Integración de AMP para terminales con Splunk

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Troubleshoot

Introducción

Este documento describe el proceso de integración entre la protección frente a malware avanzado (AMP) y Splunk.

Contribuido por Uriel Islas y Juventino Macias, editado por Jorge Navarrete, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de:

- AMP para terminales
- Interfaz de programación de aplicaciones (API)
- Splunk
- Usuario administrador en Splunk

Componentes Utilizados

- Nube pública AMP
- instancia de Splunk

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. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Paso 1. Navegue hasta la consola de AMP (<u>https://console.amp.cisco.com</u>) y navegue hasta **Cuentas>Credenciales de API**, donde puede crear secuencias de eventos.

API Credentials	View API Documentation
Collers	+ New API Credential

Paso 2. Para realizar esta integración, marque la casilla **Read & Write** como se muestra a continuación:

New	API Credential			
	Application name	caisias-amp		
	Scope Ena Alk	Read-only Read & Write Bole Command line ww API access to File Repository download audit logs		
۰	An API credential with read and write scope can make changes to your AMP for Endpoints configuration that may cause significant problems with your endpoints. Some of the input protections built into the AMP Console do not apply to the API			
		Cancel Create		

Nota: Si desea recopilar más información sobre los eventos, active la casilla **Enable Command Line**, para obtener los registros de auditoría generados desde el repositorio de archivos marque la casilla **Allow API access to File Repository**.

Paso 3. Una vez creada la secuencia de eventos, se mostrarán la ID de cliente API y la clave de API que se requieren en Splunk.

< API K	Cey Details
3rd Pa	arty API Client ID
	e36cl2c390. I
API K	ry
	23dd1317-masf-42
API cred and pase	entials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a use word, and should be treated as such.
Delete th	e API credentials for an application if you suspect they have been compromised and create new ones.
Deleting	API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.
Your API	credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.
VIEW AP	Decumentation

Precaución: Esta información no se puede recuperar por ningún medio, en caso de pérdida, se debe crear una nueva clave de API.

Paso 4. Para integrar Splunk con AMP para terminales, asegúrese de que la cuenta Admin exista en Splunk.

Usemanie	Password	Sign In	
-O admin From this website			
*O mex-amp From this website	jed out. Log in to return	red out. Log in to return to the system.	
View Saved Logins			

Paso 5. Una vez que inicie sesión en Splunk, continúe descargando AMP de las aplicaciones Splunk.



Paso 6. Busque el terminal de Cisco en el navegador de aplicaciones e instálelo (entrada de eventos de Cisco AMP para terminales).

splunk> _{Apps} ~	Administrator V Messages V Settings V Activity V Help V Find
Browse More Apps	
cisco endpoint 🕲	Best Match Newest Popular 7 Apps
CATEGORY DevOps Security, Fraud & Compliance IT Operations Utilities Business Analytics IoT & Industrial Data	the clisco AMP for Endpoints CIM Add-On Install The Clisco AMP for Endpoints CIM Add-on provides a mechanism to map data from the Clisco AMP for Endpoints Event Input App for CIM compliant applications. The add-on also provides additional workflow actions so security analysts can go straight from Splunk Events to the Clisco AMP for Endpoints console.
CIM VERSION 4.x 3.x	Category: Security, Fraud & Compliance Author: Samson Nguyen Downloads: 996 Released: 2 years ago Last Updated: a year ago View on Splunkbase
SUPPORT TYPE	title Cisco AMP for Endpoints Events Input
Developer Splunk Not Supported	The Cisco AMP for Endpoints Events Input provides a mechanism to create, update, and delete event streams in Cisco Advanced Malware Protection (AMP) for Endpoints via the API and index them in your Splunk® instance to make them searchable. All you need to do is provide your API host and credentials from your AMP for Endpoints account and specify the stream parameters. This app has been tested on Splunk v6.6.0 Less
Inputs	

Paso 7. Se requiere un reinicio de la sesión para completar la instalación en Splunk.



Paso 8. Una vez que inicie sesión en Splunk, haga clic en **Cisco AMP para terminales** en el lado izquierdo de la pantalla.



Paso 9. Haga clic en la etiqueta Configuration en la parte superior de la pantalla.

splunk	enterprise	App: Clsco AMP for Endpoints Events Input *
Inputs	New Input	Configuration
Input	s	
Crea	te a New Input	
Retriev	ing inputs	

Paso 10. Escriba las credenciales de la API generadas anteriormente desde la consola de AMP.

splunk	>enterprise	App: Cisco AMP for Endpoints Events Input *
Inputs	New Input	Configuration
Conf	iguration	
Global c	onfiguration for	Cisco AMP for Endpoints events input
AMP fo	or Endpoints Al	PLAccess Configuration
AMP to	or Endpoints API	Host '
opcor	np.cisco.com	
API CI	e address of the Ci	sco wher for Endpoints API Server that the application will access for managing event streams. Please in
Enter th	o 3rd Porty API Cilo	ant ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope
API Ke	y	
Enter th	e secret API key	
Saw	Configuration	

Nota: El punto de host de la API puede ser diferente según el Data Center en la nube que su organización señale en:

América del Norte: api.amp.cisco.com Europa: api.eu.amp.cisco.com Asia Pacífico, Japón y China: api.apjc.amp.cisco.com Paso 11. Incluya y guarde las credenciales de la API en la consola de Splunk para vincularlas con AMP.

splunk	>enterprise	App: Cisco AMP for Endpoints Events Input *
Inputs	New Input	Configuration
Conf	iguration	
Global c	onfiguration for	Cisco AMP for Endpoints events input
0 00	onfiguration succ	sessfully saved
AMP f	or Endpoints Al	PI Access Configuration
AMP to	or Endpoints API	Host *
apilar	mp.cisco.com	
Enter th	e address of the C	sco AMP for Endpoints API Server that the application will access for managing event streams. Please refer to the AMP for Endpoints API documentation for the correct hostname
API CI	ent ID 1	
e36c	12c3905be05ca	cb7
Enter th	e 3rd Party API CH	nt ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope
API Ke	y *	
a68f	433e-base-f620	041ch63#b
Enter th	é secrit API key	
Sove	Configuration	

Paso 12. Vuelva a **Input** para crear la secuencia de eventos.

lew Input	
Name *	
caislas	
Index	
main	>
In which index would you like the events to appear?	
to the second	
Stream Settings	
Stream Settings Stream Name *	
Stream Settings Stream Name * coislas	
Stream Settings Stream Name * coislas Event Types	
Stream Settings Stream Name * coislas Event Types	
Stream Settings Stream Name * coislas Event Types Groups	
Stream Settings Stream Name * caislas Event Types Groups Leave this field blank to return all Groups	

Nota: Si desea obtener de AMP todos los eventos de todos los grupos, deje en blanco los campos **Tipos de eventos** y **Grupos**.

Paso 13. Asegúrese de que la entrada se ha creado correctamente.

nputs	
Create a New Input	
Name	Index
caislas	main

Nota: Tenga en cuenta que esta integración no está oficialmente respaldada

Troubleshoot

Si al crear una secuencia de eventos se atenuan todos los campos, esto podría deberse a algunos de los motivos siguientes:

Inputs	New Input	Configuration	
New	Input		
Name			
		0	
Index			
In which	index would you i	ke the events to appear?	
Stream	Settings		
Stream	Name *		
Event 1	ypes		
Leave	this field blank	to return at Event types	÷
Groups			
Leave	this field blank	to return all Groups	s >
Save			

- 1. Inconvenientes de conectividad: Asegúrese de que la instancia de Splunk pueda ponerse en contacto con el host de la API
- 2. Host de API: Asegúrese de que el host de la API configurado en el paso 10 coincide con su organización de AMP, según el punto en el que se encuentre su empresa.
- 3. Credenciales de API: Asegúrese de que la clave API y la ID de cliente coinciden con los configurados en el paso 3.
- 4. Flujos de eventos: Asegúrese de tener menos de 4 secuencias de eventos configuradas.