

Anti-Virus

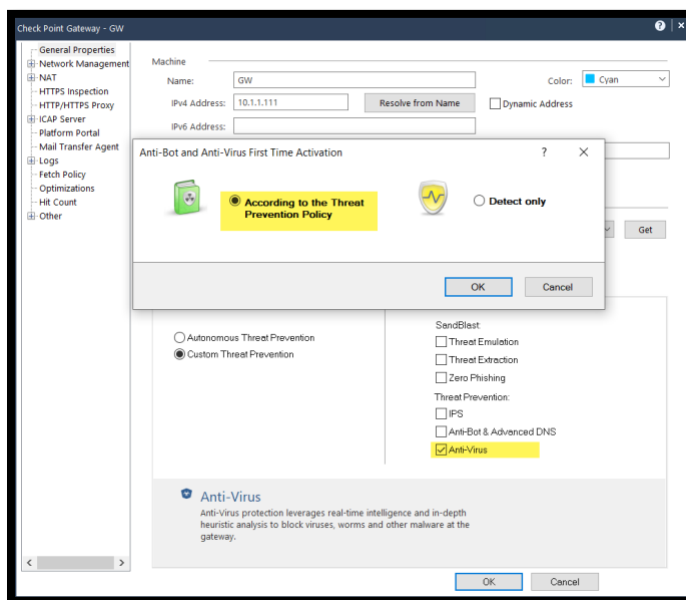
Introduction

Anti-virus solutions protect computers and remove malicious software or code designed to damage computers or data. Advanced anti-virus solution adopts methodologies that combine global scanning, human expert threat analysis, industry collaboration, cloud integration, and alerting services.

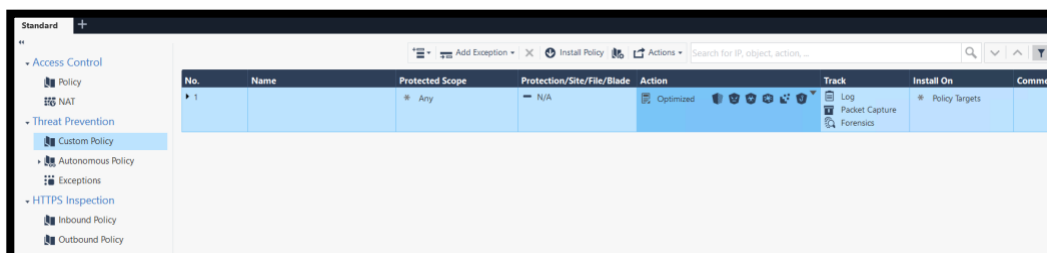
Exercise 1: Onboarding

In this exercise, we will enable and test the protections provided by the Anti-Virus blade.

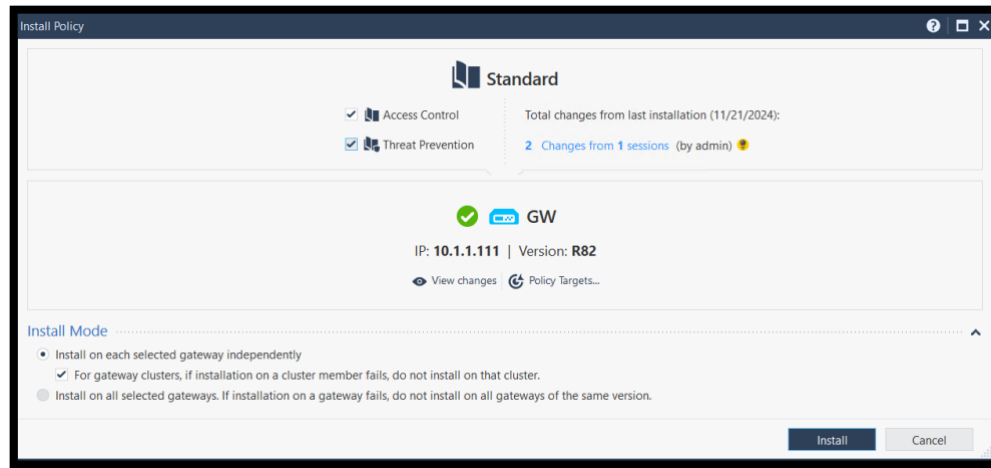
1. Edit the **GW** object and enable the **Anti-virus** blade. Make sure the **IPS** blade is disabled. And save the changes.



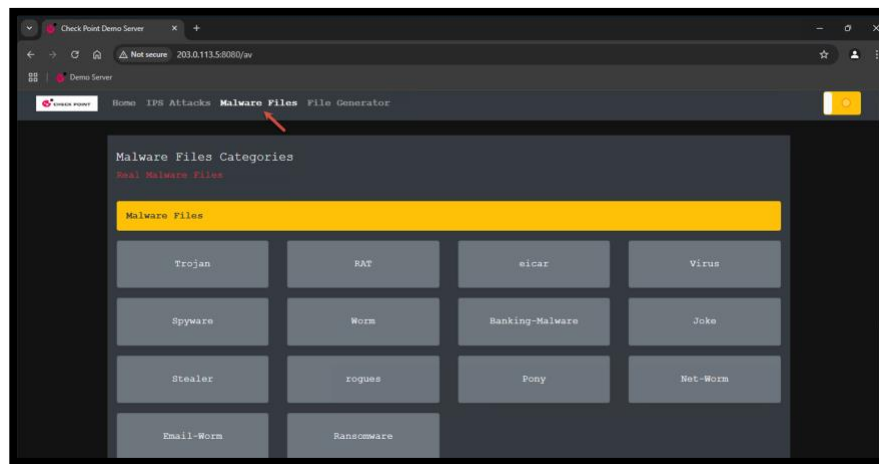
2. Review the default Threat Prevention and the assigned profile.



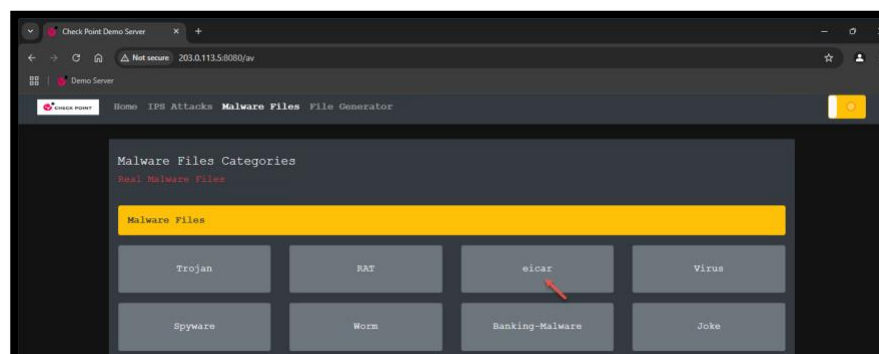
3. Install the **Access Control** and the **Threat Prevention** Policies.



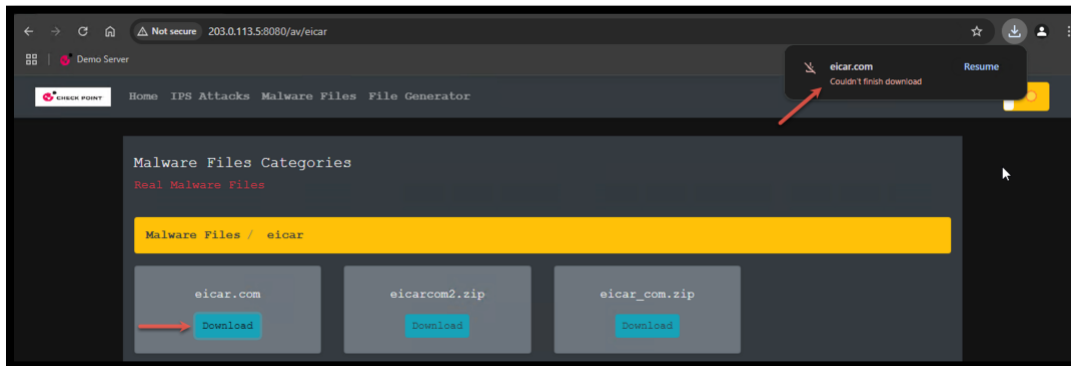
4. Open the RDP session to **win_client** and use the bookmarked link to access the Demo server <http://203.0.113.5:8080>



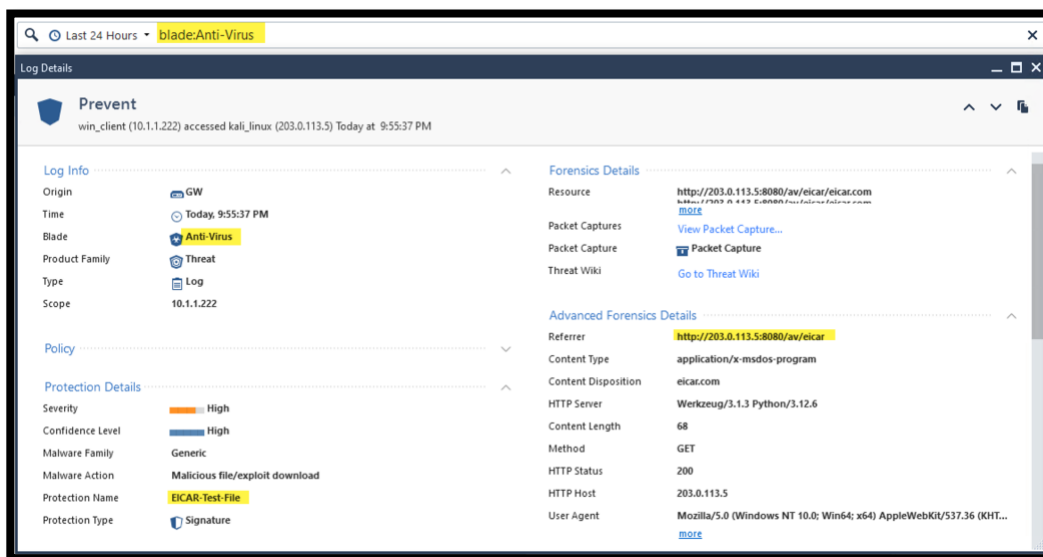
5. While in the Anti-Virus test page, open the **eicar** directory.



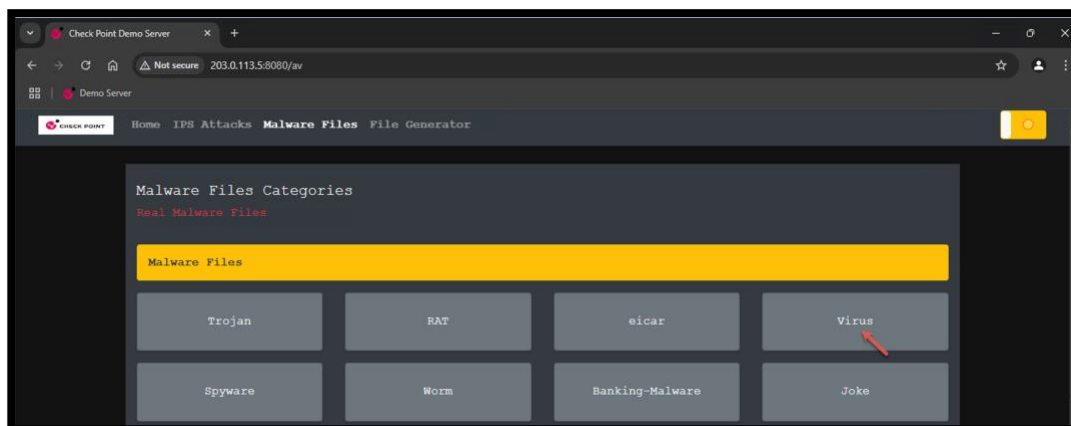
6. Try to download the file eicar.com by clicking on it. Notice that the connection was blocked.



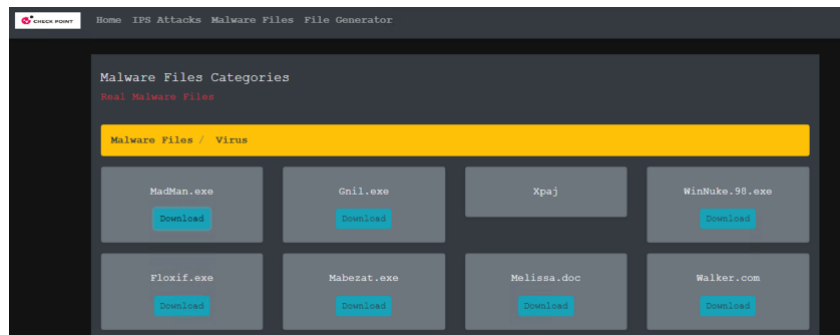
7. From SmartConsole, filter the logs to show only anti-virus logs.



8. From the Windows Client, browse to the **Virus** directory on the demo server.



9. Try to download multiple known malicious files.



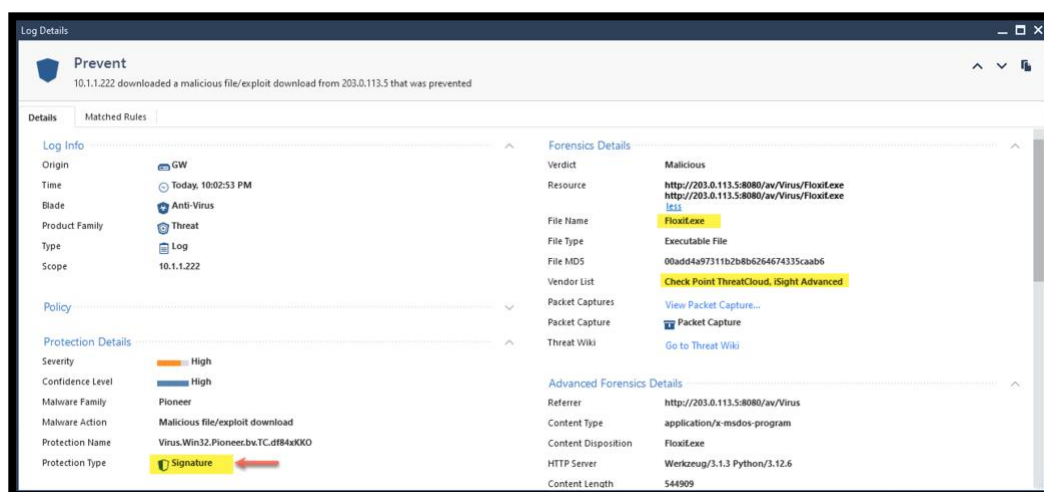
10. Reorder the default columns (drag & drop) to show the **Protection Name**, **File Name** and the **Malware family** fields by default.



Time	B.	A.	Severity	Confide...	S...	Protection Type	Malware Fam...	File Name	Protection Name	File MD5	Malware Acti...	Source	Destination	Resource
Today, 10:03:14 PM						URL Reputation	Nuker	Nuker.TC.7147dPNE	Access to site k...	win_client (10.1.1.222)	kali_linux (203.0...	htt...	htt...	htt...
Today, 10:03:10 PM						URL Reputation	Walker	Walker.TC.839bhalo	Access to site k...	win_client (10.1.1.222)	kali_linux (203.0...	htt...	htt...	htt...
Today, 10:03:06 PM						URL Reputation	Melissa	Melissa.TC.b77bcCJ	Access to site k...	win_client (10.1.1.222)	kali_linux (203.0...	htt...	htt...	htt...
Today, 10:02:54 PM						URL Reputation	Mabezat	Mabezat.TC.e4d8fjw	Access to site k...	win_client (10.1.1.222)	kali_linux (203.0...	htt...	htt...	htt...
Today, 10:02:53 PM						Signature	Pioneer	Floxif.exe	Virus.Win32.Pioneer.bv.TC.d...	00add4a97...	Malicious file/ex...	win_client (10.1.1.222)	kali_linux (203.0...	htt...
Today, 10:02:44 PM						Signature	Generic	Gnil.exe	Trojan.Win32.Generic.TC.d...	37e887b7a...	Malicious file/ex...	win_client (10.1.1.222)	kali_linux (203.0...	htt...
Today, 10:02:42 PM						Signature	Generic	MadMan.exe	Virus.DOS.MadMan.1683.TC...	a56047940...	Malicious file/ex...	win_client (10.1.1.222)	kali_linux (203.0...	htt...
Today, 9:55:37 PM						Signature	Generic	EICAR-Test-File			Malicious file/ex...	win_client (10.1.1.222)	kali_linux (203.0...	h... h... h...

11. Review the log generated for one of the files we tried to download in the previous step.

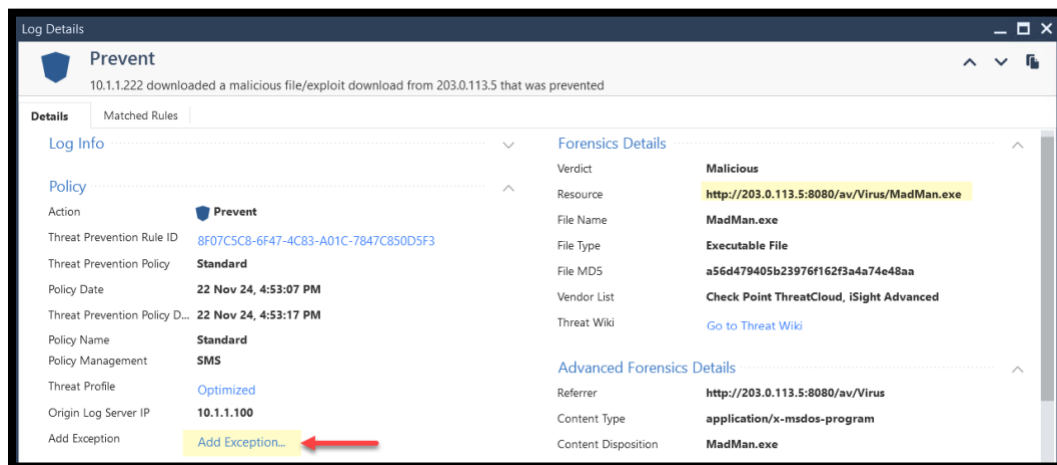
- In many cases, more than one protection or security blade can block the same attack. For example, IPS blade can block the **eicar.com** malware.
- A packet capture is generated like the IPS blade.
- Viruses can be detected by different engines. In the example above, logs that shows a **Reject** action, were detected by the **URL Reputation** engine.
- Such actions are also an indication that the block message is returned to the user.
- Other viruses were detected using their signatures. In those cases, the file download was prevented, and no message is returned.



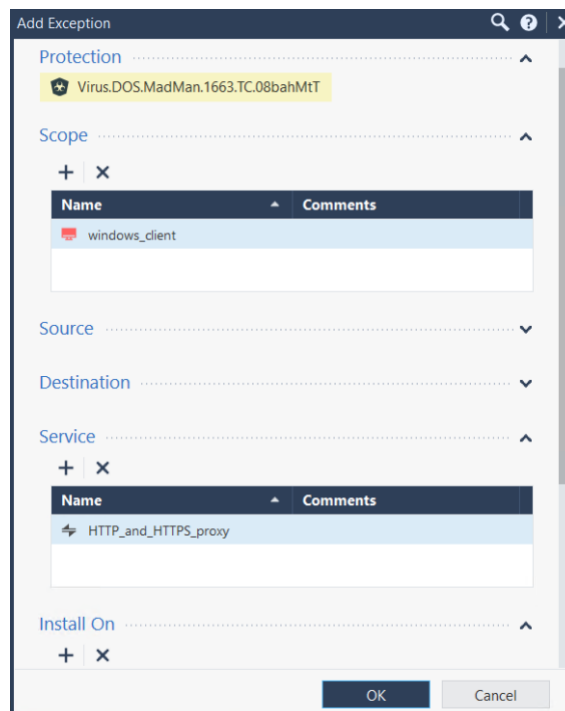
Exercise 2: Exceptions – Overriding the Default Actions

In some scenarios, it is required to override the default action of the Anti-Virus blade. For example, a file is believed to be dropped due to a false-positive verdict, or a file should be delivered for testing purposes. In this exercise, we will test creating such exceptions.

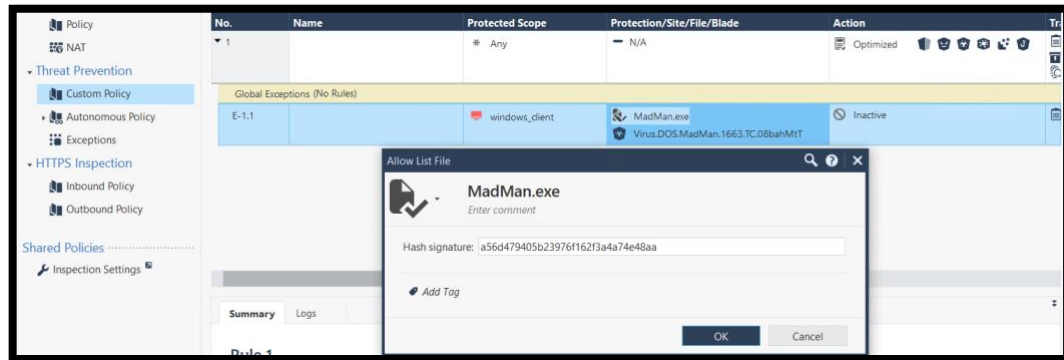
1. In the prevent log file for the last file we downloaded (MadMan.exe), click Add Exception.



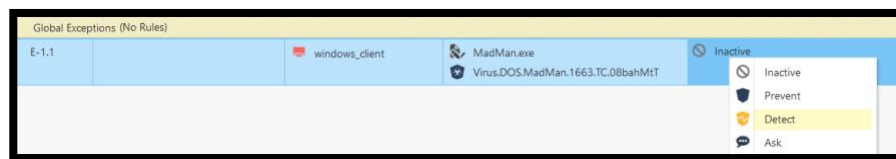
2. Review the fields and save the changes.



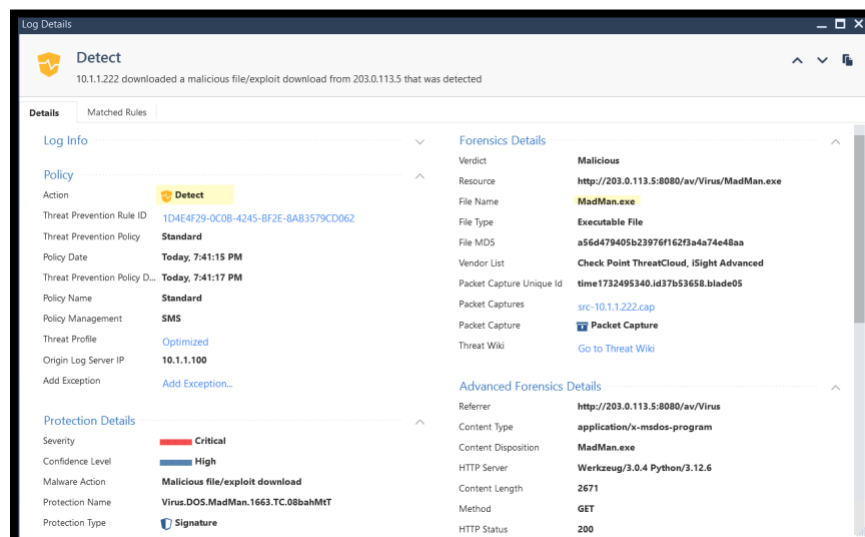
- Review the changes in the Threat Prevention rule base (Expand the rule to see the exception list).



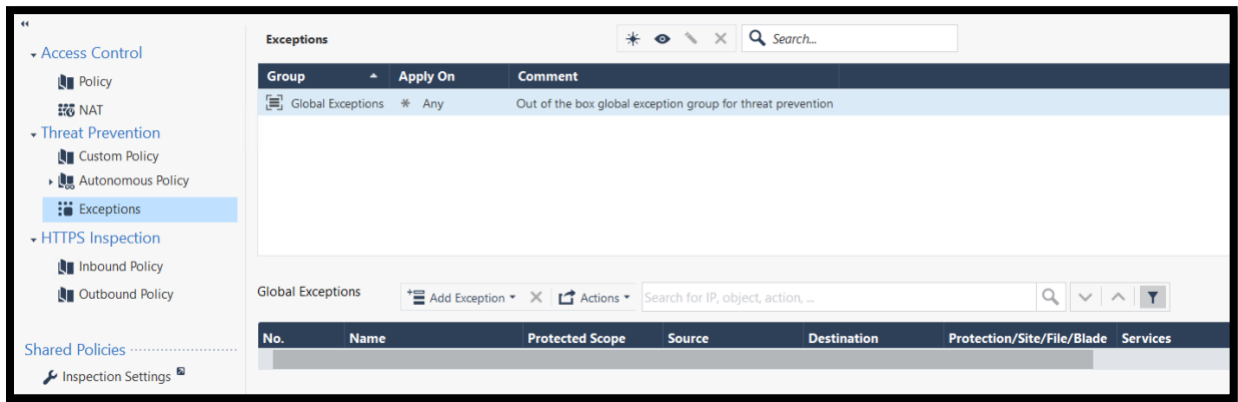
- Note that the exception was added using the protections name and the file hash (MD5).
 - Either one can enforce the rule.
- Change the action of the exception to Detect so we can get a detect log and install the Threat Prevention policy.



- Try to download the same file again and notice it is now possible download the file through the gateway and is blocked by the browser. Review the log and make sure that the file was detected.



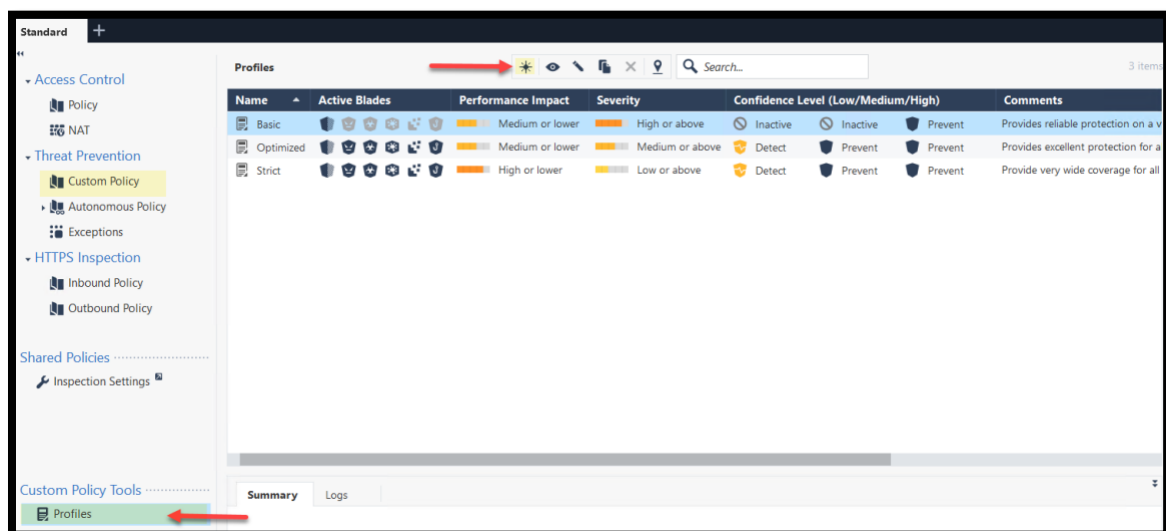
- The exception we made is known as a local exception. It is applied to one rule. Global exceptions can be added via the global exceptions list.



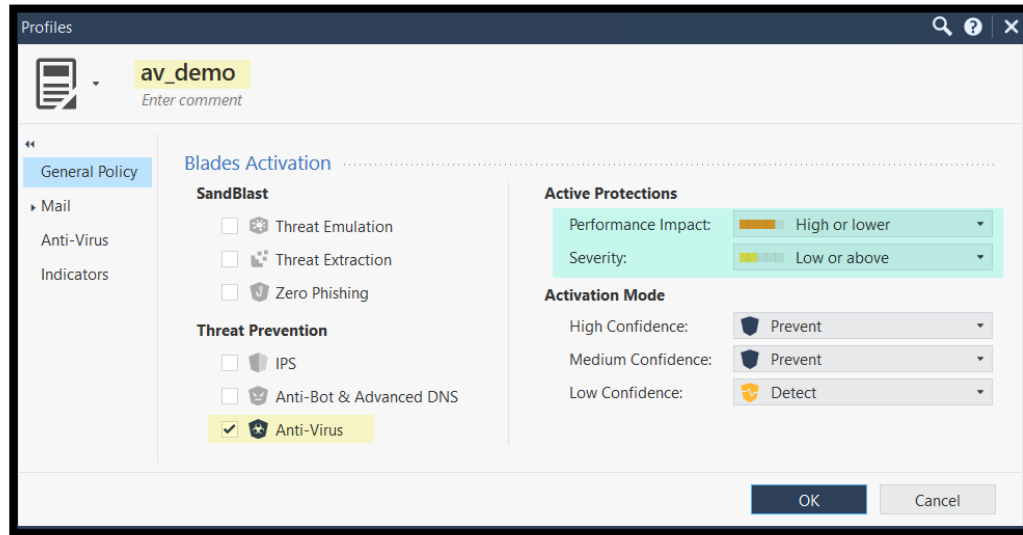
Exercise 3: Profile Customizations

It is possible to configure the Anti-Virus settings to drop/Allow/Deep inspect certain file type. In this exercise, we will create a new threat profile and customize the settings.

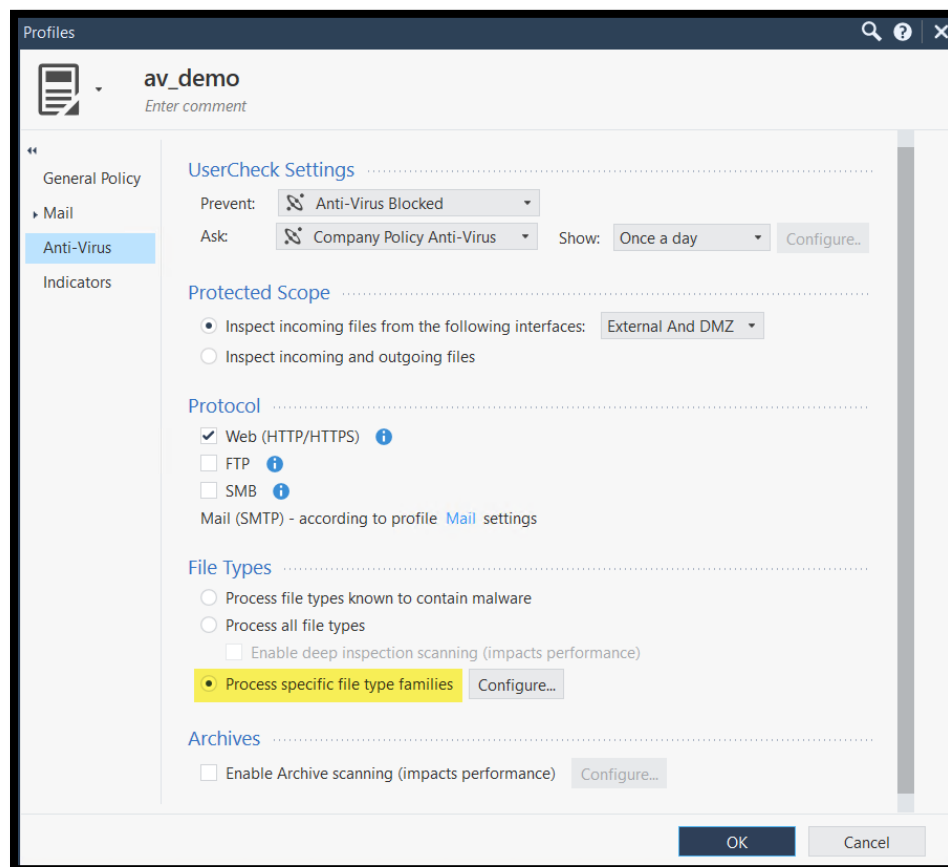
- Under the Custom Threat Prevention Policy, select Profiles and create a new profile.



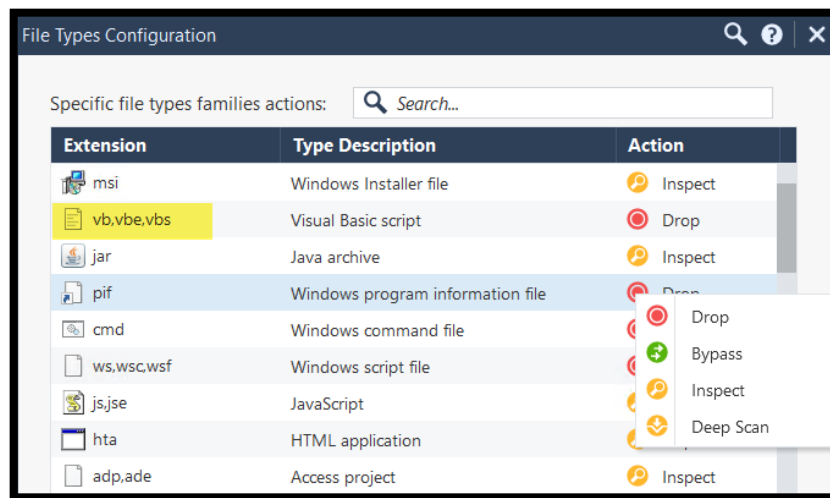
- Give it a proper name, with only Anti-Virus enabled and customize the Active Protections to match the settings below.



- Under the Anti-Virus tab in the profile settings, change the File Types settings to “Process specific file type families”.



- Click **Configure** and review the actions per file type family.

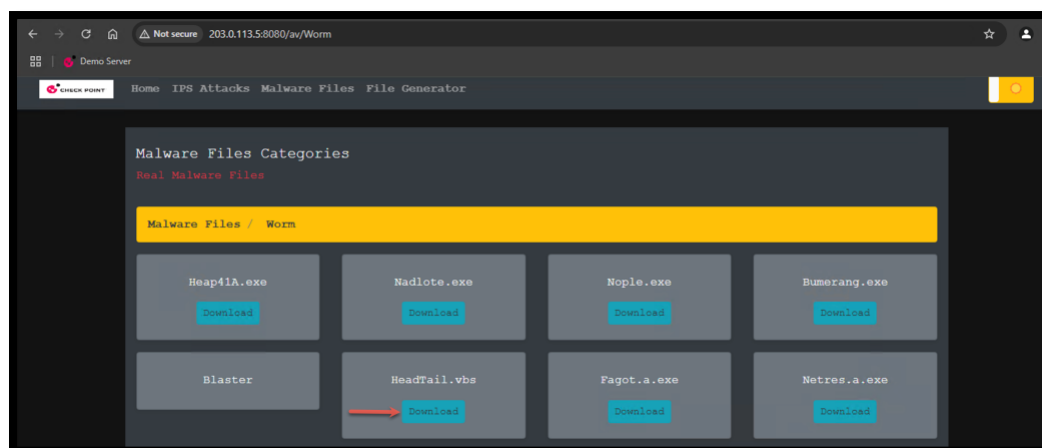


- This feature allows you to take different actions based on the file type.
- The default action for the file type with action set to Drop will always be dropped by the Anti-Virus blade.

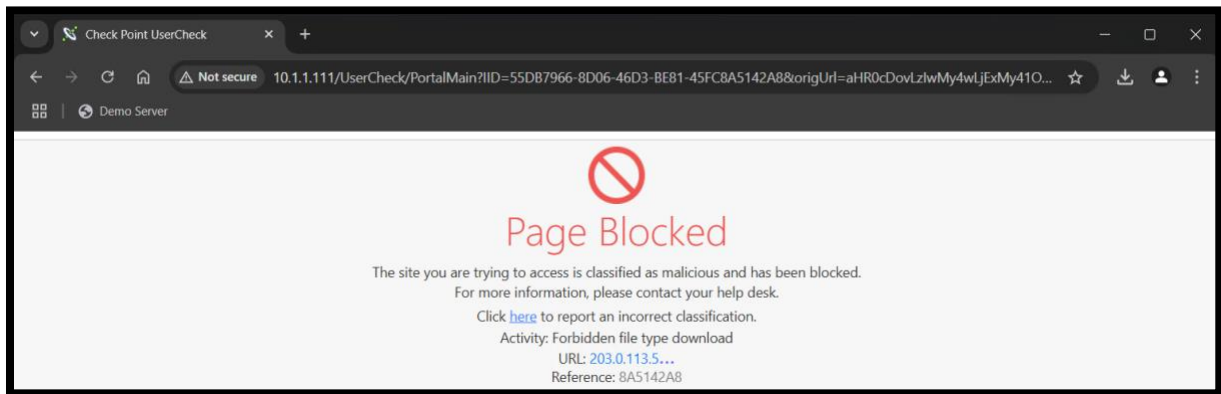
- Assign the newly created profile to the default rule in the Threat Prevention policy and Install the policy.



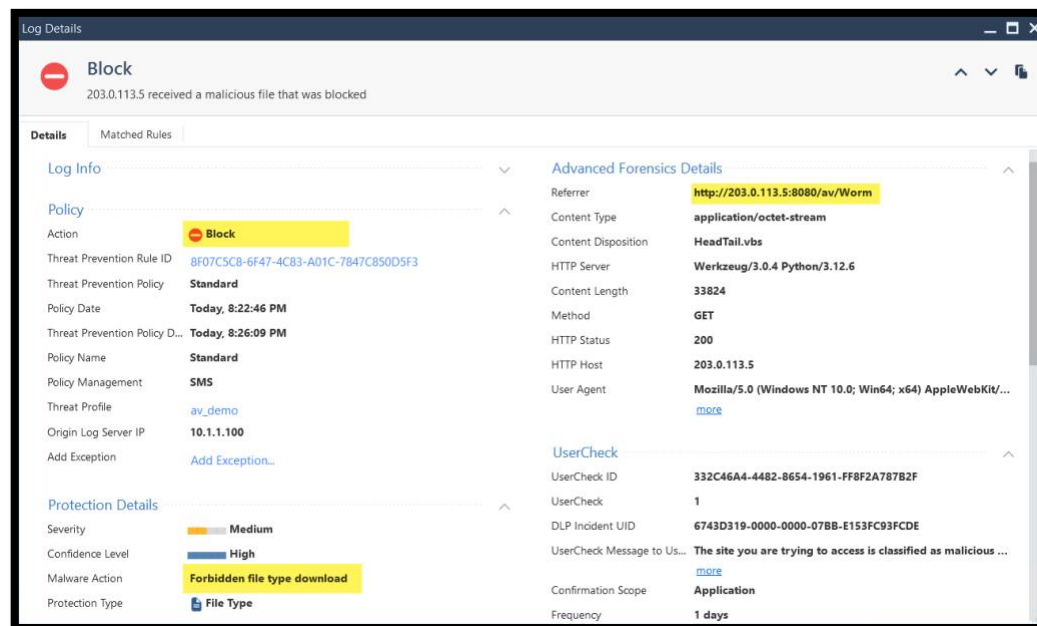
- Try to download the under Worm - > **HeadTail.vbs**



- Notice that the user is redirected to a block message. In such configurations, the GW can block the attempt without the need to analyze the file.



- Note that in the case above, it is unnecessary to consult the cloud to retrieve the verdict before enforcing the policy. The file is blocked based on its type.
- Review the log in SmartConsole and notice that the action is **Block**.

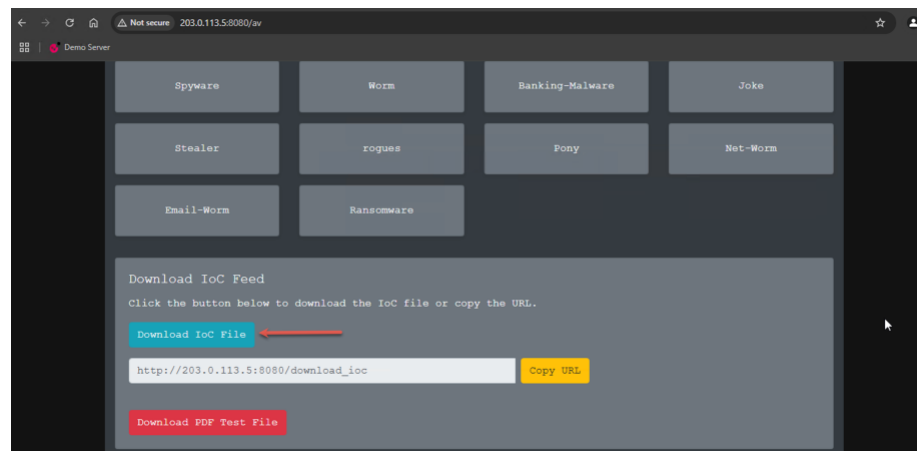


Exercise 4: Threat Indicators - IoC

Threat Indicators lets you upload Indicator files that contain sets of observables. These observables are added to the Threat Prevention policy.

- **Indicator** – Set of observables which represent a malicious activity in an operational cyber domain, with relevant information on how to interpret it and how to handle it.
- **Observable** – An event or a stateful property that can be observed in an operational cyber domain. For example: IP address, MD5 file signature, URL, Mail sender address.

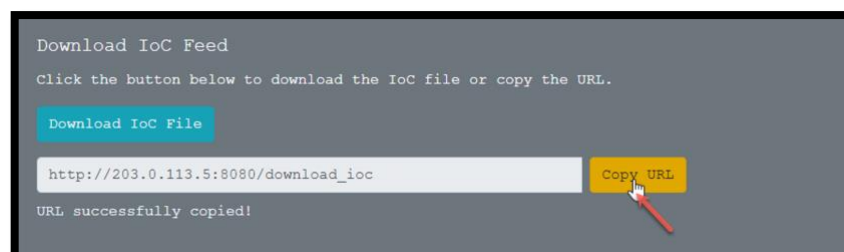
1. Download the **IoC** demo file from the Demo Server.



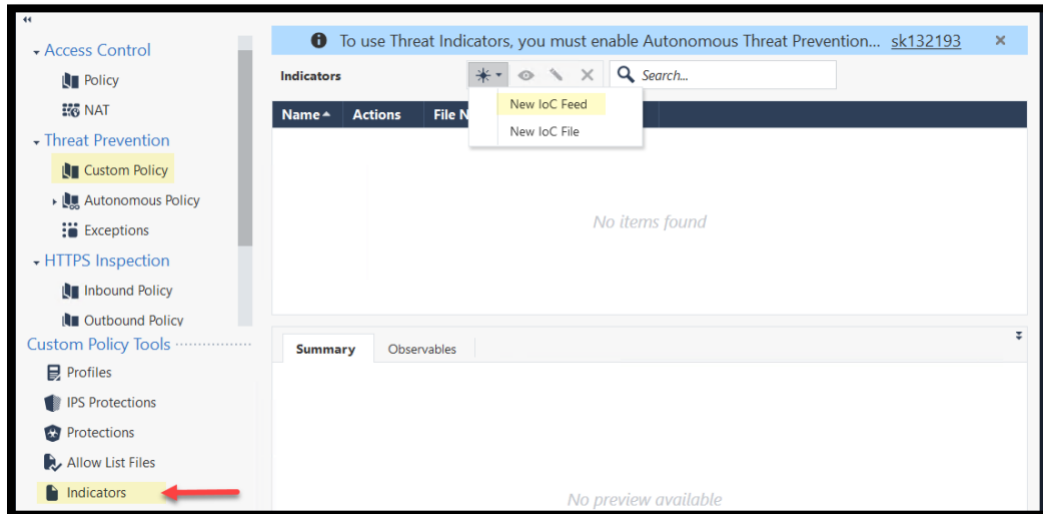
2. Open the file and review the contents and the format. The file adds a feed of observables to block a URL and a File using its MD5 with the Anti-Virus blade.

	A	B	C	D	E	F	G
1	#! DESCRIPTION = IoC Demo						
2	#! REFERENCE = SBT						
3	# All lines beginning "#" are comments						
4	# All lines beginning "!!" are metadata read by the SW						
5	# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT						
6	block_md5	20b2ca0d0694fdc37e3fb3f55754bdd4	MD5	high	high	AV	ioc_test_md5
7	block_url	http://example.com	URL	high	high	AV	ioc_test_url
8	block_domain	stamdomain.com	domain	high	high	AB	ioc_test_domain
9	block_ip	4.2.2.1	IP	high	medium	AB	ioc_block_ip
10							

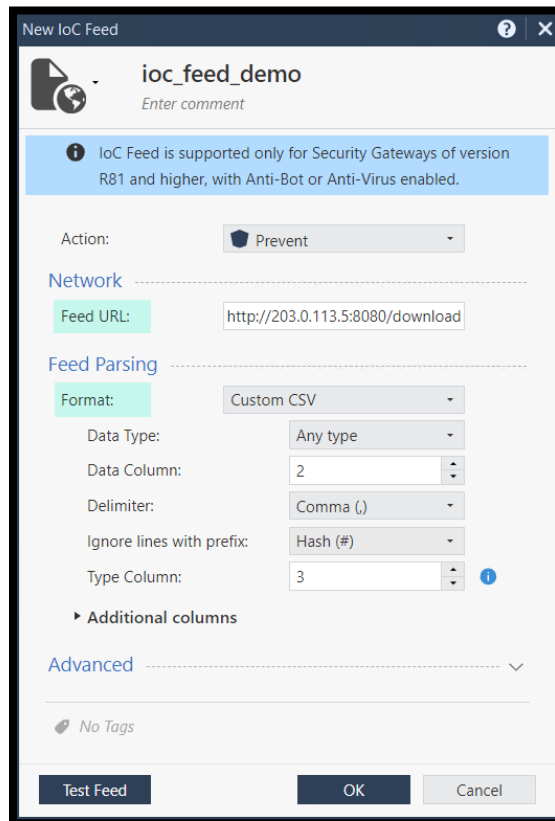
3. We can either upload the file via SmartConsole or use the feed URL and the **GW** will pull the feed automatically. Copy the link of the CSV feed file.



- Under Custom Policy -> Indicators, add a new IoC feed.



- Give it a proper name, paste the feed URL, and change the format to Custom CSV.



New IoC Feed

ioc_feed_demo
Enter comment

ioC Feed is supported only for Security Gateways of version R81 and higher, with Anti-Bot or Anti-Virus enabled.

Action: Prevent

Network

Feed URL: http://203.0.113.5:8080/download

Feed Parsing

Format: Custom CSV

Data Type: Any type

Data Column: 2

Delimiter: Comma (,)

Ignore lines with prefix: Hash (#)

Type Column: 3

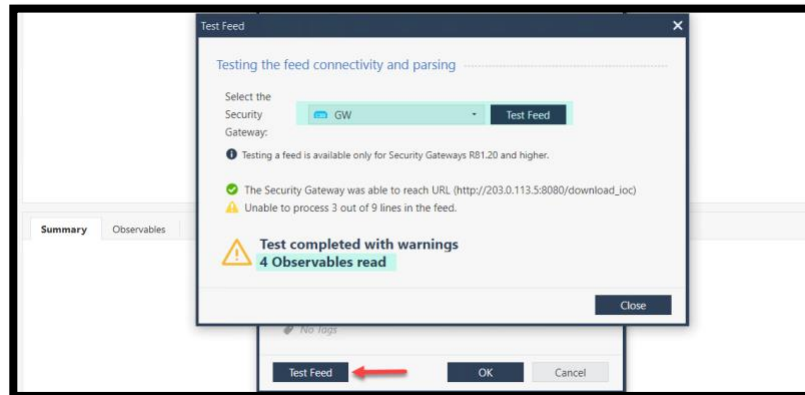
► Additional columns

Advanced

No Tags

Test Feed OK Cancel

- Test the feed from the GW and make sure it can load the observables. We will accept using HTTP site Instead of the recommended HTTPS since this is a lab environment.



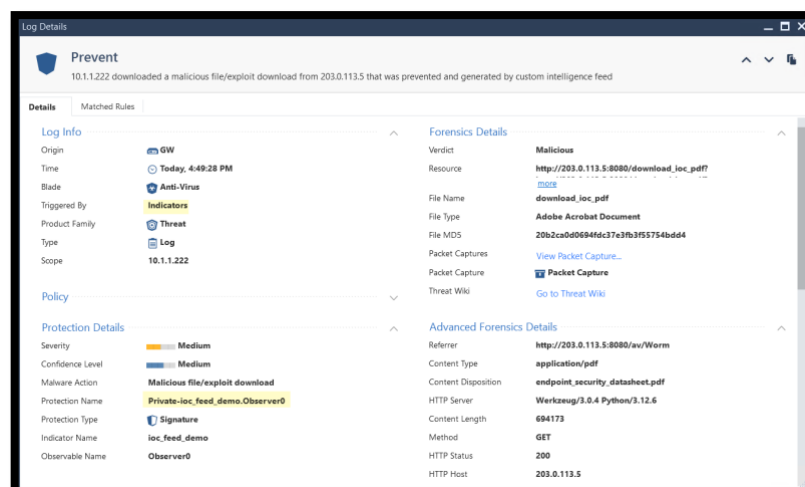
7. Confirm the feed was added successfully and Install the Threat Prevention Policy.



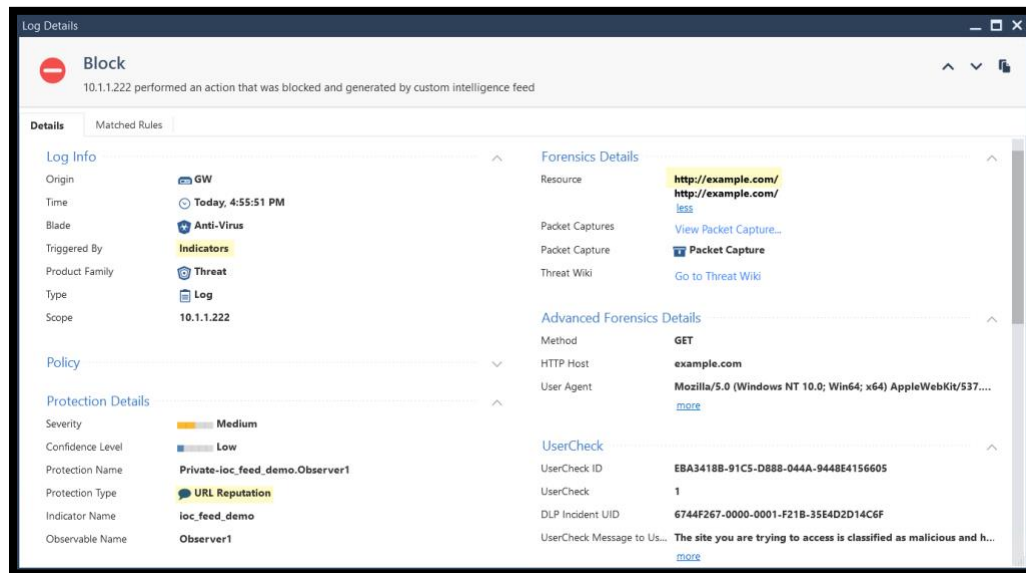
8. From the win_client, try download the PDF test file.



9. Review the log. Notice the Protection name and triggered by fields.



10. Test accessing the URL configured in the CSV feed <http://example.com> (we only configured HTTP not HTTPS).
11. Review the log and pay attention to the Protection Type.



End of Lab 6