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

Security Engineering Brazil
2023

Índice

Cenário

Dentre as funcionalidades presentes no Harmony Endpoint existe o Compliance.

HARMONY ENDPOINT PACKAGES	
Packages	• **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) **Note:** Endpoint Compliance is provided with all packages

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

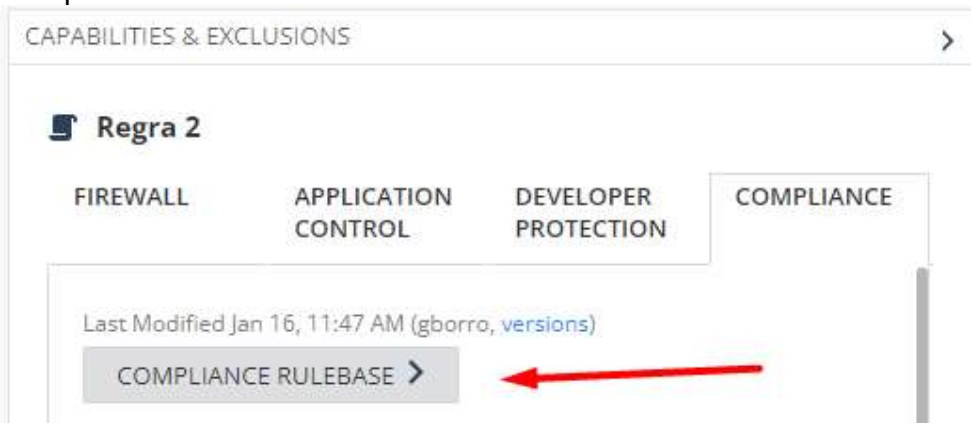
Para esse procedimento foi considerado um cenário de exemplo no qual o programa putty.exe deve estar em execução a todo momento, caso essa validação falhe deve ser rodado um sctipt chamado script.bat.

Logo, temos como pré-requisitos:

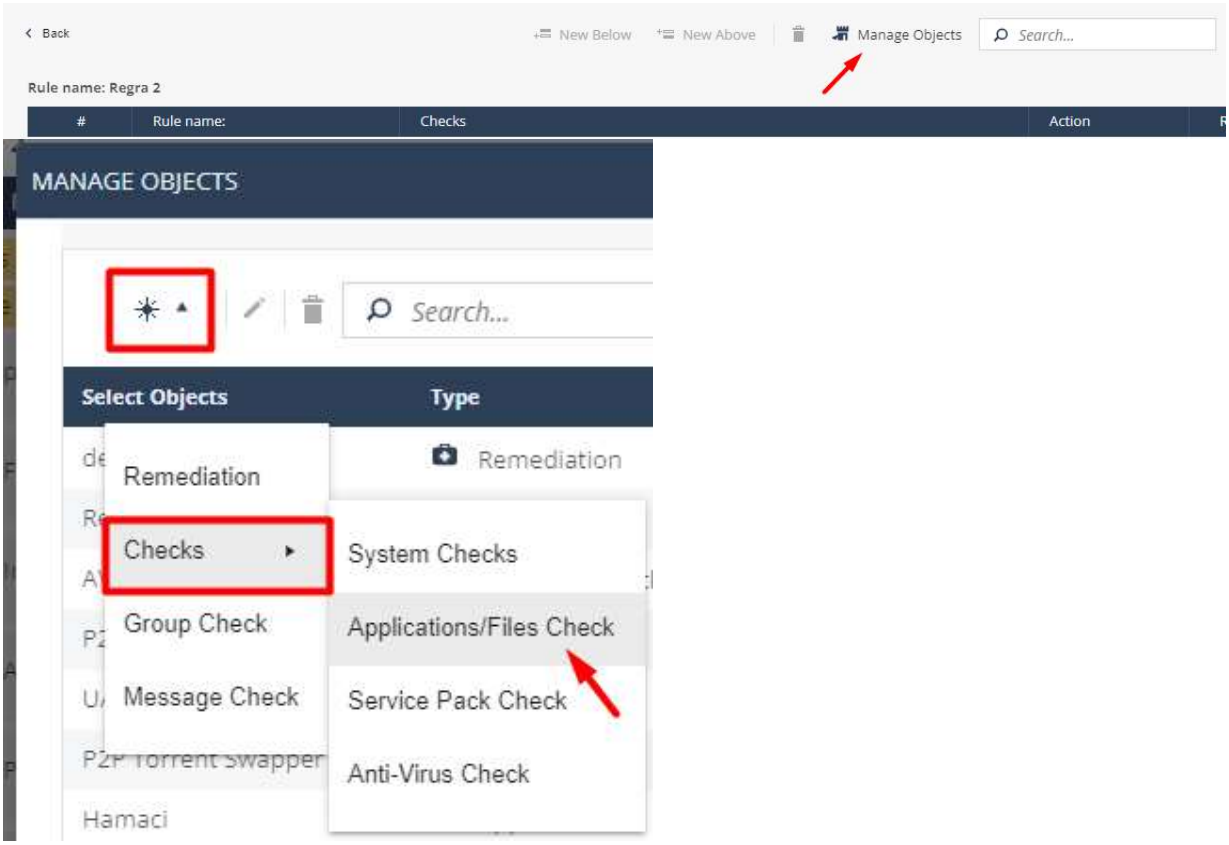
- Determinar a validação, no caso o programa rodando
- Determinar a remediação, no caso a execução do script.bat

Procedimento

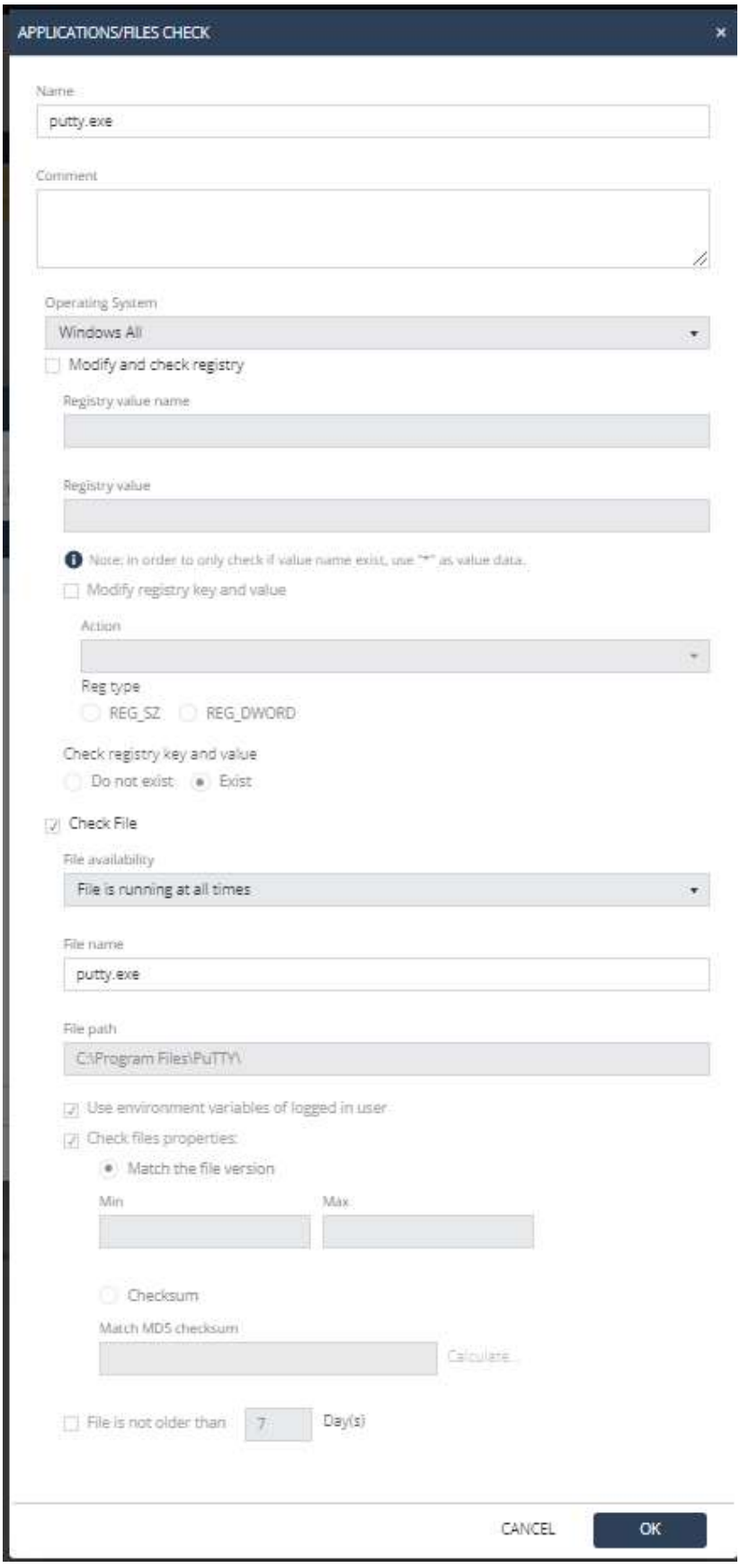
Acessar as regras de compliance em Policy > Access & Compliance > Compliance > Compliance Rulebase



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

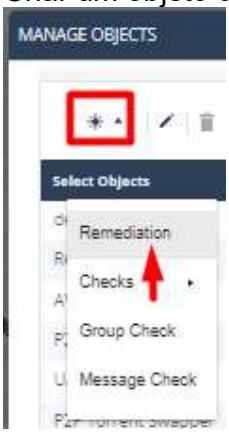


Preencher com as informações devidas:



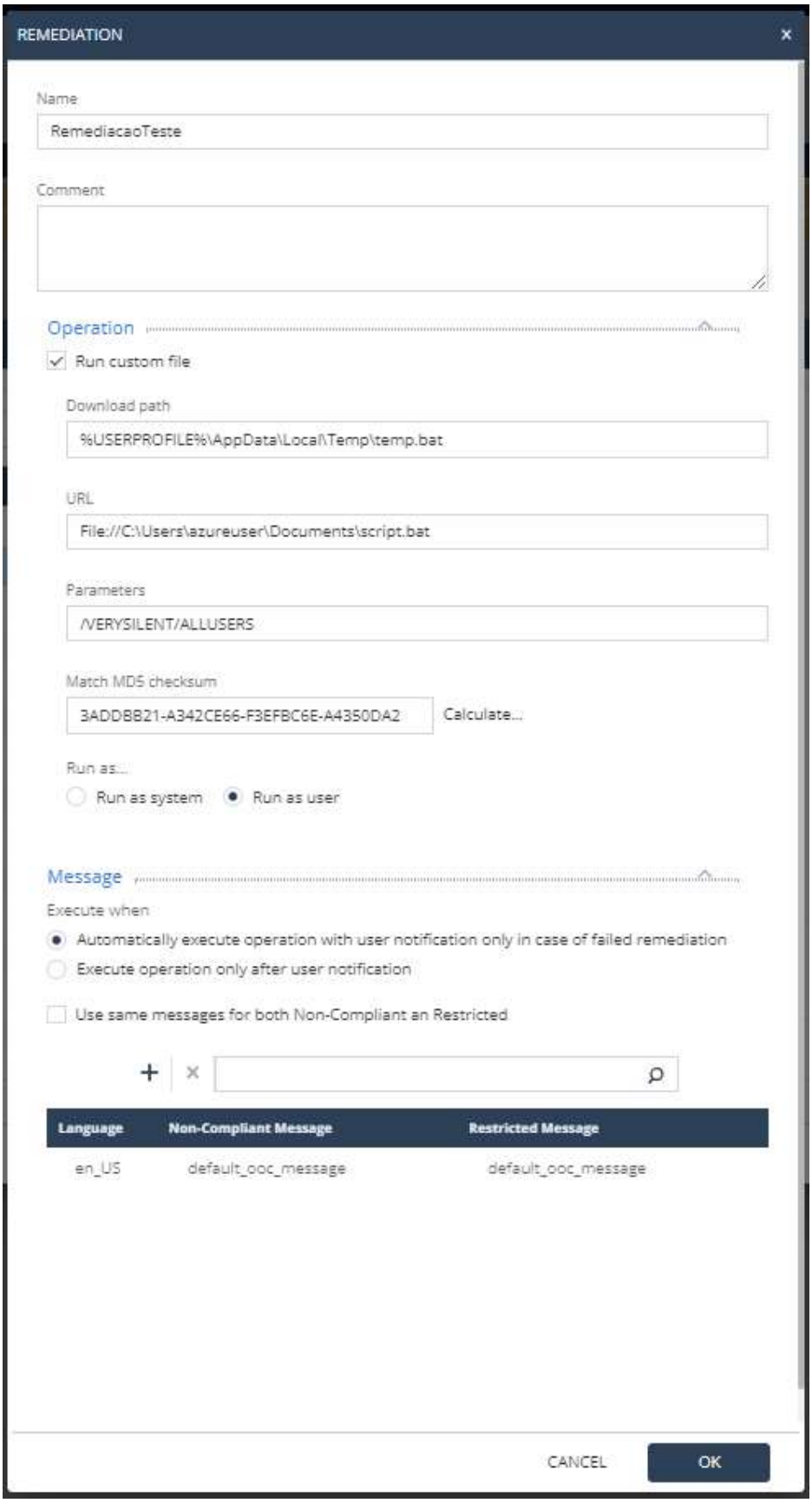
Clicar em OK

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



Referências

sk162635 – ATRG: Endpoint Security Compliance Blade

Harmony Endpoint Administration Guide - Compliance

