



The bridge to possible

Mardi 5 Octobre 2021

Inscrivez-vous ici <https://bit.ly/WEBsp-oct21>



FMC, ISE et ELK

Comment réagir en fonction de certains événements ?

Community Live - Sécurité



# Configuration

## eStreamer Event Configuration

Select the types of events that will be sent to connected eStreamer clients

- Discovery Events
- Correlation and Allow List Events
- Impact Flag Alerts
- Intrusion Events
- Intrusion Event Packet Data
- User Activity
- Intrusion Event Extra Data
- Malware Events
- File Events
- Connection Events

**Save**

Hostname

10.100.99.30

**Client qui reçoit les évènements**

**Évènements à souscrire**

# eNcore – Cisco FMC

- eNcore est l'outil permettant de collecter les événements au travers de eStreamer
- Téléchargeable sur le site de Cisco
- Version disponible pour Splunk et pour les « autres » systèmes

[Downloads Home](#) / [Security](#) / [Firewalls](#) / [Firewall Management](#) / [Firepower Management Center Virtual Appliance](#) / Firepower System Tools and APIs- eNcore for CEF

The screenshot shows the Cisco FMC download page for eNcore for CEF. On the left, there is a search bar and a navigation menu with categories like 'All Release', 'User Agent', 'Threat Containment', and 'Remediation'. The 'eNcore for CEF' category is highlighted. The main content area displays the title 'Firepower Management Center Virtual Appliance' and the release 'Release eNcore for CEF'. Below this, there is a table of file information with columns for 'File Information', 'Release Date', and 'Size'.

File Information	Release Date	Size
eStreamer client for Firepower 6.X and CEF	02-Apr-2019	0.11 MB
eStreamer-eNcore-Splunk-3662-TA-3.5.4-Cisco-License.spl <a href="#">Advisories</a>		
eStreamer-eNcore-Splunk-3662-TA-3.5.4-Cisco-License	02-Apr-2019	0.09 MB
eStreamer-eNcore-cli-3.5.4.tar.gz <a href="#">Advisories</a>		

# Exemple de règles Elastalert

```
name: Alert on custom detection
type: frequency
index: logstash-*
num_events: 1
timeframe:
  minutes: 2
filter:
- query:
  query_string:
    query: 'initiatorIpAddress : "10.100.1.252" AND @computed.firewallRuleAction : "Block" AND @computed.firewallRuleReason : "File Resume Block"'
alert_subject: "Test ELK Alert Malware"
alert:
- "email"
- "command"
email:
- "fmo@supportlan.com"
smtp_host: "smtp.gmail.com"
smtp_port: 465
smtp_ssl : true
from_addr: "testise2018@gmail.com"
smtp_auth_file: "/home/francesco/build/elastalert2/smtp_auth_file.yml"
command: ["/home/francesco/build/elastalert2/webex_test_v2.sh", "%(initiatorIpAddress)s", "%(responderIpAddress)s", "%(clientId.data)s"]
```

## Plusieurs méthodes de filtrage:

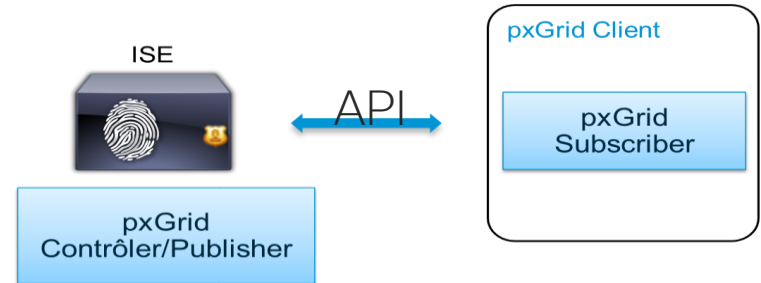
[https://elastalert2.readthedocs.io/en/latest/recipes/writing\\_filters.html#common-filter-types](https://elastalert2.readthedocs.io/en/latest/recipes/writing_filters.html#common-filter-types)

```
name: Alert on custom detection
type: frequency
index: logstash-*
num_events: 4
timeframe:
  minutes: 15
filter:
- bool:
  must:
  - terms:
    initiatorIpAddress: ["10.100.99.27"]
  - terms:
    responderIpAddress: ["10.100.1.252"]
alert_subject: "Test ELK Alert"
alert:
- "email"
- "command"
email:
- "fmo@supportlan.com"
smtp_host: "smtp.gmail.com"
smtp_port: 465
smtp_ssl : true
from_addr: "testise2018@gmail.com"
smtp_auth_file: "/home/francesco/build/elastalert2/smtp_auth_file.yml"
command: ["/home/francesco/build/elastalert2/webex_test.sh", "%(initiatorIpAddress)s"]
```

# Cisco pxGrid

Cisco pxGrid est rôle du serveur ISE qui permet d'échanger avec des équipements de l'écosystème Cisco et tierces parties certaines informations appelées « Network Context »:

- Qui est connecté au réseau
- Comment il est connecté au réseau
- Avec quel équipement?
- ...



Le pxGrid partage l'information Cisco ISE schématisée par « What, When, Who, Where, How ».

pxGrid est aussi utilisé pour indiquer à ISE de mettre un utilisateur en quarantaine.

# Aperçu des démos

## Démo 1: (Avec Cisco ISE pxGrid)

En fonction d'un événement de trafic, nous allons:

- Envoyer un courriel avec le log qui a déclenché l'alerte
- Poster un message dans une Webex room
- Lancer une commande pour changer le SGT d'un host dont le trafic sera bloqué par la FMC (règle basée sur les attributs SGT).

## Démo 2: (Sans Cisco ISE pxGrid)

En fonction d'un événement de trafic, nous allons:

- Envoyer un courriel avec le log qui a déclenché l'alerte
- Poster un message dans une Webex room
- Lancer une commande pour ajouter le host dans un groupe dynamique de la FMC dont le trafic sera bloqué par la FMC (règle basée sur ce groupe dynamique).

# Plus d'informations dans la Communauté Cisco



Rappelez-vous que ce n'est qu'un aperçu. Le mardi 5 Oct. vous aurez l'occasion de voir l'intégralité de cette présentation.

## Chasse au Trésor : 50 bons de réduction pour Cisco Press

Jusqu'au vendredi 8 Oct. Participez aussi à un tirage au sort pour gagner un clavier Logitech® K480 Bluetooth Multi-Device! | [Savoir plus](#)

## Vous préparez une Certification Cisco ?

Ce mois nous avons prévu une petite séance sur les Certifications Cisco. Joignez-nous pour découvrir les conseils de nos experts ! | [Consulter ici](#)

Dans ce webinaire vous aurez l'occasion d'apprendre beaucoup plus et vous pourrez également poser des questions aux experts qui vous répondront en direct.

À très bientôt !

Inscrivez-vous dès maintenant : <https://bit.ly/WEBsp-oct21>