Een geavanceerde aangepaste detectielijst maken in Cisco Secure-endpoint

Inhoud

[Inleiding](#)
[Achtergrondinformatie](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Geavanceerde aangepaste detectielijst maken](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de stappen om een geavanceerde aangepaste detectie (ACD) te maken in Cisco Secure-endpoint.

Achtergrondinformatie

TALOS Intelligence publiceerde een BLOG op 14 januari 2020 in reactie op Microsoft Patch dinsdag kwetsbaarheidsonthullingen.

Bijgewerkt op 15 januari: Voeg een ACD-handtekening toe voor AMP die kan worden gebruikt om exploitatie van CVE-2020-0601 te detecteren door spoofing-certificaten die zich voordoen als een Microsoft ECC-code Signing certificaatautoriteit: https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html.

De handtekening van het bestand in het TALOS BLOG dat in het ACD moet worden gebruikt:

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

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Endpoint Cloud-portal

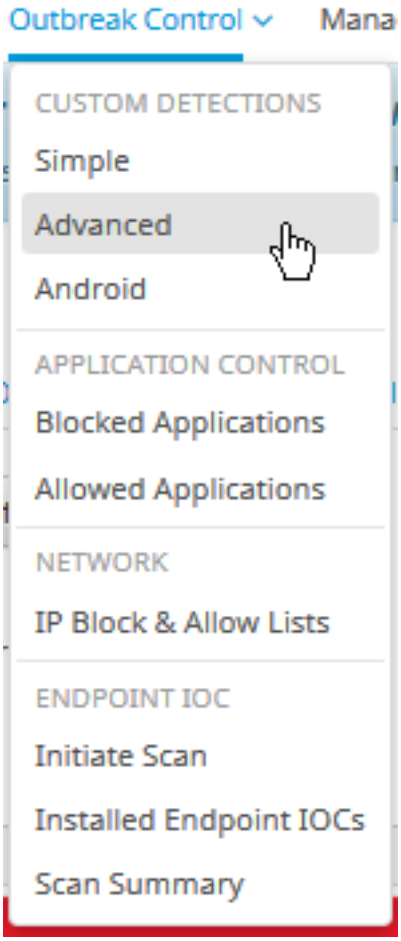
- ACD
- TALOS Blog

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die gebruikt worden begonnen met een geklaarde (standaard) configuratie. Als uw netwerk actief is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt.

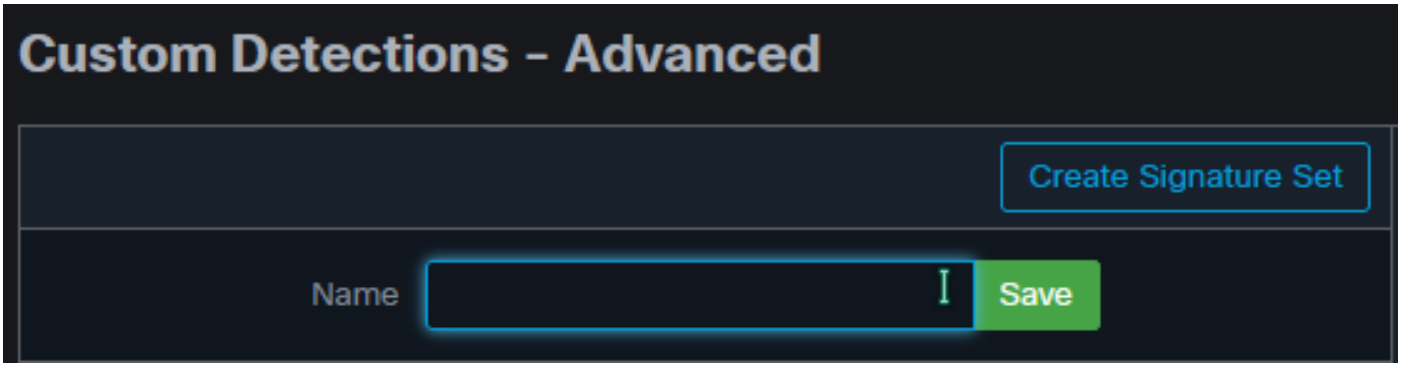
Geavanceerde aangepaste detectielijst maken

Laten we de ACD creëren om te passen.

Stap 1. Navigeer naar **Secure Endpoint Portal > Outdoorkleding > Advanced Eigen detectie** zoals in de afbeelding.

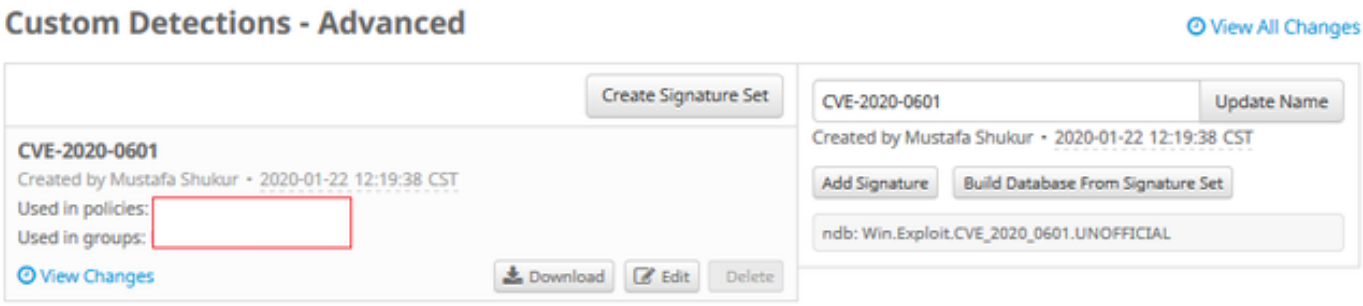


Stap 2. Begin met een naam voor de Signature-set **CVE-2020-0601** zoals in de afbeelding.



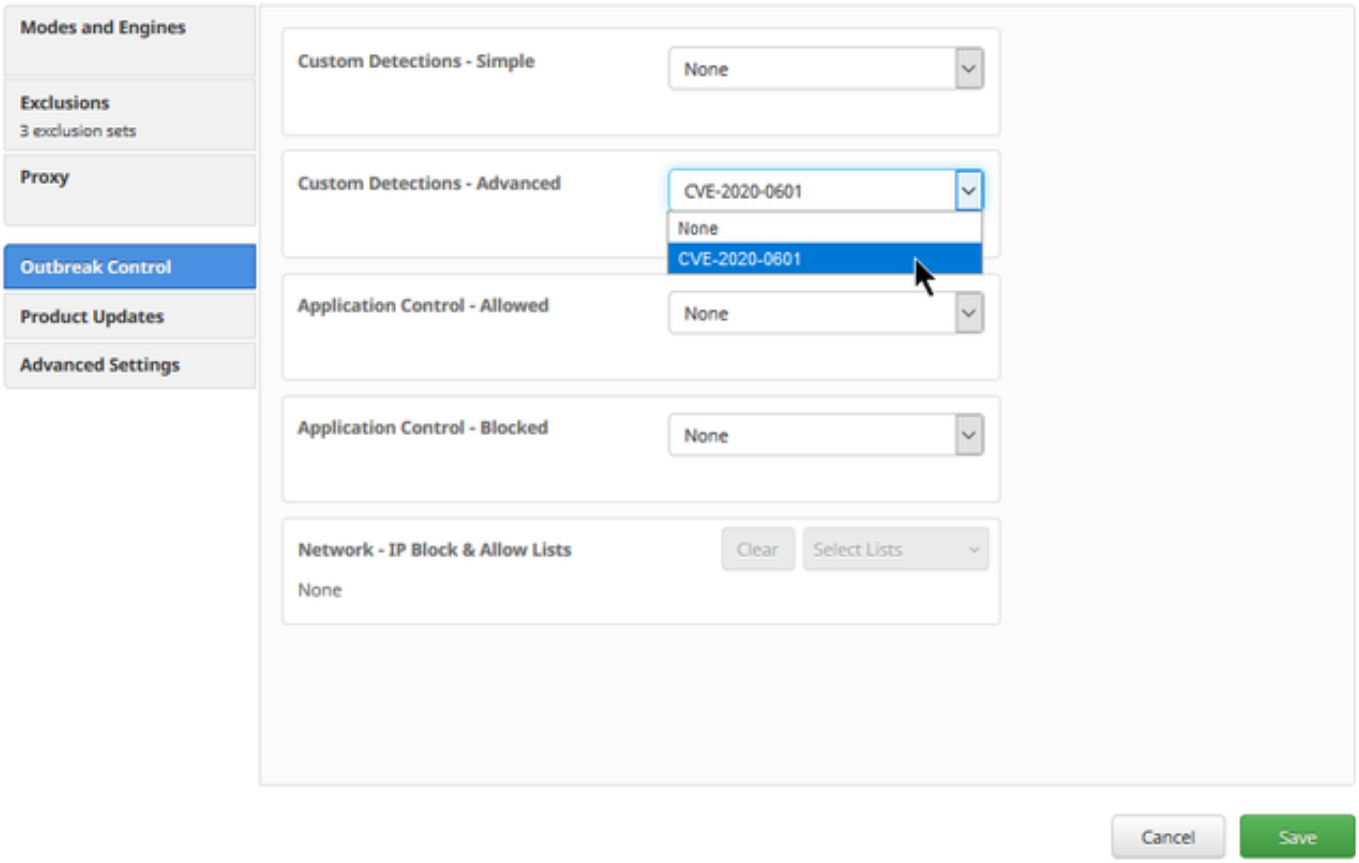
Stap 3. **Bewerk** vervolgens de nieuwe handtekeningen en **voeg deze toe**.

Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130 .

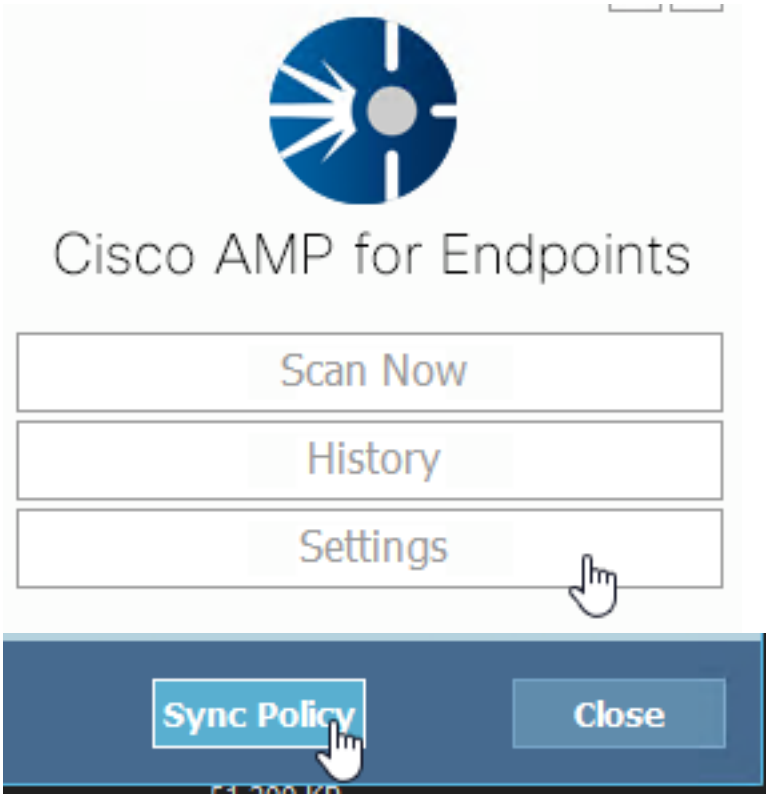


Stap 4. Selecteer **de ingebouwde database uit tekenset** en de database is opgebouwd.

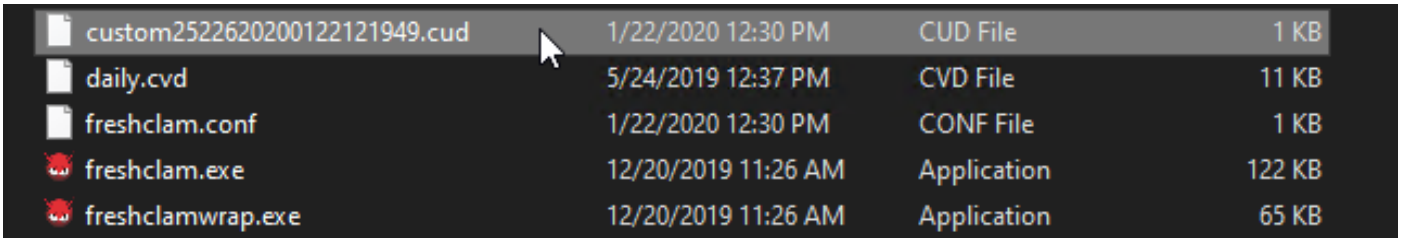
Stap 5. Wanneer u de nieuwe handleiding op een beleid toepast, klikt u op **Bewerken> Uitbraakcontrole > Aangepaste detectie >** zoals in de afbeelding.



Stap 6. Save the Policy and Sync at the connector UI zoals in de afbeelding.



Stap 7. Zoek de map **C:\Program Files\Cisco\AMP\ClamAV** voor een nieuwe map voor handtekeningen die op die dag is gemaakt zoals in de afbeelding.



Gerelateerde informatie

- Het bouwwerk dat voor de test wordt gebruikt is Windows 10 1909 dat niet beïnvloed wordt door de kwetsbaarheid per de 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
- Geldt voor: Windows 10, versie 1809, Windows Server versie 1809, Windows Server 2019, alle versies
- Technische ondersteuning en documentatie – Cisco Systems