Malware Defense
Policy Template

**Critical Security Controls**

**March 2023**

# Contents

[Contents 2](#_Toc128321846)

[Acknowledgments 3](#_Toc128321847)

[Introduction 4](#_Toc128321848)

[Purpose 4](#_Toc128321849)

[Types of Malware 4](#_Toc128321850)

[Types of Anti-malware Defenses 5](#_Toc128321851)

[Scope 5](#_Toc128321852)

[Malware Defense Lifecycle 6](#_Toc128321853)

[Malware Defense Policy Template 8](#_Toc128321854)

[Purpose 8](#_Toc128321855)

[Responsibility 8](#_Toc128321856)

[Exceptions 8](#_Toc128321857)

[Policy 8](#_Toc128321858)

[Revision History 10](#_Toc128321859)

[Appendix A: Acronyms and Abbreviations 11](#_Toc128321860)

[Appendix B: Glossary 12](#_Toc128321861)

[Appendix C: Implementation Groups 13](#_Toc128321862)

[Appendix D: CIS Safeguards Mapping 14](#_Toc128321863)

[Appendix E: References and Resources 15](#_Toc128321864)

# Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

**Editors:**

**Contributors:**

Tony Krzyzewski, SAM for Compliance Ltd
Staffan Huslid, Truesec
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Bryan Chou, CISSP, GSEC, GCED, GCIH
Bryan Ferguson
Gavin Willbond, SSS - IT Security Specialists
Ken Muir
Keala Asato
Jon Matthies
Ginger Anderson, CIS
Robin Regnier, CIS
Valecia Stocchetti, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License. (The link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.)

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization, and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to <http://www.cisecurity.org/controls/> when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

# Introduction

Malware is one of the most common threats facing an enterprise. Malware can be used to capture credentials, steal data, identify other targets within the network, and encrypt or destroy data. Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, removable media, and more. Often, malware relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives into systems. Modern malware is designed to avoid, deceive, and disable defenses. Therefore, malware defenses must be able to operate in a dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. Defenses must be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

## Purpose

The CIS Critical Security Controls® (CIS Controls®) recommend multiple information security policies that an enterprise should have in place. This includes a policy to govern defensive mitigations to prevent malware from compromising enterprise assets. This *Malware Defense Policy* is meant as a “jumping off point” for organizations needing to draft their own policies surrounding the implementation of technical and procedural defenses against malware. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decision points and areas that must be tailored to your enterprise

**Control 10 – Malware Defenses**

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

To support this Safeguard, it is important for an enterprise to develop a holistic approach to defending against malware. This approach should include deploying appropriate malware defenses for the variety of assets deployed in the enterprise, properly configuring anti-malware applications, and managing these applications This document supports the development of a process for managing the variety of applications used to respond to malware while implementing this CIS Control.

## Types of Malware

Many malware types exist, to include:

* **Virus**: A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.
* **Trojan**: A useful or seemingly useful program that contains hidden code of a malicious nature that executes when the program is invoked.
* **Ransomware**: Malicious software used to encrypt an enterprise’s data and demand payment to restore access.
* **Spyware**: Software that is secretly or surreptitiously installed into an information system to gather information on individuals or enterprise without their knowledge; a type of malicious code.[[1]](#footnote-1)

## Types of Anti-malware Defenses

Many types of malware defenses exist, to include:

* **Signature-based detection**: Anti-malware software designed to routinely download a known-bad list of malware and quarantine or remove instances of this malware when they are identified on an enterprise asset.
* **Heuristic-based detection**: A set of rules or algorithms specifically developed to detect malware. These rules can sometimes be used to identify malicious behaviors in never-before-seen malware.
* **Host-based intrusion detection software (HIDS)**: Anti-malware software that monitors the dynamic behavior and state of the system to identify if malware is present on the system. This includes monitoring communications entering and leaving the system.
* **Network-based intrusion detection system (IDS)**: Anti-malware software or a dedicated network appliance that monitors and analyzes network traffic.
* **Network-based Intrusion Prevention Systems (IPS)**: Anti-malware software or a dedicated network appliance that monitors and analyzes network traffic, and then goes the extra step to actually block suspicious and malicious traffic.
* **Application Allowlisting or Blocklisting**: Anti-malware software or capabilities built into the operating system that explicitly allows or denies the execution of software, libraries, or scripts.
* **Endpoint Detection and Response (EDR)**: A collection of tools that analyzes, detects, and responds to events on a system to identify malware, utilizing multiple anti-malware capabilities on the same system. This application is continuously monitoring events on the system for signs of infection. Normal events on the system are recorded and analyzed to establish a baseline so that commonplace habits can be identified and abnormal events can be reported.

Note that any given anti-malware package or suite will likely leverage multiple technologies from this list.

## Scope

This *Malware Defense Policy* is divided into multiple sections based on how enterprise will practically use anti-malware tools to identify and remove malware from enterprise assets. Note that for this policy, only anti-malware software on laptops, workstations, mobile devices, and servers is included. Network-based anti-malware capabilities such as network-based IDS/IPS are not included. Additionally, this policy template is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs), but are specifically geared towards Safeguards in Implementation Group 1 (IG1). In [Appendix D](#_Appendix_D:_CIS), Safeguards unique to IG1 are specifically highlighted for ease of use. For more information on the CIS Implementation Groups, see [Appendix C](#_Appendix_C:_Implementation). Additionally, a glossary in [Appendix B](#_Appendix_B:_Definitions) is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1, and are welcome to do so. Depending on an enterprise’s sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise’s needs.

# Malware Defense Lifecycle

This *Malware Defense Policy* is divided into multiple sections. These sections are shown below in Figure 1 are the high-level “steps” followed by a detailed description of what each step entails.



Figure 1. Malware Defense Lifecycle

* **Configuration** – Properly installing and configuring anti-malware software on host devices.
* **Update** – Routinely providing updates to the anti-malware software and updating signatures.
* **Detection –** Identifying malware on enterprise assets.
* **Reporting** – Users or systems alerting IT staff of any identified malicious applications, code, or scripts on enterprise assets.
* **Remediation** – Address previously identified malware.

**Configuration**

There are many types of anti-malware software and functionality. Anti-malware software is most often installed as a privileged third-party application that requires updates, as is often the case with signature-based detection. As such, that is the scope of this policy. This software must be properly installed, configured, and maintained. This anti-malware cannot just be “set and forget.” The software must be configured to run at regular intervals, and real time scanning is most effective. Note that performance issues may occur on certain platforms, with the anti-malware software consuming a large quantity of the system’s resources. This software must also be configured on what the system should do if malware is identified. Options include attempting to remove, quarantining, logging, or simply alerting an IT administrator. Be mindful that updates or upgrades for applications that are used to control anti-malware software may be modified after an update. Once an update occurs, the baseline for the application will need to be updated to reflect the new features and settings. This new baseline will require validation. The developer will likely have guidance for suggested default settings.

**Update**

Anti-malware software that is not properly updated on a regular basis will quickly lose its ability to defend against the most recently released malware. Over time, this backlog of updates will drastically reduce the effectiveness of the software’s ability to detect and identify malware. It’s not just the signatures that need to be updated, the anti-malware software itself will need to be regularly updated to account for changes in the operating system, add new features, and fix security flaws. Note that just like other software tools used in the enterprise, anti-malware software will need to be purchased and their license properly managed. Additional features may need to be purchased and any subscriptions reviewed and updated on a regular basis.

**Detection**

The anti-malware tools on enterprise assets should be configured to warn users that a threat has been detected. These tools should also be generating logs that IT can use to research the actual sequence of events that made the anti-malware suite report an infection alert. Logs can also be beneficial when there is a single system performing analysis of all logs in an enterprise such as a Security Information and Event Management (SIEM). Some enterprises may choose to disconnect an infected system from the network and revoke its access to enterprise data while there is malware actively on an asset. It is common for IT to want to upload a malicious application to a malware tool such as [Virus Total](https://www.virustotal.com/gui/home/upload). These sites and tools can provide valuable threat intelligence about malware, but may have some drawbacks that require additional research on IT’s behalf.

Additionally, users should be trained for signs of malware on their system, and what to do if the anti-malware software installed on their enterprise asset identifies a malware infection. This can be accomplished via the Security Awareness and Skills Training offered by the enterprise, codified in the enterprise’s *Security Awareness Training Policy*. Additionally, the anti-malware tools should be configured to warn users that a threat has been detected. Note that it’s never advised to shutdown or restart a computer that is infected with malware, as IT may need to analyze the system, and shutdown or restarts will either remove or partially destroy all volatile memory. It is recommended for enterprises to disconnect an infected system from the network and revoke its access to enterprise data while there is an active malware infection on an asset.

**Reporting**

Being able to block or identify malware is only part of this CIS Control; there is also a focus on centrally collecting the logs to support alerting, identification, and incident response. As malicious actors continue to develop their methodologies, many are starting to take a “living-off-the-land” (LotL) approach to minimize the likelihood of being caught. This approach refers to attacker behavior that uses tools or features that already exist in the target environment. Enabling logging, as per the Safeguards in CIS Control 8, will make it significantly easier for the enterprise to follow the events to understand what happened and why it happened. Theoretically, IG1 enterprises may not have a dedicated incident response team to respond when malware is detected. This means that ultimately, the business owner may be the appropriate party to make the call on how to go about remediation activities. At the very least, users should be trained to report malware to the appropriate contact within the IT business unit.

**Remediation**

What to do after a threat is detected on an enterprise asset will depend heavily on a variety of circumstances. Some anti-malware applications may be configured to automatically attempt to repair the issue that was discovered. In other instances, the information technology (IT) business unit may be interested in analyzing the malware. In instances where malware is left running on enterprise assets, this fact should be noted in both the enterprise’s software inventory and an exceptions register.

# Malware Defense Policy Template

## Purpose

Malware defense includes the configuration, maintenance, detection, reporting, and remediation of anti-malware software and the malware it identifies. The *Malware Defense Policy* provides the processes and procedures to accomplish those tasks. This policy applies to all departments and all assets connected to the enterprise network.

## Responsibility

* The IT business unit is primarily responsible for malware defense. Specifically, administrators are responsible for configuring the correct devices to generate, store, and transmit logs. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them. All enterprise assets are required to comply with the malware defense policy and procedures.
* Users are responsible for connecting their devices to the enterprise network, regularly applying malware signature updates, and restarting their devices as appropriate.

## Exceptions

Exceptions to this policy are likely to occur. Exception requests must be made in writing and must contain:

* The reason for the request,
* Risk to the enterprise of not following the written policy,
* Specific mitigations that will not be implemented,
* Technical and other difficulties, and
* Date of review.

## Policy

**Configuration**

1. IT must install anti-malware software on all enterprise assets where appropriate.
2. Users must not disable anti-malware software on their enterprise assets
3. Users must not modify the update frequency specified as part of *the Secure Configuration Management Policy*.

**Update**

1. Anti-malware software must be configured to automatically update.
2. IT must ensure that anti-malware signatures are kept up-to-date as they become available via an automatic update process.
3. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.

**Detection**

1. IT must ensure that anti-malware software is properly functioning on all enterprise assets.

**Reporting**

1. All confirmed high severity alerts must reported to the business owner.
2. The presence of unauthorized software must be properly investigated.

**Remediation**

1. Identified malware must be removed from enterprise assets.
2. Unauthorized software must be removed from use on enterprise assets or receive a documented exception.
3. All exceptions must be noted in the software inventory.
4. All exceptions must be noted in the exception register.

Revision History

Each time this document is updated, this table should be updated.
.

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Revision Description | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A: Acronyms and Abbreviations

|  |  |
| --- | --- |
| CIS | Center for Internet Security |
| CIS Controls | Center for Internet Security Critical Security Controls |
| COTS | Commercial-off-the-shelf |
| EDR | Endpoint Detection and Response  |
| HIDS | Host-Based Intrusion Detection Software  |
| IDS | Intrusion Detection System |
| IG | Implementation Group |
| IPS | Intrusion Prevention System |
| IT | Information Technology |
| LotL | Living off the land |
| SIEM | Security Information and Event Management |
| USB | Universal Serial Bus |

# Appendix B: Glossary

|  |  |
| --- | --- |
| Asset | Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).Source: [Asset(s) - Glossary | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/asset) |
| Enterprise assets | Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments.Source: CIS Controls v8  |
| End-user devices | Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones, and tablets as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of enterprise assets.Source: CIS Controls v8 |
| Network devices | Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets.Source: CIS Controls v8 |
| Servers | A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.Source: CIS Controls v8 |
| Spyware | Spyware: Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious codeSource: NIST SP 800-53 Rev. 5 |
| User | Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset.Source: CIS |

# Appendix C: Implementation Groups

As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

**IG1**

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

**IG2**

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information, and they can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

**IG3**

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at <https://www.cisecurity.org/controls/cis-controls-list/>.

# Appendix D: CIS Safeguards Mapping

**CIS Controls & Safeguards Covered by this Policy**

This policy helps to bolster IG1 Safeguards in CIS Control 10: *Malware Defenses*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table - Safeguards covered by IG1

|  |  |  |  |
| --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard  | CIS Safeguard Description |
| 2.3 | Reporting 2 Remediation  | Address Unauthorized Software | Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. |
| 7.3 | Update 3 | Perform Automated Operating System Patch Management | Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. |
| 7.4  | Update 1  | Perform Automated Application Patch Management | Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. |
| 10.1  | Configuration 1, 1a, 1bDetection 1 | Deploy and Maintain Anti-Malware Software | Deploy and maintain anti-malware software on all enterprise assets |
| 10.2  | Update 2  | Configure Automatic Anti-Malware Signature Updates | Configure automatic updates for anti-malware signature files on all enterprise assets. |
| 10.3  | Please see the CIS *Secure Configuration Management Policy Template*.  | Disable Autorun and Autoplay for Removable Media | Disable autorun and autoplay auto-execute functionality for removable media. |
| 17.3 | Reporting 1 | Establish and Maintain an Enterprise Process for Reporting Incidents | Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard. |

# Appendix E: References and Resources

Center for Internet Security®

<https://www.cisecurity.org/>

CIS Critical Security Controls®

<https://www.cisecurity.org/controls/>

MS-ISAC® and EI-ISAC® Service: Malicious Code Analysis Platform (MCAP)
<https://www.cisecurity.org/ms-isac/services/real-time-indicator-feeds>

European Institute for Computer Antivirus Research (EICAR) Anti-Virus Test File
<https://www.eicar.org/download-anti-malware-testfile>

ClamAV
<https://www.clamav.net>

Bitdefender® Antivirus Free
<https://www.bitdefender.com/solutions/antivirus-free-for-android.html>

OpenSCAP
<https://www.open-scap.org>

OpenVAS
<https://www.openvas.org>

Virus Total
<https://www.virustotal.com/gui/home/upload>

1. NIST SP 800-53 Rev. 5 [↑](#footnote-ref-1)