i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements – Vocabulary".
- [i.5] prEN 50770 series: "Security for operational technologies" (produced by CENELEC).
- [i.6] [EU Vulnerability Database \(EUVD\)](#).
- [i.7] BSI TR-02102-1 (Version 2026-01, 31 January 2026): "Cryptographic Mechanisms: Recommendations and Key Lengths".
- [i.8] BSI TR-02102-2 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Transport Layer Security (TLS)".
- [i.9] BSI TR-02102-3 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)".
- [i.10] BSI TR-02102-4 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Secure Shell (SSH)".
- [i.11] ANSSI Référentiel Général de Sécurité, Annex B2, version 2.0: "Gestion des clés cryptographiques - Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques".

get full document from standards.iteh.ai

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in Regulation (EU) 2024/2847 [i.1], prEN 40000-1-1 [i.4] and the following apply:

component: software or hardware intended for integration into an electronic information system

cryptographic mechanism: security-related procedure using cryptography

NOTE 1: The term “cryptographic mechanism” is used in this annex as an umbrella term covering the categories used in the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [reference], including cryptographic algorithms, primitives, schemes, protocols, protocol profiles, cipher suites, modes of operation, constructions and parameter sets.

NOTE 2: The terms “cryptographic primitive”, “cryptographic construction”, “cryptographic scheme” and “cryptographic protocol” are used consistently with the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [reference].

NOTE 3: A cryptographic mechanism can be specified at different levels of abstraction. For example, AES is a cryptographic primitive, AES-GCM is a mode of operation / authenticated encryption construction, TLS 1.3 is a protocol, a TLS 1.3 restricted cipher-suite profile is a protocol profile, and TLS_AES_128_GCM_SHA256 is a cipher suite.

cryptographic property: property provided or supported by a cryptographic mechanism

NOTE 1: Cryptographic properties include, for example, confidentiality, integrity, authenticity, entity authentication, message authentication, key establishment, key confirmation, replay protection, collision resistance, second-preimage resistance, pre-image resistance, signature unforgeability, non-repudiation, forward secrecy and password-verifier protection. Where relevant, a cryptographic property can be expressed using a formal cryptographic notion, for example IND-CPA, IND-CCA, IND-CCA2, EUF-CMA, SUF-CMA or authenticated key exchange security.

NOTE 2: A cryptographic property is distinct from a product-level technical requirement, although it can support such a requirement. For example, a secure communication requirement can rely on cryptographic properties such as confidentiality, integrity and authentication.

log: record of an operational event

machine user: virtual user used to access the system programming interfaces

monitored element: a physical or virtual device monitored by the product

product user: person having the credentials to log in to the product to operate administrative actions

secure channel: cryptographically protected communication channel

subject: product user, machine user, or a process being authenticated by the identity provider

trace: record of a system status with all relevant data that can be gathered

3.2 Symbols

Void.

3.3 Abbreviations

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

ACM	Agreed Cryptographic Mechanisms
API	Application Programming Interface
CPU	Central Processing Unit
CRA	Cyber Resilience Act
CVE	Common Vulnerabilities and Exposures
DB	Database
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
GUI	Graphical User Interface
IoT	Internet of Things
IP	Internet Protocol
OT	Operational Technology
RDPS	Remote Data Processing Solution
SIEM	Security Information and Event Management
TLS	Transport Layer Security
UC	Use Case
VPN	Virtual Private Network

4 Product context

4.0 Introduction

The product context for SIEM systems is detailed in the following clause. Product context is descriptive, and clause 4 does not contain normative requirements.