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

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 %

Critical Security Controls (Version 6): Measures, Metrics, and Thresholds				
			METRICS	
ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
11.3	What is the percentage of network devices 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 %
11.4	What is the percentage of network devices do not require two-factor authentication to administer the device (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
11.5	How long does it take to detect configuration changes to a network system (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
11.6	How long does it take to reverse unauthorized changes on network systems (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
12.1	What percentage of the organization's remote access users are not required to use two-factor authentication to remotely access the organization's network (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
12.2	What percentage of remote business systems are not managed using the same security standards as internal network systems (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
12.3	What percentage of the organization's internal systems are not on dedicated Virtual LANs (VLANs) that are segmented with access control lists (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
12.4	How many events of interest have been discovered recently on the organization's network through analysis of NetFlow configured on network devices (by business unit)?			
12.5	How long does it take before unauthorized network packets are alerted on when passing through perimeter systems (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
12.6	How long does it take to apply configuration changes to block unauthorized traffic passing through perimeter systems (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
13.1	How many unauthorized data exfiltration attempts have been detected recently by the organization's Data Loss Prevention (DLP) system (by business unit)?			
13.2	How many plaintext instances of sensitive data have been detected recently by the organization's automated scanning software (by business unit)?			
13.3	How many attempts to access known file transfer and email exfiltration websites have been detected recently (by business unit)?			
14.1	What percentage of sensitive data sets are not configured to require logging of access to the data set (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
14.2	What percentage of the organization's business systems are not utilizing host based Data Loss Prevention (DLP) software applications (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
15.1	How many rogue wireless access points have been discovered recently in the organization (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
15.2	What is the average time that it takes to remove rogue access points from the organization's network (by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
15.3	How many wireless access points or clients have been discovered using an unauthorized wireless configuration recently in the organization (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
15.4	How long does it take to generate alerts about unauthorized wireless devices that are detected (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
15.5	How long does it take for unauthorized wireless devices to be isolated/removed from the network (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
16.1	How many invalid attempts to access user accounts have been detected recently (by business unit)?			
16.2	How many accounts have been locked out recently (by business unit)?			
16.3	How many attempts to gain access to password files in the system have been detected recently (by business unit)?			
17.1	What percentage of the organization's workforce members have not completed a core information security awareness program (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
17.2	What percentage of the organization's workforce members have not completed job role specific information security awareness program (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
17.3	What percentage of the organization's workforce members have not passed general information security awareness assessments (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
17.4	What percentage of the organization's workforce members have not passed job role specific information security awareness assessments (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
18.1	What percentage of the organization's custom applications have not been recently scanned by an application security code scanner (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
18.2	What percentage of the organization's database systems have not been recently scanned by a database specific vulnerability scanner (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
18.3	What is the aggregate vulnerability rating for all application and database system in the organization (by business unit)?			
18.4	How long does it take for alerts to be generated & sent to system administrators that a vulnerability scan has or has not completed (time in minutes - by business unit)?	60 minutes	1,440 minutes (1 day)	10,080 minutes (1 week)
19.1	What percentage of the organization's workforce members have not completed job role specific information security incident handling education programs (by business unit)?	Less than 1 %	1 % - 4 %	5 % - 10 %
19.2	How many incident handling scenario exercises have been conducted recently within the organization (by business unit)?	More than 3	2 to 3	0 to 1
19.3	How many information security incidents have been documented recently within the organization (by business unit)?			
20.1	How many technical penetration tests have been performed by external penetration testers recently within the organization (by business unit)?	More than 3	2 to 3	0 to 1
20.2	How many technical penetration tests have been performed by internal workforce members recently within the organization (by business unit)?	More than 3	2 to 3	0 to 1
20.3	What is the aggregate score of all recently performed penetration tests in accordance with the organization's penetration testing scoring system (by business unit)?			

5 Critical Security Controls: Effectiveness Tests

CSC 1: Inventory of Authorized and Unauthorized Devices|Effectiveness Test

To evaluate the implementation of CSC 1 on a periodic basis, an evaluation team should connect hardened test systems to at least 10 locations on the network, including a selection of subnets associated with demilitarized zones (DMZs), workstations, and servers. Two of the systems should be included in the asset inventory database, while the other systems are not. The evaluation team should then verify that the systems generate an alert or email notice regarding the newly connected systems within 24 hours of the test machines being connected to the network. The evaluation team should verify that the system provides details of the location of all the test machines connected to the network. For those test machines included in the asset inventory, the team should also verify that the system provides information about the asset owner.

CSC 2: Inventory of Authorized and Unauthorized Software|Effectiveness Test

To evaluate the implementation of CSC 2 on a periodic basis, the evaluation team should move a benign software test program that is not included in the authorized software list to 10 systems on the network. Two of the systems should be included in the asset inventory database, while the other systems do not need to be included. The evaluation team should then verify that the systems generate an alert or email notice regarding the new software within 24 hours. The team should also verify that the alert or email is received within one additional hour indicating that the software has been blocked or quarantined. The evaluation team should verify that the system provides details of the location of each machine with this new test software, including information about the asset owner. The evaluation team should then verify that the software is blocked by attempting to execute it and verifying that the software is not allowed to run.

On systems where blocking is not allowed or blocking functionality is not available, the team should verify that the execution of unauthorized software is detected and results in a notification to alert the security team that unauthorized software is being used.

CSC 3: Secure Configurations for Hardware and Software|Effectiveness Test

To evaluate the implementation of CSC 3 on a periodic basis, an evaluation team should move a benign test system that does not contain the official hardened image, but that does contain additional services, ports, and configuration file changes, onto the network. This should be performed on 10 different random segments using either real or virtual systems. The evaluation team should then verify that the systems generate an alert regarding the changes to the software within the target service window, or within 24 hours – whichever is less. It is important that the evaluation team verify that all unauthorized changes have been detected. The team should also verify that the alert or email is received within one additional hour indicating that the software has been blocked or quarantined. The evaluation team should verify that the system provides details of the location of each machine with the unauthorized changes, including information about the asset owner.

The evaluation team should also introduce undocumented/out-of-band configuration settings and binaries using real or virtual systems on 10 random segments. The test should include making a non-persistent change, in which a change is introduced to the primary program location (/bin, Program Files, etc.), left in place for 30 - 60 minutes, then reverted to the original configuration.

The evaluation team should verify that all configuration changes and binaries are detected, and that there is a record of the non-persistent changes mentioned above. The detection data should include the nature of the change made (addition, removal, alteration, owner, permissions, contents, etc.), as well as the user account that made the change.

The evaluation team should also verify that unauthorized software is blocked by attempting to execute it and verifying that it is not allowed to run. On systems where blocking is not allowed or blocking functionality is not available, the team should verify that the execution of unauthorized software is detected and results in a notification to alert the security team that unauthorized software is being used.

In addition to these tests, the following tests should be performed:

1) File integrity checking tools should be run on a regular basis. Any changes to critical operating system, services, and configuration files should be checked on an hourly basis. Any changes should be detected and either blocked or trigger an alert that follows the above notification process.

2) Detection software should detect the disabling of system logging, as well as the truncation, modification or deletion of log files. Note that growth of logs should not trigger notifications, but suspicious changes associated with malicious activities should; examples include deletion or truncation of logs, modification of past log events, owner or permission changes, etc. Any inappropriate changes to logs should trigger an alert that follows the above notification process.

3) System scanning tools that check for software version, patch levels, and configuration files should be run on a daily basis. Any changes should be detected and either blocked or trigger an alert that follows the above notification process.

CSC 4: Continuous Vulnerability Assessment and Remediation|Effectiveness Test

To evaluate the implementation of CSC 4 on a periodic basis, the evaluation team should verify that scanning tools have successfully completed their weekly or daily scans for the previous 30 cycles of scanning by reviewing archived alerts and reports to ensure that the scan was completed. If a scan could not be completed in that timeframe, the evaluation team should verify that an alert or email was generated indicating that the scan did not finish.

CSC 5: Controlled Use of Administrative Privileges|Effectiveness Test

To evaluate the implementation of CSC 5 on a periodic basis, the evaluation team should attempt a variety of techniques to gain access and exploit administrative accounts within the system. Each of the following tests should be performed at least three times:

- Attempt to gain access to a cross section of devices within the system, using default administrative passwords.
- Attempt to log-in remotely to machines using administrative accounts directly. Verify that this is disallowed by policy.
- Attempt to log-in directly to a workstation or server with root or administrator accounts. Verify that this is disallowed by policy.
- Attempt to gain access to password files within the system using unauthorized accounts. Verify that access is disallowed and that attempts are logged and reported.
- Attempt to elevate to a privileged account on the system. Verify that the administrator password is required to perform the elevation and that the elevation is logged and reported by the system. Verify that traceability within the audit logs is provided to detail the user account that performed the elevation.
- Attempt to configure weak administrator passwords that are non-compliant with established policy. Verify that the system does not allow weak passwords to be used.
- Attempt to re-use an administrator password that was previously used for the account. Verify that the system requires unique new passwords during each update.

Each of these tests should be performed from multiple, widely distributed systems on the organization's network in order to test the effectiveness of administrator controls.

CSC 6: Maintenance, Monitoring, and Analysis of Audit Log|Effectiveness Test

To evaluate the implementation of CSC 6 on a periodic basis, an evaluation team should review the security logs of various network devices, servers, and hosts. At a minimum the following devices should be tested: two routers, two firewalls, two switches, 10 servers, and 10 client systems. The testing team should use traffic-generating tools to send packets through the systems under analysis to verify that the traffic is logged. This analysis is done by creating controlled, benign events and determining if the information is properly recorded in the logs with key information, including a date, timestamp, source address, destination address, and other details about the packet. The evaluation team should verify that the system generates audit logs and, if not, an alert or email notice regarding the failed logging should be sent within 24 hours. It is important that the team verify that all activity has been detected. The evaluation team should verify that the system provides details of the location of each machine, including information about the asset owner.

CSC 7: Email and Web Browser Protections|Effectiveness Test

To evaluate the implementation of CSC 7 on a periodic basis, an evaluation team should perform authorized phishing attempts against the organization's internal workforce members in order to determine both if the workforce members are susceptible to such attacks and whether the organization's email and browser defenses are working effectively. Specifically these phishing attacks should use both web links and malicious attachments to simulate malicious code, use social engineering methods to convince users to initiate unnecessary actions, and use other common attack methodologies used by targeting phishing attacks. The results of the test should be used to identify trends regarding the number of workforce members and individual users repeatedly susceptible to attack as well as the effectiveness of the technical controls implemented to prevent the effectiveness of the attacks. In addition to preventing the phishing attack from being successful, the organization should also verify that appropriate notifications have been made to the organization's security team to alert to the presence of the attack taking place.

CSC 8: Malware Defenses|Effectiveness Test

To evaluate the implementation of CSC 8 on a periodic basis, the evaluation team should move a benign software test program that appears to be malware (such as an EICAR file or benign hacker tools), but that is not included in the official authorized software list, to 10 systems on the network via a network share. The selection of these systems should be as random as possible and include a cross-section of the organization's systems and locations. The evaluation team should then verify that the systems generate an alert or email notice regarding the benign malware within one hour. The team should also verify that the alert or email indicating that the software has been blocked or quarantined is received within one hour. The evaluation team should verify that the system provides details of the location of each machine with this new test file, including information about the asset owner. The team should then verify that the file is blocked by attempting to execute or open it and verifying that it is not allowed to be accessed.

Once this test has been performed transferring the files to organization systems via removable media, the same test should be repeated, but this time transferring the benign malware to 10 systems via email instead. The organization should expect the same notification results as noted with the removable media test.

CSC 9: Limitation and Control of Network Ports|Effectiveness Test

To evaluate the implementation of CSC 9 on a periodic basis, the evaluation team should install hardened test services with network listeners on 10 locations on the network, including a selection of subnets associated with DMZs, workstations, and servers. The selection of these systems should be as random as possible and include a cross-section of the organization's systems and locations. The evaluation team should then verify that the systems generate an alert or email notice regarding the newly installed services within 24 hours of the services being installed on the network. The team should verify that the system provides details of the location of all of the systems where test services have been installed.

CSC 10: Data Recovery Capability|Effectiveness Test

The evaluation team should identify 5 systems in the environment and restore to a test system (physical or virtual) using the most recent backup. Verify that the system has been restored properly by comparing the restore results to the original system.

CSC 11: Secure Configurations for Network Devices|Effectiveness Test

To evaluate the implementation of CSC 11 on a periodic basis, an evaluation team should make a change to each type of network device plugged into the network. At a minimum, routers, switches, and firewalls need to be tested. If they exist, IPS, IDS, and other network devices should be included. Backups should be made prior to making any changes to critical network devices. It is critical that changes not impact or weaken the security of the device. Acceptable changes include but are not limited to making a comment or adding a duplicate entry in the configuration. The change should be performed twice for each critical device. The evaluation team should then verify that the systems generate an alert or email notice regarding the changes to the device within 24 hours. It is important that the evaluation team verify that all unauthorized changes have been detected, the account making the changes has been recorded, and the changes have resulted in an alert or email notification. The evaluation team should verify that the system provides details of the location of each device, including information about the asset owner. While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting and isolation, with notification about unauthorized configuration changes in network devices sent within two minutes.

If appropriate, an additional test should be performed on a daily basis to ensure that other protocols such as IPv6 are being filtered properly.

CSC 12: Boundary Defense|Effectiveness Test

To evaluate the implementation of CSC 12 on a periodic basis, an evaluation team should test boundary devices by sending packets from outside any trusted network to ensure that only authorized packets are allowed through the boundary. All other packets should be dropped. In addition, unauthorized packets should be sent from a trusted network to an untrusted network to make sure egress filtering is functioning properly. The evaluation team should then verify that the systems generate an alert or email notice regarding the unauthorized packets within 24 hours. It is important that the evaluation team verify that all unauthorized packets have been detected. The evaluation team should also verify that the alert or email indicating that the unauthorized traffic is now being blocked is received within one hour. The evaluation team should verify that the system provides details of the location of each machine with this new test software, including information about the asset owner. It is also important that the evaluation team test to ensure that the device fails in a state where it does not forward traffic when it crashes or becomes flooded.

CSC 13: Data Protection|Effectiveness Test

To evaluate the implementation of CSC 13 on a periodic basis, the evaluation team should attempt to move test data sets that trigger DLP systems but do not contain sensitive data outside of the trusted computing environment via both network file transfers and removable media. Each of the following tests should be performed at least three times:

- Attempt to transfer large data sets across network boundaries from an internal system.
- Attempt to transfer plaintext test data sets of personally identifiable information (that trigger DLP systems but do not contain sensitive data) across network boundaries from an internal system (using multiple keywords specific to the business).
- Attempt to transfer encrypted test data sets across network boundaries from an internal system to identify if the exfiltration is reported.
- Attempt to maintain a persistent network connection for at least 10 hours across network boundaries between an internal and external system, even though little data may be exchanged.
- Attempt to maintain a network connection across network boundaries using an anomalous service port number between an internal and external system.
- Insert a USB token into an organization system and attempt to transfer example test data to the USB device.

Each of these tests should be performed from multiple, widely distributed systems on the organization's network in order to test the effectiveness of the monitoring systems. Once each of these events has occurred, the time it takes for enterprise staff to respond to the event should be recorded.

CSC 14: Controlled Access Based on the Need to Know|Effectiveness Test

To evaluate the implementation of CSC 14 on a periodic basis, the evaluation team should create two test accounts each on 10 representative systems in the enterprise: five server machines and five client systems. For each system evaluated, one account should have limited privileges, while the other should have privileges necessary to create files on the systems. The evaluation team should then verify that the non-privileged account is unable to access the files created for the other account on the system. The team should also verify that an alert or email is generated based on the attempted unsuccessful access within 24 hours. Upon completion of the test, these accounts should be removed.

CSC 15: Wireless Access Control|Effectiveness Test

To evaluate the implementation of CSC 15 on a periodic basis, the evaluation team should configure 10 unauthorized but hardened wireless clients and wireless access points to the organization's network and attempt to connect them to its wireless networks. In the case of wireless access points, these access points should not be directly connected to the organization's trusted network. Instead, they should simply be configured to act as a wireless gateway without physically connecting to a wired network interface. In the case of scanning for wireless access points from a wired interface, the connected access point should have the wireless radio disabled for the duration of the test. These systems should be configured to test each of the following scenarios:

- A wireless client with an unauthorized service set identifier configured on it.

- A wireless client with improper encryption configured.
- A wireless client with improper authentication configured.
- A wireless access point with improper encryption configured.
- A wireless access point with improper authentication configured.
- A completely rogue wireless access point using an unauthorized configuration.

When any of the above-noted systems attempt to connect to the wireless network, an alert should be generated and enterprise staff should respond to the alerts to isolate the detected device or remove the device from the network.

CSC 16: Account Monitoring and Control|Effectiveness Test

To evaluate the implementation of CSC 16 on a periodic basis, the evaluation team should attempt a variety of techniques to gain access to user accounts within the system. Each of the following tests should be performed at least three times:

1) Attempt to configure weak user account passwords that are non-compliant with established policy. Verify that the system does not allow weak passwords to be used.
2) Attempt to re-use a user account password that was previously used for the account. Verify that the system requires unique new passwords during each update.
3) Attempt to capture passwords by monitoring network traffic to server resources. Remediate any instances where passwords are transmitted in clear text.
4) Attempt to gain access to password files stored on the system. If successful, identify whether passwords are cryptographically secured.

Each of these tests should be performed from multiple, widely distributed systems on the organization's network in order to test the effectiveness of user account controls.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps|Effectiveness Test

None.

CSC 18: Application Software Security|Effectiveness Test

To evaluate the implementation of CSC 6 on a monthly basis, an evaluation team should use a web application vulnerability scanner to test for each relevant type of flaw identified in the regularly updated list of the "25 Most Dangerous Programming Errors" by MITRE and the SANS Institute. The scanner should be configured to assess all of the organization's Internet-accessible web applications to identify such errors. The evaluation team should verify that the scan is detected within 24 hours and that an alert is generated.

In addition to the web application vulnerability scanner, the evaluation team should also run static code analysis tools and database configuration review tools against Internet-accessible applications to identify security flaws on a monthly basis.

The evaluation team should verify that all high-risk vulnerabilities identified by the automated vulnerability scanning tools or static code analysis tools have been remediated or addressed through a compensating control (such as a web application firewall) within 15 days of discovery.

The evaluation team should verify that application vulnerability scanning tools have successfully completed their regular scans for the previous 30 cycles of scanning by reviewing archived alerts and reports to ensure that the scan was completed. If a scan was not completed successfully, the system should alert or send email to enterprise administrative personnel indicating what happened. If a scan could not be completed in that timeframe, the evaluation team should verify that an alert or email was generated indicating that the scan did not finish.

CSC 19: Incident Response and Management|Effectiveness Test

None.

CSC 20: Penetration Tests and Red Team Exercises|Effectiveness Test

None.

History

Document history		
V1.1.1	August 2016	Publication