

Threat Emulation

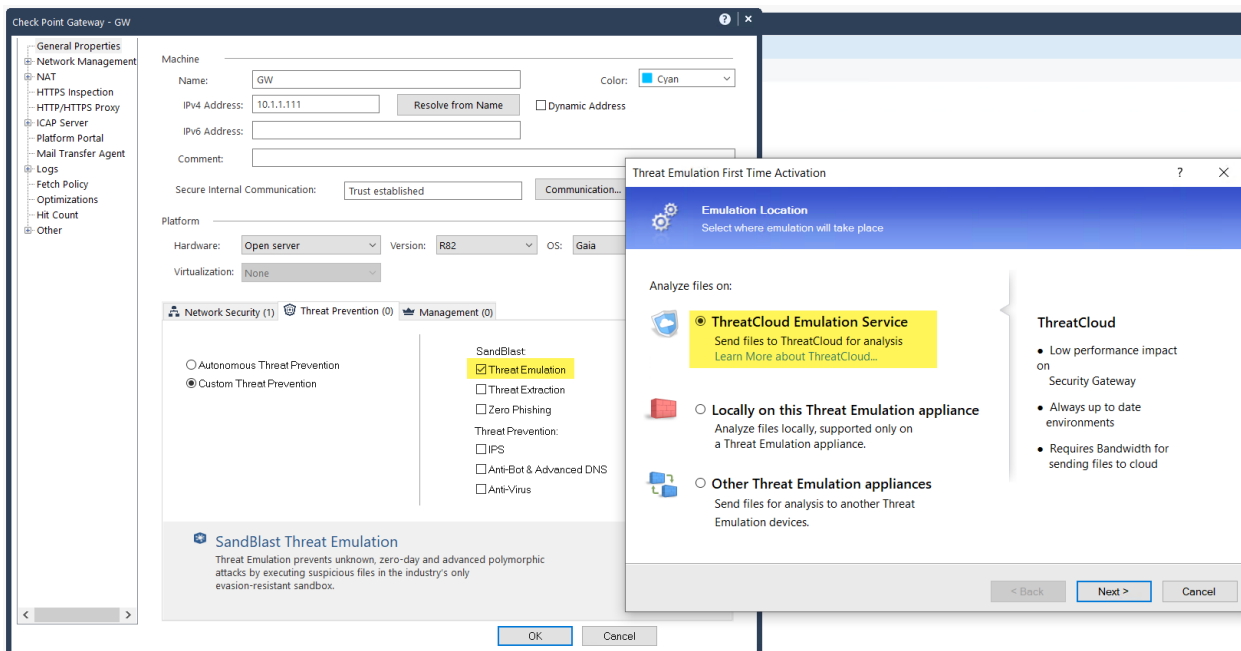
Introduction

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.

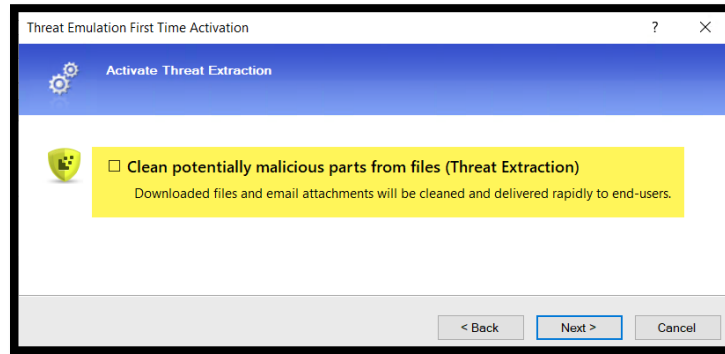
Exercise 1: Onboarding

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.

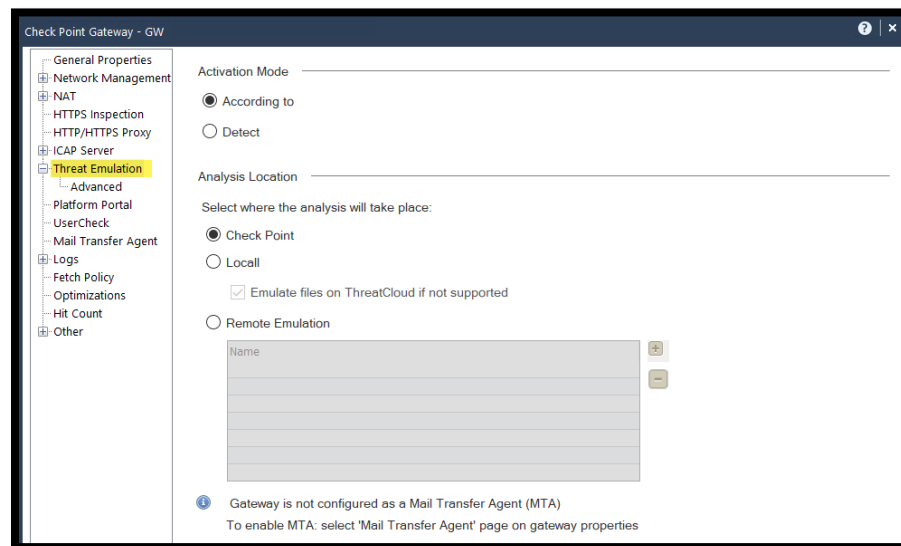
1. Edit the GW object and enable the Threat Emulation blade. Disable all other Threat Prevention blades.



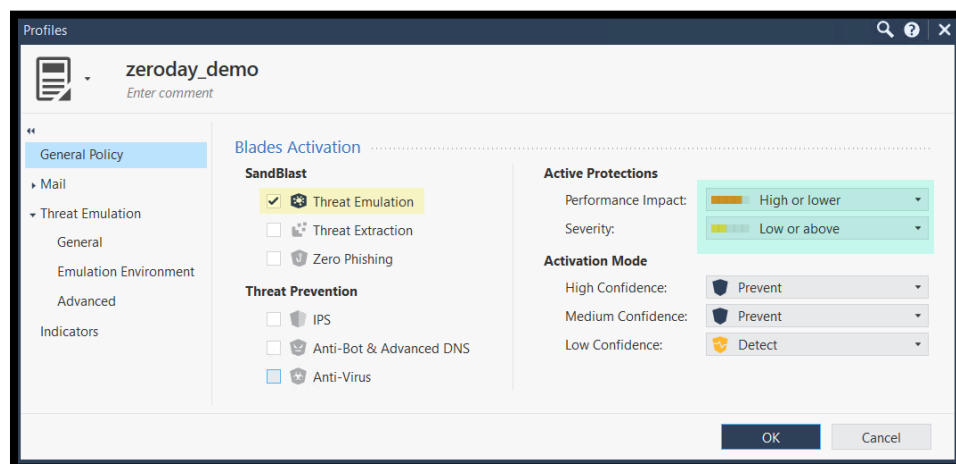
2. In the activation wizard, use the default choice to send the files to the Threat Cloud, and uncheck the option to enable Threat Extraction for now.



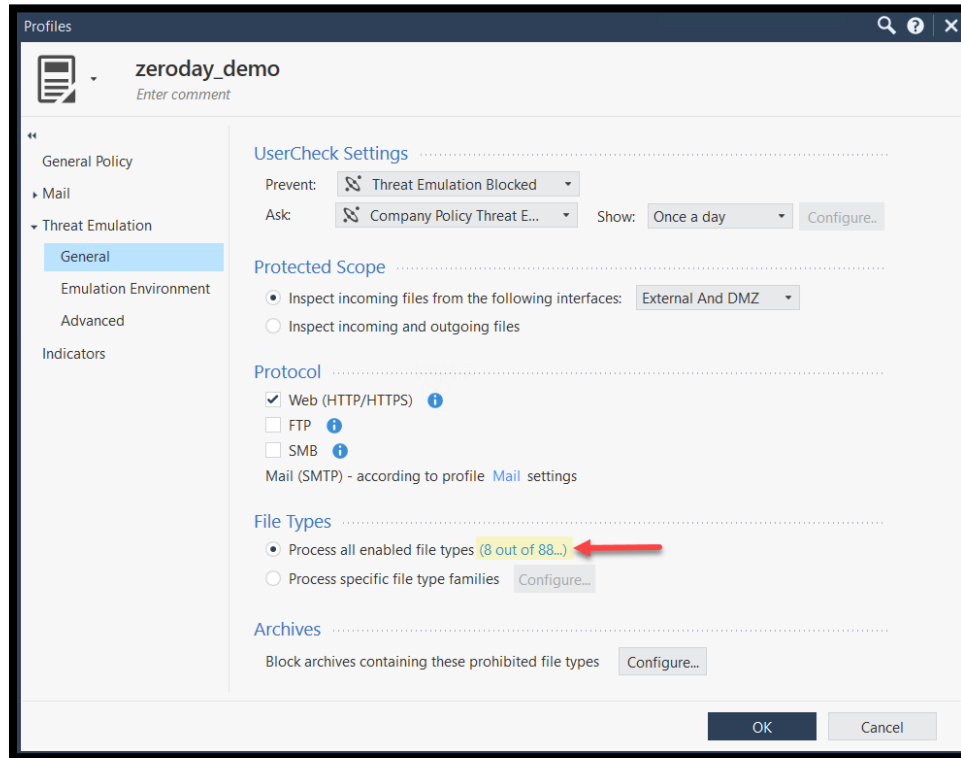
- Review the Threat Emulation tab, notice that all the choices we made via the first time wizard can be modified later.



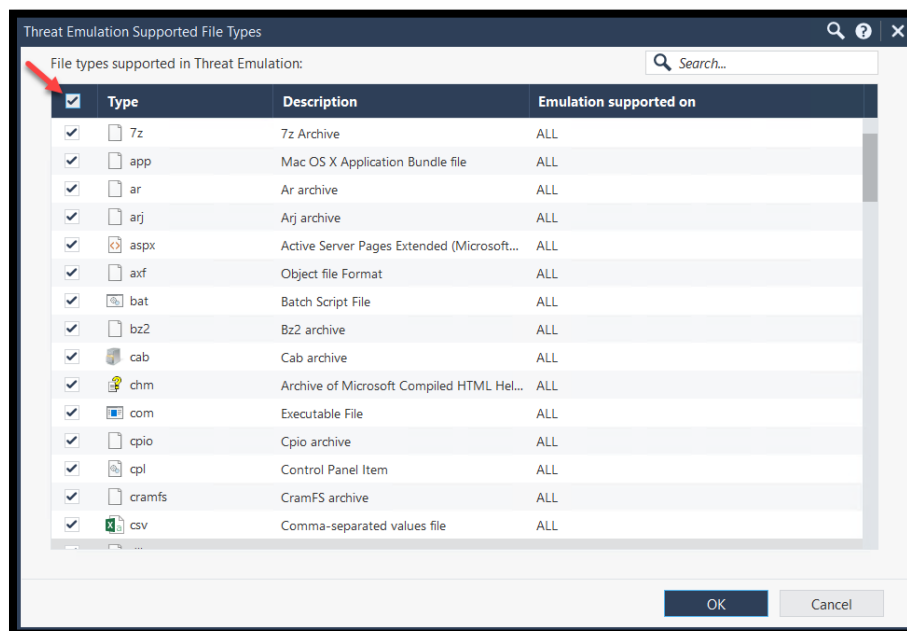
- Create a new profile with only Threat Emulation Enabled.



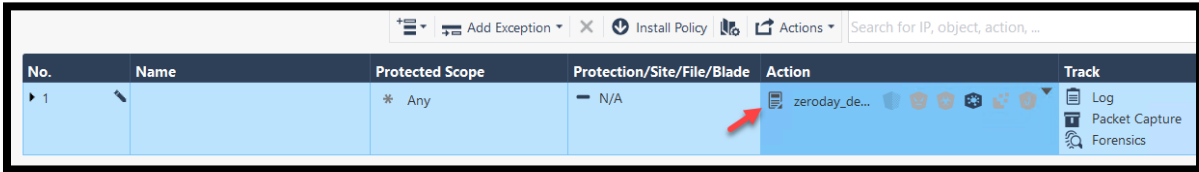
- Review the settings under the General tab and click on the enabled file link. By default only a few file types are enabled by default.



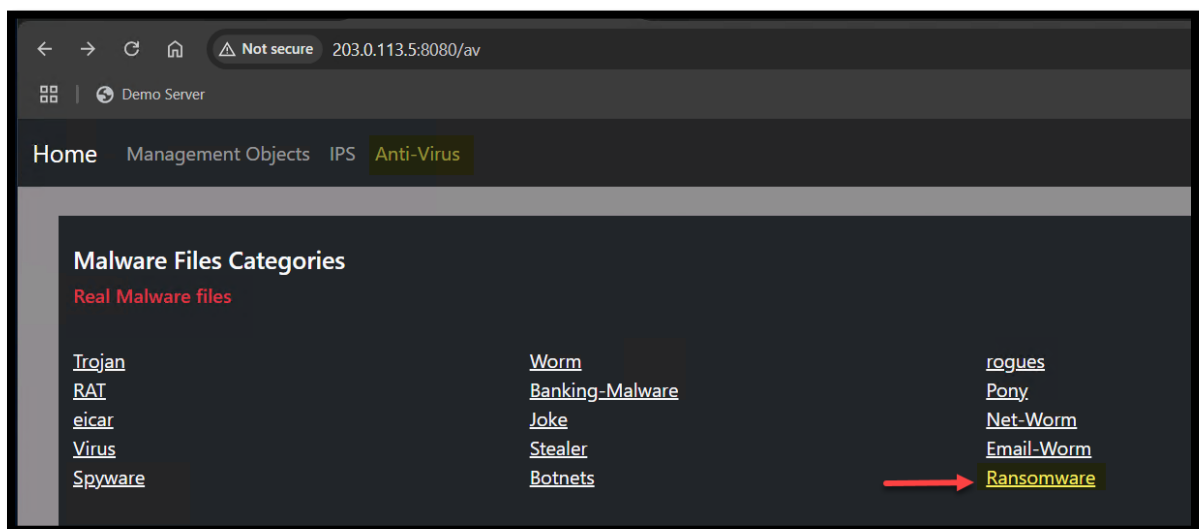
- Check all supported file types. The Threat Emulation blade will investigate all supported file types.



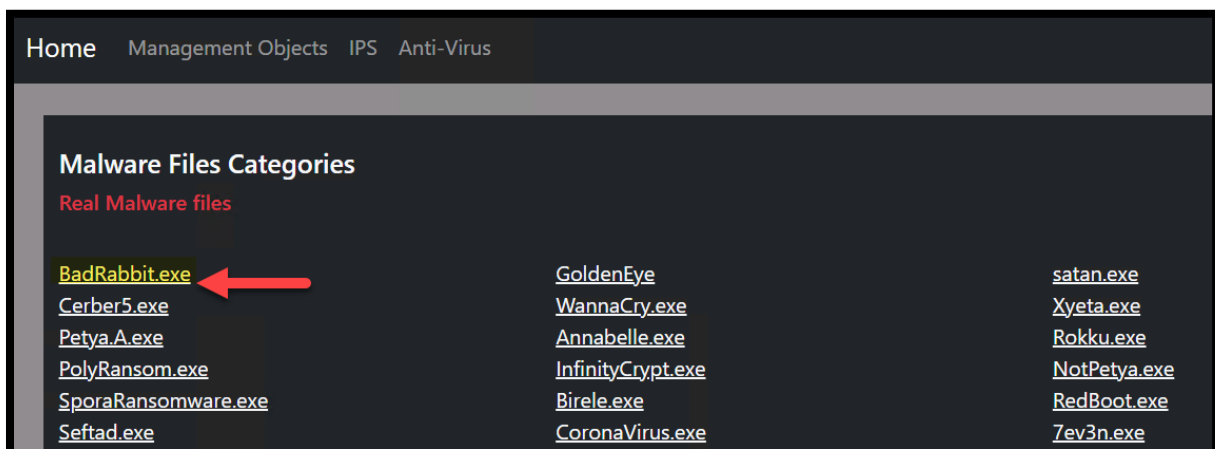
- Confirm that the correct profile is assigned to the Threat Prevention rule and Install the Access Control and Threat Prevention Policies.



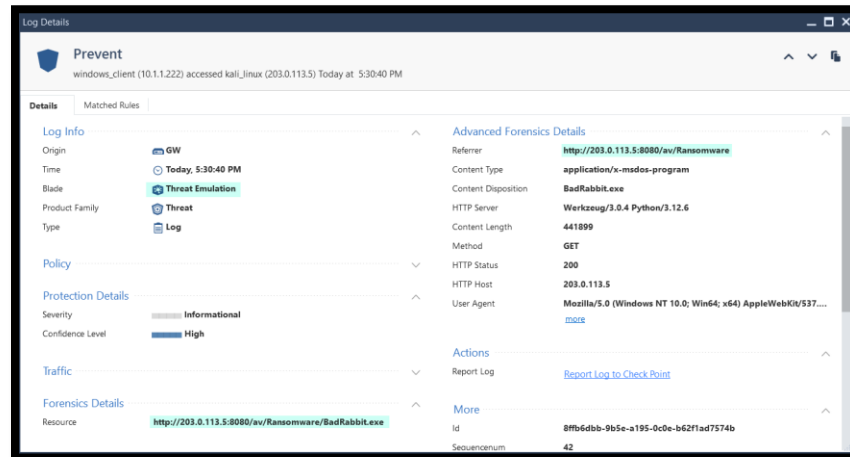
- From the Windows client, open the demo server and open the Ransomware directory



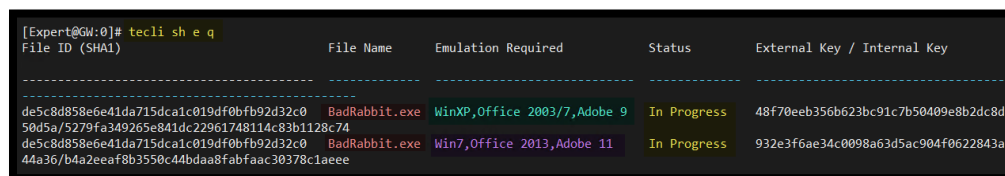
- Try to download the BadRabbit.exe ransomware.



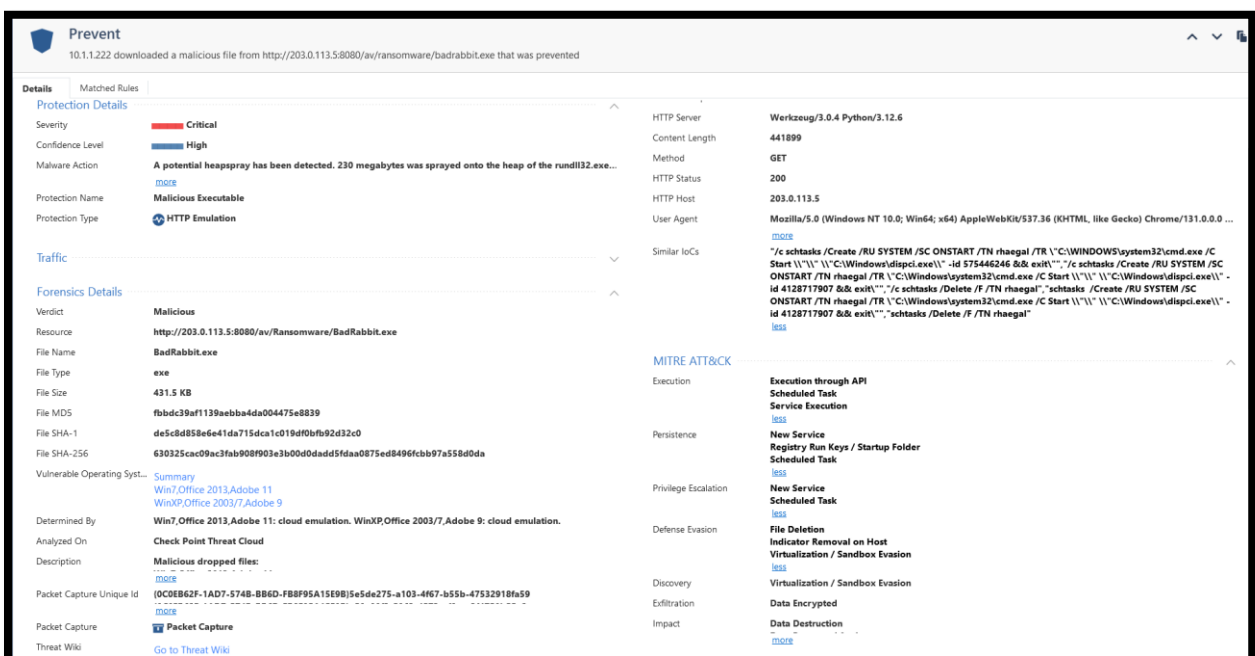
- Check the log in SmartConsole, notice that the log still has limited fields. The investigation is expected to take around 5 minutes to complete even though the file is blocked instantly.



11. To monitor the progress of the file investigation on the cloud, connect to the GW over ssh 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.



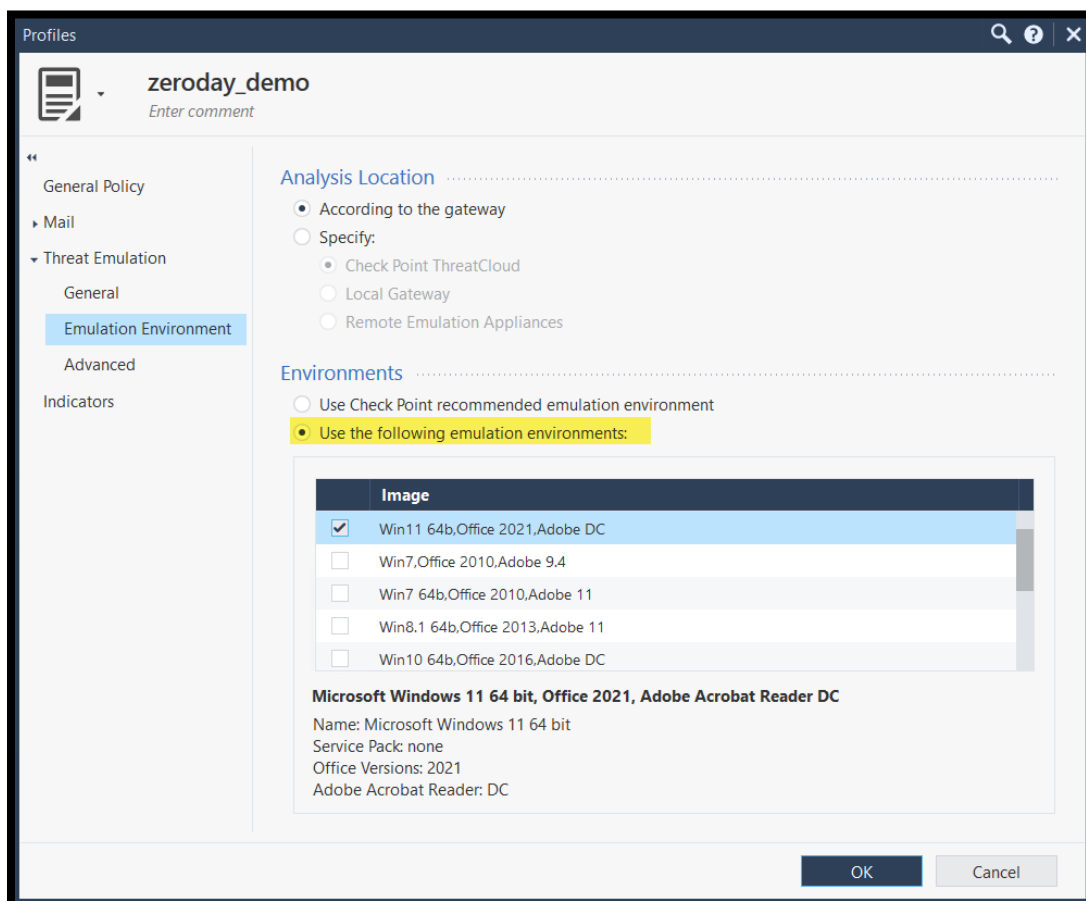
Exercise 2: Threat Emulation Reports

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 report from 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:
 - o `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 ID (SHA1)	File Name	Emulation Required	Status	External Key / Internal Key
aa63c521b64602fa9c3a73dadd412fdaf181b690 9809e8f0a21/3195dcb4e98ae60599edc6dfa2e695e9b5d064cf	WinNuke.98...	Win11 64b,Office 2021,Ado...	In Progress	b68c34831d505d38d550adb764e90

- 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.

Block

10.1.1.222 downloaded a malicious file from http://203.0.113.5:8080/av/virus/winnuke.98.exe that was blocked

Details

Matched Rules

Policy

Protection Details

Severity

Confidence Level

Malware Action

Protection Name

Protection Type

Traffic

Forensics Details

Verdict

Resource

File Name

File Type

File Size

File MD5

File SHA-1

File SHA-256

Vulnerable Operating Syst...

Determined By

Analyzed On

Packet Capture Unique Id

Packet Capture

Threat Wiki

Content Type

Content Disposition

HTTP Server

Content Length

Method

HTTP Status

HTTP Host

User Agent

UserCheck

UserCheck ID

UserCheck

DLP Incident UID

UserCheck Message to Us...

Confirmation Scope

Frequency

UserCheck Interaction Na...

UserCheck Reference

Actions

Remediation

Report Log

More

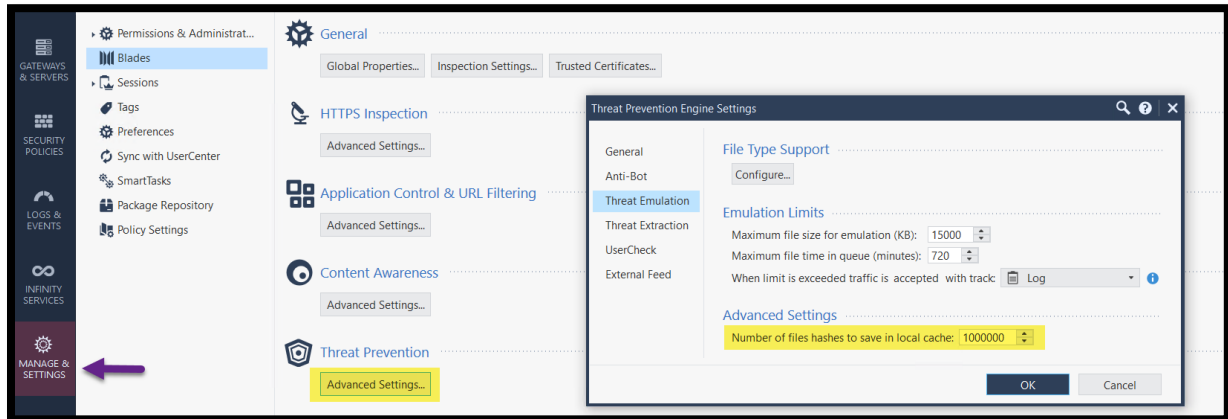
Id

Sequencium

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 exercise.

- 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.



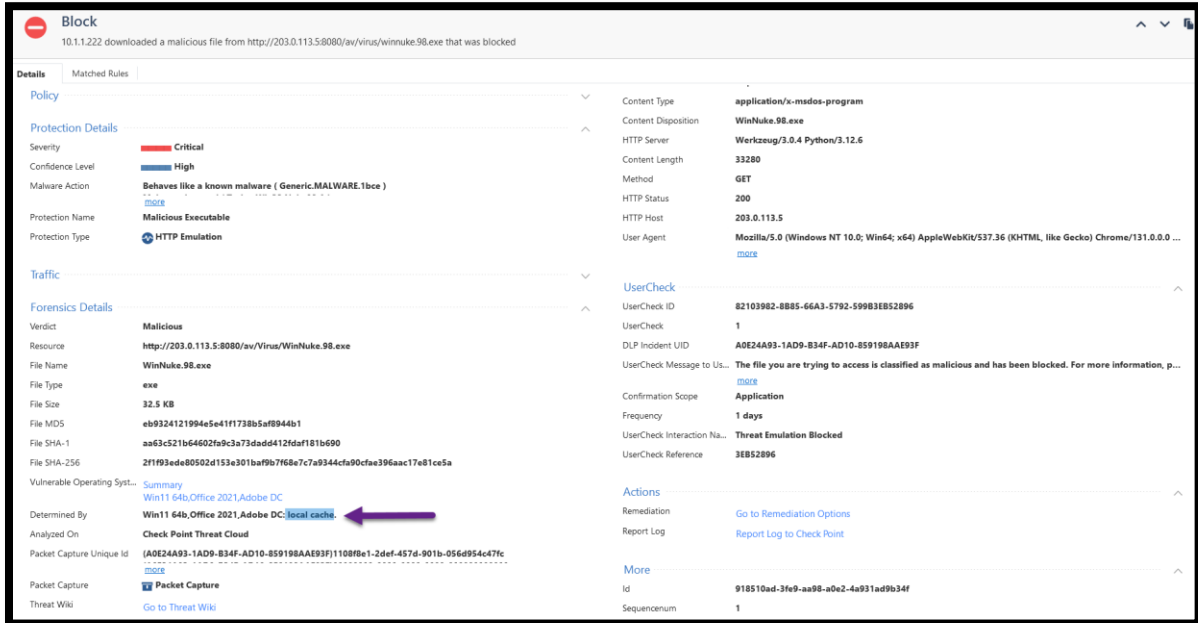
2. Login to the GW over SSH and review the content of the local cache. Use the command “tecli cache dump all” to see the content of the cache.

```
[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
|747070c74d0400cffe28f8ea17b64297f14cfbd|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 known 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.



Block
10.1.1.222 downloaded a malicious file from http://203.0.113.5:8080/av/virus/winuke.98.exe that was blocked

Details | Matched Rules

Policy

Protection Details

Severity: Critical

Confidence Level: High

Malware Action: Behaves like a known malware (Generic.MALWARE.1bce) [more](#)

Protection Name: Malicious Executable

Protection Type: HTTP Emulation

Traffic

Forensics Details

Verdict: Malicious

Resource: http://203.0.113.5:8080/av/virus/winuke.98.exe

File Name: WinNuke.98.exe

File Type: exe


File Size: 32.5 KB

File MD5: eb9324121994e5e41f1738b5af9944b1

File SHA-1: aa63c521b64602f9c3a73dadd412daf181b690

File SHA-256: 2f1f93ede80502d153a301ba9b7f68e7c7a9344cfa90cfae396aac17e81ce5a

Vulnerable Operating Syst... [Summary](#)

Determined By: Win11 64b,Office 2021,Adobe DC [Local cache](#) 

Analyzed On: [Check Point Threat Cloud](#)

Packet Capture Unique Id: (A0E24A93-1AD9-B34F-AD10-859198AAE93F)1108f8e1-2def-457d-901b-056d954c47fc [more](#)

Packet Capture: Packet Capture

Threat Wiki: [Go to Threat Wiki](#)

Content Type: application/x-msdos-program

Content Disposition: WinNuke.98.exe

HTTP Server: Werkzeug/3.0.4 Python/3.12.6

Content Length: 33280

Method: GET

HTTP Status: 200

HTTP Host: 203.0.113.5

User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 ... [more](#)

UserCheck

UserCheck ID: 82103982-8B85-66A3-5792-59983E852896

UserCheck: 1

DLP Incident UID: A0E24A93-1AD9-B34F-AD10-859198AAE93F

UserCheck Message to Us...: The file you are trying to access is classified as malicious and has been blocked. For more information, p... [more](#)

Confirmation Scope: Application

Frequency: 1 days

UserCheck Interaction Na...: Threat Emulation Blocked

UserCheck Reference: 3EB52896

Actions

Remediation: [Go to Remediation Options](#)

Report Log: [Report Log to Check Point](#)

More

Id: 918510ad-3fe9-aa98-a0e2-4a931ad9b34f

Sequencium: 1

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 through analysis since the cache is empty.

```
[Expert@GW:0]# tecli sh em qu
File ID (SHA1)File NameEmulation RequiredStatusExternal Key / Internal Key
-----
713b4678c05a76dbd22e6f8d738c9ef655e70226Gnil.exeWin11 64b,Office 2021,Ado...In Progress2a01d30b45c28faa6d7b1fd101900489256476af/505262f1dd0139a9ec38f6bbc66792e5fd6037e
```

End of Lab 8