SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **MALWARE DEFENSE**	Procedure 8.24.01

I. PROCEDURE STATEMENT

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

II. RESPONSIBILITY

The Information Technology ("IT") division is responsible for all log management functions. 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, such as applying updates in a regular manner or restarting their systems. All enterprise assets are required to comply with the enterprise audit logging procedures.

III. DEFINITIONS

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.

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.

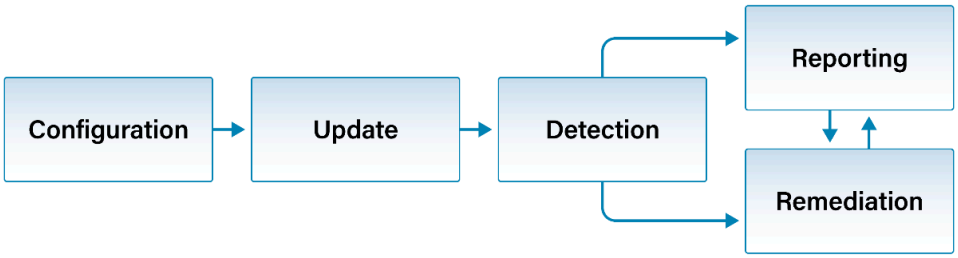
- **Heuristic-based detection**: A set of rules or algorithms specifically developed to detect malware. These rules can sometimes be used to identify malicious behaviors in never-before-seen malware.

- **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.

IV. 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.

V. 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.

VI. 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.

VII. 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. 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 College's *Security Awareness Training Policy 8.09*. 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.

VIII. 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 IT.

IX. 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, IT 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.

LEGAL REFERENCES:

- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, Control 10 (Malware Defenses)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

Adopted: September 2025

Revised: N/A