ESET Tech Center

Knowledgebase > Legacy > ESET Security Management Center > 7.x > Ransomware Shield - enable Audit mode and exclude an application from detection (7.x)

Ransomware Shield - enable Audit mode and exclude an application from detection (7.x)

Anish | ESET Nederland - 2019-12-30 - Comments (0) - 7.x

Issue

ESET business products (version 7 and later) include **Ransomware Shield**. This new security feature is a part of HIPS and protects computers from ransomware. When ransomware is detected on a client computer, you can view the detection details in ESMC Web Console in **Threats**.

By default, Ransomware Shield blocks all applications with potential ransomware behavior. If there is a legitimate application or script automatically running on the managed computer and performing operations that are evaluated as ransomware behavior (moving files across folders, encrypting files and folders), you may want to exclude it from being blocked by ESET business product.

Solution

ESMC Web Console Policy settings for ESET business products include **Audit mode**. When Audit mode is enabled, applications with ransomware behavior are allowed to run and are only logged in ESMC Web Console in **Threats**. The administrator can decide to block the potential detected threat or allow it permanently by adding it to exclusions.

Follow these steps to exclude applications on a managed computer from being detected as ransomware:

- 1. Open the ESET Security Management Center (ESMC) Web Console.
- 2. Click **Policies**, select the policy for ESET business product, and then click **Policies** \rightarrow **Edit**.

(CSet)	SECURITY MANAGEMENT	CENTER			Gv	Computer Name	QUICK LINKS 🗢	⑦ HELP ♥ 옷 ADMINISTRATOR 글	>9 MIN
		Policies		ACCESS GROUP Selec	t 🗎 SHOW UNA	ISSIGNED 🔽 🛅 All (29)	Tags	ADD FILTER PRESE	TS 🗢 🔿
G		Policies		- NAME		POLICY PRODUCT	TAGS	DESCRIPTION	© ^
		∧ All		Antivirus - N	faximum security	ESET Endpoint for macOS (O		Taking advantage of advance	
		✓ ℓ Custom Policies		Device cont	rol - Maximum se	ESET Endpoint for Windows		All devices are blocked. Whe	
ini De		✓		Device cont	rol - Read only	ESET Endpoint for Windows		All devices can only be read	
<u>a</u>				Firewall - Bl	ock all traffic exce	ESET Endpoint for Windows		Block all traffic except conne	
۲	Policies			Logging - Fi	Il diagnostic log	ESET Endpoint for Windows		This template will ensure that	
~				Logging - Lo	og important eve	ESET Endpoint for Windows		Policy ensures that warnings,	
Φ			۱r	Antivirus - 8	alanced	ESET Endpoint for Windows		Security configuration recom	
5 V.			1 ⁻	Antivirus - N	faximum security	ESET Endpoint for Windows		Taking advantage of machin	
4			1	Visibility - B	alanced	ESET Endpoint for Windows		Default setting for visibility. S	
			1-	Visibility - Ir	visible mode	ESET Endpoint for Windows		Disabled notifications, alerts	
		Tags	5	-	educed interactio	ESET Endpoint for Windows		Disabled statuses, disabled n	
		formation of the	í -		eal-time scanner	ESET File Security for Windows		Optimized performance for s	
			i	Show Details					
		test		New	faximum security	ESET File Security for Windo		Taking advantage of advance	
	Test 3 Test 4	Test 3	_	Tags Edit	lent mode	ESET File Security for Windo		Suitable for multi-user server	
		Test 4	_) Duplicate	i reputation and	ESET Endpoint for Windows		Enables ESET LiveGrid clou	
		Test comapny 2		Change Assignments	reputation and	ESET Mail Security for Micros		Enables ESET LiveGrid® clou	
			1 CLI	Import	reputation and	ESET File Security for Windo		Enables ESET LiveGrid	
				Export	sks - Recommen	ESET Full Disk Encryption		Enables full disk encryption f	
			3	Access Group	t disk only - Reco	ESET Full Disk Encryption		Enables full disk encryption f	\sim
	COLLAPSE			ACTIONS 🗢	NEW POLICY			٥ ٩	0100

Figure 1-1 Click the image to view larger in new window

3. Click Settings \rightarrow Detection Engine \rightarrow HIPS.

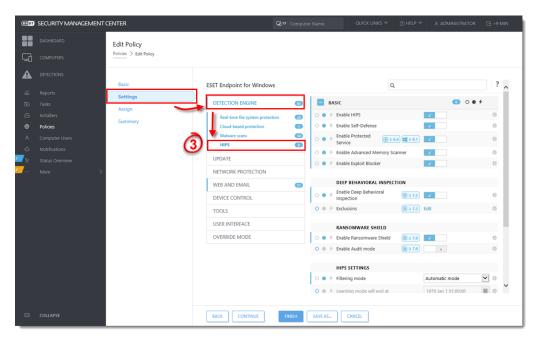


Figure 1-2 Click the image to view larger in new window

4. Click the slider bar next to **Enable Audit mode** to enable this setting and click **Finish** to apply the Policy settings.

Use Enable Audit Mode with care

When you apply **Enable Audit mode**, automatic ransomware protection is turned off and the managed computer is not protected against ransomware.

(CSet)	SECURITY MANAGEMENT	CENTER							
		Edit Policy							٦
돠		Policies > Edit Policy							
▲		Basic	ESET Endpoint for Windows		٩			?	
2		Settings						. ^	
Ð		Assign	DETECTION ENGINE	3 E BASIC			• • • •		
 ⊚	Installers Policies	Summary		28	able HIPS able Self-Defense			0	
×	Computer Users			50 0 4 Er	able Protected			0	
φ			HIPS	Se	able Advanced Memory Scan			0	
<u>ه ب</u>			UPDATE		able Exploit Blocker	×		0	
4			NETWORK PROTECTION		EEP BEHAVIORAL INSPECTIO				
				Er	able Deep Behavioral	©≥7.2 ✓			
			DEVICE CONTROL	In	spection	(0 ≥ 7.2) Edit		0	
			TOOLS	0070		(JETE) EUR			
			USER INTERFACE		ANSOMWARE SHIELD				
			OVERRIDE MODE		able Ransomware Shield	© ≥ 7.0 ✓		0	
							U		
					PS SETTINGS				
				 ○ ● ≠ Fil ○ ● ≠ Le 		Automatic n 1970 Jan 1 (
				0 0 % Le	arning make will end at	1970 Jan 1 0	1:00:00	0	
e	COLLAPSE			H SAVE AS	CANCEL				

Figure 1-3 Click the image to view larger in new window

- 5. On the managed computer, run the application with ransomware behavior.
- 6. Return to ESMC Web Console and click Detections. You can see the information about the potential ransomware application detected on the client computer. In the **Action** column, there is a note **allowed by audit**.

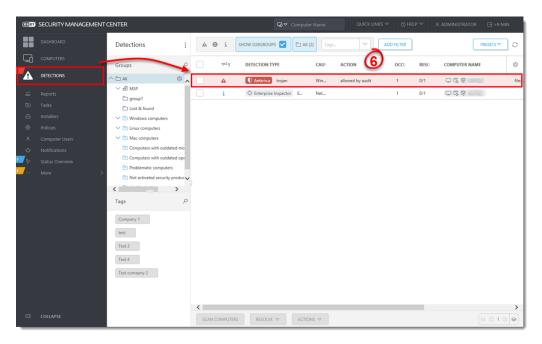


Figure 1-4 Click the image to view larger in new window

7. Click the threat and click **Show Details**. Verify the path to the application in **Object URI** and make sure that you want to exclude the threat from detection. Then click **Close**.

Use Exclusions with caution

Exclusions increase the exposure of managed computer to malware.

eser	SECURITY MANAGEMENT	CENTER				G∼	Computer Name	QUICK LINKS	▼ () HEL	.p マ	A ADMINISTRATOR	금 >9 MI	N
		Detections	:		0 i	SHOW SUBGROUPS 🗹	Tags	. 🔻	ADD FILTER			PRESETS 🗢	0
G		Groups	Q		≂25	DETECTION TYPE	CAUS	ACTION	OCCU	RESO	COMPUTER NAME		٢
A	DETECTIONS		© 🔨		A	Antivirus trojan	Win	allowed by audit	1	0/1			file:/
¥ ₽ £ © < ¢ < ;; • • • 0 1 0 × ;;		 MSP group1 Latk found This found This computers This computers The computers Computers with outdate Computers with outdate Computers with outdate Togs Tags Test 4 Test computer 2 	d opr		i	Detection i Show Details · Mark As Resolved · Mark As Not Reco Computers Actions ↓ Scan Path · Create Exclusion	\sim		1	0/1	060		
E	COLLAPSE			< SCAP	N COMPUTE	RS RESOLVE 🗢	Actions 🗢				(⊲ ⊙ 1 ⊙	>

Figure 1-5 Click the image to view larger in new window

8. Click the detection and select Create exclusion.

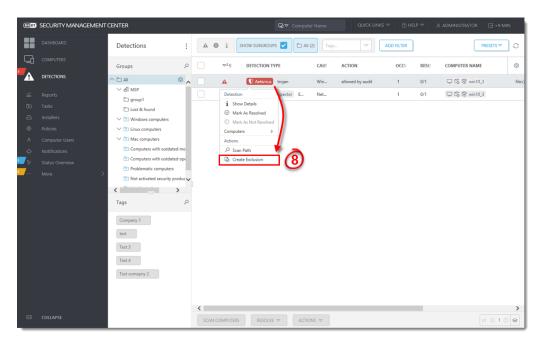


Figure 1-6 Click the image to view larger in new window

9. Select the **Exclusion criteria**. The recommended option is pre-selected based on the detection type. Select the check box **Resolve matching alerts** to automatically resolve the alerts covered by the exclusion. Optionally, you can add a **Comment**.

CSet	SECURITY MANAGEMENT	CENTER		G ▼ Computer Name	QUICK LINKS 🗢	⊙ HELP マ		🖃 >9 MIN		
		Settings Target	Do not trigger detections for: Any file with the SHA-1 hash (
	DETECTIONS	Preview	i Some versions	of the security products may not support all exclusio	n criteria. <u>More informati</u>	on				
а в е е е е е			9 Exclusion criteria	Path & Detection Exclude each file by path and detection Exclude each file by its SMA-1 hash Exclude each file by its SMA-1 hash Detection Exclude each detection]]					
<u>4</u>			Auto-resolving	Resolve matching alerts						
			Target Comment (for all exclusions)	A1				< >		
			Target							
e				ICEL FINISH						

Figure 1-7 Click the image to view larger in new window

10. Click Target and select computer(s) or group(s) where the exclusion will be applied and click Finish

CSET	SECURITY MANAGEMENT	CENTER		Computer Name	QUICK LINKS 🗢 💿 I	HELP マ 옷 ADMINISTRATOR	금 >9 MIN
==		Settings					
G		Target	i Exclusion is by default c	reated for all user accessible computers (ho	ome group of the user creating th	ne exclusion). You can change assignme	ents below.
	DETECTIONS	Preview	ADD COMPUTERS ADD	GROUPS REMOVE TARGETS			
		6	TARGET NAME	TARGET DESCRIPTION	TARGET TYPE		
Þ		•	All		Static Group		
					ousic croop		
۲							
~							
Φ							
<mark>۶ /</mark> ۴							
			Preview				
E			CONTINUE	FINISH			

- 11. Ransomware Shield no longer detects the excluded application.
- 12. Edit the Policy for ESET business product and click the slider bar next to **Audit mode** to turn it off and ensure the automatic ransomware protection of the managed computer.

(ISer)	SECURITY MANAGEMENT	CENTER	G.						N
		Edit Policy							
교		Policies > Edit Policy							
•		Basic	ESET Endpoint for Windows			٩		?	
		Settings	ESET Endpoint for Windows			ď			`
		Assign	DETECTION ENGINE	63	BASIC		O ● 4		
		Summary	Real-time file system protection	23 0	● 🦩 Enable HIPS		×	0	
	Policies	Summary	Cloud-based protection				4	0	
~			Malware scans HIPS	<u> </u>	 	ed (€ ≥ 6.6) (≥ 8.1)	A	0	
¢					● 🦩 Enable Advano	ed Memory Scanner	×	0	
≶_/γ			UPDATE	0	● 🦩 Enable Exploit	Blocker	×	0	
4			NETWORK PROTECTION						
			WEB AND EMAIL	g		ORAL INSPECTION			
			DEVICE CONTROL	0	 Finable Deep Be Inspection 	ehavioral (0 ≥ 7.2)	1 A	0	
			TOOLS	0	Exclusions	(€ ≥ 7.2)	Edit	0	
			USER INTERFACE		RANSOMWAR				
			OVERRIDE MODE	- N	Enable Ransom			0	
					 <i>f</i> Enable Audit m 		- 12	0	
					HIPS SETTING	s			
				0	Filtering mode		Automatic mode	v •	
				0	• 🖩 Learning mode	will end at	1970 Jan 1 01:00:00	11 o	1
	COLLAPSE		BACK CONTINUE	FINISH	/E AS CANCEL)			

Figure 1-8 Click the image to view larger in new window

Comments (0)