ETSI TR 103 305-1 V2.1.1 (2016-08)

CYBER;
Critical Security Controls for Effective Cyber Defence;
Part 1: The Critical Security Controls

Reference

RTR/CYBER-0012-1

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

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 1 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence, as identified below:

Part 1: "The Critical Security Controls";

Part 2: "Measurement and auditing";

Part 3: "Service Sector Implementations";

Part 4: "Facilitation Mechanisms".

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 captures and describes the top twenty Enterprise industry level cybersecurity best practices that provide enhanced cyber security, developed and maintained by the Center for Internet Security (CIS) (formerly the Council on CyberSecurity) as an independent, expert, global non-profit organization. The CIS provides ongoing development, support, adoption, and use of the Critical Security Controls [i.1]. The Controls reflect the combined knowledge of actual attacks and effective defences of experts from every part of the cyber security ecosystem. This ensures that the Controls are an effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The Controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions. The defences identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defence and response capability that can be maintained and improved. The five critical tenets of an effective cyber defence system as reflected in the Critical Security Controls are:

- Offense informs defence: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defences. Include only those controls that can be shown to stop known real-world attacks.

- Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in a computing environment.
- Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
- Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures, and to help drive the priority of next steps.
- Automation: Automate defences so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

Introduction

The evolution of cyber defence is increasingly challenging. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to privacy, denial of service - these have become endemic. Access exists to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogues of security controls, and countless security checklists, benchmarks, and recommendations.

But all of this technology, information, and oversight has become a veritable "Fog of More:" competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings great benefits, but it also means that data and applications are now distributed across multiple locations, many of which are not within the organization's infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem.

Focus is needed to establish priority of action, collective support, and keeping knowledge and technology current in the face of rapidly evolving problems and an apparently infinite number of possible solutions. The most critical areas need to be addressed and the first steps taken toward maturing risk management programs. This includes a roadmap of fundamentals, and guidance to measure and improve the implementation defensive steps that have the greatest value. These issues led to, and drive, the Critical Security Controls. The value is determined by knowledge and data - the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Initiating Implementation

Some of the Critical Security Controls, in particular CSC 1 through CSC 5, are foundational, and are the primary recommended actions to be taken. This is the approach taken by, for example, the DHS Continuous Diagnostic and Mitigation (CDM) Program. A similar approach is recommended by the Australian Signals Directorate (ASD) with their "Top Four Strategies to Mitigate Targeted Intrusions" - a well-regarded and demonstrably effective set of cyber-defense actions that map very closely into the CIS Critical Security Controls.

1 Scope

The present document describes 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 measures reflect the combined knowledge of actual attacks and effective defences.

The present document is technically equivalent and compatible with The Center for Internet Cybersecurity [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: "Critical Security Controls for Effective Cyber Defense Version 6.0," October 15, 2015.

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

[i.2] NIST SP 800-57 Part 1-Rev. 4: "Recommendation for Key Management".

[i.3] IEEE 802.1X-2010: "Port Based Network Access Control".

[i.4] ETSI TR 103 305-2: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing".

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

NOTE: Found at the website https://www.cisecurity.org/critical-controls.cfm.

quick win: actions that can be relatively easily taken with minimal resources that have a significant cyber security benefit

3.2 Abbreviations

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

802.1x	Institute of Electrical and Electronic Engineers Standard for Port-based Network Access Control [i.3]
ACK	ACKnowledge
ACL	Access Controls List
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
ASD	Australian Signals Directorate
ASLR	Address Space Layout Randomization
BYOD	Bring Your Own Device
C2	Command and Control
CCE™	Common Configuration Enumeration
CD	Compact Disc
CDM	Continuous Diagnostic and Mitigation
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
CPE™	Common Platform Enumeration
CSC	Critical Security Control or Capability
CVE®	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DBIR	Data Breach Investigations Report
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DMZ	DeMilitarized Zone
DNS	Domain Name System
DVD	Digital Versatile Disc or Digital Video Disc
EAP	Extensible Authentication Protocol
EMET	Enhanced Mitigation Experience Toolkit
HSM	Hardware Security Modules
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	IDentifier
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NAC	Network Access Control
NIST	National Institute of Standards and Technology
OTP	One Time Password
OVAL®	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
RDP	Remote Desktop Protocol
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Program
SEM	Security Event Manager
SIEM	Security Information Event Management or Security Incident Event Management
SIM	Subscriber Information Module
SP	Special Publication
SPF	Sender Policy Framework
SQL	Structured Query Language
SSL	Secure Sockets Layer

SYN	SYNchronize
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VNC	Virtual Channel Network
VPN	Virtual Private Network
WAF	Web Application Firewall
WIDS	Wireless Intrusion Detection System
WPA2	Wi-Fi Protected Access II
XCCDF	Extensible Configuration Checklist

NOTE: CPE®, CVE™, OVAL® and CCE™ are trademarks of The MITRE Corporation operating as a non-profit Federally Funded Research and Development Center (FFRDC) of the U.S. Department of Homeland Security. See http://stixproject.github.io/legal/. Both CVE® and OVAL® are registered service marks. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the product named. Equivalent products may be used if they can be shown to lead to the same results.

4 Critical Security Controls

4.0 Structure of the Critical Security Controls Document

The presentation of each Critical Security Control in the present document includes:

- A description of the importance of the Control (Why is This Control Critical) in blocking or identifying presence of attacks and an explanation of how attackers actively exploit the absence of this control.
- A chart of the specific actions ("sub-controls") that organizations are taking to implement, automate, and measure effectiveness of this control.
- Procedures and Tools that enable implementation and automation.
- Sample Entity Relationship Diagrams that show components of implementation.

In addition to the present document, ETSI TR 103 305-2 [i.4], can be referenced for implementing each control.

4.1 CSC 1: Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why Is This Control Critical?

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to the network. Attackers also look for devices (especially laptops) which come and go off of the enterprise's network, and so get out of synch with patches or security updates. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal jump points or victims. Additional systems that connect to the enterprise's network (e.g. demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

As new technology continues to come out, BYOD (bring your own device) - where employees bring personal devices into work and connect them to the enterprise network - is becoming very common. These devices could already be compromised and be used to infect internal resources.

Managed control of all devices also plays a critical role in planning and executing system backup and recovery.

Table 1: CSC 1: Inventory of Authorized and Unauthorized Devices

CSC 1: Inventory of Authorized and Unauthorized Devices		
Family	**Control**	**Control Description**
System	1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
System	1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
System	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
System	1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created should also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data should be identified, regardless of whether they are attached to the organization's network.
System	1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x should be tied into the inventory data to determine authorized versus unauthorized systems [i.3].
System	1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.

CSC 1 Procedures and Tools

This Control includes both technical and procedural actions, united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. It links to business governance by establishing information/asset owners who are responsible for each component of a business process that includes information, software, and hardware. Organizations can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Others use more modest tools to gather the data by sweeping the network, and manage the results separately in a database.

Maintaining a current and accurate view of IT assets is an ongoing and dynamic process. Organizations can actively scan on a regular basis, sending a variety of different packet types to identify devices connected to the network. Before such scanning can take place, organizations should verify that they have adequate bandwidth for such periodic scans by consulting load history and capacities for their networks. In conducting inventory scans, scanning tools could send traditional ping packets (e.g. ICMP Echo Request) looking for ping responses to identify a system at a given IP address. Because some systems block inbound ping packets, in addition to traditional pings, scanners can also identify devices on the network using transmission control protocol (TCP) synchronize (SYN) or acknowledge (ACK) packets. Once they have identified IP addresses of devices on the network, some scanners provide robust fingerprinting features to determine the operating system type of the discovered machine.

In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.

Many organizations also pull information from network assets such as switches and routers regarding the machines connected to the network. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization's asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network [i.3].

Wireless devices (and wired laptops) may periodically join a network and then disappear, making the inventory of currently available systems very dynamic. Likewise, virtual machines can be difficult to track in asset inventories when they are shut down or paused. Additionally, remote machines accessing the network using virtual private network (VPN) technology may appear on the network for a time, and then be disconnected from it. Whether physical or virtual, each machine using an IP address should be included in an organization's asset inventory.

CSC 1 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.

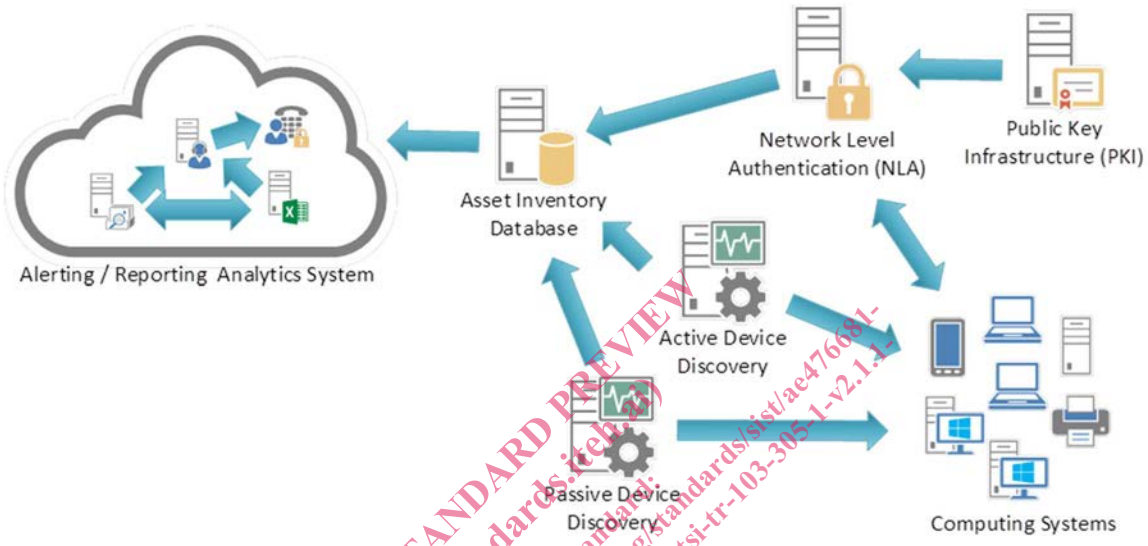

Figure 1

4.2 CSC 2: Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why Is This Control Critical?

Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

Managed control of all software also plays a critical role in planning and executing system backup and recovery.

Table 2: CSC 2: Inventory of Authorized and Unauthorized Software

CSC 2: Inventory of Authorized and Unauthorized Software		
Family	**Control**	**Control Description**
System	2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
System	2.2	Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.
System	2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
System	2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

CSC 2 Procedures and Tools

Whitelisting can be implemented using a combination of commercial whitelisting tools, policies or application execution tools that come with anti-virus suites and with operating systems. Commercial software and asset inventory tools are widely available and in use in many enterprises today. The best of these tools provide an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.

Features that implement whitelists are included in many modern endpoint security suites. Moreover, commercial solutions are increasingly bundling together anti-virus, anti-spyware, personal firewall, and host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), along with application white and black listing. In particular, most endpoint security solutions can look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these tools offer custom whitelists based on executable path, hash, or regular expression matching. Some even include a gray list function that allows administrators to define rules for execution of specific programs only by certain users and at certain times of day.

CSC 2 System Entity Relationship Diagram

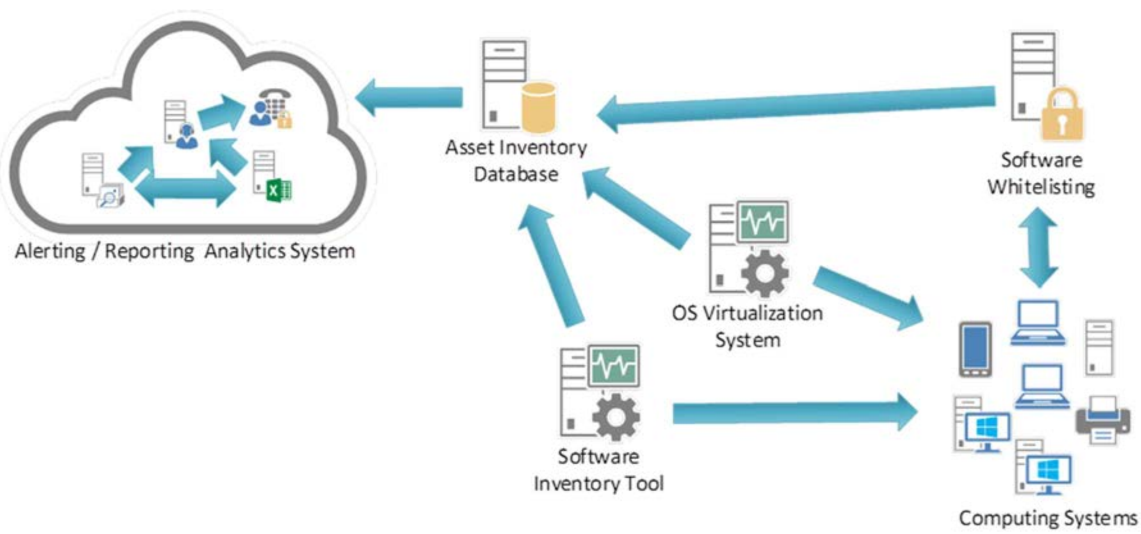

Figure 2

4.3 CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why Is This Control Critical?

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared to ease-of-deployment and ease-of-use - not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices (the Procedures and Tool section below provides resources for secure configurations). Even if a strong initial configuration is developed and installed, it should be continually managed to avoid security "decay" as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network-accessible services and client software..

Table 3: CSC 3: Secure Configurations for Hardware and Software

CSC 3: Secure Configurations for Hardware and Software		
Family	**Control**	**Control Description**
System	3.1	Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
System	3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.
System	3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.
System	3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.
System	3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the Su or Sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).
System	3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

CSC 3: Secure Configurations for Hardware and Software		
Family	**Control**	**Control Description**
System	3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows® systems or Puppet for Unix systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

CSC 3 Procedures and Tools

Rather than start from scratch developing a security baseline for each software system, organizations should start from publicly developed, vetted, and supported security benchmarks, security guides, or checklists. Excellent resources include:

- The Center for Internet Security Benchmarks Program (https://www.cisecurity.org/).
- The NIST National Checklist Program (https://web.nvd.nist.gov/view/ncp/repository).

Organizations should augment or adjust these baselines to satisfy local policies and requirements, but deviations and rationale should be documented to facilitate later reviews or audits.

For a complex enterprise, the establishment of a single security baseline configuration (for example, a single installation image for all workstations across the entire enterprise) is sometimes not practical or deemed unacceptable. It is likely that one will need to support different standardized images, based on the proper hardening to address risks and needed functionality of the intended deployment.

EXAMPLE: A web server in the DMZ vs. an email or other application server in the internal network.

The number of variations should be kept to a minimum in order to better understand and manage the security properties of each, but organizations then should be prepared to manage multiple baselines.

Commercial and/or free configuration management tools can then be employed to measure the settings of operating systems and applications of managed machines to look for deviations from the standard image configurations. Typical configuration management tools use some combination of an agent installed on each managed system, or agentless inspection of systems by remotely logging in to each managed machine using administrator credentials. Additionally, a hybrid approach is sometimes used whereby a remote session is initiated, a temporary or dynamic agent is deployed on the target system for the scan, and then the agent is removed.

CSC 3 System Entity Relationship Diagram

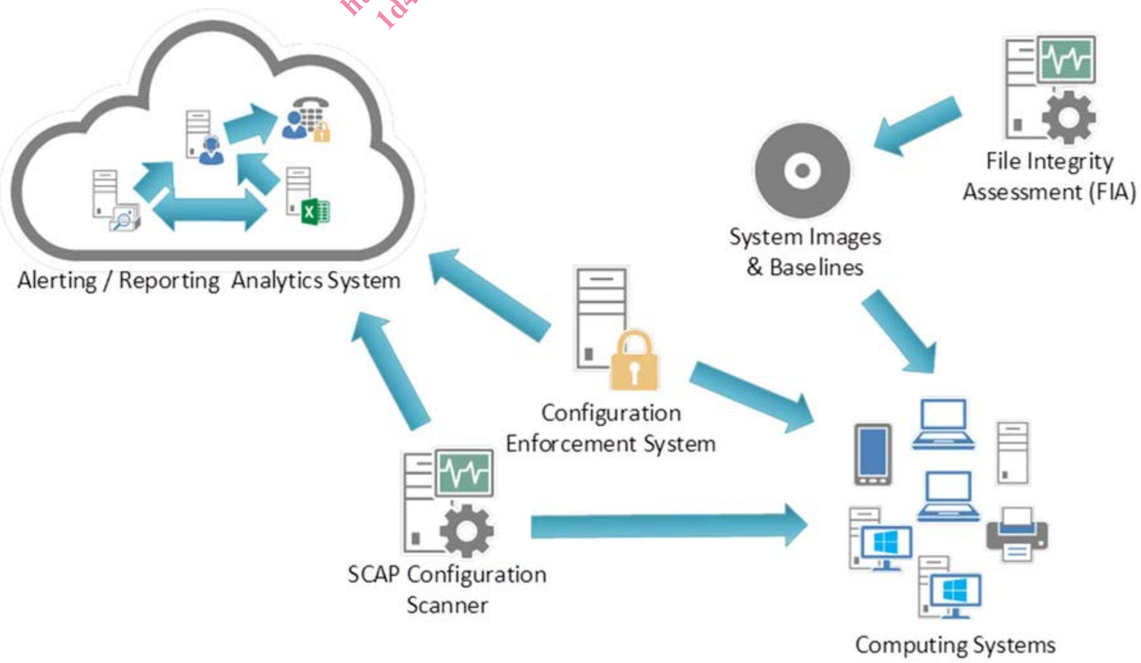

Figure 3