ETSI TR 103 305-2 V1.1.1 (2016-08)

TECHNICAL REPORT

CYBER;
Critical Security Controls for Effective Cyber Defence;
Part 2: Measurement and auditing

Reference

DTR/CYBER-0012-2

Keywords

Cyber Security, Cyber-defence, information assurance

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.3].

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 present document is intended as an evolving repository for guidelines on measurement and auditing of Critical Security Control implementations. Measurement is an essential component of any successful security program. To support good decision-making, the current state of a protected IT system or network should assessed. Means should exist to measure and report on progress. The records kept constitute an audit.

Introduction

The Critical Security Controls ("the Controls") have always included a set of Metrics for every Control in order to help adopters manage implementation projects. Adopters can use the sample Metrics as a starting point to identify key information to help track progress, and to encourage the use of automation.

However, there is considerable security "fog" around the use of the terms. For example, there are lots of things that can be measured, but it is very unclear which of them are in fact worth measuring (in terms of adding value to security decisions). And since there are very few "absolutes" in security, there is always the challenge of making a judgment about the measurement value that is "good enough" in terms of managing risk.

The problem of inconsistent terminology across the industry cannot be solved, but consistency within the Critical Security Controls can be enhanced. The definitions found in a NIST article, Cyber Security Metrics and Measures are a useful point of departure. [i.1] This approach separates the attribute being measured (the "Measure") from a value judgment of what is "good" or "good enough".

1 Scope

The present document is an evolving repository for measurement and effectiveness tests of Critical Security Control implementations. The CSC are a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks.

The present document is also technically equivalent and compatible with the 6.0 version of the "CIS Controls Measurement Companion Guide" October 2015, which can be found at the website http://www.cisecurity.org/critical-controls/ [i.1].

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 reference 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] The Center for Internet Cybersecurity: "A Measurement Companion to the CIS Critical Security Controls" version 6, October 15, 2015.

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

[i.2] Paul E. Black, Karen Scarfone and Murugiah Souppaya, Cyber Security Metrics and Measures, in Handbook of Science and Technology for Homeland Security, Vol. 5, Edited by John G. Voeller.

NOTE: Available at https://hissa.nist.gov/~black/Papers/cyberSecurityMetrics2007proof.pdf.

[i.3] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts that are maintained by the Center for Internet Security and found at the website http://www.cisecurity.org/critical-controls/

measure: concrete, objective attribute, such as the percentage of systems within an organization that are fully patched, the length of time between the release of a patch and its installation on a system, or the level of access to a system that a vulnerability in the system could provide [i.2]

metric: abstract, somewhat subjective attribute, such as how well an organization's systems are secured against external threats or how effective the organization's incident response team is [i.2]

NOTE: An analyst can approximate the value of a metric by collecting and analyzing groups of measures, as is explained later 3 and CSC 12.

3.2 Abbreviations

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

CIS	Center for Internet Security
CSC	Critical Security Control or Capability
DLP	Data Loss Prevention
DMZ	DeMilitarized Zone
EICAR	European Expert Group for IT-Security
ID	Identifier
IDS	Intrusion Detection System
IPS	Intrusion prevention system
IPv6	Internet Protocol version 6
IT	Information Technology
LAN	local area network
NIST	National Institute of Standards and Technology
NLA	Network Level Authentication
SCAP	Security Content Automation Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

4 Critical Security Controls: Measures Metrics, and Thresholds

4.0 Control measures, metrics, and thresholds

For each Control, a list of Measures is presented in the table below. Each Measure is given a unique ID number to allow tracking.

NOTE: These numbers do not correspond to the individual sub-controls in the Critical Security Controls document.

These Measures are similar to what "Metrics" in previous versions of the Controls.

For each Measure, Metrics are presented, which consist of three "Risk Threshold" values. These values represent an opinion from experienced practitioners, and are not derived from any specific empirical data set or analytic model. These are offered as a way for adopters of the Controls to think about and choose Metrics in the context of their own security improvement programs. (This is sometimes described, e.g. by NIST, for each of the Risk Thresholds as a "lower-level metric". The "higher-level metric" is the collection of the three Risk Thresholds. When an Enterprise chooses a specific Threshold, that becomes a "benchmark" against which that Enterprise measures progress).

Separately, for every Control, an Effectiveness Test is presented in clause 5. These provide a suggested way to independently verify the effectiveness of the implementation for each Critical Security Control.

Table 1: Critical Security Controls (Version 6): Measures, Metrics and Thresholds

Critical Security Controls (Version 6): Measures, Metrics, and Thresholds				
			METRICS	
ID	**Measure**	**Lower Risk Threshold**	**Moderate Risk Threshold**	**Higher Risk Threshold**
1.1	How many unauthorized devices are presently on the organization's network (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
1.2	How long, on average, does it take to remove unauthorized devices from the organization's network (by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
1.3	What is the percentage of systems on the organization's network that are not utilizing Network Level Authentication (NLA) to authenticate to the organization's network (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
1.4	How many hardware devices have been recently blocked from connecting to the network by the organization's Network Level Authentication (NLA) system (by business unit)?			
1.5	How long does it take to detect new devices added to the organization's network (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
1.6	How long does it take to isolate/remove unauthorized devices from the organization's network (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
2.1	How many unauthorized software applications are presently located on business systems within the organization (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
2.2	How long, on average, does it take to remove unauthorized applications from business systems within the organization (by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
2.3	What is the percentage of the organization's business systems that are not running software whitelisting software that blocks unauthorized software applications (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
2.4	How many software applications have been recently blocked from executing by the organization's software whitelisting software (by business unit)?			
2.5	How long does it take to detect new software installed on systems in the organization (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
2.6	How long does it take to remove unauthorized software from one of the organization's systems (time in minutes - by business unit)?	60 minutes	1,440 Minutes (1 day)	10,080 minutes (1 week)
3.1	What is the percentage of business systems that are not currently configured with a security configuration that matches the organization's approved configuration standard (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
3.2	What is the percentage of business systems whose security configuration is not enforced by the organization's technical configuration management applications (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
3.3	What is the percentage of business systems that are not up to date with the latest available operating system software security patches (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
3.4	What is the percentage of business systems that are not up to date with the latest available business software application security patches (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
3.5	How many unauthorized configuration changes have been recently blocked by the organization's configuration management system (by business unit)?			
3.6	How long does it take to detect configuration changes to a system (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
3.7	How long does it take to reverse unauthorized changes on systems (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)

Critical Security Controls (Version 6): Measures, Metrics, and Thresholds				
			METRICS	
ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
4.1	What is the percentage of the organization's business systems that have not recently been scanned by the organization's approved, SCAP compliant, vulnerability management system (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
4.2	What is the average SCAP vulnerability score of each of the organization's business systems (by business unit)?			
4.3	What is the total SCAP vulnerability score of each of the organization's business systems (by business unit)?			
4.4	How long does it take, on average, to completely deploy operating system software updates to a business system (by business unit)?	1,440 minutes (1 day)	10,080 minutes (1 week)	43,200 minutes (1 Month)
4.5	How long does it take, on average, to completely deploy application software updates to a business system (by business unit)?	1,440 minutes (1 day)	10,080 minutes (1 week)	43,200 minutes (1 Month)
5.1	How many unauthorized elevated operating system accounts (local administrator/root) are currently configured on the organization's systems (by business unit)?			
5.2	How many unauthorized elevated application accounts are currently configured on the organization's systems (by business unit)?			
5.4	What percentage of the organization's elevated accounts do not require two-factor authentication (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
5.5	How many attempts to upgrade an account to administrative privileges have been detected on the organization's systems recently (by business unit)?			
5.6	How many attempts to gain access to password files within the system have been detected on the organization's systems recently (by business unit)?			
5.7	How long does it take for administrators to be notified about user accounts being added to super user groups (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
6.1	What percentage of the organization's systems do not currently have comprehensive logging enabled in accordance with the organization's standard (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
6.2	What percentage of the organization's systems are not currently configured to centralize their logs to a central log management system (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
6.3	How many anomalies/events of interest have been discovered in the organization's logs recently (by business unit)?			
6.4	If a system fails to log properly, how long does it take for an alert about the failure to be sent (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
6.5	If a system fails to log properly, how long does it take for enterprise personnel to respond to the failure (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
7.1	How many unsupported web browsers have been detected on the organization's systems (by business unit)?			
7.2	How many unsupported email clients have been detected on the organization's systems (by business unit)?			
7.3	How many events of interest have been detected recently when examining logged URL requests made from the organization's systems (by business unit)?			
7.4	What percentage of devices are not required to utilize network based URL filters to limit access to potentially malicious websites (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %

Critical Security Controls (Version 6): Measures, Metrics, and Thresholds				
			METRICS	
ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
7.5	What percentage of the organization's users, on average, will inappropriately respond to an organization sponsored email phishing test (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
8.1	What percentage of systems have not been deployed with enabled and up-to-date anti-malware systems (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
8.2	How many instances of malicious code have been detected recently by host based anti-malware systems (by business unit)?			
8.3	How many instances of malicious code have been detected recently by network based anti-malware systems (by business unit)?			
8.4	What percentage of the organization's applications are not utilizing application sandboxing products (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
8.5	How long does it take the system to identify any malicious software that is installed, attempted to be installed, executed, or attempted to be executed on a computer system (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
8.6	How long does it take the organization to completely remove the malicious code from the system after it has been identified (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
9.1	What is the percentage of the organization's systems that are not currently running a host based firewall (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
9.2	How many unauthorized services are currently running on the organization's business systems (by business unit)?			
9.3	How many deviations from approved service baselines have been discovered recently on the organization's business systems (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
9.4	How long does it take systems to identify any new unauthorized listening network ports that are installed on network systems (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
9.5	How long does it take to close or authorize newly detected system services (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
10.1	What percentage of the organization's systems have not recently had their operating system or application binaries backed up (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
10.2	What percentage of the organization's systems have not recently had their data sets backed up (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
10.3	What percentage of the organization's backups have not recently been tested by the organization's personnel (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
10.4	What percentage of the organization's systems do not have a current backup that is not available to online operating system calls (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
10.5	How long, on average, does it take to notify system personnel that a backup has failed to properly take place on a system (by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
11.1	What is the percentage of network devices that are not currently configured with a security configuration that matches the organization's approved configuration standard (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
11.2	What is the percentage of network devices whose security configuration is not enforced by the organization's technical configuration management applications (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %