Filtrer les règles de détection en fonction de la version SRU et LSP des périphériques Firepower gérés par FMC

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Procédure de filtrage des règles Snort

Introduction

Ce document décrit comment filtrer les règles de détection basées sur la version Cisco Secure Rule Update (SRU) et Link State Packet (LSP) des périphériques firepower gérés par le centre de gestion Firepower (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de l'open source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- · Cet article s'applique à toutes les plates-formes Firepower
- Cisco Firepower Threat Defense (FTD), qui exécute la version 7.0.0 du logiciel
- Firepower Management Center Virtual (FMC) qui exécute la version 7.0.0 du logiciel

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Dans le contexte des systèmes de détection des intrusions (IDS) et des systèmes de prévention des intrusions (IPS), « SID » signifie « Signature ID » ou « Snort Signature ID ».

Un SID (Snort Signature ID) est un identifiant unique attribué à chaque règle ou signature dans son ensemble de règles. Ces règles sont utilisées pour détecter des modèles ou des comportements spécifiques dans le trafic réseau qui peuvent indiquer une activité malveillante ou des menaces pour la sécurité. Chaque règle est associée à un SID pour faciliter la référence et la gestion.

Pour plus d'informations sur l'open-source Snort, veuillez visiter le site web SNORT.

Procédure de filtrage des règles Snort

Pour afficher les SID de la règle Snort 2, accédez à FMC Policies > Access Control > Intrusion, cliquez ensuite sur l'option SNORT2 dans l'angle supérieur droit, comme indiqué dans l'image :

| Intrusion Policies Network Analysis Policies | | | | | | | | | |
|---|-------------|-----------------------|----------|---------------------------------------|---------|---------|-----------|----------------|---------------|
| Show Snort 3 Sync status O Q Search by Intrusion Policy, Description, o | | scription, or Base | | All IPS Rules | IPS Map | ping 🕕 | Comp | are Policies | Create Policy |
| Intrusion Policy | Description | Base Policy | | Usage Information | | | | | |
| FTD1_Intrusion | | Balanced Security and | Connecti | No Access Control Policy No Device | | Snort 2 | 2 Version | Snort 3 Versio | on 🖊 🗄 🖆 🗑 |

Snort 2

Naviguez jusqu'à Rules > Rule Update et sélectionnez la dernière date pour filtrer le SID.

| Policy Information Rules Cisco Recommendations | Rules Rule Configuration Rule Content | Filter: | | |
|---|---|-------------------------------|---|--|
| > Advanced Settings | Category | SRU:"Snort | Rule Upda | te 2023 04 11 001 vrt" |
| > Policy Layers | Classifications Microsoft Vulnerabilities Microsoft Worms | 0 selected ru Rule State ▼ | les of 2961 Event Fi | Itering ▼ Dynamic State ▼ Alerting ▼ Comments ▼ |
| Platform Specific Preprocessors Priority Rule Update | GID | SID | Message 🔿 | |
| | 1 | 60221 | BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt | |
| | Snort Rule Update 2021 05 03 001 vrt | 1 | 60220 | BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt |
| Short Rule Update 2 06 001 vrt Short Rule Update 2 11 001 vrt Changed | 06 001 vrt Snort Rule Update 2023 04 | 1 | 60648 | BROWSER-CHROME Chrome IPC memory dump attempt |
| | 11 001 vrt Changed | 1 | 60647 | BROWSER-CHROME Chrome IPC memory dump attempt |
| 2 37 3 | New ▶ Isp rel 20210503 2107 | 1 | 60945 | BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt |

Mise à jour des règles

| Rules | | | | | < Back |
|---------------------------|--|---------------|-----|------|--------|
| Rule Configuration | Filter | | | | |
| Rule Content | Filter: | | | | |
| Category | SRU:"Snort Rule Update 2023 04 11 001 vrt" | | | | × 0 |
| Classifications | 0 selected rules of 16 | | | | |
| Microsoft Vulnerabilities | | | | | |
| Microsoft Worms | Policy | | | | |
| Platform Specific | Rule State Event Filtering Dynamic State Alerting Comments | | | | |
| Preprocessors | | | | | |
| Priority | GID SID Message ↑ | -> | • • | 0 | , 💻 |
| Rule Update | UIUIZ readme file detected | ~ | | | |
| 04 10 001 vrt | | | | | î |
| Snort Rule Update 2023 | 1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation | \rightarrow | | | - |
| | | < < | 1 | of 1 | > > |

Disponible Sid's sous les règles de snort

Sélectionnez une option requise sous Rule State comme illustré dans l'image.

| Rules | | | | | | | < Back |
|------------------------------------|-----------------------|----------------|---|---------------|-----|------|--------|
| Rule Configuration Rule Content | Filter: | | | | | | |
| Category | SRU:"Snort R | ule Update 20 | 023 04 11 001 vrt" | | | | × 0 |
| Classifications | 16 selected rule | es of 16 | | | | | |
| Microsoft Vulnerabilities | D | | | | | | |
| Microsoft Worms | Policy | | ¥ | | | | |
| Platform Specific | Rule State 🔻 | Event Filterir | ng Dynamic State Alerting Comments | | | | |
| Preprocessors | Generate Eve | nte | | | | | |
| Priority | Generate Eve | 1115 | sage ↑ | \rightarrow | • • | 0 | - |
| Rule Update | Drop and Ger | nerate Events | tme file detected | ~ | | | |
| 04 10 001 vrt | 04 10 001 vrt Disable | | MINDOWO Nicesset Windows AED are adultant acceletion | | | | î |
| Snort Rule Update 2023 | | | -WINDOWS MICrosoft Windows AFD.sys privilege escalation | \rightarrow | | | Ψ. |
| | | | | < < | 1 | of 1 | > > |

Sélection des états de règle

Pour afficher les SID de la règle Snort 3, accédez à FMC Policies > Access Control > Intrusion , puis cliquez sur l'option SNORT3 dans l'angle supérieur droit, comme indiqué dans l'image :

| Intrusion Policies Network Analysis Policies | | | | | | | |
|--|-------------|--------------------------------|---------------------------------------|--------------------|--------------------------|--|--|
| Show Snort 3 Sync status Show Snort 3 Sync status | | escription, or Base | All IPS Rules | IPS Mapping Compa | re Policies Create Polic | | |
| Intrusion Policy | Description | Base Policy | Usage Information | | | | |
| FTD1_Intrusion | | Balanced Security and Connecti | No Access Control Policy No Device | Snort 2 Version | Snort 3 Version 🖍 🛱 🖆 | | |

Snort 3

Naviguez jusqu'à Advanced Filters et sélectionnez la date la plus récente pour filtrer le SID comme indiqué dans l'image.

| < Intrusion Policy Policy Name FTD1_Intrusion | | V | Used by: No Access Control Policy No Device | | | | | |
|---|--|--|---|--|--|--|--|--|
| Mode Prevention Image: Base Policy Balanced Security and Connectivity Disabled 39249 Alert 470 Block 9151 Overridden 0 Pass 0 Drop 0 Reject 0 | | | | | | | | |
| Rule Groups | | | Back To Top | | | | | |
| 50 items + Search Rule Group Excluded Included | All Rules All rules assigned to current intrusion po | licy irrespective of rule group | | | | | | |
| Overridden | Rule Action V Q. Search by CVE, SID, Reference Info, or Rule Message | | | | | | | |
| All Rules Reco | 48,870 rules Pres | et 470 Alert rules 9,151 Block rules 39,249 S: Advanced Filters | Disabled rules 0 Overridden rules | | | | | |
| > Browser (6 groups) | GID:SID Info | Rule Action 1 | Assigned Groups | | | | | |
| > Server (8 groups) | > 1:28496 🖸 BROWSER-IE Mic | rosoft Internet Explore 🔺 Alert (Default) 🗸 | Browser/Internet Explo 🖷 💻 🖡 | | | | | |

Filtres Snort 3

r

Advanced Filters

| LSP | Select | ~ |
|------------------------------|-----------------------------|--------|
| | Show Only * 🗹 New 🗹 Changed | |
| Classifications | Select | \sim |
| Microsoft Vulnerabilities | Select | ~ |
| | Cancel | OK |

a

LSP sous filtre avancé

| Advanced Fi | lters | 0 |
|-------------------------------|--|----------------|
| LSP | Isp rel 20230420 1056 | ~ |
| | Show Only * 🗹 New 🗹 Changed | |
| Classifications | Select | \sim |
| Microsoft Vulnerabilities | Select | ~ |
| | Cancel | ٢ |
| sion LSP | | |
| All Rules | | |
| Rule Action | Isp:lsp rel 20230420 1056 × | |
| 2 🝸 48,870 rules | Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Adv Rule Action 1 Assigned Groups | vanced Filters |
| 1:300509 Г 1 MALWARE-I | BACKDOOR Win.Backdoor Block (Default) | 唱 🗭 |

Filtre prédéfini pour les Sid

Sélectionnez une option requise sous Rule state comme illustré dans l'image.

| | All Rules All rules assigned | to current intrusion policy irrespective | of rule group | | | |
|---|---------------------------------|--|--------------------------|------------------|---|---|
| | Rule Action | Isp:lsp rel 20230420 | 1056 X | | × | |
| | ZZ ₩ ZZ ↑ 4d | Info | Rule Action | Assigned Groups | | |
| | > 🖌 1:30050 | 9 | loor 😑 Block (Default) 🗸 | Malware/Backdoor | í | |
| ŀ | _ | | | | | ÷ |

Action Règle

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.