Importing Custom IOC's in Smart Console R80.20

Eric Johnson
December 11th, 2018

Process Summary

This document will focus on a new enhancement available in R80.20 allowing for users to import custom IOC settings in your Threat Prevention policy, through your Smart Console dashboard.

IOC – Indicator of Compromise

IOC Description

IOC's convey an attack campaign by specific observable patterns and with additional information intended to represent artifacts & behaviors of interest within a cyber-security context.

The goal of importing custom IOC's is to allow the input of private feeds into your specific Anti-Virus & Anti-Bot engines in addition to your Check Point Updates & Threatcloud feed. Along with assistance in managing, implementing, exchanging & auditing threat indicators.

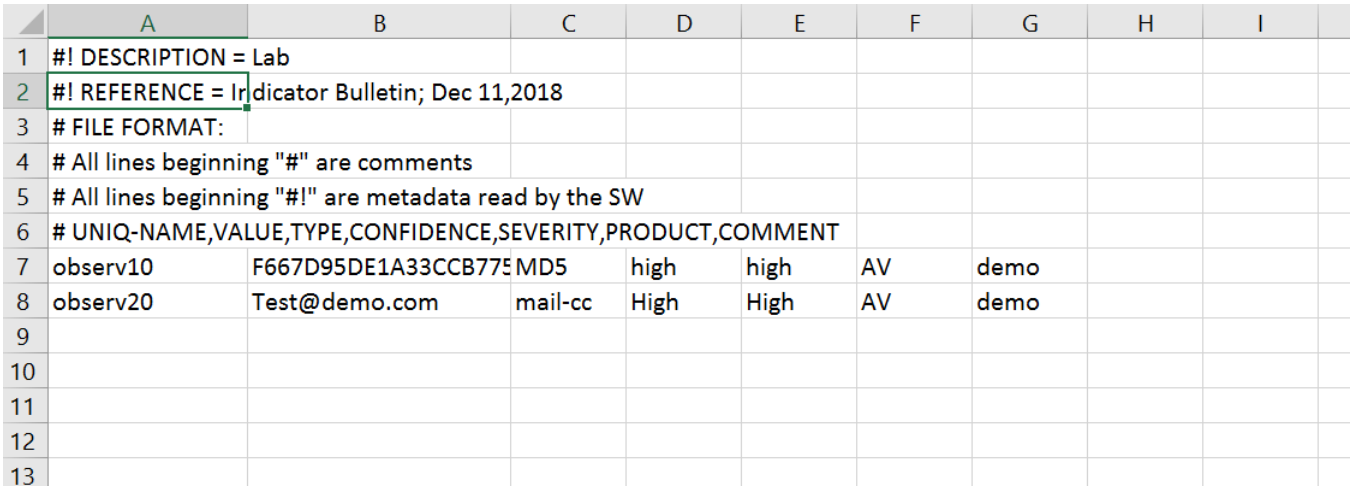
Required IOC File Format

Each indicator file should be in either CSV or STIX XML format, and should contain records of equal size.

Field		Description	Valid Values	Value Criteria	Optional
UNIQ-NAME		Name of the observable	Free text	Must be unique	No
VALUE		A value that is valid for the type of the observable	See the table below	See the table below	No
TYPE		Type of the observable	• URL • Domain • IP • IP Range • MD5 • Mail-subject • Mail-from • Mail-to • Mail-cc	Not case sensitive	No

			• Mail-reply-to		
CONFIDENCE		Degree of confidence the observable presents	• low • medium • high • critical	Default - high	Yes
SEVERITY		Degree of threat the observable presents	• low • medium • high • critical	Default - high	Yes
PRODUCT		Check Point Software Blade that processes the observable	• AV • AB	AV - Check Point Anti-Virus Software Blade (default) AB - Check Point Anti-Bot Software Blade **Note** - only the Anti-Virus Software Blade can process MD5 observables.	Yes

.CSV Example -



	A	B	C	D	E	F	G	H	I
1	#! DESCRIPTION = Lab								
2	#! REFERENCE = Indicator Bulletin; Dec 11,2018								
3	# FILE FORMAT:								
4	# All lines beginning "#" are comments								
5	# All lines beginning "#!" are metadata read by the SW								
6	# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT								
7	observ10	F667D95DE1A33CCB775	MD5	high	high	AV	demo		
8	observ20	Test@demo.com	mail-cc	High	High	AV	demo		
9									
10									
11									
12									
13									

STIX Example -

```
: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:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    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://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address_Object.xsd"
    id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
    version="1.0.1"
    >
    <stix:STIX_Header>
        <stix:Title>Example watchlist that contains IP information.</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-33fe3b22-0201-47cf-85d0-97c02164528d">
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
            <indicator:Description>Sample IP Address Indicator for this watchlist. This contains one indicator with a set of three IP addresses in the watch
            <indicator:Observable  id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
                <cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">
                    <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
                        <AddressObject:Address_Value condition="Equals" apply_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Addr
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
:/stix:STIX_Package>
```

When importing at STIX file severity & confidence will automatically be set to high

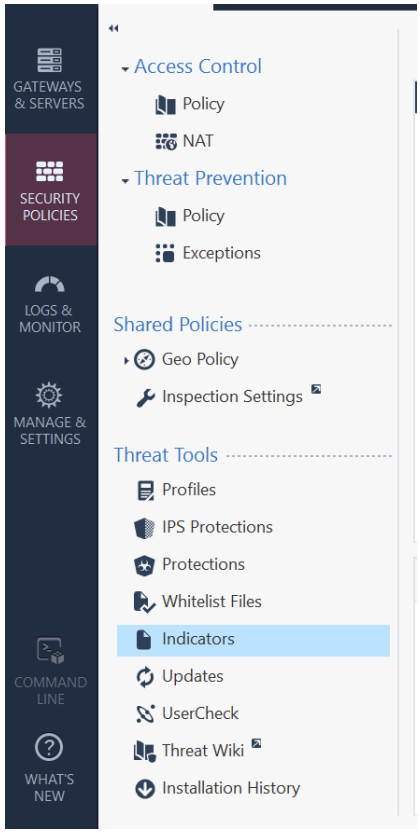
IOC Importing Guide via (Smart Console)

1. Log into smart console and navigate to “Security Policies” tab.

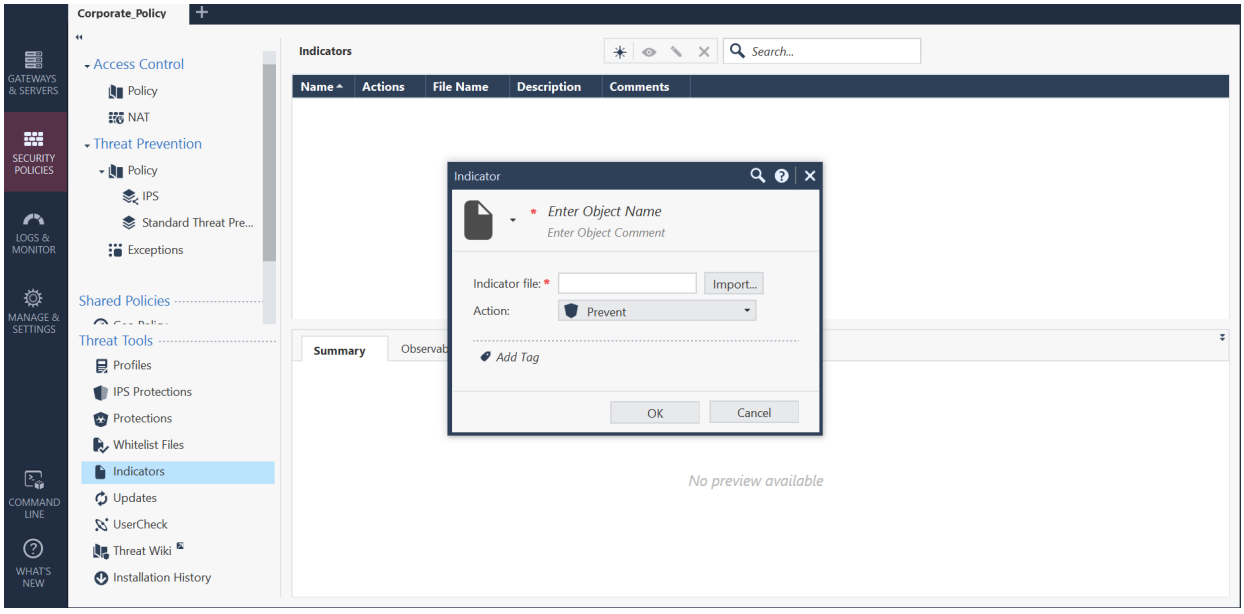
This is a task done through Anti-virus & Anti-bot blade so you must click “Threat Prevention” in order to view the “Indicators” tab.

Only the Anti-virus blade can process MD5 observable types

2. Under “Threat Tools” in the bottom left corner click “Indicators”.



3. A new window will open up, and you'll navigate to the top center and click on the star icon for new items



4. You'll be able to name the indicator, import the IOC file, and set 1 of 4 options.

   Ask – *Threat Prevention Blade will ask what to do with a detected observable*.

   Prevent – *Threat Prevention Blade will block a detected observable.*

   Detect – *Threat Prevention Blade will create a log, but let observable pass.*

   Inactive – *Threat Prevention Blade does nothing.*

   You can also edit these actions after uploading file

5. Easiest way to view any logged observables is through your Threat Prevention logs.
6. To delete, simply click desired observable and select delete.

About Check Point Software

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to corporate enterprises and governments globally. Its solutions protect customers from 5th-generation cyber-attacks with an industry leading catch rate of malware, ransomware and other targeted attacks. As of 2018 the company has approximately 5,000 employees worldwide. Headquartered in Tel Aviv, Israel, the company has development centers in Israel, California (ZoneAlarm), Sweden (Former Protect Data development center), and Belarus. The company has main offices in the United States, in San Carlos, California, in Dallas, Texas, and in Ottawa, Ontario (Canada).

References

Monitoring and Handling Alerts, sc1.checkpoint.com/documents/R80.10/SmartConsole_OLH/EN/-_ktjOvSNsVDDJA210OA3g2.htm.

"Indicators of Compromise as a Way to Reduce Risk." *Securelist - Kaspersky Lab's Cyberthreat Research and Reports*, securelist.com/indicators-of-compromise-as-a-way-to-reduce-risk/71915/.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193&partition=General&product=Anti-Virus

