

Como configurar uma regra de compliance com remediação automática no Harmony Endpoint

Índice

Cenário 3
Pré-requisitos..... 3
Procedimento..... 3
Referências..... 6

Cenário

Dentre as funcionalidades presentes no Harmony Endpoint existe o Compliance.

HARMONY ENDPOINT PACKAGES	
Packages	<ul style="list-style-type: none">• Data Protection – includes Full Disk Encryption and Removable Media Encryption, including Access Control and Port Protection• Harmony Endpoint Basic – includes Anti-Malware, Anti-Ransomware, Zero-day Phishing, Advanced Threat Prevention, & Endpoint Detection and Response (EDR)• Harmony Endpoint Advanced – includes Harmony Endpoint Basic, plus Threat Emulation and Threat Extraction• Harmony Endpoint Complete – includes Harmony Endpoint Advanced, plus Data Security (Full Disk and Media Encryption) <p>Note: Endpoint Compliance is provided with all packages</p>

O Compliance foi criado para apoiar no estabelecimento de um baseline de configuração em um ambiente.

E esse baseline pode considerar diversos tipos de validação como chave de registro, arquivo, processo e etc. E caso a validação resulte em falha podem ser executadas algumas ações como notificação, isolamento da máquina, execução de script e etc.

Pré-requisitos

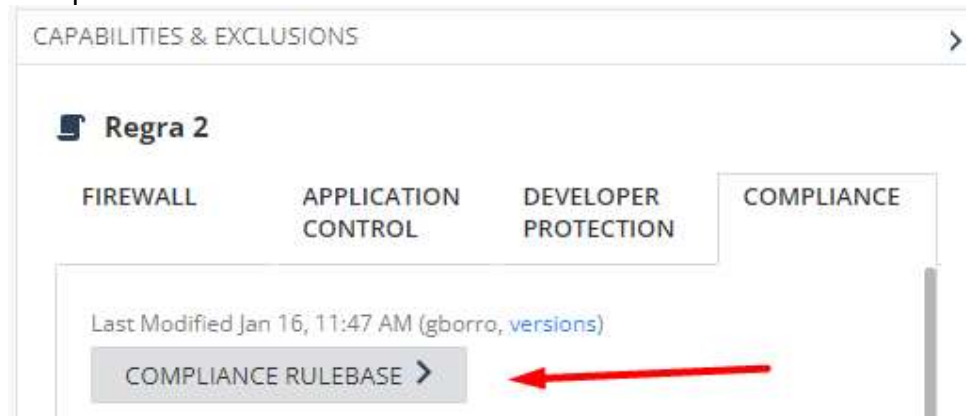
Para esse procedimento foi considerado um cenário de exemplo no qual o programa putty.exe deve estar em execução a todo momento, caso essa validação falhe deve ser rodado um script chamado script.bat.

Logo, temos como pré-requisitos:

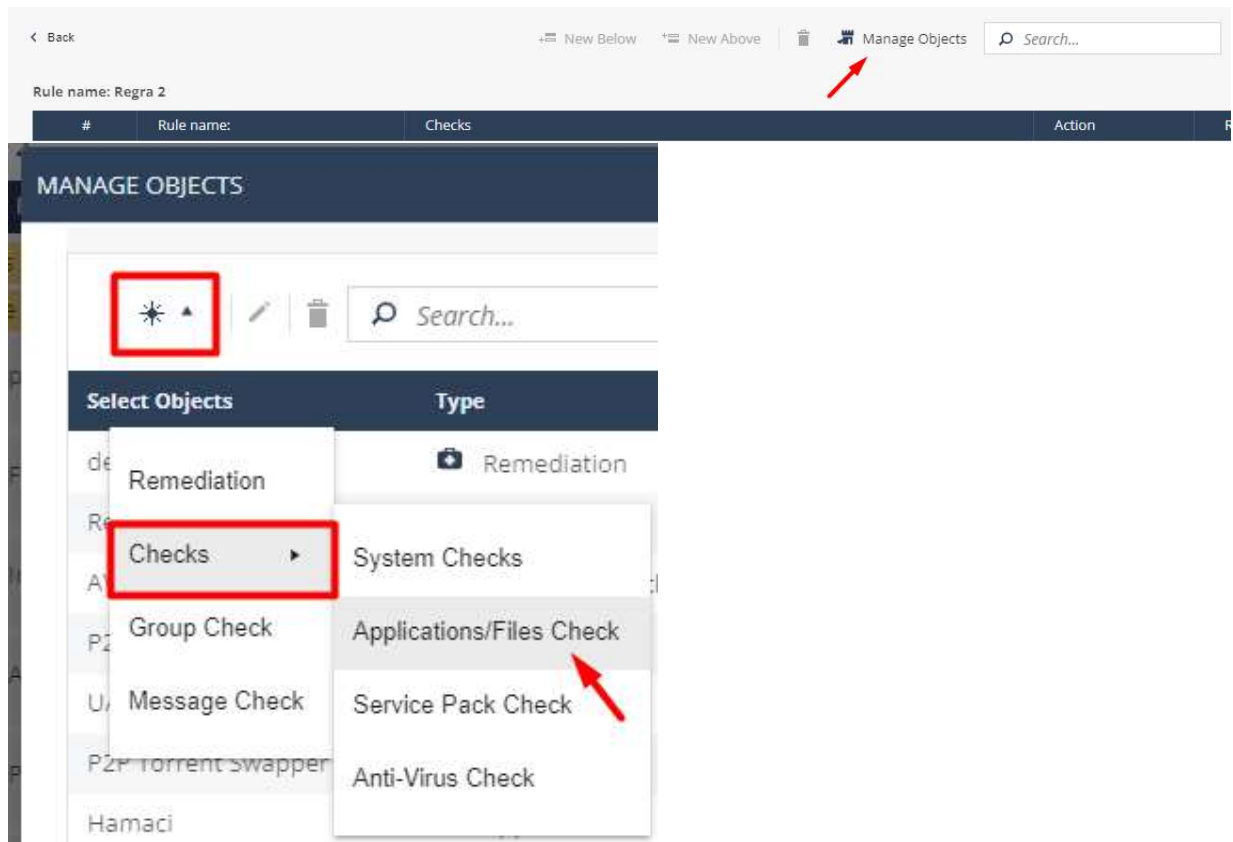
- Determinar a validação, no caso o programa rodando
- Determinar a remediação, no caso a execução do script.bat

Procedimento

Acessar as regras de compliance em Policy > Access & Compliance > Compliance > Compliance Rulebase



Dentro de Manage Objects, criar um objeto de Check de aplicação/arquivo:



Preencher com as informações devidas:

APPLICATIONS/FILES CHECK ✕

Name:

Comment:

Operating System:

Modify and check registry

Registry value name:

Registry value:

i Note: In order to only check if value name exist, use "" as value data.

Modify registry key and value

Action:

Reg type: REG_SZ REG_DWORD

Check registry key and value: Do not exist Exist

Check File

File availability:

File name:

File path:

Use environment variables of logged in user

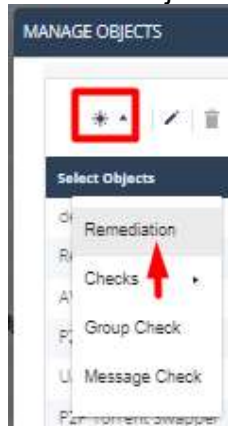
Check files properties:

- Match the file version
- Min: Max:
- Checksum
- Match MD5 checksum:

File is not older than Day(s)

Clicar em OK

Criar um objeto de remediação



Preencher de acordo:

Download path: %USERPROFILE%\AppData\Local\Temp\temp.bat

URL: <File://C:\Users\azureuser\Documents\script.bat>

Parameters: /VERYSILENT/ALLUSERS

MD5: valdiar o MD5 do arquivo

REMEDIATION
✕

Name

Comment

Operation

Run custom file

Download path

URL

Parameters

Match MD5 checksum

 Calculate...

Run as...

Run as system Run as user

Message

Execute when

Automatically execute operation with user notification only in case of failed remediation

Execute operation only after user notification

Use same messages for both Non-Compliant an Restricted

+
×

🔍

Language	Non-Compliant Message	Restricted Message
en_US	default_ooc_message	default_ooc_message

CANCEL OK

Referências

[sk162635 – ATRG: Endpoint Security Compliance Blade](#)

[Harmony Endpoint Administration Guide - Compliance](#)