MICROSOFT WINDOWS 11 STIG
CHEF DOCUMENTATION

Version 1, Release 3

26 August 2023

Developed by DISA for the DOD

TABLE OF CONTENTS

Page

1. BACKGROUND

Chef is an open source, cross-platform configuration management solution used to define and enforce system and application configurations. This package provides Chef configurations that implement most of the Windows 11 Security Technical Implementation Guide (STIG). While the content has been tested during development, all possible system and environmental factors could not be tested. Before using this content in a production environment, users are advised to perform testing with the intended settings in their own test environment. There is no mandate to use this content; it is published as a resource to assist in the application of security guidance to the user's systems. It is to be used in the manner and to the extent that it assists with this goal.

Many Windows configuration settings can be applied using Group Policy. This Chef configuration does not leverage Group Policy. Therefore, this content is most useful for systems that are not using Group Policy or to manage a subset of configuration settings that are not being managed through Group Policy.

2. INSTALLATION

The following instructions are for standalone installation using chef-client for testing purposes. A production environment will likely use Chef Server and Chef Clients. Refer here for details.

2.1 Installing Chef Client

Install the Windows 11 Chef Client from here.

2.2 Extracting

Unzip the **`win11STIG-chef.zip`** file.

3. CONFIGURATION

3.1 Simple

To apply the default STIG Chef configuration to the local machine only, run the **`enforce.ps1`** script in PowerShell to enforce the STIG. If prompted, accept the license. To tailor the configuration, follow the steps in the next section.

3.2 Custom

To customize the STIG Chef configuration, adjust the attributes in the file **`cookbooks\Win11STIG\attributes\default.rb`**. This file contains configuration data to define which configuration settings to manage and the values for these settings. Edit this configuration file in a text editor to best suit each system's requirements as needed. For example, to turn off STIG rule ID 253278, set the "Manage" attribute equal to **`false`**. To set STIG rule ID 253301's maximum password age to 90, set the "Maximum_Password_Age" attribute to **`90`**.

```
default['win11STIG']['stigrule_253278']['Manage'] = false
default['win11STIG']['stigrule_253278']['Setting']['Telnet_Client_Ensure'] = :remove

default['win11STIG']['stigrule_253301']['Manage'] = true
default['win11STIG']['stigrule_253301']['Setting']['Maximum_Password_Age'] = 90
```

For more information on attributes, refer here.

Note: While useful for testing, this approach is not recommended for a production Chef Server environment. Rather than changing the cookbook defaults, which may change in future versions of the cookbook, override attributes using Chef capabilities such as roles or environments.

3.3 Defaults

Some of the available settings are not managed by default. In cases where different rules apply depending on the domain role (domain controller, member server, or standalone), defaults are based on the standalone case. Other STIG rules have hardware requirements that cannot be managed by Chef, and while their configurations are provided here, they are not managed by default. Some settings require site-specific values, and these settings are not managed by default.

4. CONTENT EXTRACTION

This compliance extraction methodology returns results based on a system's compliance with the enforcement content. This may be different from STIG compliance. For example, multiple values may be allowed by the STIG but will be marked as "fail" if the value does not match the single exact value in the enforcement content. Additionally, if a value is customized in such a way as to violate a STIG rule, it will be marked as "pass" since it matches the enforcement content's expected value.

At the completion of a successful Chef run, a Chef handler can extract configuration results into XCCDF results. Use of this handler can be controlled by modifying the following variable in the **`cookbooks\win11STIG\attributes\default.rb`** file:

```
default['win11STIG']['XCCDF_result']['Manage'] = true
```

Configuration of the handler is controlled by modifying the following variables in the **`cookbooks\win11STIG\recipes\default.rb`** file:

```
chef_handler 'Chef::Handler::StigXml' do
  source "#{Chef::Config[:file_cache_path]}/stig_xml.rb"
  arguments :stigName => U_MS_Windows_11_STIG_V1R3_Manual-xccdf.xml',
:path => '/path/where/to/write/results.xml'
```

The resource above controls the arguments to the handler writing the XCCDF results file to the :path using the manual STIG named :stigName. The XCCDF results file is output by default as **`C:\Users\Username\AppData\Local\Temp\xccdf-results.xml`** if no :path is provided.

Note: The STIG name provided above should match the STIG release and version number for which the Chef content is built.

Chef provides a means of checking compliance without enforcement called **`--why-run`** mode. To use this mode, run the following:

```
chef-client -z -o win11STIG --why-run
```

Note: For the content extraction handler to function, a prior run without **`--why-run`** must have completed successfully.