THREAT PREVENTION INDICATORS OF COMPROMISE MANAGEMENT

December 2018

Andy Thomas
athomas@checkpoint.com

Overview

Even though Check Point Threat intelligence is the most comprehensive threat intelligence repository in the security industry, many customers still require a mechanism to import Indicator of Compromise (IOC) threat Intelligence from third party sources. These sources may include intelligence harvested from their own network or ecosystem, intelligence feed from other security providers, or third party feeds from industry specific consortiums.

The purpose of this document is to walk you through the step by step process of importing of the IOCs via the SmartConsole GUI as well as the use of the R80.20 management API function for importing IOCs via command line.

Assumptions & Requirements

This guide makes the following assumptions:

- The customer is running at least R80.x as the Check Point management server
- For use the API IOC import section, you must be running R80.20 as your Check Point management server.
- The API used in this example is the management API provided by R80.20 and above. It is not to be confused with the Threat Prevention API that is used to submit files to Check Point Threat Emulation and Extraction appliances or the Check Point cloud for sandboxing of files or threat extraction cleaning of files.

Note: You may find minor variances in the steps required if you use a different version of Windows Server, but the process is generally the same.

System Architecture Overview

Component	Description
Check Point SmartConsole (R80.20)	A unified application to manage Check Point's R80 & above security architecture.
GAIA based Check Point Security Management Server	Check Point GAIA R80.20 Security Management Server.

Indicators Definition and File Structure

As with most network and endpoint security solutions, the meaning of indicators of compromise usually means file hashes, URLs, domains, or IP addresses; however, Check Point does not limit indicators to the criteria but includes mail attributes as well. The full list of document IOCs found in the Check Point Threat Prevention admin guide are found below.

- URL
- Domain
- IP
- IP Range
- MD5
- Mail-subject
- Mail-to
- Mail-from
- Mail-cc
- Mail-reply-to

Indicators can be imported using two different file types. The first file type is a simple csv file formatted using Check Point provided field names. The Field Names are highlighted within the file. The second type is an xml file using the STIX format.

The explanation of each field is below.

UNIQ-NAME	A unique name of the observable. Cannot be the same name used within the indicator file.
VALUE	The value field is the value of the observable. It would be the actual file, domain, URL, etc.
TYPE	Type would be the type of IOC and corresponds to list above
CONFIDENCE	Confidence level of the IOC. Values are Low, Medium, and High
SEVERITY	Severity of the IOC. Values are Low, Medium, High, and Critical
PRODUCT	The options for this field is Antivirus(AV) or Antibot(AB)
COMMENT	Comment about IOC or attack

CSV formatted File

Example of a CSV Indicator File

```
#! DESCRIPTION = indi file,,,,,,
"#! REFERENCE = Indicator Bulletin; Feb 20, 2014",,,,,,
# FILE FORMAT:,,,,,,
"# All lines beginning ""#"" are comments",,,,,,
"# All lines beginning ""#!"" are metadata read by the SW",,,,,,
"# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT",,,,,,
observ1,8d9b6b8912a2ed175b77acd40cbe9a73,MD5,medium,medium,AV,FILENAME:WUC
Invitation Letter Guests.doc
observ2,76700f862a0c241b8f4b754f76957bda,MD5,high,high,AV,FILENAME:essais~.swf|
NOTE:FWS type Flash file
observ7,http://somemaliciousdomain.com/uploadfiles/upload/exp.swf?info=
789c333432d333b4d4b330d133b7b230b03000001b39033b&infosize=00840000
,URL,high,high,AV,IPV4ADDR:196.168.25.25
observ8,svr01.passport.ServeUser.com,Domain,low,high,AB,TCP:80|
IPV4ADDR:172.18.18.25|NOTE:Embedded EXE Remote C&C and Encoded Data
observ9,somemaliciousdomain2.com,Domain,,low,AV,TCP:8080|IPV4ADDR:172.22.14.10
observ10,http://www.bogusdomain.com/search?q=%24%2B%25&form=MOZSBR&pc=
MOZI,URL,low,low,AB,IPV4ADDR:172.25.1.5
observ11,http://somebogussolution.com/register/card/log.asp?isnew=-1&LocalInfo=
Microsoft%20Windows%20XP%20Service%20Pack%202&szHostName= ADAM-
E512679EFD&tmp3=tmp3,URL,medium,,AB,
observ14,172.16.47.44,IP,high,medium,AB,TCP:8080
observ15,172.16.73.69,IP,medium,medium,AV,TCP:443|NOTE:Related to Flash
exploitation
observ16,abc@def.com,mail-to,,high,AV,"NOTE:truncated; samples have appended to
the subject the string ""PH000000NNNNNNN"" where NNNNNNN is a varying number"
observ34,stamdomain.com,domain,,,AB,
observ35,stamdomain.com,mail-from,high,medium,AV,
observ37,xyz.com,mail-from,medium,medium,AB,
observ38,@xyz.com,mail-from,medium,medium,AB,
   observ39,a@xyz.com,mail-from,medium,medium,AB,
```

Example of a STIX 1.0 XML Indicator File

```
<stix:STIX_Package
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:indicator="http://stix.mitre.org/Indicator-2"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
xmlns:example="http://example.com/"
xsi:schemaLocation="
http://stix.mitre.org/stix-1 ../stix_core.xsd
http://stix.mitre.org/Indicator-2 ../indicator.xsd
http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
http://cybox.mitre.org/objects#FileObject-2 ../cybox/objects/File_Object.xsd
http://cybox.mitre.org/default_vocabularies-2
../cybox/cybox_default_vocabularies.xsd"
id="example:STIXPackage-ac823873-4c51-4dd1-936e-a39d40151cc3"
version="1.0.1">
<stix:STIX_Header>
<stix:Title>Example file watchlist</stix:Title>
```

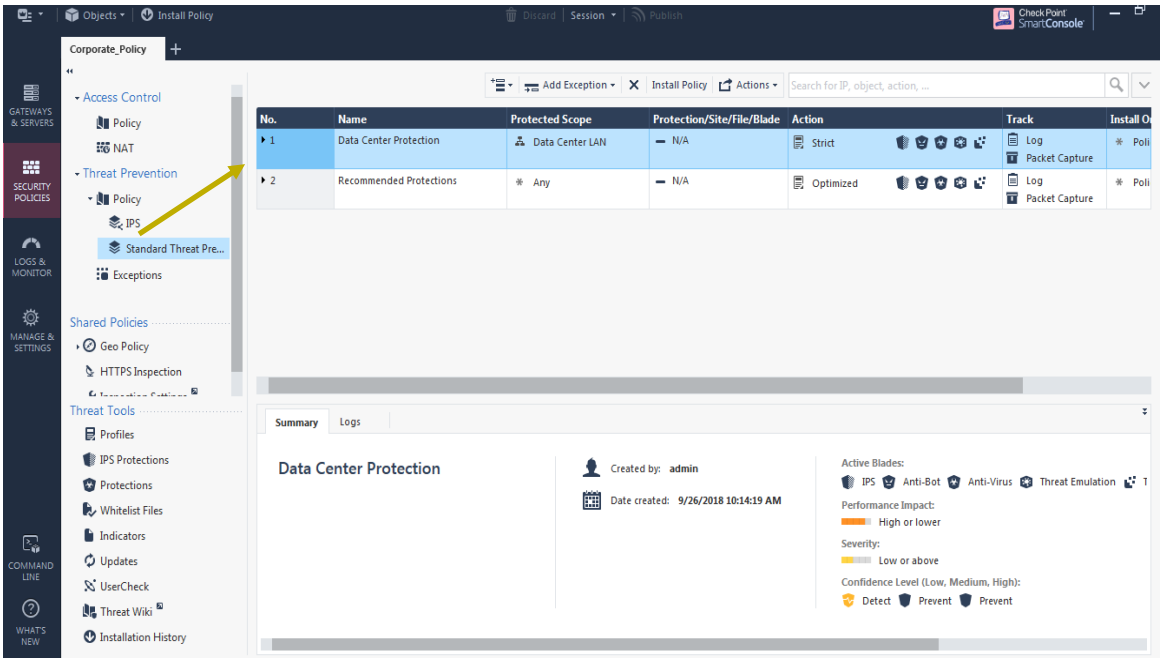


```
<stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators -
Watchlist</stix:Package_Intent>
</stix:STIX_Header>
<stix:Indicators>
<stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-
611935aa-4db5-4b63-88ac-ac651634f09b">
<indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">File Hash
Watchlist</indicator:Type>
<indicator:Description>Indicator that contains malicious file
hashes.</indicator:Description>
<indicator:Observable id="example:Observable-c9ca84dc-4542-4292-af54-
3c5c914ccbbc">
<cybox:Object id="example:Object-c670b175-bfa3-48e9-a218-aa7c55f1f884">
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0"
condition="Equals">MD5</cyboxCommon:Type>Configuring Advanced Threat Prevention
Settings
Threat Prevention Administration Guide R80.20 | 113
<cyboxCommon:Simple_Hash_Value condition="Equals"
apply_condition="ANY">0522e955aaee70b102e843f14c13a92c##comma##0522e955aaee70b102
e843f14c13a92d##comma##0522e955aaee70b102e843f14c13a92e</cyboxCommon:Simple_Hash_
Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>
```

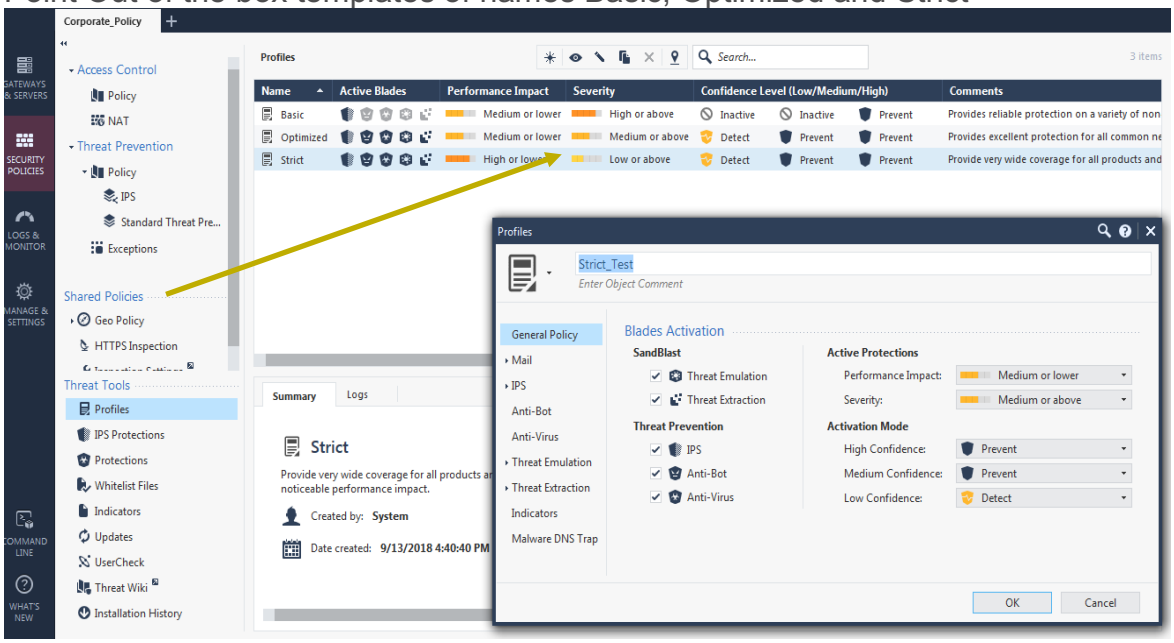

Indicators Assignment and File Import

Indicators can be imported directly into a given Threat Prevention profile or they can be imported into the in the general Indicators section in the Threat Prevention Policy view. The Indicators can be activated or Disabled per Threat Prevention Policy.

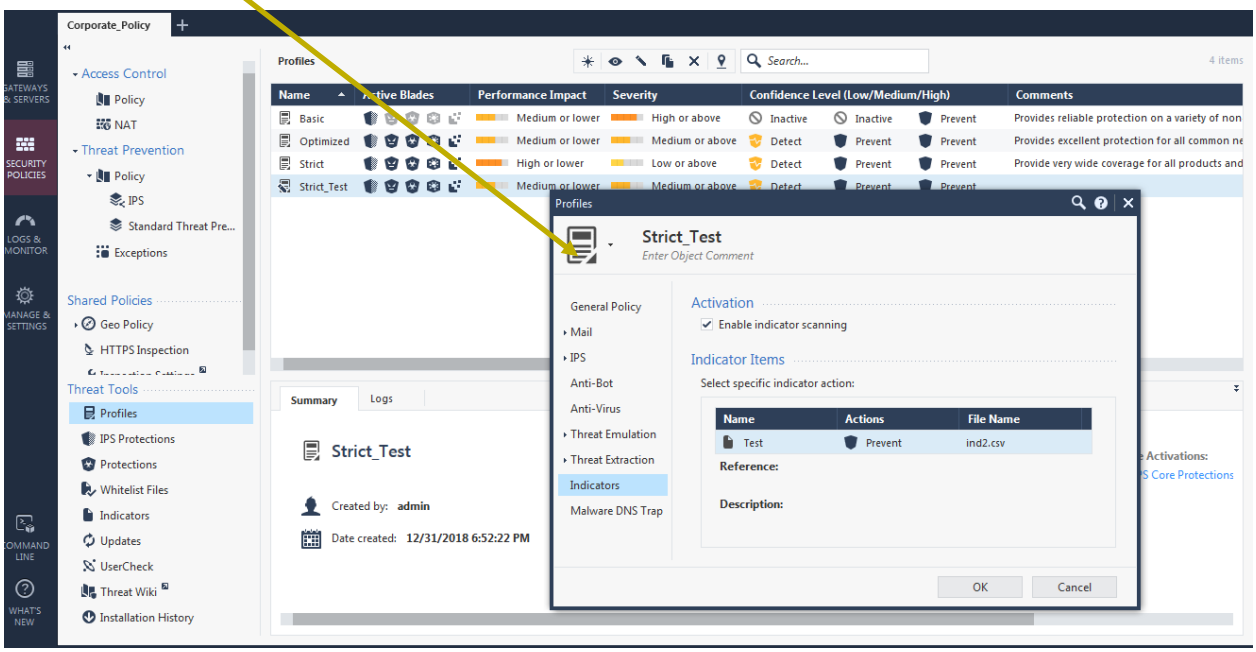
1. First Launch the SmartConsole Dashboard and switch to your Threat Prevention Policy view



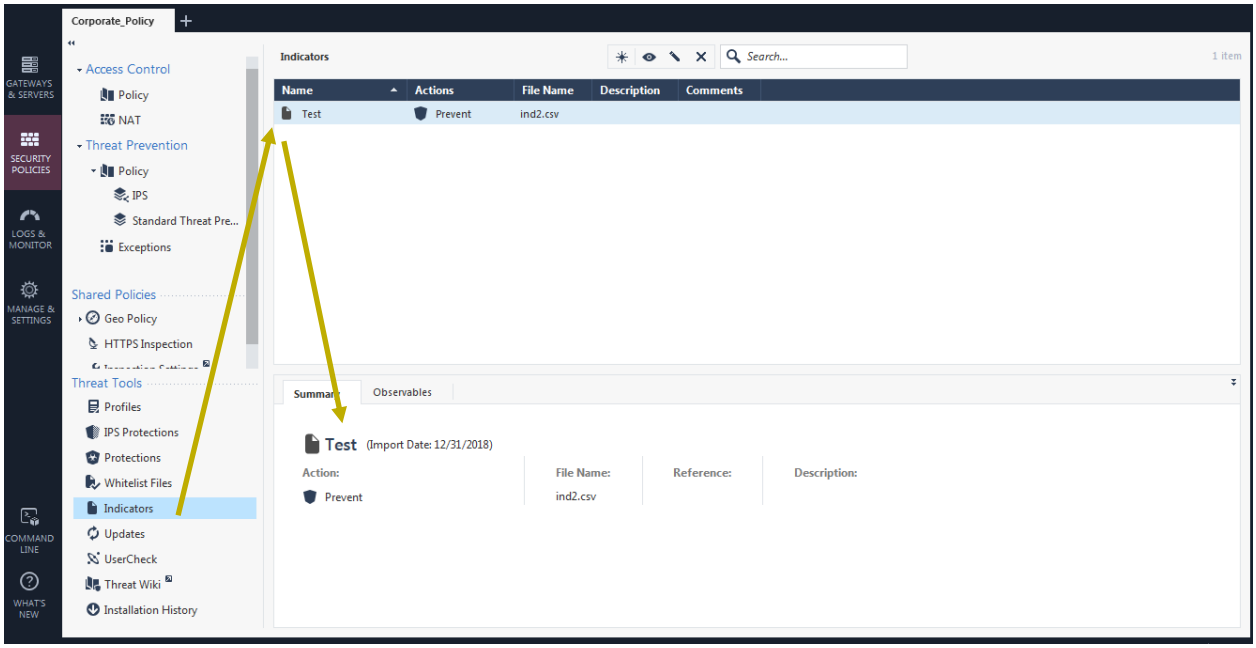
2. Next, switch the view to Profiles by clicking on Profiles. Next, create a Read/Write Threat Prevention Profile similar to the one below. Note: You cannot edit the Check Point Out of the box templates of names Basic, Optimized and Strict



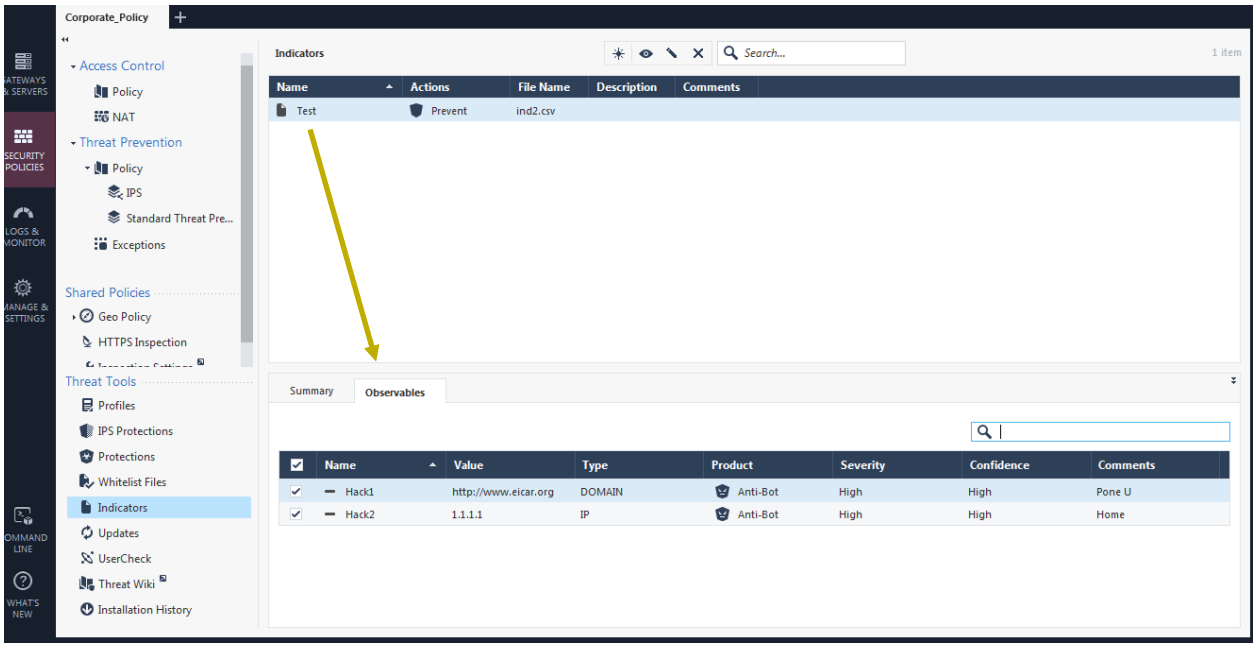
3. If you open the newly created profile, and then click Indicators you will see an Indicator list that has been populated from a file and the associated file name. Notice the Enable Indicator Scanning Checkbox in this view. This is how you activate or disable the Indicator list in the particular profile.



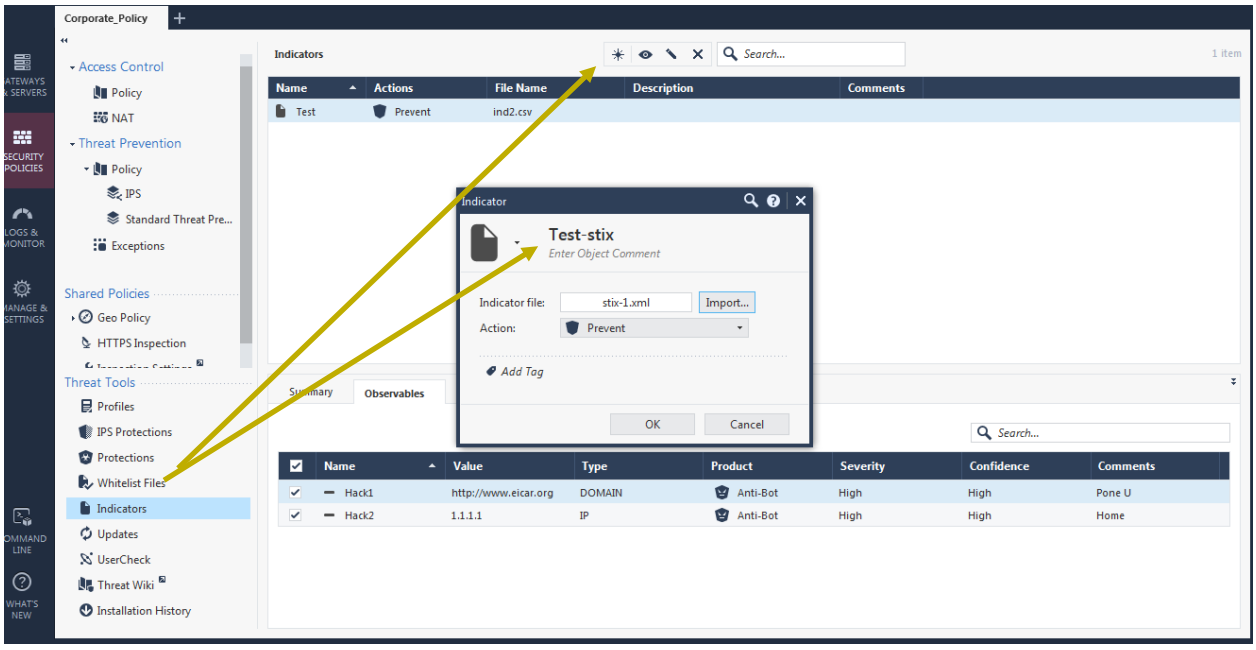
4. To see the Global Indicators list, close all dialogue windows and click Indicators on the side navigation bar. You will then see the list of Indicator files imported and summary info on the file import and action status for the file



5. Next, Click on Observables to see the IOCs imported from the file.



6. To import the indicators file, Click the Create Star at the top left of the action bar and then assign a name to your Indicator import. Now select your Indicator file and then select the Action (Prevent, Detect, Inactive) for the indicator list.

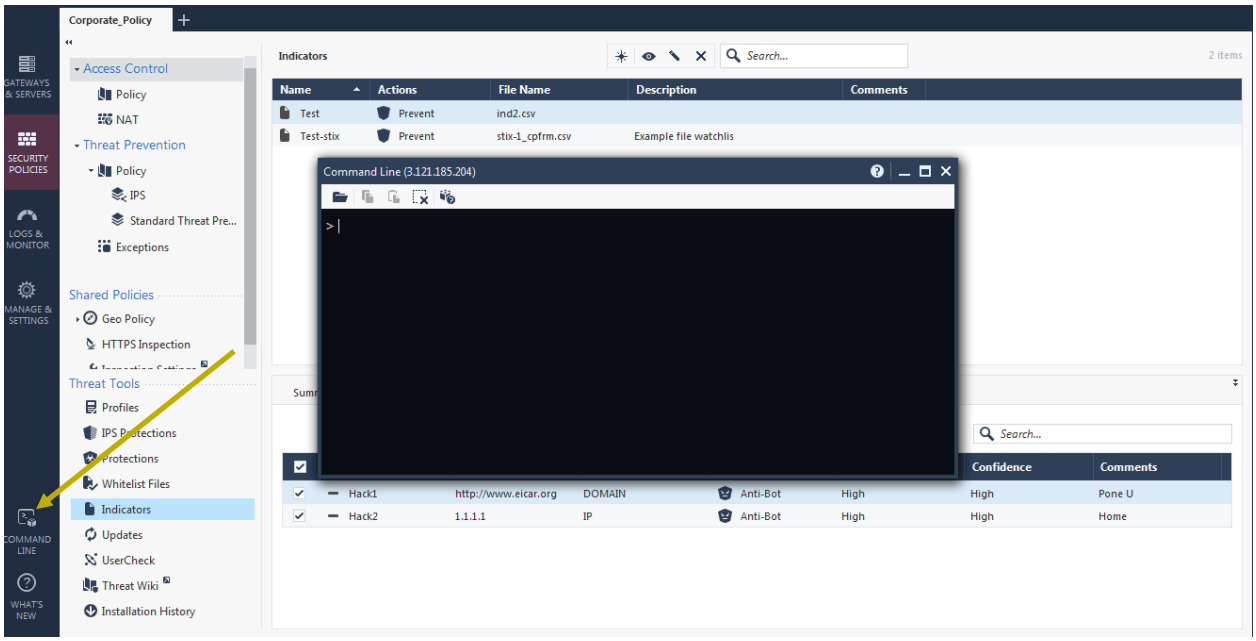


7. Now that the indicators are imported, you can activated or disable then in the profiles as you desire. Once you have done that, you will need to push the Threat Prevention policy to all the desired gateways. Remember that you do not need to push the access control policy since you only modified the Threat Prevention policy.

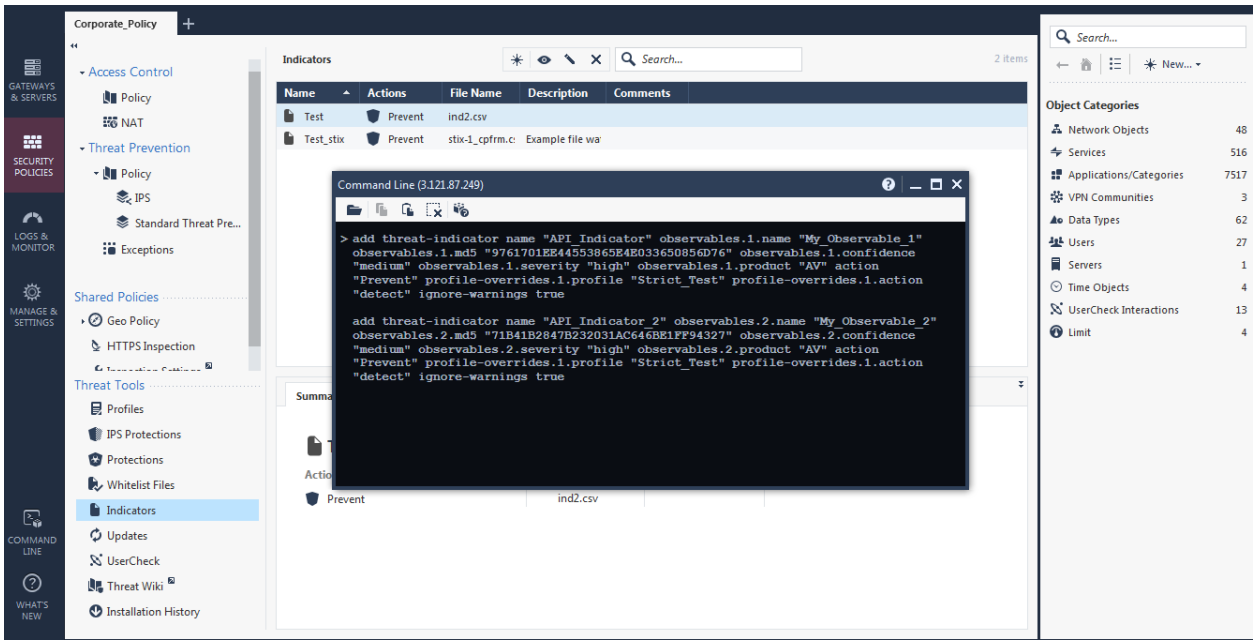
IOC Addition via the management API

As mentioned, Check Point has extended the management API in R80.20 to include the addition of 3rd party IOCs into the Check Point management system. To add the IOCs in batch, you can copy the commands directly into the management cli window or you can also use a raw data file associated with the commands. In this example, we will use the direct commands. The API reference guide that documents the command usage can be found at [Management API Guide 1.3]

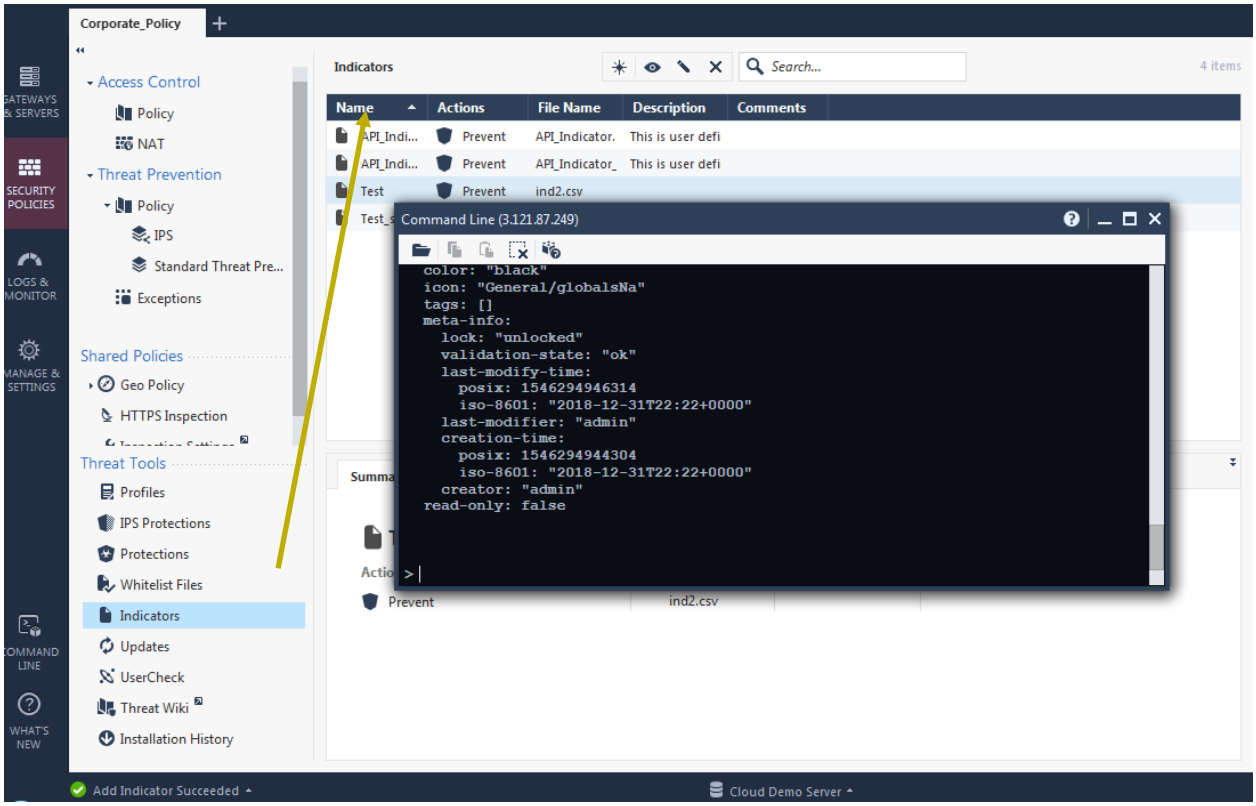
1. Open the management CLI window



2. All you need to do next is issue your commands API commands to add the IOCs. I have provided two samples that I have copied into the command window and a screen with the results. .



3. You will then see the results scroll. Notice the two new IOCs that were added via the API in the Indicators list.



Now that you have added the IOCs, all you need to do is publish your changes and push your Threat Prevention Policy to your corresponding gateways.

Additional Resources

R80.20 Threat Prevention Admin Guide	R80.20 Threat Prevention Admin Guide.
Management API Reference Guide 1.3 - Threat Indicator	Download the corresponding RDP application for your client Management API Threat Indicator
Sample Threat Indicator API commands	add threat-indicator name "API_Indicator" observables.1.name "My_Observable_1" observables.1.md5 "9761701EE44553865E4E033650856D76" observables.1.confidence "medium" observables.1.severity "high" observables.1.product "AV" action "Prevent" profile-overrides.1.profile "Strict_Test" profile-overrides.1.action "detect" ignore-warnings true add threat-indicator name "API_Indicator_2" observables.2.name "My_Observable_2" observables.2.md5 "71B41B2847B232031AC646BE1FF94327" observables.2.confidence "medium" observables.2.severity "high" observables.2.product "AV" action "Prevent" profile-overrides.1.profile "Strict_Test" profile-overrides.1.action "detect" ignore-warnings true

