Threat Emulation

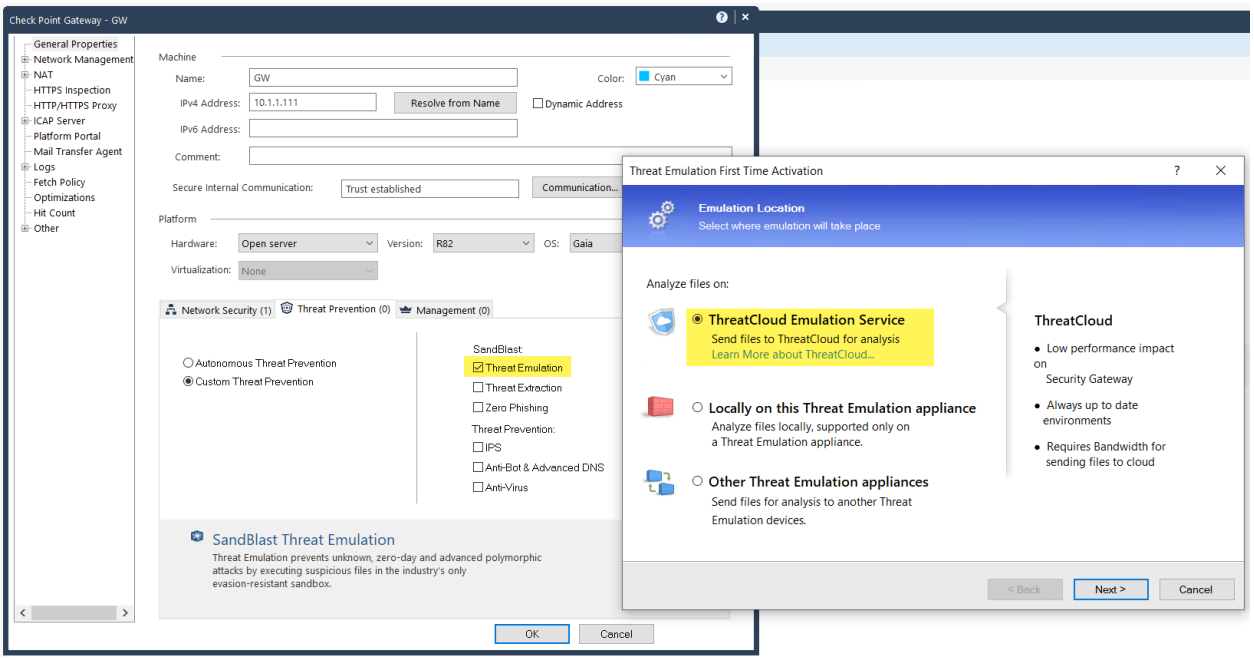
Introduction

quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The emulation service reports and automatically shares the newly identified threat information with other customers.

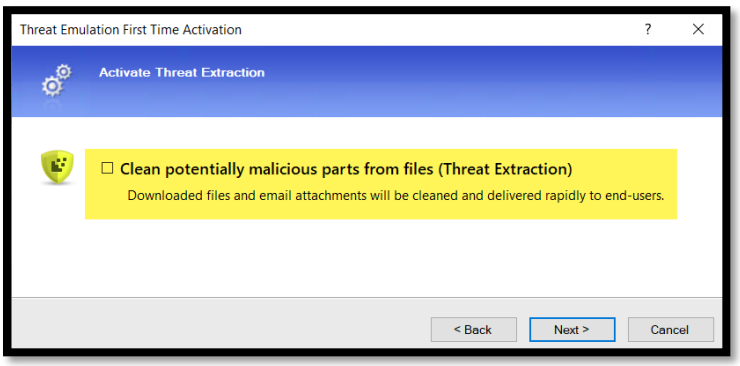
Exercise 1: Onboarding

In this exercise, we will enable the Threat Emulation blade. We do not have a local TE appliance, and we will be sending the files to the Threat Cloud for emulation.

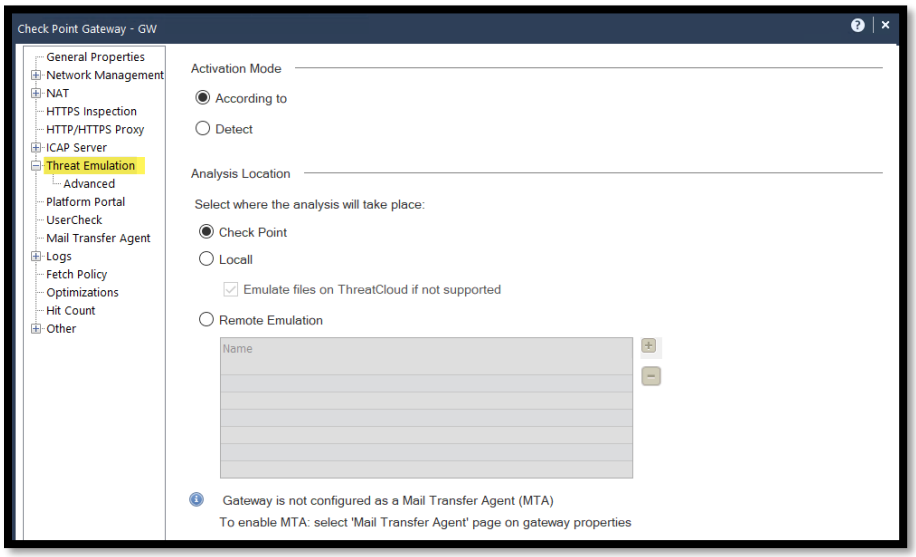
1. Edit the GW object and enable the Threat Emulation blade. Disable all other Threat Prevention blades.



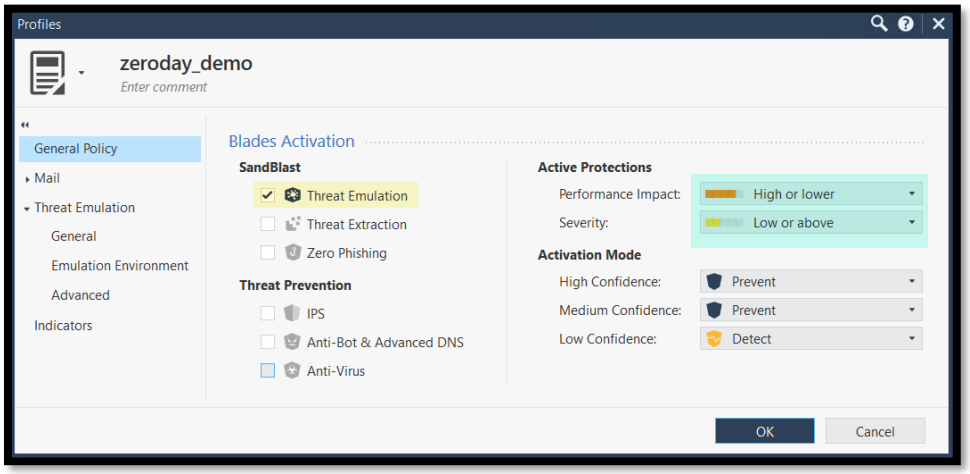
2. In the activation wizard, use the default choice to send the files to the Threat Cloud, and uncheck the option to enable Threat Extraction for now.



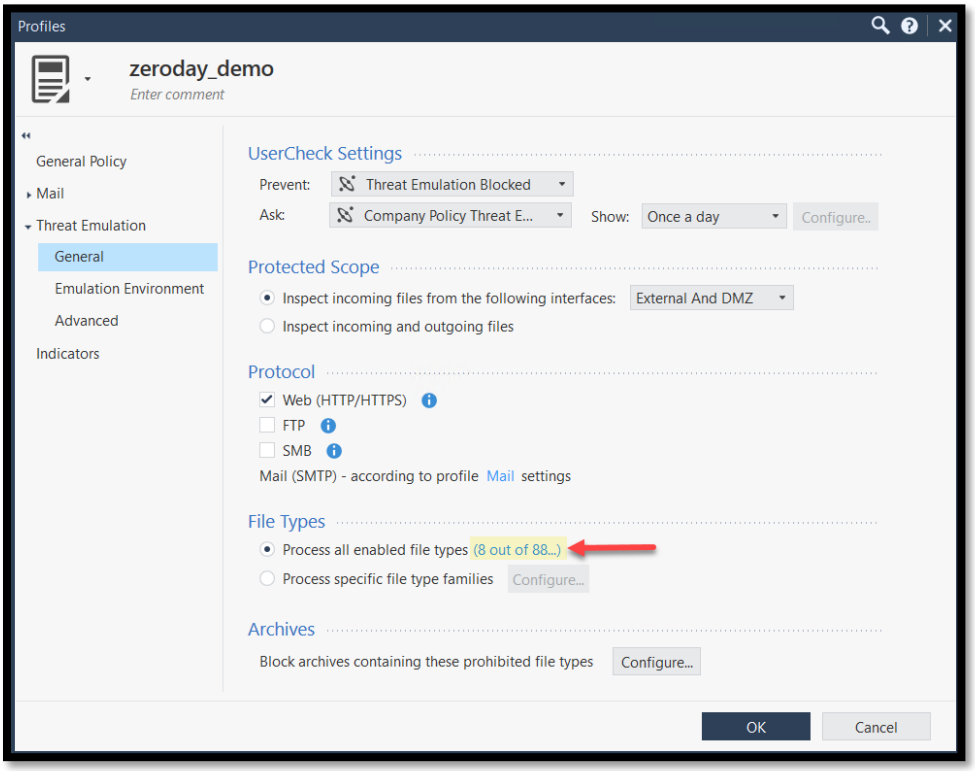
3. Review the Threat Emulation tab, notice that all the choices we made via the first time wizard can be modified later.



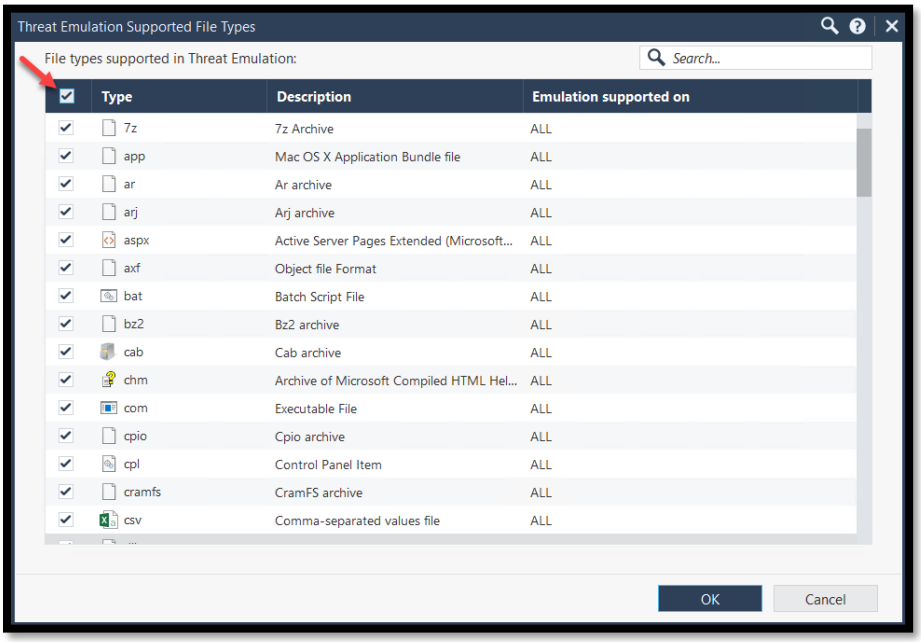
4. Create a new profile with only Threat Emulation Enabled.



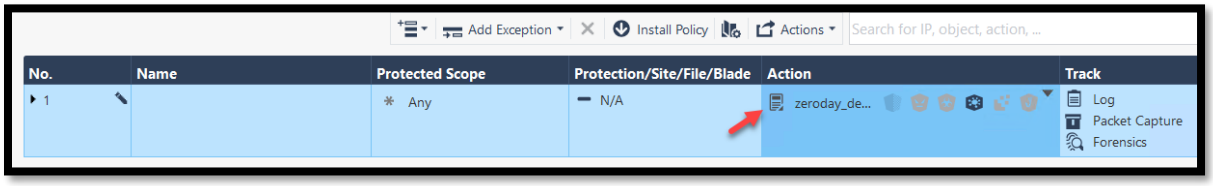
5. Review the settings under the General tab and click on the enabled file link. By default only a few file types are enabled by default.



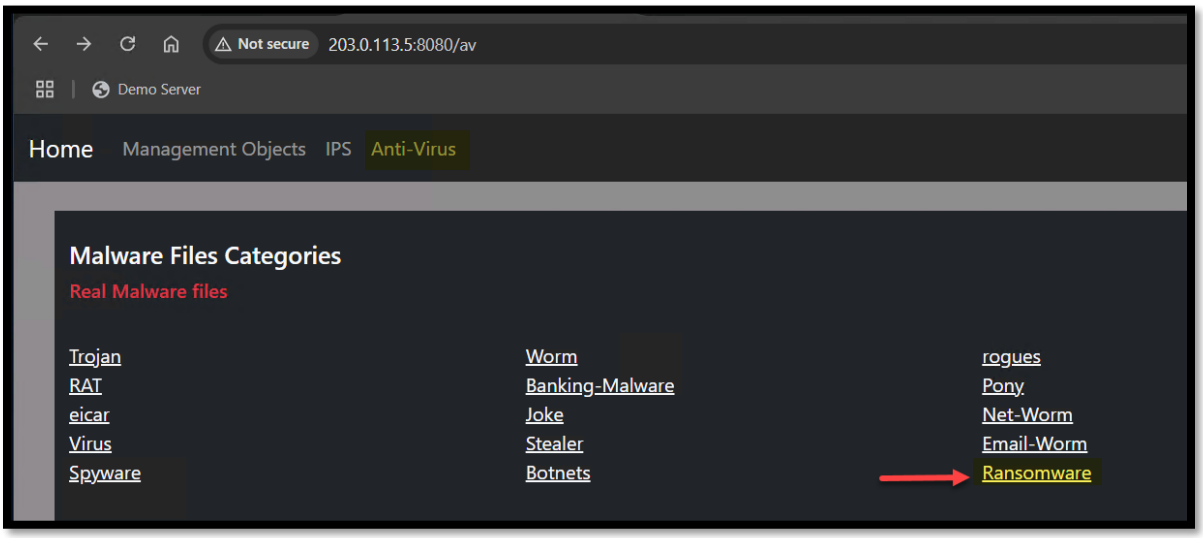
6. Check all supported file types. The Threat Emulation blade will investigate all supported file types.



7. Confirm that the correct profile is assigned to the Threat Prevention rule and Install the Access Control and Threat Prevention Policies.

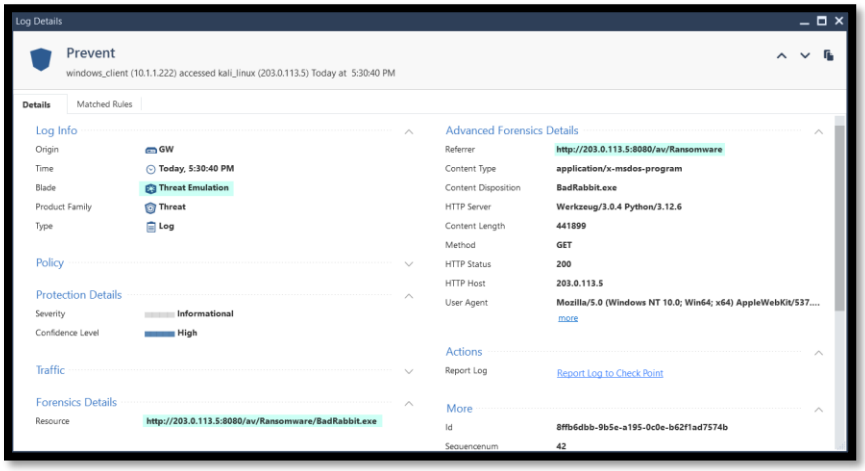


8. From the Windows client, open the demo server and open the Ransomware directory

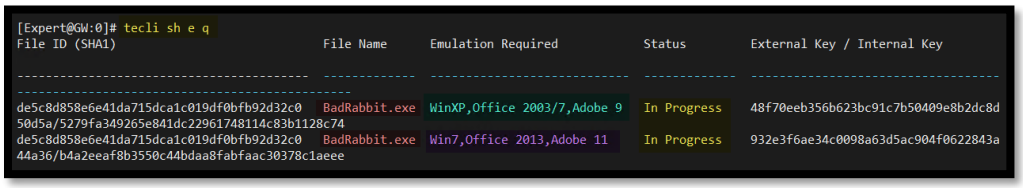


9. Try to download the BadRabbit.exe ransomware.

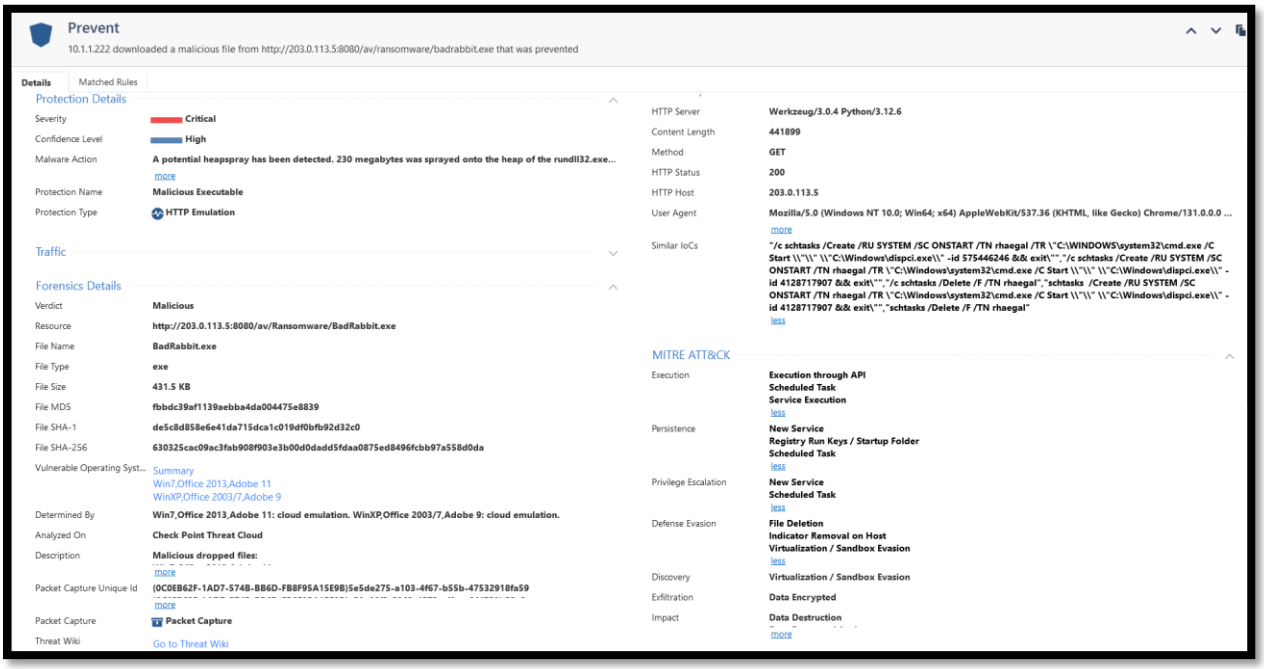
10. Check the log in SmartConsole, notice that the log still has limited fields. The investigation is expected to take around 5 minutes to complete even though the file is blocked instantly.



11. To monitor the progress of the file investigation on the cloud, connect to the GW over shh and use the command (tecli show cloud queue).



12. Once the investigation is done and the queue is empty, refresh the logs and notice that the log file was updated with the full investigation results.



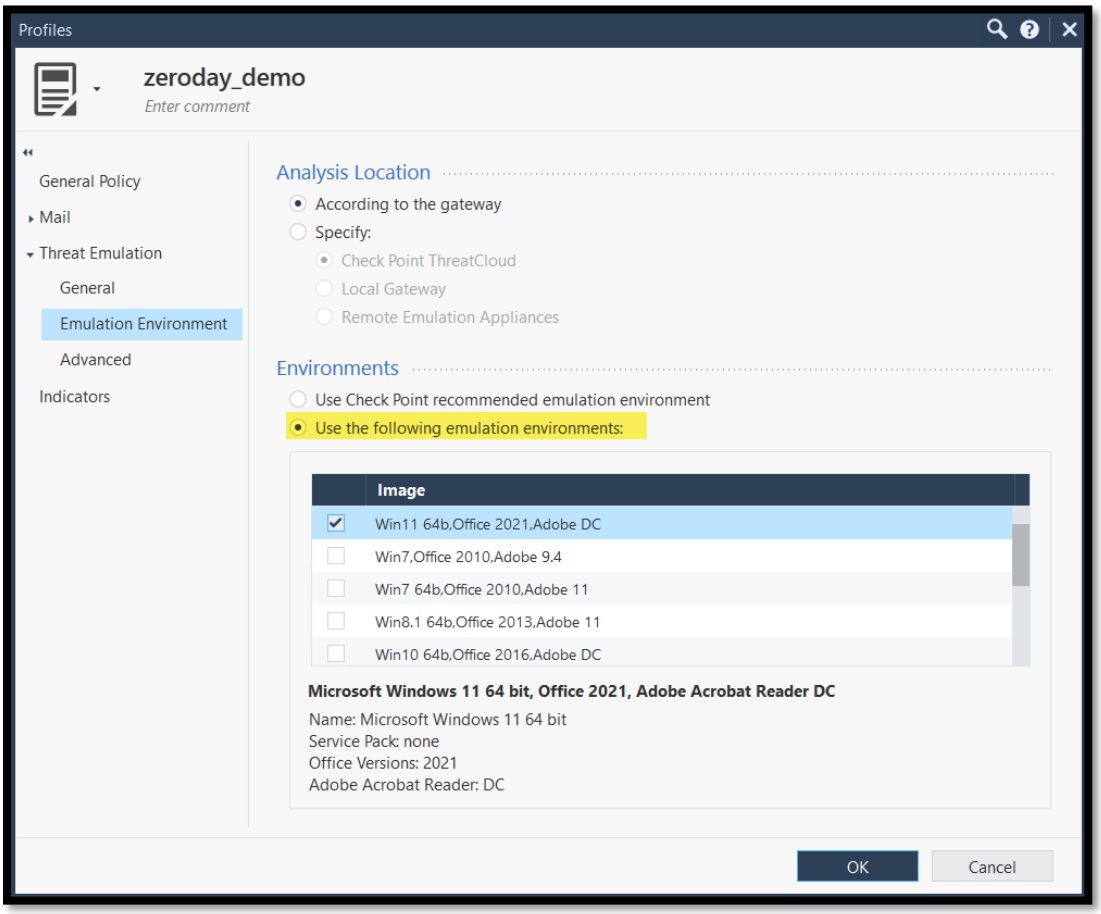
Exercise 2: Threat Emulation Reports

Exercise 3: Threat Emulation Environment

By Default, all files are analyzed on the recommended images, Windows XP and windows7 with Adobe 11 and MS Office 2013 installed. Those two OS versions are less secure than the more recent versions and more malicious activities might be recorded.

However, in some cases, we would like to change the analysis to be done on specific images. In this exercise, we will change the emulation to be done only on Windows 11 images.

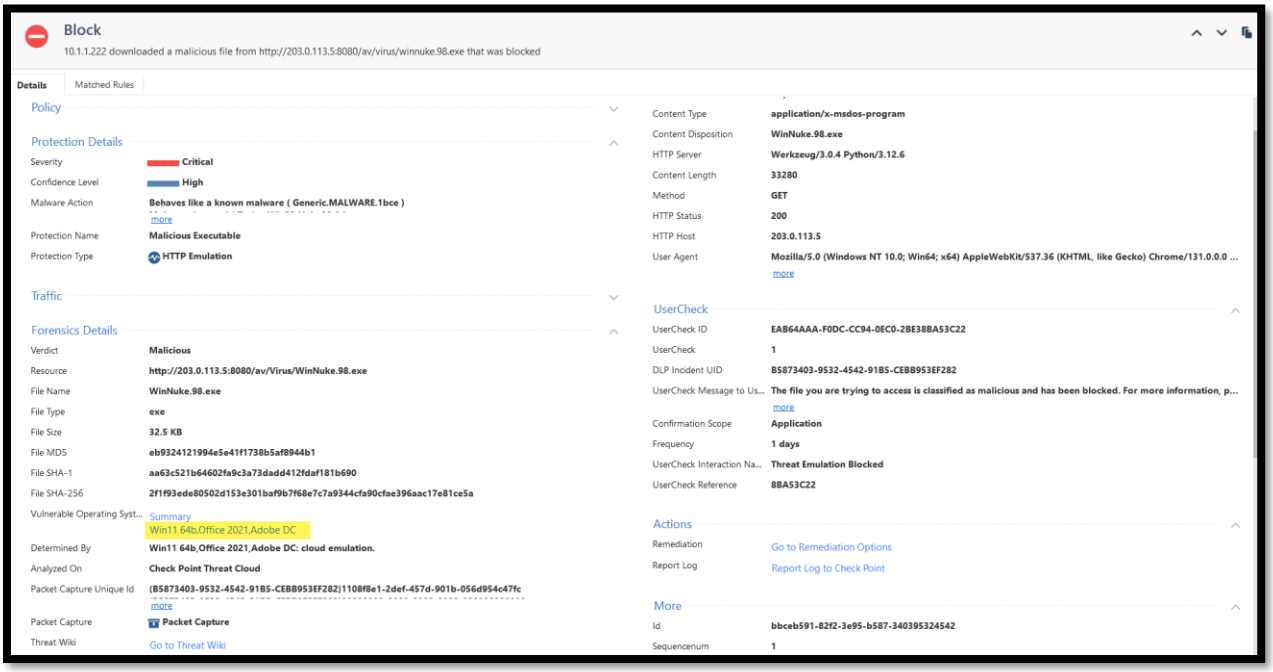
1. Edit the profile and change the emulation environment to Windows 11 only. Notice that the Log will only show a repot form windows 11. Install the Threat Prevention policy.



2. Try to download a malicious file from the demo server. Notice that while the file can be blocked instantly, the full report will be available once the analysis is complete. Monitor the progress of the file analysis using the command:
   - tecli sh em que


```
Last login: Thu Nov 28 13:44:23 2024 from 10.1.1.200
[Expert@GW:0]# tecli sh e q
File ID (SHA1)                            File Name      Emulation Required            Status         External Key / Internal Key

----------------------------------------  -------------  ----------------------------  -------------  ----------------------------
----------------------------------------------------
aa63c521b64602fa9c3a73dadd412fdaf181b690   WinNuke.98...  Win11 64b,Office 2021,Ado...  In Progress    b68c34831d505d38d550adb764e90
9809e8f0a21/3195dcb4e98ae60599edc6dfa2e695e9b5d064cf
```

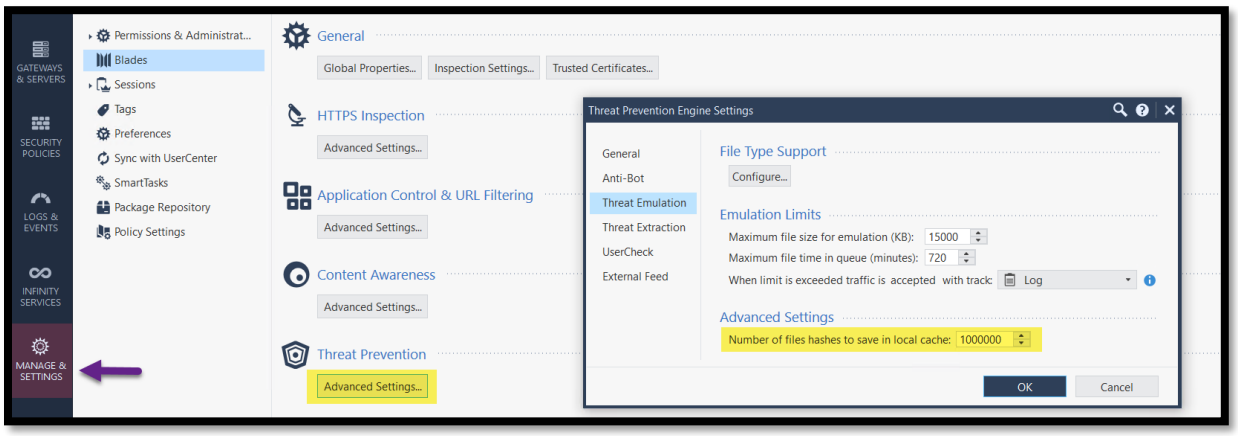
3. Once the Emulation is done and the queue is empty, review the logs and notice that OS and the report is showing windows 11 as expected.



Exercise 4: Threat Emulation Advanced Settings

Multiple settings can be modified globally to all Threat Emulation enabled Gateways. Those settings include, The maximum file size scanned by TE, the time files wait in queue, cache size and the file type support. We will navigate through the settings in this escercise.

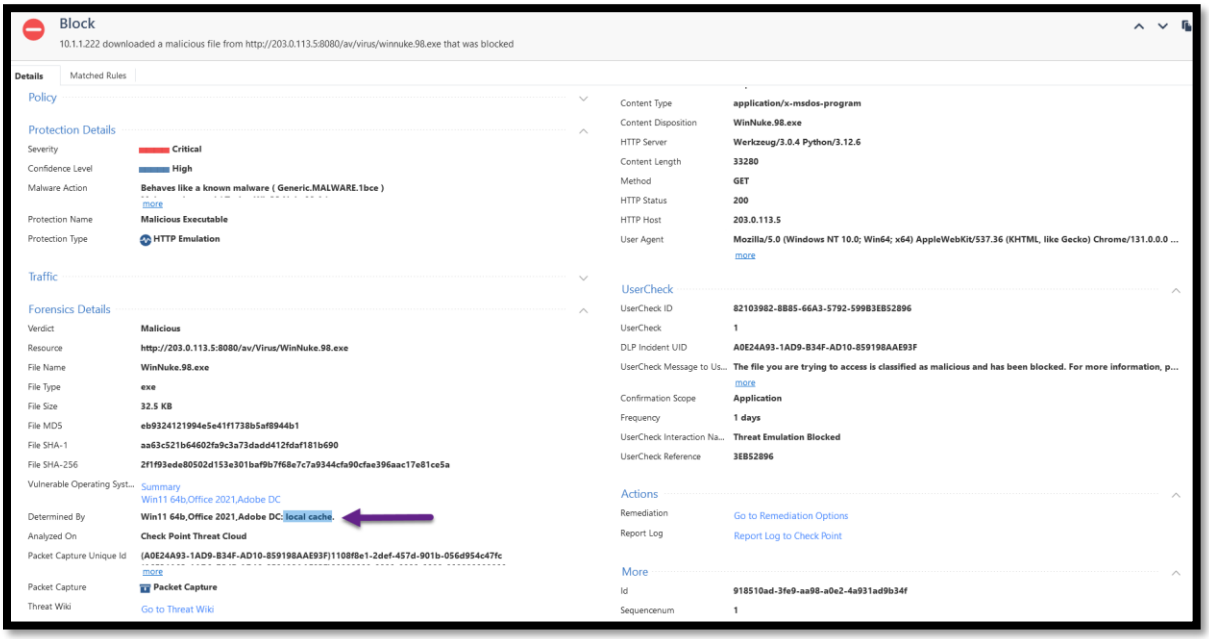
1. Navigate to the Threat Prevention advanced settings. Notice that the Maximum file size scanned by default is 15 MB. The size of cache is 1M entries.



2. Login to the GW over SSH and review the content of the local cache. Use the command “tecli cache dump all” to see the content of the cache.

```
[Expert@GW:0]# tecli cache dump all

Images Uid List
===============
Image UID: 1108f8e1-2def-457d-901b-056d954c47fc, Image: Win11 64b,Office 2021,Adobe DC

|sha1                                    |file type |image                        |verdict   |confidence|severity  |date      |hits |ttl       |comment
|----------------------------------------|----------|-----------------------------|----------|----------|----------|----------|-----|----------|----------
---------
|e686139d5ed8528117ba6ca68fe415e4fb02f2be|exe       |Win7,Office 2013,Adobe 11    |malicious |High      |Critical  |11-28-2024|1    |12-6-2024 |dlpu_te

|e686139d5ed8528117ba6ca68fe415e4fb02f2be|exe       |WinXP,Office 2003/7,Adobe 9  |malicious |High      |Critical  |11-28-2024|1    |12-6-2024 |dlpu_te

|747070c74d0400cffeb28fbea17b64297f14cfbd|exe       |Win7,Office 2013,Adobe 11    |malicious |High      |Critical  |11-28-2024|1    |12-6-2024 |dlpu_te
```

3. Files that are handled already, have entries in the local cache. In case a file verdict is already knows and saved in the cache, the decision will be forced without having to rescan the file. Try to download a file twice and notice that the second attempt is blocked based on the decision from the local cache.



4. To clear the cache entries, use the command “Tecli cache clean” or tecli c c

```
[Expert@GW:0]# tecli c c

[Expert@GW:0]# tecli c d a

Images Uid List
===============
Image UID: 1108f8e1-2def-457d-901b-056d954c47fc, Image: Win11 64b,Office 2021,Adobe DC

|sha1                                    |file type |image                          |verdict   |confidence|severity  |date      |hits |ttl       |comment

|----------------------------------------|----------|-------------------------------|----------|----------|----------|----------|-----|----------|-----------------------
---------
```

5. Attempt to download a file and notice that all files are now go though analysis since the cache is empty.

```
[Expert@GW:0]# tecli sh em qu
File ID (SHA1)                           File Name      Emulation Required            Status         External Key / Internal Key

----------------------------------------- -------------- ----------------------------- -------------- ------------------------------------------------------------------------------
---------
713b4678c05a76dbd22e6f8d738c9ef655e70226  Gnil.exe       Win11 64b,Office 2021,Ado...  In Progress    2a01d30b45c28faa6d7b1fd101900489256476af/505262f1dd0139a9ec38f6bbc66792e5
fdc6037e
```

End of Lab 8

