

Harmony Endpoint 簡易運用ガイド 除外設定: Threat Emulation / Extraction、Zero-Phishing

Policy > Policy Capabilities > Exclusion Center Policy > Global Exclusion

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

YOU DESERVE THE BEST SECURITY



- ・除外設定の概要
- Webダウンロード時のThreat Emulation/Extraction、 Zero-Phishingの除外設定





除外設定の概要(1/2)

- Harmony Endpointによる検査から特定のオブジェクトを除外できます
- 除外設定は、[ログ]のレコードから右クリックで作成するか、除外メニューで作成します
- 組織全体に適用することも、個別ルールに適用することもできます



除外設定の概要(2/2)

- セキュリティ機能ごとにドメイン名、フォルダパス名、ファイルハッシュ値などで除外指定します
- <u>除外設定を行うことでセキュリティ機能による脅威の検査が行われなくなります。Web サイトやファイル等の安全性を</u> 確認した上で慎重に実施してください

セキュリティ機能		除外指定方法				
URL フィルタ	Domain/URL					
Anti-Malware	Infection by name	Process Path	File Path	Folder Path		
Threat Emulation	Domain	SHA-1 Hash	Folder Path			
Threat Extraction	Domain	SHA-1 Hash				
Zero Phishing	Domain					
Anti-Ransomware	Folder Path	Certificate	Protection Name	Process Path		
Behavioral Guard	Folder Path	Certificate	Protection Name	Process Path		
Anti-Bot	Domain	URL	Protection Name	Process	IP Range	
Anti-Exploit	Process Path	Protection Name				
Forensics - Quarantine	Certificate	File Path	Folder Path	MD5 Hash	SHA-1 Hash	File Extension
Forensics - Monitoring	Process Path	Certificate				

Webダウンロード時の Threat Emulation / Extraction の除外設定

除外設定の概要

- ファイルをダウンロードもしくは、認証情報を入力する Web サーバのドメイン名、IP アドレスを指定して、
 Web ダウンロード時のThreat Emulation / Extraction、Zero-Phishing による検査、無害化の除外設定を行えます
- 1. ドメイン名の指定方法
 - http/s、*、またはその他の特殊文字を使用せずにドメイン名を指定してください
 - 例1-1:www.checkpoint.com
 - ホスト名を省略すると、指定したドメインのすべての FQDN が除外されます
 - 例1-2: checkpoint.com
 - www.checkpoint.com、www2.checkpoint.com などが除外されます
 - ドメイン名を指定すると、指定したドメインのサブドメイン、下位ドメインも除外されます
 - 例1-3:com
 - すべての com ドメインが 除外されます
- 2. IP アドレスの指定方法

CHECK POINT

- URL の FQDN 部分が IP アドレスの場合、IP アドレスを指定してください
 - 例2-1:192.168.100.100
- 複数の IP アドレスを範囲指定する際は、ネットマスクを指定してください
 - 例2-2:192.168.100.0/24

NEW EXCLUSION		
Exclusion		
Threat Emulation, Extraction and	Zero Phishing Exclu	sions 🔻
Method		
Domain		-
Value *		
www.checkpoint.com		
Comment		
	CANCEL	ОК

除外設定の作成画面を表示

- Global Exclusionsもしくは、Exclusion Centerの画面で、★ Add をクリックします
- NEW EXCLUSION 画面が開きます

Global Exclusions での全組織への適用

Check Point 🔎 **...**-AT HARMONY ENDPOINT **...**-TAT HARMONY ENDPOINT 0 🗿 cpjdemo006 🗸 Ø Check Point < Ð C Default settings Ð Threat Prevention Threat Prevention OVERVIEW * Add Actions - O Search... 10 items Actions - 🔎 Search... Install Policy 0 items **Policy Capabilities** Add **Policy Capabilities** LΠ Global Exc Exclusion **Global Exclusions** Method Value ⊂xclusion POLICY Forensics -> Mon ★ Add をクリック **-**★ Add をクリック Rule Exclusion NEW EXCLUSION × ASSET MANAGEME Certificate McAfee ePO Development (SPC) Certificate Certificate Access Rules Exclusion 0 Certificate Certificate Symantec Corporation Access & Compliance Certificate Certificate Trend Micro Anti Bot -> URL Filtering exclusions -Method Domain/URL -Value * Add to all rules CANCEL

Exclusion Center での個別ルールへの適用

Threat Emulation の除外設定画面を表示

- 1. NEW EXCLUSION の画面で、「Exclusion」のドロップダウンリストをクリックします
- 2. 「Threat Emulation, Extraction and Zero Phishing Exclusions」を選択します
- 3. Threat Emulation、Extraction、Zero-Phishingの除外設定画面に切り替わります

NEW EXCLUSIO ① 「Exclusion」 のドロップダウン リストをクリック Exclusion ❶
Anti Bot -> URL Filtering exclusions
Anti-Malware -> Exclude Infection by name
Anti-Malware -> Process exclusions (on-access only)
Anti-Malware -> File & Folder exclusions (system_scheduled and on Fo ② 「Threat Emulation, Extraction and Zero Phishing Exclusions」 を選択 Fo
Threat Emulation, Extraction and Zero Phishing Exclusions
Threat Emulation -> Anti Exploit Exclusions
CANCEL OK

う 日 1 り う よ う	③ 除外設定画面が切り替わったこと を確認
NEW EXCLUSION	
Exclusion 0 Threat Emulation,	Extraction and Zero Phishing Exclusions 🔹
Method	
Domain	•
Value *	
Comment	
	CANCEL

除外条件を設定

- 1. 「Method」が Domain となっていることを確認します
- 2. 「Value」に除外条件を入力します
- 3. 「OK」をクリックします



除外設定を適用(組織全体に適用する場合) (1/2)

- 1. Global Exclusions の画面が表示され、除外設定が作成されていることを確認します
- 2. Save ボタンをクリックします
- 3. Install Policy ボタンをクリックします



除外設定を適用(組織全体に適用する場合)(2/2)

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます

*	HARMONY ENDPOINT	畫 cpja	lemo006 🗸		Ø	Û.	Check Point	
INST	FALL POLICY							× Ð
LI TH	he following changes were made since the la	ast policy insta	allation. Review the cha	inges and click on 'instal	ll' to insta	ll policy.		1 em
	Changed Rules Settings (2)						<u>^</u>	
	Rule Name		Policy Type	Changes			Modified C	
Ē	🖌 Eval		Threat Prevention	Settings were chang	ed		11/10/2022	1
+	✓ Default settings		Threat Prevention	Settings were chang	ed		12/7/2022,	
1		_						
C	Changed Rule Order and Assignments	(0)		4 11.5			~	
					(') 			
Ę					CANCE		INSTALL	
ġ.	Endpoint Client							
	Browse Client							

除外設定を適用(個別ルールに適用する場合) (1/2)

- 1. Exclusion Center の画面が表示され、除外設定が作成されていることを確認します
- 2. OK ボタンをクリックします
- 3. Policy Capabilities 画面が表示されたら、Save ボタンをクリックします
- 4. Install Policy ボタンをクリックします





除外設定を適用(個別ルールに適用する場合) (2/2)

- INSTALL POLICY の画面が表示されたら、「INSTALL」をクリックします
- 以上で、除外設定の適用は完了です
- 10分程度でクライアントにポリシーが反映されます

	TARMONY ENDPOINT	า cpjdemo006 v		Check Point
INST	TALL POLICY			×
Т	The following changes were made since the la	st policy installation. Review the ch	nanges and click on 'install' to install p	> >
-1	Changed Rules Settings (1)			
	Rule Name	Policy Type	Changes	Modified C
Ŧ	 Default settings 	Threat Prevention	Settings were changed	12/9/2022,
1	Changed Rule Order and Assignments	(0)		
F			クリック	
Ċ,			CANCEL	INSTALL
Ŷ	▼ Export Package	Download		
Ğ₽	Endpoint Client	Download	d Emulation & Extraction	Prevent -
	Browse Client			



THANK YOU

YOU DESERVE THE BEST SECURITY