

Sophos Endpoint Detection and Response

Early Access Program - Testing Guide

Prerequisites for performing exercises:

- 2 Endpoints both enrolled in EDR EAP
- Download 'Sophos HIPS Test (exe)'* from <u>http://sophostest.com</u> on both endpoints
- Download 'Unknown.exe'* from: http://sophostest.com/reputation/index.html on both endpoints
- Wait about 20 minutes before running tests

* EAP endpoints will be enhanced so that details on detected or suspicious portable executable files will be frequently sent to Sophos Central (approx. every 15 minutes). This then gives the admin the ability to search for file names or SHA-256 hashes to identify which endpoints have seen those suspect files to investigate further or take action. Searches can also be run on processes from within an existing Threat Case (formerly RCA). Keep in mind that Sophos Central will only store details on portable executable files that have a bad or uncertain reputation and therefore will only return results on those files where a query is matched. The test files downloaded for these exercises have an uncertain reputation and therefore details will be sent to Central on those files.

Exercise 1 will walk through a scenario where there has been an endpoint detection event and will walk through the typical investigation of a detection and how new capabilities can be leveraged for this investigation

New Functionality Tested: Threat Case new look and feel, Requesting Labs latest intelligence, Admin Led Isolation, Item Search Result from Threat Case

- 1. Run Sophos HIPs Test (exe) on endpoint 1
 - a. -Detection- Toast message displays bottom right corner



2. Within a few minutes a new Threat Case should appear in Sophos Central for the detection, Check Sophos Central > Endpoint Protection > Threat Case.

Note: The Threat Case is the new name for what used to be referred to as the Root Cause Analysis (RCA). We have implemented several additional features to make it easier for admins to conduct deeper investigation into detected threats.

3. When the Threat Case has been uploaded you should see the most recent Threat Case named "HPmal/Eicar-A"

En Overv	Endpoint Protection - Detected Threat Cases Overview / Endpoint Protection Deshbaard / Detected Threat Cases							
Search Q Status All V Priority: All V						Close Delete		
	Status	Time Created 👻	Priority	Name	User	Device		
	New	Sep 26, 2018 12:09 PM	Low	HPmal/Eicar-A	514810-RS4-ENT\Administrator	514810-rs4-ent		
	New	Sep 26, 2018 10:52 AM	Medium	ML/PE-A	470610-RS4-ENT\Administrator	470610-rs4-ent		
	New	Sep 26, 2018 9:54 AM	High	HPmal/Eicar-A	514810-RS4-ENT\Administrator	514810-rs4-ent		

On Entering the Threat Case, note the new look of the threat case, there are a few new things to be aware of.

Note the new 'Suggested Next Steps' section that highlights any processes in the threat chain that have an uncertain reputation which may require further investigation, also note the new actions available in the suggested next steps.

Endpoint Protection	Help 👻 Sophos Inc -Standar	Kevin Smith d · Super Admin		
Summary		Suggested Next Steps		
Detection name:	HPmal/Eicar-A	Set a status for the threat case	Priority: Low 🔻	Status: New 🔻
Root Cause: 🕜	explorer.exe	Investigate 1 process that we've marked with an "un	certain" reputation.	1
Possible data involved: 🝞	no business files	See graph below for details		
Where:	On Victim-1-Win7 that belongs to VICTIM-1-	Isolate this computer while you investigate 🝞		
	WIN7\Victim1Admin	Scan the computer		
When:	Detected on Sep 18, 2018 3:55 PM			

New iconography is used to represent the different types of artefacts in the Threat Cases:



Finally note how processes with an uncertain reputation are also highlighted in the graph to distinguish artefacts that may warrant further investigation:



4. Click on the Sophos_hips_test.exe file to expand the flyout to get more detail on this file with an uncertain reputation:

>		Consult					
•		Search	What does this d				
-							
Process de	etails						
Reputation at t	ime case was	Uncert	tain				
SOPHOSLABS Threat Intelligence							
As of Fri, Sep 7	, 2018 8:47 AM						
Observed capabilities: Exhibits generic malicious behavior Triggers malware detections by Sophos Anti- Virus Executes code to read CPU configuration							
Request Latest Intelligence Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. Learn More							
Path:							
c:\users\victim est.zip\sophos_	1admin\appdata _hips_test.exe	\local\temp\temp	1_sophos_hips_t				
Name:	sophos_hips_	_test.exe					
Process ID:	1940						

Note when clicking on the flyout, the SHA-256 hash of this process is checked with SophosLabs and existing Labs intelligence on the file is displayed on the file. The date provided details when the file was last analysed. The Observed capabilities section will highlight suspicious behaviours of the file. If looking to get the very latest intelligence on a file, click the link to 'Request the Latest Intelligence' this sends a command from Sophos Central to the endpoint in question and the file is submitted to SophosLabs for a detailed analysis. The feedback will be provided in a few minutes. Only portable executable files that have been highlighted as process images in the Threat Case can be submitted for analysis at this point in time.

5. At this point let's assume we think there is something bad happening on the endpoint where the detection occurred, and we want to isolate the endpoint. At the top of the Threat Case click "Isolate this computer"

Endpoint Protection - HPn Overview / Endpoint Protection Dashboard / Detect	nal/Eicar-A ed Threat Cases / HPmal/Eicar-A		Help 👻 Sophos · Super Admin
Summary		Suggested Next Steps	
Detection name:	HPmal/Eicar-A	Set a status for the threat case	Priority: Low 👻 Status: New 👻
Root Cause: 🕜	firefox.exe	Investigate 1 process that we've marked with an "uncertain" reputation.	
Possible data involved: 🕜	no business files	See graph below for details	
Where:	On 514810-rs4-ent that belongs to 514810-RS4-ENT\Administrator	Isolate this computer while you investigate ?	
When:	Detected on Sep 26, 2018 11:50 AM	Scan the computer	

After clicking the button, a command is sent from Central to isolate the endpoint. Within a few minutes the endpoint should pop up an alert that the endpoint has been isolated. Once isolated all TCP and UDP connections should be blocked by the endpoint. From browser http connections a block page similar to the one below should be seen on the isolated endpoint:

Blocked request: endpoint isolated
ocation: 172.217.10.227
ccess to this website is blocked while your computer is isolated for security reaso

6. On the Configure > Settings page under Endpoint Protection the Admin Isolated Computers page will provide a list of all computers that are currently Admin Isolated.

En	dpoint Protection	Soph	Help - Kevin Smith -			
Searc	h Q					Remove from Isolation
	Computer name	Date isolated 👻	Last user	IP	Isolated by	Comments
	VM72222215778	Sep 27, 2018 11:00	VM72222215778\Admin	192.168.1.55, fe80::5c01	Kevin Smith	test
1 - 1 of 1	1 < >					
€						

7. Select the endpoint that was isolated and click the button to Remove from Isolation

Note: Endpoints can also be Admin Isolated directly from the Manage Protection > Computers page when you select an endpoint:

Endpoint Protec	tion - VN	172222215778			Help - Kevin Smith - Sophos Inc -Standard · Super Admin
	1	SUMMARY	EVENTS	() STATUS	
	Recent I	Events			View More
	i	Sep 27, 2018 11:00 AM	Computer isolated by Kevir	n Smith	
Isolated by Admin	i ()	Sep 26, 2018 4:32 AM	Update succeeded		
Remove from Isolation VM72222215778	i (*)	Sep 24, 2018 3:59 PM	Running malware cleaned ool.exe'	up: 'HPmal/Eicar-A' at 'C:\Users\Admin\do	ownloads\recipeaddictst

8. At this stage of the test we want to identify if any other endpoints have seen this potentially malicious file. Go back into the Threat Case for this detection and click on the Sophos_hips_test.exe file in the Threat Case graph. From the flyout click the option to perform a search:

>		Search	Clean and block What does this do) ??
Process de Reputation at tin created:	tails me case was	Uncert	ain	^
SOPHOSLA As of Fri, Sep 7, Observed capabilities: Request Latest Note: Requestin sent to Sophos	BS Threat Inte 2018 8:47 AM EICAR test file of Exhibits generic Triggers malwa Virus Executes code t Intelligence g the latest intellifor additional anal	elligence detection malicious beh re detections b to read CPU cor gence will caus ysis. Learn Mor	avior y Sophos Anti- nfiguration e your files to be re	
Path: c:\users\victim1 est.zip\sophos_	.admin\appdata\lo hips_test.exe	cal\temp\temp	1_sophos_hips_t	Î
Name: Process ID:	sophos_hips_te 1940	st.exe		_

Note: Endpoints enrolled in the EDR early access program will start submitting metadata on portable executable files that have a poor or uncertain reputation to Sophos Central. The search in this case is running a query on this metadata to see if any other endpoints have seen the SHA-256 hash of this file.

9. In the search results we should see that the file was also seen on the second endpoint the file was downloaded to, as the file wasn't run on the second endpoint the 'First run' date should be blank

En	Endpoint Protection – Item Search Results Overview / Endpoint Protection Dashboard / Threat Search Results								
Search for: c:\users\victimladmin\appdata\local\temp\temp1_sophos_hips_test zip\sophos_hips_test exe Search by SHA 256: 3eeea788a32ceaf324c2a0d23745b0aabf00a8535bbf0a7c24e3eb528eab7506 Found on 0 computers									
Clean and block									
								What does this do?	
								Save Search	(
Origin	ating search item:								
	Name	Computer	Admin isolated		First run		Latest status by path	RCA	
	sophos_hips_test.exe	Victim-1-Win7	No		Sep 27, 2018 12:0	MA 00	Sep 18, 2018 03:56 PM	HPmal/Eicar-A	
									Þ
Found	on 5 other computers:								
	Name	Computer	Admin isolated	First run		Latest status by p	bath		
	sophos_hips_test.exe		No			Sep 11, 2018 11 Discovered	:00 AM C:\Users\Administrator\Downlo t.exe	ads\sophos_hips_tes	

Exercise 2 will walk through a scenario where we have received intelligence on a potential new threat to be aware of. In the example we've been given a file hash and have been asked to investigate.

New Functionality Tested: Threat Search, Clean and Block capability

- 1. On one your endpoints, run the unknown.exe that was downloaded as part of the pre-requisites. Note the file will open and run and there is no detection in this case.
- 2. In the next step let's run a search across the estate to see what endpoints have seen the file hash we are interested in. From the Endpoint Protection Dashboard in Sophos Central, paste 'b1657b54541d4534e9e9b7a328148aa94b4100a626dfb6f276cdf9742b14515e' into the Threat Search window and click the Search button (this is the SHA-256 hash of the unknown.exe file dropped on to our test systems as part of the requisites):

Endpoint Protection - Dashbor Overview / Endpoint Protection Dashboard		Help Sophos Inc -S	Kevin Smith tandard · Super Admin			
Most Recent Threat Cases						See all threat cases
TIME CREATED	PRIORITY	TYPE		USER	DEVICE	
Sep 26, 2018 9:47 PM	High	ML/PE-A		DESKTOP-5N1NAMJ\kevin	DESKTOP-5N1NAMJ	
Sep 26, 2018 3:41 PM	Low	ML/PE-A		devbox32\dev	devbox32	
Sep 26, 2018 3:10 PM	High	ML/PE-A		devbox32\dev	devbox32	
Sep 26, 2018 3:03 PM	Low	ML/PE-A		devbox32\dev	devbox32	
Sep 26, 2018 2:39 PM	Low	ML/PE-A		devbox32\dev	devbox32	
Threat search Search for potential threats on your network Enter one or more SHA 256 file hashes or file names b1657b54541d4534e9e9b7a328148aa94b4100a626dfb6f276cdf9742b14515d Searches on hashes or file names will return portable executable files with uncertain reputation.		Recent threat se	on two endpoints	Created on Sep 25, 2018 03:23 PM Sep 11, 2018 09:58 AM	See all searches	
		Search				

3. The search results should return that both endpoints have seen this file:

Enc	Endpoint Protection - Threat Search Results Overview / Endpoint Protection Dashboard / Threat Search Results Soy								
Search f Found of	Search for: 1 items View items Found on 8 computers								
Jearci					Save Search				
	Computer	Admin isolated	No of items found	Details					
	VM72222215778	No	1	See details					
	DESKTOP-5N1NAMJ	No	1	See details					

4. Click on the See Details link to see what was specifically found on one of the endpoints. Assuming we believe the file to be bad, let's click the Clean and Block action:

Endpoint Protect	ction - Search Deta Dashboard / Threat Searches / Thr	The search Results / Search Der	tails			Help - Kevin Smith Sophos Inc - Standard - Super Admin
1 of 1 found on VM72222215778						
SHA 256 hesh	Name	First run	^	Latest status		
b1657b54541d4534e9e9b 7a328148aa94b4100a626 dfb6f276cdf9742b14515e	unknown.exe	Sep 19, 2018 12:01 PM		Sep 19, 2018 12:01 PM Discovered	C:\Users\Admin\DOWNLOADS\unknown.exe	Clean and block

5. You are asked to provide the reason why you are adding the file to the Clean and block list, enter some text and click Confirm:

Clean and block	×
 You're about to: Clean up this item (with associated files or registry keys) on computers where it's been found. Add the item to the blocked list so that other computers can't run it. 	
Why are you blocking this item? Suspected bad file	
Note: You can see items you've blocked or unblock them in your Blocked Items list in Settings.	
Cancel Confirm	1

Note: The Clean and Block action will apply to portable executable files only and will not apply to PE files that have a good reputation according to Sophos. The Blocked Items list will apply to all endpoints in the estate. *Note to EAP customers the Blocked Items list will also apply to all endpoints regardless of whether they are assigned to the EAP or not.

- 6. Within a few minutes your endpoints will receive new policy that should prevent the Unknown.exe file from being executed. Run Unknown.exe on either endpoint
 - *a.* Unknown.exe should **not** run. We should see a toast message saying the item has been blocked by admin



7. Shortly after adding to the Block list, Unknown.exe should be cleaned from both endpoints



8. If we realise an error was made and we want to remove the SHA-256 hash for unknown.exe from the Blocked Items list, go to Global Settings > Endpoint Protection > Blocked Items. From the Blocked Items page select the SHA-256 hash we added and click the Remove button. Then click the Save button:



9. Within a few minutes as the new policy is applied to the endpoints the unkown.exe should be released from quarantine and should again be executable.

This concludes the testing guide, as new capabilities are released the guide will be updated to help test new functionality.