Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Top 10 IT security actions: Number 4 harden operating systems and applications

Management

ITSM.10.090

Canada

Foreword

This is an UNCLASSIFIED publication issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email or phone our Contact Centre:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on Month XX, 2024.

Revision history

Revision	Amendments	Date
1	First release.	Month XX, 2024

D97-4/10-090-2024E-PDF
978-0-660-71584-1

Overview

One of our top 10 recommended IT security actions is to harden operating systems (OS) and applications (apps). One way to harden OS and applications is by configuring them with additional security features. This document outlines the various actions you can take when hardening your OS and applications to ensure that your organizational networks and systems are protected against common cyber threats. The guidance in this document is based on the security controls from IT security risk management: A lifecycle approach (ITSG-33) [1].

This publication is part of a suite of publications that focuses on the recommendations found in the Cyber Centre's Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089) [2]. While implementing all 10 of the recommended security actions can reduce your organization's vulnerability to cyber threats, you should review your current cyber security activities to determine whether additional actions are required.

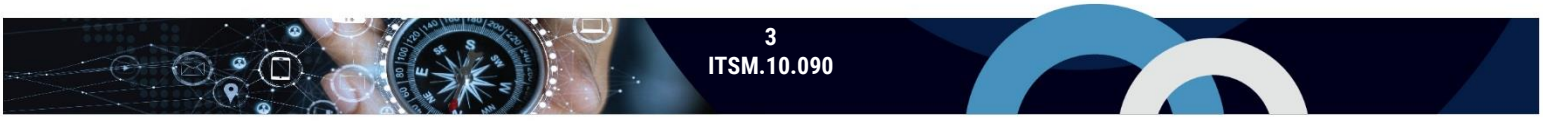


Table of contents

List of figures

List of tables

List of annexes

1 Introduction

To prevent compromises to Internet-connected assets and infrastructures, we have outlined 10 recommended security actions in Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089) [2]. Included are recommendations for hardening OS and applications. Your organization should be aware of all the applications being used and inventory them as part of you overall asset inventory process.

To ensure you are safeguarding these applications and the information they use, you should apply additional security controls to harden operating systems and applications. The use of the default, out-of-the-box configuration does not provide an adequate level of security for most organizations. By applying the security controls noted in this publication, your organization will enhance the configuration and protection of your OS and applications. For more information on selecting and applying security controls, see IT security risk management: A lifecycle approach (ITSG-33) [1].

To prevent compromises of Internet-connected assets and infrastructures, your organization should deactivate all nonessential ports (for example, transmission control protocol (TCP) and user datagram protocol (UDP)) and services and remove all unnecessary accounts. Assess all third-party applications for components or functions that are not needed and should be deactivated or require human intervention before they are activated, like macros. You should also have enterprise-level auditing and an anti-malware solution as part of your secure configuration for your systems.

If using cloud or managed services, your provider may be responsible for hardening OS and applications, depending on your service and deployment models. For example, in an infrastructure as a service (IaaS) or a platform as a service (PaaS) model, your organization is responsible for hardening OS and applications. In a software as a service (SaaS) model, the cloud service provider (CSP) is responsible for hardening OS and applications. Your organization is responsible for all its on-premises (on-prem) equipment when incorporating any hybrid components or solutions.

Procuring the assistance of a managed security services provider (MSSP) may be beneficial for your organization. An MSSP can assist in your hardening efforts including determining and implementing your baseline configuration settings, endpoint detection and monitoring, managed firewalls and anti-virus services.

Regardless of your environment, you should confirm with vendors whether they incorporate the following when selecting OS and apps for your organization:

- commitment to built-in security controls (for example, secure-by-design principles)
- demonstratable security practices (for example, secure programming)
- ongoing review and maintenance of the security of their products

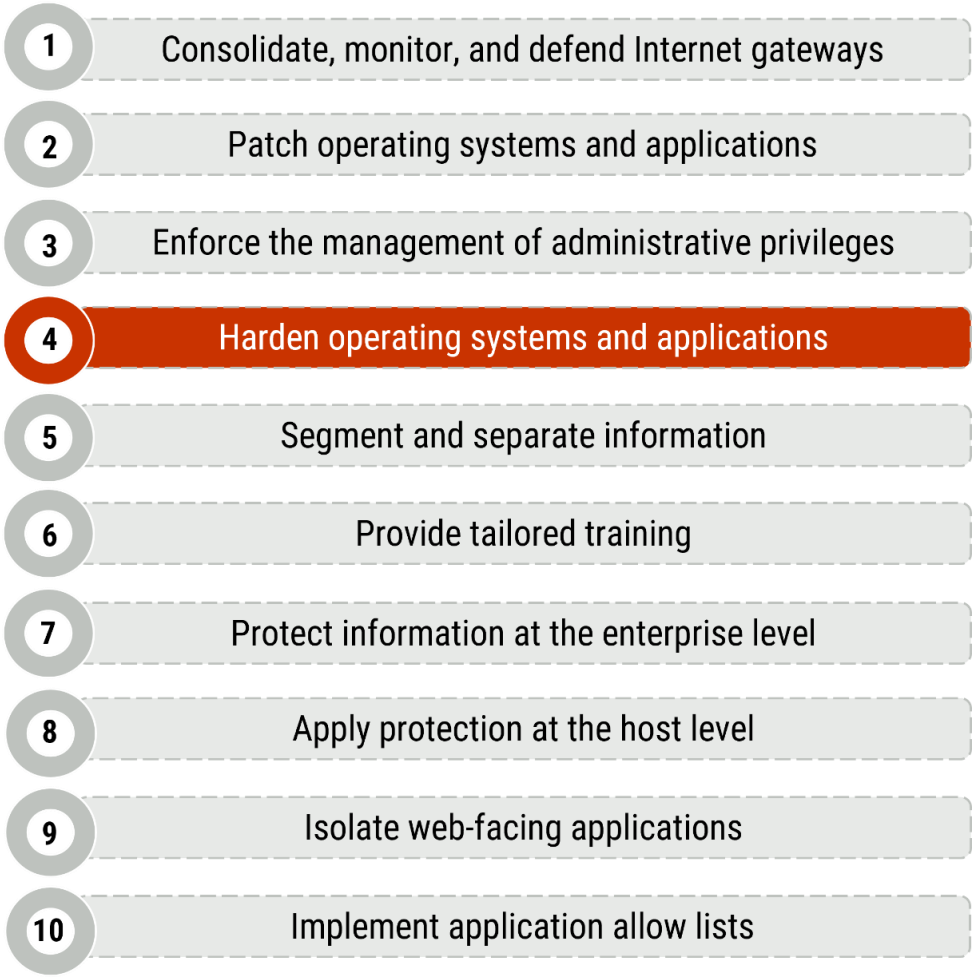
2 Top 10 IT security actions

This document provides guidance on hardening OS and applications. Hardening your organization's OS and applications reduces your organization's exposure to cyber threats that could compromise your networks, systems and IT assets. This guidance is based on the advice in Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089) [2] and the security controls listed in Annex 3A - Security control catalogue (ITSG-33) [2].

Our top 10 recommended IT security actions, which are listed in Figure 1 below, are based on our analysis of trends in cyber security threat activities and the impact of those threat activities on Internet-connected networks. By implementing all 10 actions, you can address many of your organization's IT security vulnerabilities.

Cyber security threats that are common to many organizations may impact you differently. To ensure your organization's security needs are appropriately met, review your current security and risk management activities.

Figure 1: Top 10 IT security actions – Number 4 harden operating systems and applications



Long description: Figure 1 provides a list of the top 10 IT security actions. Item number 4. Harden operating systems and applications, is highlighted as it is the security action that applies to this publication. Figure 1 includes the following 10 items in the list:

1. Consolidate, monitor, and defend internet gateways
2. Patch operating systems and applications
3. Enforce the management of administrative privileges
4. **Harden operating systems and applications**
5. Segment and separate information
6. Provide tailored training
7. Protect information at the enterprise level
8. Apply protection at the host level
9. Isolate web-facing applications
10. Implement application allow lists

2.1 Relationship to the IT security risk management process

Our top 10 security actions are taken from the security controls listed in Annex 3A of ITSG-33 [2]. ITSG-33 [2] describes the roles, responsibilities and activities that help organizations manage their IT security risks. It also includes a catalogue of security controls, such as standardized security requirements to protect the confidentiality, integrity, and availability of IT assets. These security controls are divided into the following 3 classes, which are further divided into several families (or groupings) of related security controls:

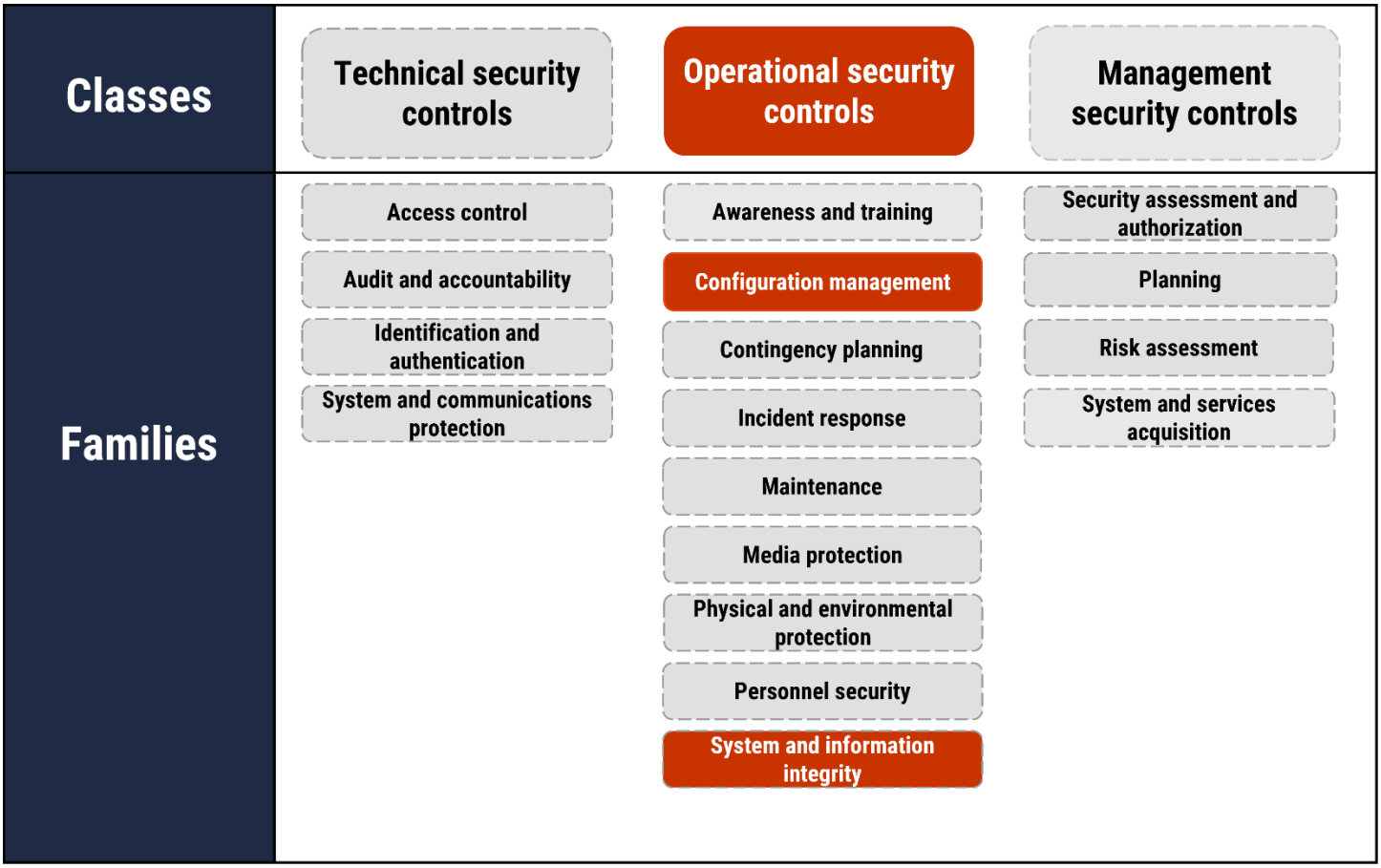
- **Technical security controls:** Security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software and firmware components
- **Operational security controls:** Information system security controls that are primarily implemented and executed by people and typically supported using technology, such as supporting software
- **Management security controls:** Security controls that focus on management IT security and IT security risks

As illustrated in Figure 2 below, this document addresses operational security controls that fall under the Configuration Management (CM) and System and Information Integrity (SI) control families, such as:

- **CM-2 Baseline configuration**
- **CM-6 Configuration settings**
- **CM-7 Least functionality**
- **SI-3 Malicious code protection**
- **SI-4 Information system monitoring**

See Annex A of this document for more information on controls CM-2, CM-6, CM-7, SI-3, and SI-4.

Figure 2: Applicable security control classes and families as described in ITSG-33



Long description: As depicted in Figure 2 with highlighted text, this publication focuses on technical, operational, and management security controls. It includes some of the actions that fall under the Access Control and System and Communication Protection control families.

The full list of classes of security controls and their related control families or groupings is also presented in Figure 2, as follows:

Technical security controls

- Access control
- Audit and accountability
- Identification and authentication
- System and communications protection

Operational security controls

- Awareness and training
- **Configuration management**

- Contingency planning
- Incident response
- Maintenance
- Media protection
- Physical and Environmental Protection
- Personnel Security
- **System and Information Integrity**

Management security controls

- Security assessment and authorization
- Planning
- Risk assessment
- System and services acquisition

3 An introduction to hardening operating system and applications

To protect your network, systems, and data we recommend your organization harden your OS and all applications in use. Hardening is a process intended to eliminate a threat actor's ability to leverage attack vectors by patching vulnerabilities and turning off nonessential services. Your organization should apply security updates, patches, and service packs to your OS and apps, including those provided by a third party as soon as they are available. Your vulnerability management approach should be based on your organization's risk assessment. Automating these processes will alleviate some of the resource requirements to monitor and apply these processes and ensure your OS is running in the least vulnerable state possible.

There may be instances when non-security-related updates and patches to your OS may have an overall negative impact to the security posture of your organization's services, as these updates can add new services or change the behaviour of existing services.

Hardening also involves proper configuration management when deploying new applications and systems. While allowing OS and applications to be installed and run with out-of-box configurations may save time and seem more convenient, this deployment and use can pose significant risks to your organization.

The National Institute for Standards and Technology's (NIST) National Checklist Program for IT products: Guidelines for checklist users and developers (SP 800-70 Rev. 4) [3] contains a repository of security checklists or benchmarks that provide organizations with guidance on setting the security configurations for OS and applications. Using these checklists can minimize your attack surface, reduce vulnerabilities to your network, lessen the impact of successful attacks on your organization, and identify changes that should be made or might otherwise have gone undetected.

While configurations should be done at the beginning of the OS or application deployment cycle, it may also be necessary to reconfigure these components as your operational needs and security requirements evolve. Before reconfiguring or upgrading your IT systems or their components, your organization should consider your specific business needs and security requirements by:

- identifying all enterprise architecture design and security requirements
- completing a threat and risk assessment
- identifying hardware and firmware components for endpoint devices
- controlling all applications used in your organization

3.1 Enterprise architecture design and security requirements

All enterprise architecture design and security requirements should be identified before applying the recommendations in this document. A full picture of the complete enterprise architecture will help your organization identify the appropriate security features and tools for your business needs and security requirements. Once security features and tools are implemented, your organization should continue to monitor these features and tools as a part of your ongoing risk management activities. Regular monitoring ensures security controls continue to be effective.

3.2 Hardening guidelines and frameworks

Your organization's hardening guidance should be followed as closely as possible, as it was developed with the intention of mitigating or blocking specific threat vectors. If a need to deviate from the hardening guidance should arise, your IT security team should fully understand the risks associated with the deviation and be prepared to mitigate the potential threat vectors that might be created as a result. Your organization should exercise caution in deviating from your hardening guidance.

There are several hardening guidelines or frameworks available. The following subsections provide an overview of the 3 most prominent guidelines available to organizations.

3.2.1 Center for Internet Security guidelines

The Center for Internet Security (CIS) has established hardening benchmarks for organizations of all sizes and all geographical locations to follow to harden IT assets. The benchmarks are best practices and baseline configurations that they recommend to securely configure an application or system. The benchmarks are "consensus-based" which means they are established and agreed upon by a large group of cyber security experts and industry subject matter experts. These benchmarks are generally accepted across governments, business, various industries, and academia.

3.2.2 Defense Information Systems Agency guidelines

The Defense Information Systems Agency releases Security Technical Implementation Guides (STIGs) that provide guidance and compliance benchmarks for organizations. While STIGs provide specific requirements and guidance for United States government departments, like the Department of Defense, they are useful starting points for all organizations. STIGs are reliable and are derived from thorough research conducted by subject matter experts. STIGs provide baselines and guidance for many operating systems, applications, and devices. These baselines are meant to make your hardware and software as secure as possible. STIGs also provide guidance on network management, configuration, and monitoring. It is important to note that not all STIG targets or baselines are applicable to Canadian organizations.

3.2.3 National Security Agency and Cybersecurity and Infrastructure Security Agency guidance

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) have released several guidance pieces on hardening devices, OS, and applications. Most notably, they jointly released the Kubernetes Hardening Guide [4] technical report. CISA has also released Key Findings to Improve Monitoring and Hardening of Networks [5] and a joint technical report.

The Kubernetes Hardening Guide [5] provides recommendations on configuration and hardening guidance for setting up and securing a Kubernetes cluster. Kubernetes is an open-source system, often hosted in a cloud environment, that automates deployment, scaling, and management of applications run in containers. A container is a runtime environment that contains a software package and its dependencies.

Key Findings to Improve Monitoring and Hardening of Networks [5] provides details on the activities and key findings from a CISA red team assessment. The guidance provides recommendations for improving your cyber security posture. It also

provides key hardening actions to take immediately that will improve the security of your organization's environment. The immediate actions recommended are:

- Establish a security baseline of normal network activity, tune network and host-based appliances to detect anomalous behaviour
- Conduct regular assessments to ensure appropriate procedures are created and can be followed by security staff and end user
- Enforce phishing-resistant multi-factor authentication (MFA) to the greatest extent possible

For more information on implementing and enforcing MFA, see Steps for effectively deploying multi-factor authentication (MFA) - ITSAP.00.105 [6].

There are several mitigation measures noted by CISA that align with their Cross-Sector Cybersecurity Performance Goals (CPGs). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cyber security frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. For more information on the CPGs, see Cross-Sector Cybersecurity Performance Goals [7].

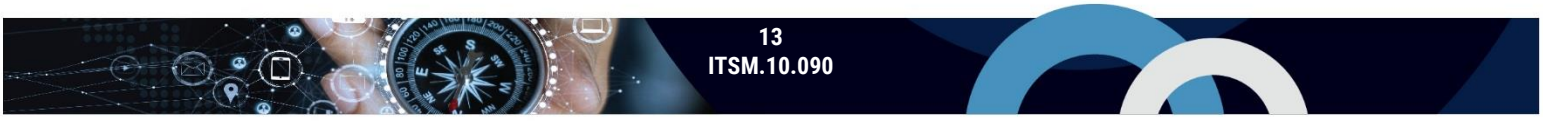
3.3 Hardware and firmware

Your organization should consider your hardware and firmware when buying and implementing endpoint devices, such as servers, desktops, laptops, mobile devices, and tablets. New endpoint devices should be set up with the hardware and firmware components identified in your device guidelines.

To leverage security functionality within your devices and OS, the following hardware and firmware components should be in place:

- unified extensible firmware interface (UEFI) to activate Secure Boot:
  - UEFI should not be configured to run in legacy basic input and output system (BIOS) mode
  - UEFI must support secure firmware updates
- trusted platform module (TPM) 2.0 (devices that use TPM 1.2 can be upgraded)
- hard drive formatting with global unique identifier (GUID) partition table (not master boot record [MBR] formatting)
- hypervisor code integrity to accordance with your OS, like Device Guard for Windows
- 64-bit CPU with Intel virtualization technology (VT-x) or Advanced Micro Dynamics virtualization (AMD-V) and extended page tables (also called second level address translation [SLAT])

Mobile devices and tablets must also be included in your organization's hardening plans. The guidance in this publication is also applicable to on-prem and mobile devices.



3.4 Authentication systems

Your organization should harden your authentication systems by securing your applications' authentication pathways. To do this, you should conduct the following activities:

- Change the default passwords on the server
- Review the authentication workflow and identify logic errors in which threat actors could use to exploit your systems
- Remove outdated algorithms
- Deactivate or delete unnecessary accounts
- Implement a privilege access management (PAM) solution
- Disallow users from bypassing any step in a multi-step authentication process
    - Note: This would not apply to emergency access capabilities (or "break glass" accounts) for privileged users
- Implement proper session management controls
- Deploy web application protections, such as web application firewalls (WAFs) or web application proxies (WAPs) to mitigate the exploitation of vulnerabilities

3.5 Application control

Controlling the installation, use, and connectivity of applications in your environment is a key element of hardening applications and securing your network, systems, and data. You should ensure that these applications are managed and their use controlled in accordance with your organization's threat and risk assessment and subsequent policies and procedures. It would be beneficial for your organization to implement application allow lists to give you some control over which apps can execute on your systems. For more information, see the Top 10 IT security action items: No. 10 Implement application allow lists - ITSM.10.095 [8].

Users without administrative privileges should not be permitted to install any applications on a corporate device or within your corporate environment. Many applications can be targets for threat actors who use social engineering and other tactics to trick employees into installing applications infected with malware. It is recommended that your organization have a suite of pre-approved applications available to your employees for download. This lessens the burden on your IT administrators and allows your users to find applications that they find useful for their roles within the organization. We also recommend that your organization have a set suite of mandatory software and applications that are not to be deactivated, uninstalled, or deleted by users who do not have administrative privileges. For administrators, we recommend your organization use a dedicated administrative workstation, for example, a privileged access workstation (PAW) or a secured administrative workstation (SAW) that does not have access to applications or that is not connected to the Internet.

3.6 Challenges of applications

While hardening your OS and applications is a top recommended security action, it does not come without its challenges. Particularly with applications, hardening can be difficult, as there is an enormous volume of applications available. We recommend conducting a review of all applications available in your environment, including standard and third-party apps, and deactivate or remove those that are not needed.

4 Security controls for hardening

Annex 3A - Security control catalogue (ITSG-33) [2] presents the following security controls that are appropriate and applicable for hardening your OS and applications in use across your organization. The following subsections detail the security control and the related actions your organization should take to harden your OS and applications.

4.1 Baseline configuration (CM-2)

Your OS and applications should not be deployed in their default state. Ensuring your organization adjusts the configuration settings of your OS and your applications will enhance your security posture and make it more difficult for threat actors to compromise your environment. You can consult and use recommended security settings from the vendor and trusted sources, like the CIS benchmarks.

Your organization should develop, document, and maintain a current baseline configuration for all your systems and system components, including the communications and connectivity-related components. Your baseline configurations should include details about your information systems components, including software, network components and mobile device deployments. Baseline configurations should also be established for your OS, including the version and patch history. Your organization should ensure the most recent versions of your OS and apps are implemented as soon as the update is available. Running off older or unsupported versions of your OS can expose your organization to vulnerabilities and exploitation techniques that have been mitigated in the newest version. To keep up to date with components and to ensure you deploy the latest versions or additional new features, your organization may want to assign an owner to each component. This owner would be responsible for the configuration of the component.

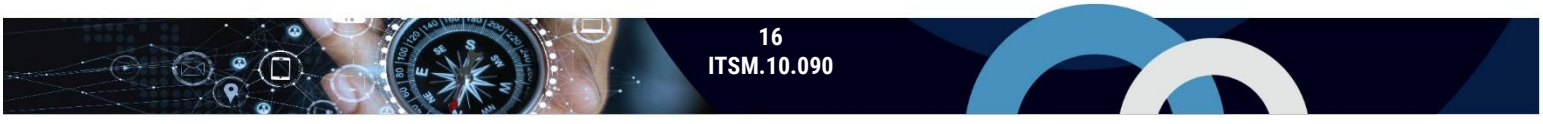
Your baseline configuration settings should be reviewed on a regular basis to ensure they meet the needs of your evolving environment, including future builds, releases, and changes to your systems or operations. They should always reflect your current enterprise architecture.

Your organization should establish organization-wide configuration settings and subsequently derive specific settings for your information systems. These established settings become part of your systems configuration baseline.

4.2 Configuration settings (CM-6)

Configuration management includes security controls that support the management and control of all components of your information systems, like hardware, software, and configuration items. Configuration settings are the set of parameters that can be changed in hardware, software, firmware, OS, network components, and applications that impact the security posture or the functionality of your systems. Secured configuration settings should include some of the following:

- configuration resources, through files or applications
- account, file, and directory permission settings
- functions, ports, protocols, services, and remote connection settings
- application control



Your IT products should be established and documented to ensure you deploy the most restrictive mode that is consistent with your operational requirements. If there is a need to deviate from these predetermined configuration settings, your organization should have an approval process in place to ensure each use case is reviewed, documented, and approved by management for a defined period to support operational requirements. Your organizational policies and procedures should also ensure that changes to your configuration settings are monitored and controlled and that any anomalies noted are documented and investigated.

If your organization engages with a CSP, you must ensure you review and control versioning within IaaS and PaaS circumstances. In accordance with SaaS elements, it is recommended that your organization work with your CSP to ensure the latest versions are in use and that any issues or concerns can be rapidly and adequately addressed by the provider.

4.3 Least functionality (CM-7)

Your organization may have a wide variety of information systems available within your environment. You should ensure you review the functions and services they provide to determine which ones are necessary to support your essential organizational operations. For cloud operations, ensure you review the access policies and account capabilities.

Your systems should be configured to provide only the functions and capabilities essential for your operational requirements. Prohibiting or restricting the use of certain items can significantly enhance your security posture and allow your organization to better protect your operating environment. To prevent the unauthorized connection of devices, transfer of information or tunnelling, you should consider prohibiting or restricting certain:

- functions, such as auto-execute or file sharing
- ports or protocols, like FTP and HTTP
- services, like domain name service (DNS), mail transport agents (MTAs), or the dynamic host configuration protocol (DHCP)

Additionally, while it can be convenient to provide multiple services from a single system component, this can increase risks to your organization. You could overlimit the services provided by one component. Where feasible, your organization should limit your component functionality to a single function per device, such as having separate email servers and web servers.

Your organization should develop policies and procedures that establish what functions and services of your systems will be permitted and which will be deactivated or eliminated. These policies and procedures should assist your organization in determining which applications are necessary and most useful and provide guidelines on how to remove applications that are no longer needed from your environment.

You can leverage network scanning tools, intrusion detection and prevention systems, and endpoint protections such as firewalls and host-based intrusion detection systems (HIDS) to identify and prevent the use of prohibited functions, ports, protocols, and services.

4.4 Malicious code protection (SI-3)

Employing malicious code protection mechanisms, such as anti-virus and anti-malware tools, will enhance your organization's overall cyber security posture. You should deploy these tools to all entry and exit points on your systems, like firewalls, servers, and devices to detect and eradicate malicious code from your systems. Anti-virus and anti-malware tools can assist your organization in the detection and quarantining of suspected or known malicious code before it enters your environment. It is vital that these security tools are updated whenever a new release is available, as established in your organization's configuration management policy.

When working in a cloud environment, you should determine what security features and functions your CSP offers and work with them to properly identify and implement additional services that you require to secure your environment.

Many of these security products require signatures to detect malicious code. While this approach is effective when malicious code has been identified and a signature is available, it will not offer your organization robust protection. You should also consider deploying a host-based intrusion prevention system (HIPS) and a HIDS to protect your organization's systems against both known and unknown malicious attacks. Both HIDS and HIPS can detect anomalies in behaviour associated with your users or your applications. A HIPS will enhance your overall protection against malicious code as it can detect signature-based malicious code and implement actions to protect your environment. HIPS will identify and block abnormal behaviour and detect malicious code that has yet to be identified by security vendors. Implementing and maintaining a HIPS can be complex and will require dedicated resources to execute. When deploying host-based detection tools, your organization should identify the workstations and servers that are most crucial to your business operations and deploy HIPS and HIDS to them.

You should also ensure your organization uses an OS that has been recently released or is the newest version available from the vendor. Your organization should decommission or replace older releases of your OS where possible, especially if they are no longer supported by the vendor. The older versions may create security vulnerabilities which can be exploited by threat actors.

When your OS has a new release, your organization should update your malicious code protection mechanisms to ensure your environment is defended. Your malicious code mechanisms can be configured in accordance with your configuration management policies. They should perform periodic scans of your systems and frequent or real-time scans of external traffic and data attempting to enter your environment. Your mechanisms should also quarantine, block, or alert your system administrators when malicious code is detected. For false positives, ensure your organizational policies address the receipt of any false positive while you're detecting, investigating, or eradicating malicious code, as well as any potential or real impacts on the availability of your systems.

In instances where the malicious code mechanisms your organization has in place do not detect malicious code (for example, logic bombs or back door attacks), the other safeguards discussed in this publication will ensure that software and system components perform only those functions they are intended to.

4.5 Information system monitoring (SI-4)

Your organization should monitor your network and systems to ensure you can keep your environment secure. The main goal of system monitoring is to detect anomalies in traffic, system performance, or user behaviour and implement swift mitigation measures to thwart a potential threat actor from compromising your environment. Your system monitoring should include capabilities to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections. System entry points, such as firewalls, must also be monitored and associated logs ought to be reviewed on a regular basis. It is also a best practice to monitor your endpoints and treat them as high-value targets, as they can provide access to hosts if compromised.

To have inclusive monitoring, your organization should first identify your security baseline to determine what normal traffic looks like on your network. From there, you can expand or refine the parameters for your monitoring tools to ensure you are capturing the necessary data to actively monitor and protect your network and systems.

Your organization should deploy an intrusion detection system (IDS) and an intrusion protection system (IPS) to work in tandem to enhance the overall security of your systems. The information gathered from your intrusion monitoring tools should be secured and access be limited to those who require it to perform the functions of their job or role. The data from your monitoring tools should be protected and audited to ensure there has been no unauthorized access, modifications, or deletion. You can also consider a HIDS or a HIPS to detect anomalies in your traffic that might indicate persistence techniques or certain types of movement, like lateral movement.

As part of the application control actions discussed in Section 3.5, your organization should capture and review the application control event logs to determine whether any potential malicious behaviours can be detected. These logs can supplement your system logs and assist in your ability to investigate and respond to incidents as they arise.

In addition to monitoring traffic, an Identity, Credential, and Access Management (ICAM) system can be implemented to monitor who is accessing your resources, from which locations, and at what time. ICAM can also help to determine a baseline in user behaviour patterns and can serve as an alert to anomalous behaviours within your environment. ICAM reduces the risk of cyber attacks to your organization by preventing unauthorized access to your networks, systems, and data. For more information, see Identity, Credential, and Access Management (ICAM) (ITSAP.30.018) [9].

5 Summary

Hardening operating systems and applications is just one aspect of improving your cyber security posture. By ensuring you have established baseline configuration settings that are maintained and reviewed regularly, following the principle of least functionality, and protecting and monitoring against malicious threat actors, your organization will harden your environment.

To further enhance your environment and best protect your organization against cyber threats, you should review and implement all the actions recommended in Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089) [1]. Your organization should also take additional measures including:

- educating employees on cyber security
- protecting endpoint devices by applying patches
- segmenting your networks
- implementing an application allow list
- isolating web-facing applications

6 Supporting content

6.1 List of abbreviations

Term	Definition
AC	Access control (security control family)
CIS	Center for Internet Security
CISA	Cybersecurity & Infrastructure Security Agency
CPG	Cross-Sector Cybersecurity Performance Goals
CSP	Cloud service provider
DHCP	Dynamic host configuration protocol
DISA	Defense Information Systems Agency
DNS	Domain name service
GC	Government of Canada
HIPS	Host-based intrusion prevention system
HIDS	Host-based intrusion detection system
IA	Identification and authentication (security control family)
IaaS	Infrastructure as a service
IT	Information technology
MSP	Managed service provider
NCP	National Checklist Program
NSA	National Security Agency
OS	Operating system
PaaS	Platform as a service
PAM	Privileged access management
PAW	Privileged access workstation
PIN	Personal identification number
SaaS	Software as a service
SAW	Secured administrative workstation
SC	System communication protection (security control family)
SLAT	Second level address translation
STIG	Security technical implementation guide
TCP	Transmission control protocol
UDP	User datagram protocol

6.2 Glossary

Term	Definition
Availability	A value that is assigned to information assets, software, and hardware (infrastructure and its components). Data with the highest possible availability rating must always be accessible. Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Break glass account	A “break glass” account is an emergency access account that has highly privileged access, and is not directly assigned to specific individuals. Emergency access accounts are limited to emergency or "break glass"' scenarios where normal administrative accounts can't be used.
Confidentiality	A value that is assigned to a set of information to indicate its sensitivity level and any access restrictions that prevent unauthorized people from accessing it.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Defence-in-depth	The use of multiple layers of security controls and measures to help reduce the likelihood of a successful cyber attack.
Endpoint	A remote computing device (for example, laptop, desktop, mobile phone) that communicates with a network to which it is connected.
Firewall	A security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside.
Integrity	A value that is assigned to information to indicate how sensitive it is to data loss. Implied in its definition is that integrity includes protecting information from being modified or deleted unintentionally or when it’s not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Intrusion detection	A security service that monitors and analyzes network or system events to warn of unauthorized access attempts. The findings are provided in real-time (or near real-time).
IT asset	The components of an information system, including business applications, data, hardware, and software.
Least privilege	The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.
Management security control	A class of security controls that focus on the management of IT security and IT security risks.

Term	Definition
Multi-factor authentication	A tactic that can add an additional layer of security to your devices and account. Multi-factor authentication requires additional verification (like a PIN or fingerprint) to access your devices or accounts. Two-factor authentication is a type of multi-factor authentication.
Operational security control	A class of security controls primarily implemented and executed by people and typically supported by technology (for example, supporting software).
Phishing	An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
Ransomware	A type of malware that denies a user's access to a system or data until a sum of money is paid.
Risk	The likelihood and the impact of a threat using a vulnerability to access an asset.
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied by using a variety of security solutions, including security products, security policies, security practices, and security procedures.
Technical security control	A class of security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
Threat	Any potential event of act (deliberate or accidental) or natural hazard that could compromise IT assets and information.
Threat and risk assessment	A process of identifying system assets and how these assets can be compromised, assessing the level of risk that threats pose to assets, and recommending security measures to mitigate threats.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited by a threat actor to adversely affect an organization's assets or operations.

6.3 References

Number	Reference
1	Canadian Centre for Cyber Security. IT security risk management: A lifecycle approach (ITSG-33). November 2012.
2	Canadian Centre for Cyber Security. Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089). September 2021.
3	National Institute of Standards and Technology. National Checklist Program for IT products: Guidelines for checklist users and developers (SP 800-70 Rev. 4). February 2018.
4	Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA). Kubernetes Hardening Guide. August 2022.
5	Cybersecurity and Infrastructure Security Agency (CISA). Key Findings to Improve Monitoring and Hardening of Networks. Feb 2023.
6	Canadian Centre for Cyber Security. Steps for effectively deploying multi-factor authentication (MFA) - ITSAP.00.105. May 2023.
7	Cybersecurity and Infrastructure Security Agency (CISA). Cross-Sector Cybersecurity Performance Goals. March 2023.
8	Canadian Centre for Cyber Security. Top 10 IT security action items: No. 10 Implement application allow lists (ITSM.10.095). August 2022.
9	Canadian Centre for Cyber Security. Identity, Credential, and Access Management (ITSAP.30.018). August 2022.

Annex A ITSG-33 Security control catalogue

A.1 Operational security controls: Configuration management

Table 1 describes controls **CM-2 Baseline configuration**, **CM-6 Configuration settings**, and **CM-7 Least functionality**, as defined in Annex 3A of ITSG-33 [2].

Table 1: ITSG-33 Operational security controls: CM-2, CM-6, and CM-7

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
CM-2	Baseline configuration	(A) The organization develops, documents, and maintains under configuration control a current baseline configuration of the information system.	**Reviews and updates:** The organization reviews and updates the baseline configuration of the information system: i. [*Organization-defined frequency*]. ii. When required due to [*Organization-defined circumstances*]. iii. As an integral part of information system component installations and upgrades. See related control CM-5. **Automation support for accuracy and currency:** The organization uses automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. See related controls CM-7 and RA-5. **Retention of previous configurations:** The organization retains [*organization-defined previous versions of baseline configurations of the information system*] to support rollback.	CM-3 CM-6 CM-8 CM-9 SA-10

			Development and test environments: The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration. See related controls CM-4 and SC-3. **Configure systems, components, or devices for high-risk areas:** i. The organization issues [*organization-defined information systems, system components, or devices*] with [*organization-defined configurations*] to individuals travelling to locations that the organization deems to be of significant risk. ii. The organization apples [*organization-defined security safeguards*] to the devices when the individuals return.	
CM-6	Configuration settings	(A) The organization establishes and documents configuration settings for information technology products employed within the information system using [*organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements. (B) The organization implements the configuration settings. (C) The organization identifies, documents, and approves any deviations from established configuration settings for [*organization-defined information system components*] based on [*organization-defined operational requirements*].	**Automated central management, application, and verification:** The organization uses automated mechanisms to centrally manage, apply, and verify configuration settings for [*organization-defined information system components*]. See related controls CA-7 and CM-4. **Respond to unauthorized changes:** The organization uses [*organization-defined security safeguards*] to respond to unauthorized changes to [*organization-defined configuration settings*]. See related controls IR-4 and SI-7.	AC-19 CM-2 CM-3 CM-7 SI-4

		(D) The organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.		
CM-7	Least functionality	(A) The organization configures the information system to provide only essential capabilities. (B) The organization prohibits or restricts the use of the following functions, ports, protocols, and services: [*organization-defined prohibited or restricted functions, ports, protocols, and services*].	**Periodic review:** The organization review the information system [*organization-defined frequency*] to identify unnecessary and non-secure functions, ports, protocols, and services. The organization deactivates [*organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and non-secure*]. See related controls AC-18, CM-7, IA-2. **Prevent program execution:** The information system prevents program execution in accordance with [*Select (one or more): organization-defined policies regarding software program use and restrictions; rules authorizing the terms and conditions of software program use*]. See related control CM-8. **Registration compliance:** The organization complies with [*organization-defined registration requirements for functions, ports, protocols, and services*]. **Unauthorized software and blacklisting:** The organization identifies [*organization-defined software programs not authorized to execute on the information system*].	AC-6 CM-2 RA-5 SA-5 SC-7

			The organization uses an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system. The organization reviews and updates the list of unauthorized software programs [*organization-defined frequency*]. See related controls CM-6 and CM-8. **Authorized software and whitelisting:** The organization identifies [*organization-defined software programs authorized to execute on the information system*]. The organization uses a deny-all, permit-by-exception policy to allow authorized software programs to execute on information systems. The organization reviews and updates the list of authorized software programs [*organization-defined frequency*]. See related controls CM-2, CM-6, CM-8, SA-10, SC-34, and SI-7.	

A.2 Operational security controls: System and information integrity

Table 2 describes controls **SI-3 Malicious code protection** and **SI-4 Information system monitoring**, as defined in Annex 3A of ITSG-33 [2].

Table 2: ITSG-33 Operational security controls: SI-3 and SI-4

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
SI-3	Malicious code protection	(A) The organization uses malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. (B) The organization updates malicious code protection mechanisms whenever new releases are available according to organizational configuration management policies and procedures. (C) The organization configures malicious code protection mechanisms to: i. Perform periodic scans of the information system [*organization-defined frequency*] and real-time scans of files from external sources at [*select one or more: endpoints, network entry and exist points*] as the files are downloaded, opened, or executed according to organizational security policies. ii. [*Select one or more organization-defined action: block malicious code, quarantine malicious code, send alert to administration*] in response to malicious code detection.	**Central management:** The organization centrally manages malicious code protection mechanisms. See related controls AU-2 and SI-8. **Automatic updates:** The information system automatically updates malicious code protection mechanisms. See related control SI-8. **Updates only by privileged users:** The information system updates malicious code protection mechanisms only when directed by a privileged user. See related controls AC-6 and CM-5. **Testing and verification:** The organization tests malicious code protection mechanisms [*organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system. The organization verifies that both detection of the test case and associated incident reporting occur. See related controls CA-2, CA-7, and RA-5.	CM-3 MP-2 SA-4 SA-8 SA-12 SA-13 SC-7 SC-26 SC-44 SI-2 SI-4 SI-7

		(D) The organization addresses the receipt of false positive during malicious code detection and eradication and the resulting potential impact on the availability of information systems.	**Non-signature-based detection:** The information system implements malicious code detection mechanisms that are based on non-signatures. **Detect unauthorized commands:** The information system detects [*organization-defined unauthorized operating system commands*] through the kernel application programming interface at [*organization-defined information system hardware components*] and [*select one or more: issues a warning, audits the command execution, prevents the execution of the command*]. See related control AU-6. **Authenticate remote commands:** The information system implements [*organization-defined security safeguards*] to authenticate [*organization-defined remote commands*]. See related controls SC-12, SC-13, and SC-23. **Malicious code analysis:** The organization uses [*organization-defined tools and techniques*] to analyze the characteristics and behaviour of malicious code. The organization incorporates the results from malicious code analysis into organization incident response and flaw remediation processes.	
SI-4	Information system monitoring	(A) The organization monitors the information system to detect: i. attacks and indicators of potential attacks according to	**System-wide intrusion detection system:** The organization connections and configures individual intrusion detection tools into an information-system wide intrusion detection system.	AC-3 AC-4 AC-8 AC-17

		[*organization-defined monitoring objectives*]. ii. unauthorized local, network, and remote connections. (B) The organization identifies unauthorized use of the information system through [*organization-defined techniques and methods*]. (C) The organization deploys monitoring devices to: i. strategically within the information system to collect essential information. ii. at ad hoc locations within the system to track specific types of transactions of interest to the organization. (D) The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion. (E) The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information. (F) The organization obtains legal opinion regarding information system monitoring activities in accordance with Canadian legislation and policies, directives, and standards.	**Automated tools for real-time analysis:** The organization uses automated tools to support near real-time analysis of events. **Automated tool integration:** The organization uses automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanism in support of attack isolation and elimination. **Inbound and outbound communication traffic:** The information system monitors inbound and outbound communications traffic [*organization-defined frequency*] for unusual or unauthorized activities or conditions. **System-generated alerts:** The information system alerts [*organization-defined personnel or roles*] when indications of compromise or potential compromise occur. See related controls AU-5 and PE-6. **Automated response to suspicious events:** The information system notifies [*organization-defined incident response personnel, identified by name or role*] of detected suspicious events and takes [*organization-defined least-disruptive actions to terminate suspicious events*]. **Test monitoring tools:** The organization tests intrusion-monitoring tools [*organization-defined frequency*].	AU-2 AU-7 AU-9 AU-12 CA-7 IR-4 PE-3 RA-5 SC-7 SC-26 SC-35 SI-3 SI-7

		(G) The organization provides [*organization-defined information system monitoring information*] to [*organization-defined personnel or roles*] [*select one or more: as needed; organization-defined frequency*].	See related control CP-9. **Visibility of encrypted communications:** The organization makes provisions so that [*organization-defined encrypted communications traffic*] is visible to [*organization-defined information system monitoring tools*]. **Analyze communications traffic anomalies:** The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*organization-defined interior points within the system, such as subnetworks and subsystems*] to discover anomalies. **Automated alerts:** The organization uses automated mechanism to alert security personnel of the following inappropriate of unusual activities with security implications [*organization-defined activities that trigger alerts*]. See related controls AC-18, IA-3. **Analyze traffic and events patterns:** The organization analyzes communications traffic and event patterns for the information system. The organization develops profiles representing common traffic patterns and events. The organization uses the traffic and event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives. See related controls AC-18, IA-3.	

			Wireless intrusion detection: The organization uses a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises and breaches to the information system. See related controls: AC-18 and IA-3. **Wireless to wireline communications:** The organization uses an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks. See related control AC-18. **Correlate monitoring information:** The organization correlates information from monitoring tools employed throughout the information system. See related control AU-6. **Integrated situational awareness:** The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness. Se related control SA-12. **Analyze traffic and covert exfiltration:** The organization analyzes outbound communications traffic at the external boundary of the information system (for example, system perimeter) and at [*Organization-defined interior points within the system, such as subsystems and subnetworks*] to detect covert exfiltration of information.	

			Individuals posing greater risk: The organization implements [*organization-defined additional monitoring*] of individuals who have been identified by [*organization-defined sources*] as posing an increased level of risk. **Privileged user:** The organization implements [*organization-defined additional monitoring*] of privileged users. **Probationary periods:** The organization implements [*organization-defined additional monitoring]* of individuals during [*organization-defined probationary period*]. **Unauthorized network services:** The information system detects network services that have not been authorized or approved by [*organization-defined authorization or approval processes]* and [*select one or more: audits, alerts to organization-defined personnel or roles*]. See related controls AC-6, CM-7, SA-5, SA-9. **Host-based devices:** The organization implements [*organization-defined host-based monitoring mechanisms*] at [*organization-defined information system components*]. **Indicators of compromise:** The information system discovers, collects, distributes, and uses indicators of compromise.	