

Crie uma lista de detecção personalizada avançada no Cisco Secure Endpoint

Contents

[Introduction](#)

[Informações de Apoio](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Criar lista de detecção personalizada avançada](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve as etapas para criar uma ACD (Advanced Custom Detection, detecção personalizada avançada) no Cisco Secure Endpoint.

Informações de Apoio

A TALOS Intelligence publicou um BLOG em 14 de janeiro de 2020 em resposta às Divulgações de Vulnerabilidade de Terça-Feira de Correção da Microsoft.

Atualizado em 15 de janeiro: Adicionada uma assinatura ACD para AMP que pode ser usada para detectar a exploração do CVE-2020-0601 ao falsificar certificados mascarados como uma autoridade de certificado de assinatura de código ECC da Microsoft:

<https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html>.

A assinatura do arquivo encontrado no BLOG TALOS a ser usado no ACD:

- Win.Exploit.CVE_2020_0601:1*:06072A8648CE3D020106*06072A8648CE3D020130
- <https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt>

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Portal de nuvem do Cisco Secure Endpoint

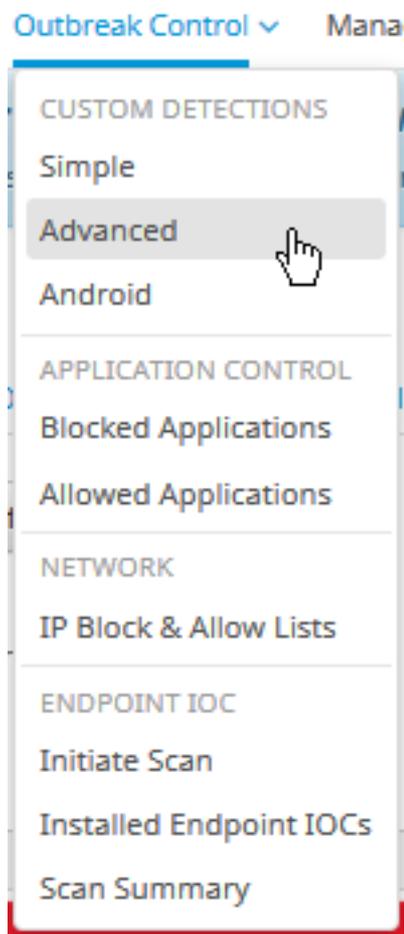
- ACD
- Blog TALOS

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados começaram com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Criar lista de detecção personalizada avançada

Agora, vamos criar o ACD para corresponder.

Etapa 1. Navegue até **Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection** (Portal de endpoint seguro > Controle de epidemia > Detecção personalizada avançada como mostrado na imagem).



Etapa 2. Comece com um nome para o conjunto de assinaturas **CVE-2020-0601** como mostrado na imagem.

Custom Detections - Advanced

Create Signature Set

Name

Save

Etapa 3. Em seguida, **edite** esse novo conjunto de assinaturas e **adicione assinatura**.
Win.Exploit.CVE_2020_0601:1*:06072A8648CE3D020106*06072A8648CE3D020130 .

Custom Detections - Advanced

[View All Changes](#)

Create Signature Set

CVE-2020-0601 Update Name

Created by Mustafa Shukur · 2020-01-22 12:19:38 CST

Used in policies:

Used in groups:

[View Changes](#) [Download](#) [Edit](#) [Delete](#)

Add Signature [Build Database From Signature Set](#)

ndb: Win.Exploit.CVE_2020_0601.UNOFFICIAL

Etapa 4. Selecione **Build Database From Signature Set** e o banco de dados foi criado.

Etapa 5. Aplique o novo Conjunto de Assinaturas a uma Política, clique em **Editar > Controle de Epidemia > Detecções Personalizadas > Avançado** como mostrado na imagem.

Modes and Engines

Exclusions
3 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Custom Detections - Simple

Custom Detections - Advanced
None
CVE-2020-0601

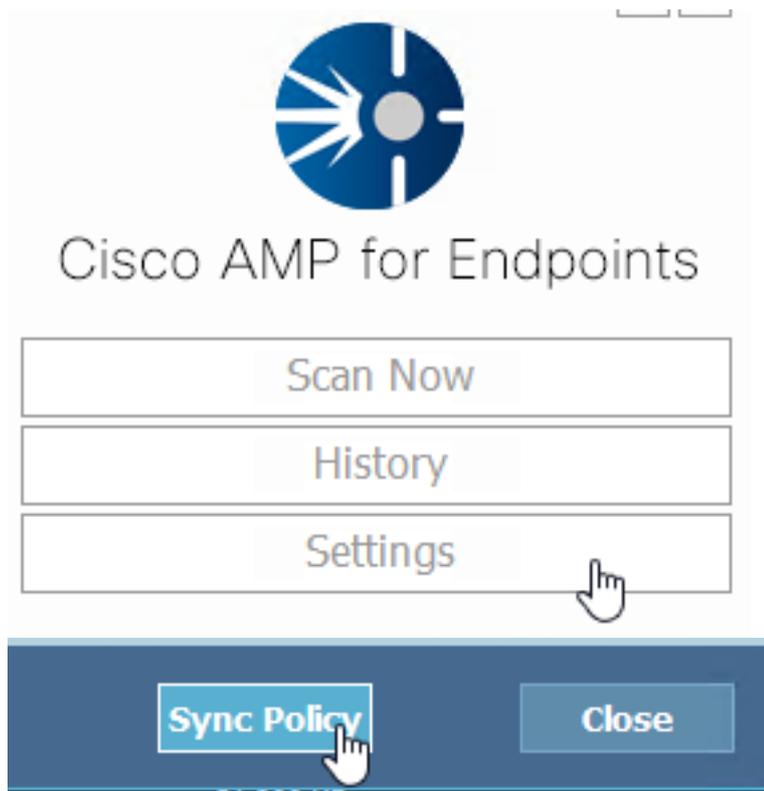
Application Control - Allowed

Application Control - Blocked

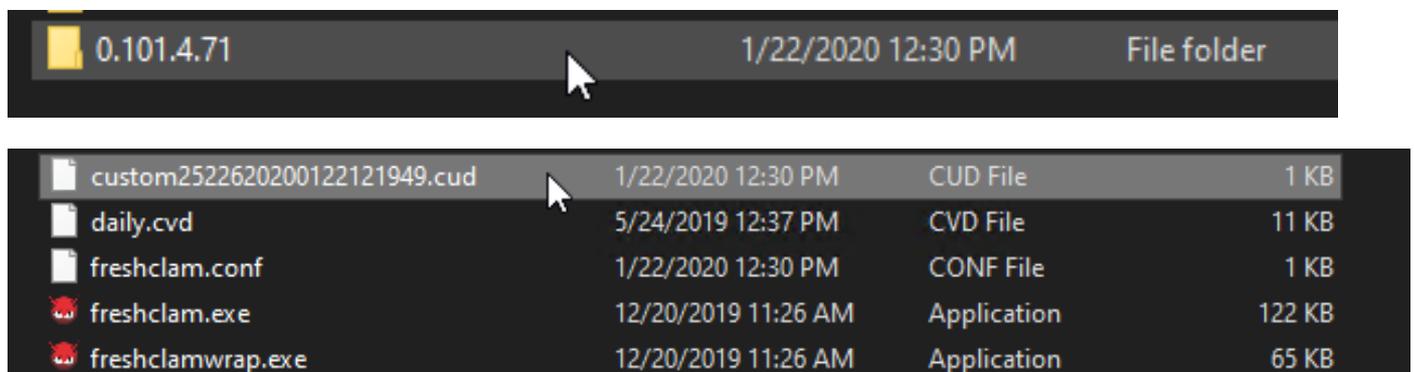
Network - IP Block & Allow Lists [Clear](#) [Select Lists](#)

[Cancel](#) [Save](#)

Etapa 6. Salve a política e a sincronização na interface do usuário do conector, conforme mostrado na imagem.



Passo 7. Procure no diretório C:\Program Files\Cisco\AMP\ClamAV uma nova pasta Signature criada nesse dia, como mostrado na imagem.



Informações Relacionadas

- A compilação usada para o teste é o Windows 10 1909, que não é afetado pela vulnerabilidade por MSKB; <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601>
- <https://support.microsoft.com/en-us/help/4534273/windows-10-update-kb4534273>
- Aplica-se a: Windows 10, versão 1809, Windows Server versão 1809, Windows Server 2019, todas as versões
- [Suporte Técnico e Documentação - Cisco Systems](#)