# Solucionar problemas de prevenção de exploração em endpoints seguros

## Contents



## Introduction

Este documento descreve a configuração do mecanismo de prevenção de exploração no console do Secure Endpoint e como executar a análise básica.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos.

- Acesso do administrador ao console do Secure Endpoint
- Conector de endpoint seguro
- Recurso de Prevenção de Exploração habilitado

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- Conector versão 7.3.15 ou posterior
- Windows 10 versão 1709 e posterior ou Windows Server 2016 versão 1709 e posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

O procedimento descrito neste documento é útil para executar uma análise básica com base nos eventos, disparados no console e sugere que você explore as exclusões de prevenção caso conheça o processo e o utilize em seu ambiente.

O mecanismo de prevenção de exploração oferece a capacidade de proteger seus endpoints contra ataques de injeção de memória comumente usados por malware e outros ataques de dia zero a vulnerabilidades de software sem patches. Quando detecta um ataque contra um processo protegido, ele é bloqueado e gera um evento, mas não é colocado em quarentena.

## Processos protegidos

O mecanismo de Prevenção de Exploração protege esses processos de 32 e 64 bits (conector Secure Endpoint Windows versão 6.2.1 e posterior) e seus processos filhos:

- Aplicativo do Microsoft Excel
- Aplicativo do Microsoft Word
- Aplicativo Microsoft PowerPoint
- Aplicativo do Microsoft Outlook
- Navegador do Internet Explorer
- Navegador Mozilla Firefox
- Navegador Google Chrome
- Aplicativo Microsoft Skype
- Aplicativo TeamViewer
- Aplicativo VLC Media player
- Host de Script do Microsoft Windows
- Aplicativo Microsoft Powershell
- Aplicativo Adobe Acrobat Reader
- Servidor de Registro da Microsoft
- Mecanismo do Agendador de Tarefas da Microsoft
- Executar Comando DLL da Microsoft
- Host de Aplicativos HTML da Microsoft
- Host de Script do Windows
- Ferramenta de Registro de Assembly da Microsoft
- ZOOM
- Folga
- Equipes Cisco Webex
- Equipes da Microsoft

## Processos excluídos

Estes processos são excluídos (não monitorados) do mecanismo de prevenção de exploração devido a problemas de compatibilidade:

- Serviço McAfee DLP
- Utilitário McAfee Endpoint Security

### Exploit Prevention versão 5 (Conector versão 7.5.1 e posterior)

O conector para Windows Secure Endpoint 7.5.1 inclui uma atualização significativa para a prevenção de exploração. Os novos recursos nesta versão incluem:

- Proteger unidades de rede: Protege automaticamente os processos executados a partir de unidades de rede contra ameaças como ransomware
- Proteger processos remotos: Protege automaticamente os processos executados remotamente em computadores protegidos que usam um usuário autenticado no domínio (admin)
- Desvio de AppControl por meio de rundll32: Interrompe linhas de comando rundll32 especialmente criadas que permitem executar comandos interpretados
- Desvio de UAC: Bloqueia o escalonamento de privilégios por processos mal-intencionados; evita que o mecanismo de Controle de Conta de Usuário do Windows ignore
- Credencial de navegadores/cofres Mimikatz: Se ativada, a Prevenção de exploração protege contra roubo de credenciais no Microsoft Internet Explorer e nos navegadores Edge
- Exclusão de cópia de sombra: Rastreia a exclusão de cópias de sombra e intercepta a API COM no Serviço de Cópias de Sombra de Volume da Microsoft (vssvc.exe)
- Hashes SAM: Protege contra roubo de credenciais de hash SAM por Mimikatz, intercepta tentativas de enumerar e descriptografar todos os hashes SAM no hive do Registro **Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users**

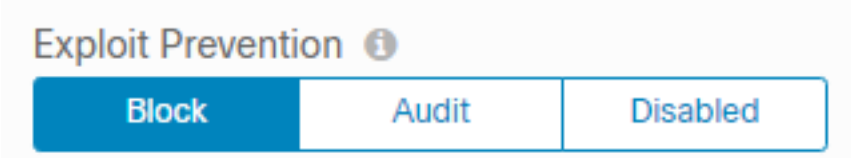
- Proteger processos executados: Injete nos processos que são executados, se eles tiverem sido iniciados antes da instância de Prevenção de Exploração (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe)

Todos esses recursos são ativados por padrão quando a Prevenção de exploração está ativada na política.

## Configuração

Para habilitar o mecanismo de Prevenção de Exploração, navegue para **Modos e Mecanismos** em sua política e selecione o modo de Auditoria, o modo de Bloqueio ou o modo Desabilitado, como mostrado na imagem.

> **Note**: O modo de auditoria está disponível apenas no conector de Windows do Secure Endpoint 7.3.1 e posterior. As versões anteriores do conector tratam o modo de auditoria como o modo de bloqueio.

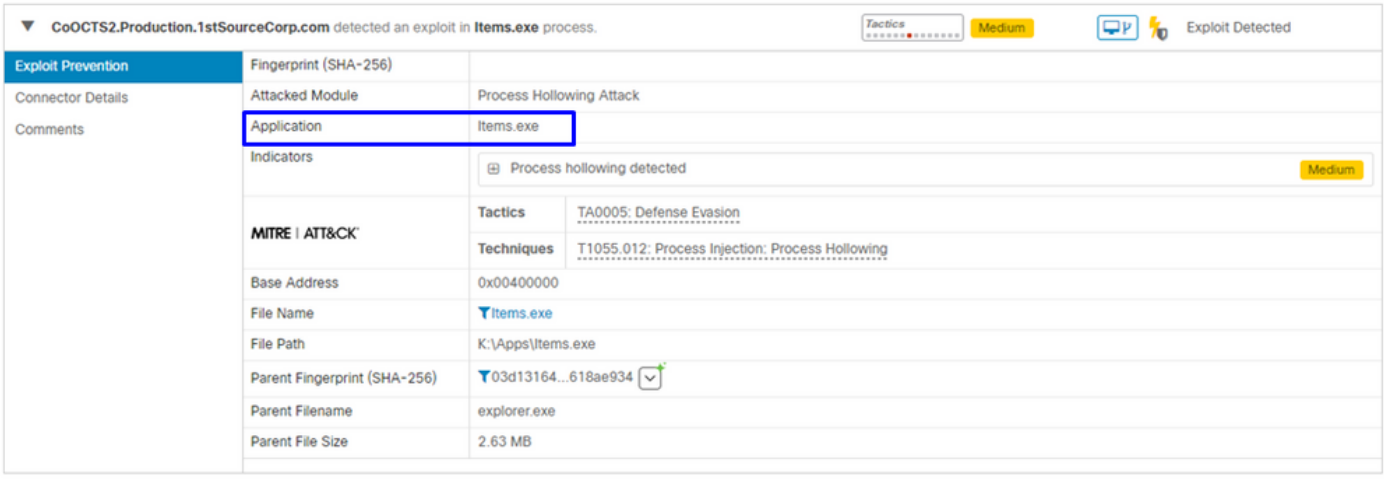



> **Note**: No Windows 7 e no Windows Server 2008 R2, você precisa aplicar o patch para o Microsoft Security Advisory 303929 antes de instalar o conector.

## Detecção

Quando a detecção é acionada, uma notificação pop-up é exibida no endpoint, como mostrado na imagem.

O console exibe um evento de prevenção de exploração, como mostrado na imagem.

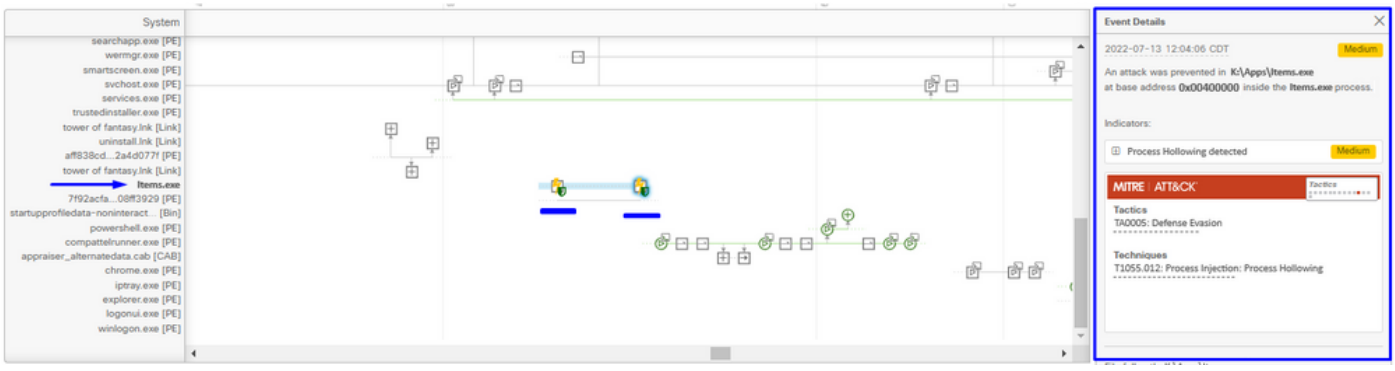



# Troubleshoot

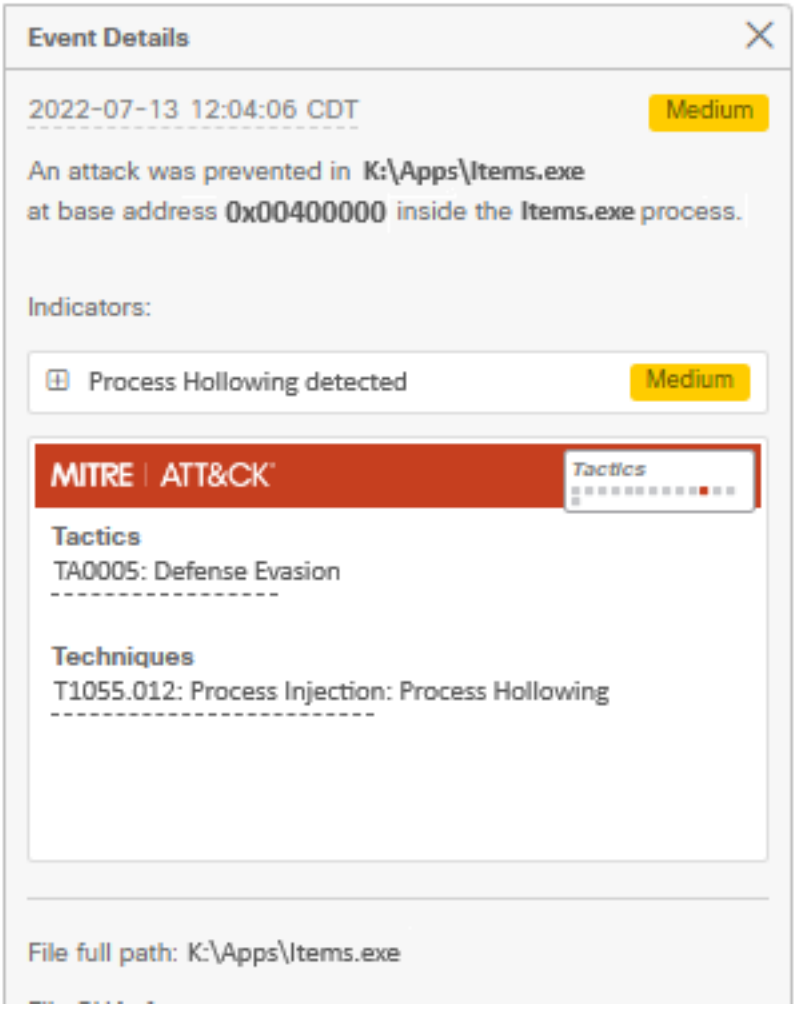
Quando um evento de prevenção de exploração é acionado no console, uma forma de identificar o processo detectado é baseada nos detalhes para fornecer visibilidade dos eventos que ocorreram enquanto o aplicativo ou processo era executado, você pode navegar para a **trajetória do dispositivo**.

Etapa 1. Clique no ícone **Device Trajetory** que aparece no evento Exploit Prevention, como mostrado na imagem.


Etapa 2. Localize o ícone de Prevenção de exploração na linha do tempo da Trajetória do dispositivo para ver a seção **Detalhes do evento**, como mostrado na imagem.




Etapa 3. Identificar os detalhes do evento e avaliar se o processo ou aplicativo é confiável/conhecido em seu ambiente.




## Detecção de falsos positivos

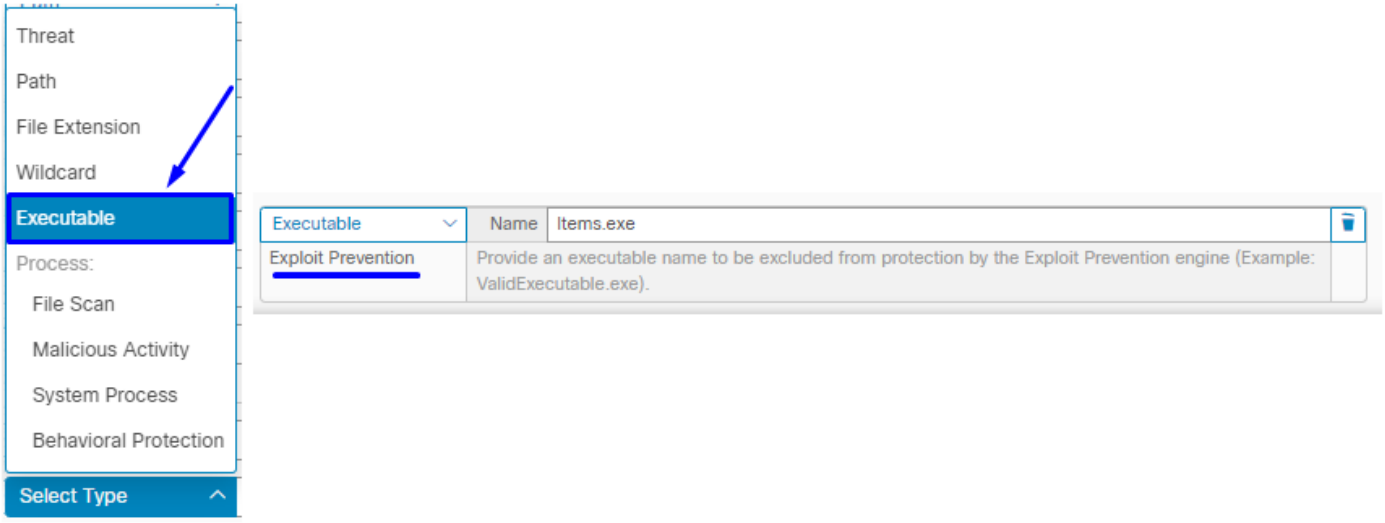
Uma vez identificada a detecção e se o processo/executável for confiável e conhecido pelo seu ambiente, ele pode ser adicionado como uma exclusão. Para evitar que o conector faça a varredura para ele.

As exclusões de executáveis só se aplicam a conectores com Prevenção de Exploração (Conector versão 6.0.5 e posterior) habilitada. Uma exclusão de executável é usada para excluir determinados executáveis do mecanismo de prevenção de exploração.

> **Cuidado**: não há suporte para curingas e extensões diferentes de exe.

Você pode verificar a lista de Processos Protegidos e excluir qualquer um do mecanismo de Prevenção de Exploração. É necessário especificar o nome do executável no campo de exclusão de aplicativos. Você também pode excluir qualquer aplicativo do mecanismo. As exclusões de executáveis precisam corresponder exatamente ao nome do executável no formato **name.exe**, como mostrado na imagem.

> **Note**: Todos os executáveis excluídos da Prevenção de Exploração precisam ser reiniciados após a exclusão ser aplicada ao conector. E se você desativar a Prevenção de exploração, precisará reiniciar qualquer um dos processos protegidos que estavam ativos.




> **Note**: Verifique se o conjunto de exclusão foi adicionado à política aplicada ao conector afetado.

Finalmente, você pode monitorar o comportamento.

Caso a detecção da Prevenção de Exploração persista, entre em contato com o suporte do TAC para executar uma análise mais profunda. Aqui você pode encontrar as informações necessárias:

- Captura de tela do evento de prevenção de exploração
- Captura de tela da trajetória do dispositivo e detalhes do evento
- SHA256 do aplicativo/processo afetado
- O problema ocorre com a prevenção de exploração desativada?
- O problema ocorre com o serviço do conector de Ponto de Extremidade Seguro desabilitado?
- O endpoint tem algum outro software de segurança ou antivírus?
- Qual é o aplicativo afetado? Descrever sua função
- Arquivo de diagnóstico (logs do pacote de depuração) com o modo de depuração ativado quando o problema ocorre (neste artigo, você encontrará como coletar o arquivo de diagnóstico)

## Informações Relacionadas

- Guia do usuário do Secure Endpoint
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.