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.

Custom Detection	ons - Advanced	
		Create Signature Set
Name	Ι	Save

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

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

Custom Detections - Advanced

	Create Signature Set	CVE-2020-0601	Update Name
CVE-2020-0601 Created by Mustafa Shukur • 2020-01-22 12:19:38 CST Used in policies: Used in groups:		Created by Mustafa Shukur + 2020-01-22 Add Signature Build Database From Si ndb: Win.Exploit.CVE_2020_0601.UNOFFI	2 12:19:38 CST gnature Set
O View Changes	🛓 Download 🖉 Edit 🛛 Delete		

O View All Changes

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.

Custom Detections - Simple None Custom Detections - Advanced None Application Control - Allowed None Network - IP Block & Allow Lists Clear Select Lists	Modes and Engines			_		
xclusions exclusion sets roxy Custom Detections - Advanced CvE-2020-0601 None Application Control - Allowed None Application Control - Blocked None Network - IP Block & Allow Lists Clear Select Lists		Custom Detections - Simple	None	\sim		
roxy utbreak Control roduct Updates dvanced Settings Application Control - Allowed None Application Control - Blocked None Network - IP Block & Allow Lists Clear Select Lists	exclusions exclusion sets					
utbreak Control roduct Updates dvanced Settings Application Control - Allowed None Application Control - Blocked None None None Select Lists	гоху	Custom Detections - Advanced	CVE-2020-0601	~		
utbreak Control roduct Updates dvanced Settings Application Control - Allowed None Application Control - Blocked None Network - IP Block & Allow Lists Clear Select Lists			None			
roduct Updates dvanced Settings Application Control - Allowed None Application Control - Blocked None Network - IP Block & Allow Lists Clear Select Lists	utbreak Control		CVE-2020-0601			
dvanced Settings Application Control - Blocked None Network - IP Block & Allow Lists Clear None	roduct Updates	Application Control - Allowed	None			
Application Control - Blocked None Network - IP Block & Allow Lists Clear None Select Lists	dvanced Settings					
Network - IP Block & Allow Lists Clear Select Lists V None		Application Control - Blocked	None	~		
Network - IP Block & Allow Lists Clear Select Lists ~ None						
None		Network - IP Block & Allow Lists	Clear Select Lists	~		
		None				
					Cancel	

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

Cisco AMP for Endpoints
Scan Now
History
Settings
Sync Policy Close

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.

🔄 0.101.4.71		1/22/2020) 12:30 PM	File folder
	~			
custom2522620200122121949.cud		1/22/2020 12:30 PM	CUD File	1 KB
📄 daily.cvd	~	5/24/2019 12:37 PM	CVD File	11 KB
📄 freshclam.conf		1/22/2020 12:30 PM	CONF File	1 KB
👼 freshclam.exe		12/20/2019 11:26 AM	Application	122 KB
👼 freshclamwrap.exe		12/20/2019 11:26 AM	Application	65 KB

Gerelateerde informatie

- Het bouwwerk dat voor de test wordt gebruikt is Windows 10 1909 dat niet beïnvloed wordt door de kwetsbaarheid per de MSKB; <u>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601</u>
- 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