ETSI TR 103 305 V1.1.1 (2015-05)

TECHNICAL REPORT

CYBER;
Critical Security Controls for Effective Cyber Defence

Reference

DTR/CYBER-003

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
http://portal.etsi.org/tb/status/status.asp

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 (http://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).

Modal verbs terminology

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

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

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 Council on CyberSecurity as an independent, expert, global non-profit organization. The Council provides ongoing development, support, adoption, and use of the Critical Controls [i.5]. See (www.counciloncybersecurity.org). The Critical Security 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 5 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 your 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 have become a veritable "Fog of More": competing options, priorities, opinions, and claims. The threats have evolved, the actors have become smarter, and users have become more mobile. Data is now distributed across multiple locations, many of which are not within our organization's infrastructure anymore. With more reliance on cloud computing data centres, the data and even applications are becoming more distributed. In a complex, interconnected world, no enterprise can think of its security as a standalone problem, and collective action is nearly impossible.

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.

The Critical Security Controls and Other Risk Management Approaches

The Critical Security Controls are not a replacement for comprehensive mandatory compliance or regulatory schemes. The Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff.

Although lacking the formality of traditional Risk Management Frameworks, the Critical Security Controls process constitutes a "foundational risk assessment" - one that can be used by an individual enterprise as a starting point for immediate, high-value action, is demonstrably consistent with formal risk management frameworks, and provides a basis for common action across diverse communities (e.g. that might be subject to different regulatory or compliance requirements).

The Critical Security Controls also proactively align with and leverage ongoing work in security standards and best practices. Examples include: the Security Content Automation Program (SCAP) and Special Publication 800-53 [i.1] (Recommended Security Controls for Federal Information Systems and Organizations) sponsored by the National Institute of Standards and Technology (NIST); the Australian Signals Directorate's "Top 35 Strategies to Mitigate Targeted Cyber Intrusions"; and the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002:2013 [i.4] Information technology - Security techniques - Code of practice for information security controls. References and mappings to these can be found at www.counciloncybersecurity.org.

Initiating Implementation

Some of the Critical Security Controls, in particular CSC 1 through CSC 5, are foundational, and should be considered as the actions to be taken. This is the approach taken by, for example, the DHS Continuous Diagnostic and Mitigation (CDM) Program.

For a highly focused and direct starting point, five especially useful actions have the most immediate impact on preventing attacks. These actions are specially noted in the Controls listings, and consist of:

1) application whitelisting (found in CSC 2);

2) use of standard, secure system configurations (found in CSC 3);

3) patch application software within 48 hours (found in CSC 4);

4) patch system software within 48 hours (found in CSC 4); and

5) reduced number of users with administrative privileges (found in CSC 3 and CSC 12).

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 5.1 version of the "The Critical Security Controls for Effective Cyber Defence," 10 July 2014, which can be found at the website http://www.counciloncybersecurity.org/critical-controls/.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

The following referenced documents are necessary for the application of the present document.

Not applicable.

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] NIST Special Publication 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations".

[i.2] NIST Special Publication 800-57: "Recommendation for Key Management - Part 1: General".

[i.3] NIST Special Publication 800-132: "Recommendation for Password-Based Key Derivation - Part 1: Storage Applications".

[i.4] ISO/IEC 27002:2013: "Information technology -- Security techniques -- Code of practice for information security controls".

[i.5] Council on Cybersecurity: "The Critical Security Controls for Effective Cyber Defence".

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 Council on Cybersecurity and found at the website http://www.counciloncybersecurity.org/critical-controls/

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
ACK	Acknowledge
ACL	Access Controls List
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
ASLR	Address Space Layout Randomization
BYOD	Bring Your Own Device
C2	Command and Control
CA	Certificate Authority
CCE$^{\text{TM}}$	Common Configuration Enumeration
CD	Compact Disc
CDM	Continuous Diagnostic and Mitigation
CP	Certificate Policy
CPE$^{\text{TM}}$	Common Platform Enumeration
CPS	Certificate Practice Statement
CSC	Critical Security Control or Capability
CVE$^{\text{TM}}$	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMZ	demilitarized zone
DNS	Domain Name system
DVD	Digital Versatile Disc or Digital Video Disc
EAP	Extensible Authentication Protocol
EICAR	European Expert Group for IT-Security
EMET	Enhanced Mitigation Experience Toolkit
FTP	File Transfer Protocol
HSM	Hardware Security Modules
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identifier
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
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
NICE	National Initiative on Cybersecurity Education
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OTP	One Time Password
OVAL®	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
RDP	Remote Desktop Protocol
SANS	SysAdmin, Audit, Networking, and Security
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Program
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
UTC	Universal Time Coordinated
VLAN	Virtual Local Area Network
VMS	Vulnerability Management System
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
XML	Extensible Markup Language

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 in blocking or identifying presence of attacks and an explanation of how attackers actively exploit the absence of this control.

- Listing of the specific actions that organizations are taking to implement, automate, and measure effectiveness of this control. The sub-controls are grouped into four categories:

  - Easy actions that provide significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide such substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

  - Visibility and attribution measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

  - Improved information security configuration and hygiene to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

- Advanced sub-controls that use new technologies or procedures that provide maximum security but are harder to deploy or more expensive or require more highly skilled staff than commoditized security solutions.

- Procedures and tools that enable implementation and automation.
- Metrics and tests to assess implementation status and effectiveness.
- Sample entity relationship diagrams that show components of implementation.

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 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.

How to Implement This Control

Table 1

ID #	Description	Category
CSC 1-1	Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analysing their traffic should be employed.	*Quick win*
CSC 1-2	Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.	*Quick win*
CSC 1-3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	*Quick win*
CSC 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 has to 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 have to be identified, regardless of whether they are attached to the organization's network.	Visibility/ Attribution
CSC 1-5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x has to be tied into the inventory data to determine authorized versus unauthorized systems.	Configuration/ Hygiene
CSC 1-6	Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.	Configuration/Hygiene

ID #	Description	Category
CSC 1-7	Utilize client certificates to validate and authenticate systems prior to connecting to the private network.	Advanced

CSC 1 Procedures and Tools

This Control requires 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 the business 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 (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 looking 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.

Wireless devices (and wired laptops) may periodically join a network and then disappear, making the inventory of currently available systems churn significantly. 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 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1) How long does it take to detect new devices added to the organization's network (time in minutes)?

2) How long does it take the scanners to alert the organization's administrators that an unauthorized device is on the network (time in minutes)?

3) How long does it take to isolate/remove unauthorized devices from the organization's network (time in minutes)?

4) Are the scanners able to identify the location, department, and other critical details about the unauthorized system that is detected (yes or no)?

CSC 1 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

1) How many unauthorized devices are presently on the organization's network (by business unit)?

2) How long, on average, does it take to remove unauthorized devices from the organization's network (by business unit)?

3) What is the percentage of systems on the organization's network that are not utilizing Network Access Control (NAC) to authenticate to the organization's network (by business unit)?

4) What is the percentage of systems on the organization's network that are not utilizing Network Access Control (NAC) with client certificates to authenticate to the organization's network (by business unit)?

CSC 1 Effectiveness Test

To evaluate the implementation of Control 1 on a periodic basis, the evaluation team will 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 have to be included in the asset inventory database, while the other systems are not. The evaluation team has to then verify that the systems generate an alert or e-mail notice regarding the newly connected systems within 24 hours of the test machines being connected to the network. The evaluation team has to 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 has to also verify that the system provides information about the asset owner.

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.

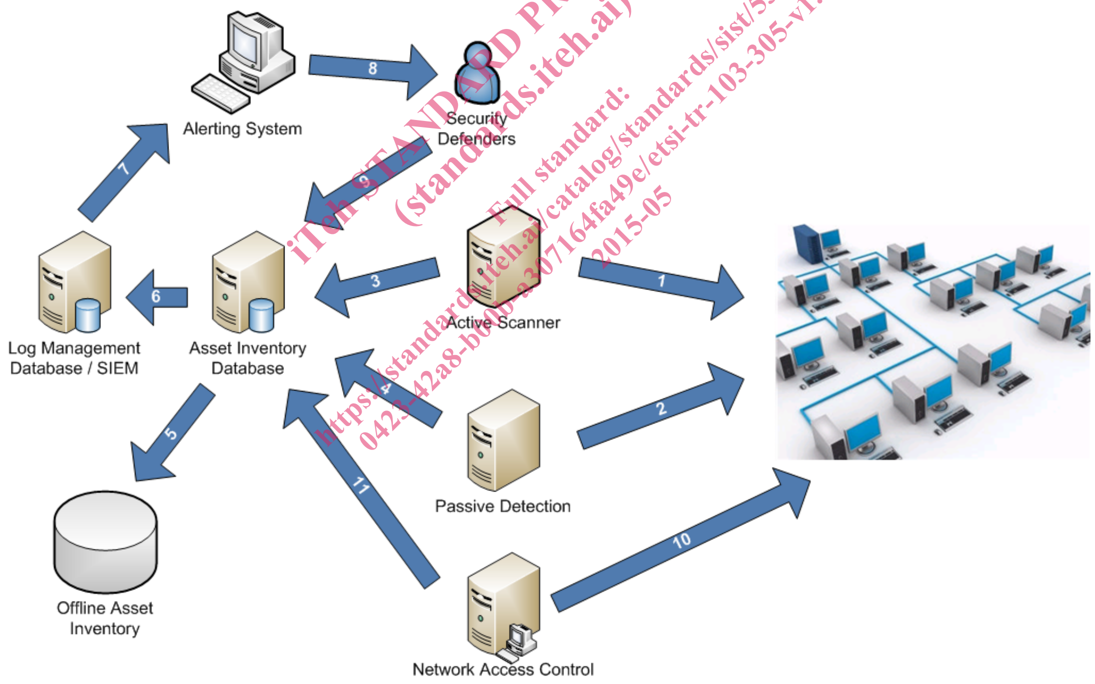

Figure 1

A control system is a device or set of devices used to manage, command, direct, or regulate the behaviour of other devices or systems. In this case, we are examining hardware devices on the organization's network. These systems should be able to identify if new systems are introduced into the environment that have not been authorized by enterprise personnel. The following list of the steps in figure 1 shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

- Step 1: Active device scanner scans network systems.
- Step 2: Passive device scanner captures system information.
- Step 3: Active scanner reports to inventory database.

- Step 4: Passive scanner reports to inventory database.
- Step 5: Inventory database stored offline.
- Step 6: Inventory database initiates alert system.
- Step 7: Alert system notifies security defenders.
- Step 8: Security defenders monitor and secure inventory database.
- Step 9: Security defenders update secure inventory database.
- Step 10: Network access control continuously monitors network.
- Step 11: Network access control checks and provides updates to the asset inventory database.

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.

How to Implement This Control

Table 2

ID #	Description	Category
CSC 2-1	Deploy application whitelisting technology 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. When protecting systems with customized software that may be seen as difficult to whitelist, use item 8 below (isolating the custom software in a virtual operating system that does not retain infections).	*Quick win (One of the "First Five")*
CSC 2-2	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.	Quick win

ID #	Description	Category
CSC 2-3	Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components).	Quick win
CSC 2-4	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. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level.	Visibility/ Attribution
CSC 2-5	The software inventory systems have to be integrated with the hardware asset inventory so that all devices and associated software are tracked from a single location.	Visibility/ Attribution
CSC 2-6	Dangerous file types (e.g. .exe, .zip, .msi) should be closely monitored and/or blocked.	Configuration/ Hygiene
CSC 2-7	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.	Advanced
CSC 2-8	Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.	Advanced
CSC 2-9	Deploy software that only provides signed software ID tags. A software identification tag is an XML file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management.	Advanced

CSC 2 Procedures and Tools

Whitelisting can be implemented using commercial whitelisting tools or application execution tools that come with anti-virus suites and with Windows®. 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 of programs allowed to run 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 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1) How long does it take to detect new software installed on systems in the organization (time in minutes)?

2) How long does it take the scanners to alert the organization's administrators that an unauthorized software application is on a system (time in minutes)?

3) How long does it take to alert that a new software application has been discovered (time in minutes)?

Are the scanners able to identify the location, department, and other critical details about the unauthorized software that is detected (yes or no)?