



POLICIA FEDERAL ARGENTINA

Procedimiento FortiSandbox

**Superintendencia FEDERAL DE TECNOLOGÍAS DE
LA INFORMACIÓN Y COMUNICACIONES**



Instalación FortiSandbox

EDICIÓN 1
Tipo de Documento: IMPLEMENTACIÓN
Versión: 1.0 / 2023
Página 2 de 10

Tabla de contenido

SÍNTESIS	3
CARACTERÍSTICAS TÉCNICAS.....	3
DASHBOARD	4
VM JOBS	5
FILE ON-DEMAND.....	5
URL ON-DEMAND	6
VM SETTINGS.....	8
OPERATION CENTER.....	9
REVISIONES Y MODIFICACIONES:.....	10



Instalación FortiSandbox

EDICIÓN 1

Tipo de Documento:
IMPLEMENTACIÓN

Versión: 1.0 / 2023

Página 3 de 10

Fortinet FortiSandbox 1000F

Consolidated Security for Virtual Environments

FORTINET
PLATINUM PARTNER



Síntesis

FortiSandbox es una solución de seguridad que esgrime una tecnología de aprendizaje automático para identificar y aislar amenazas avanzadas en tiempo real. Inspecciona el tráfico de la red, los archivos y las URL en busca de actividad maliciosa, incluidas las amenazas de día cero, y utiliza tecnología de espacio aislado (virtualizado) para analizar archivos sospechosos de forma segura.

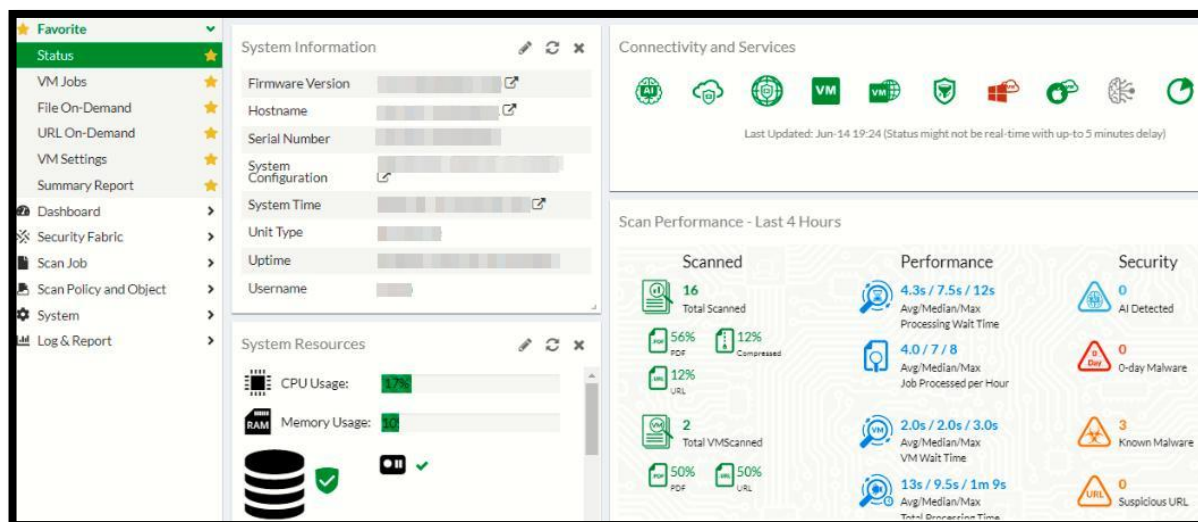
La solución es compatible con varios sistemas operativos y tipos de archivos, y proporciona funciones de generación de informes para identificar y responder rápidamente a las amenazas.

Características técnicas

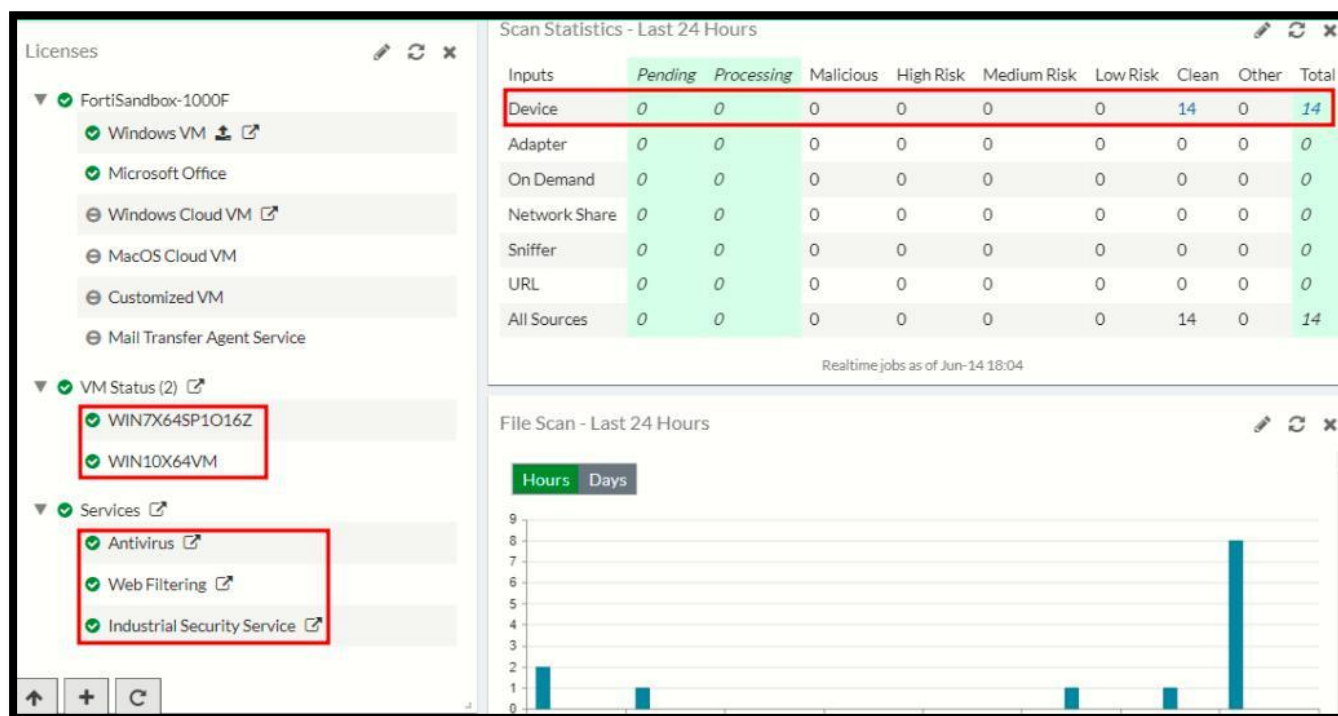
Rendimiento de sistema		Modelo / Producto
Número de máquinas virtuales	14	FortiSandbox 1000F
Análisis Estático Basado en IA	Si	
Tiempo de Análisis Dinámico	1 a 3 minutos	
Sistema de Detección Anti-Evasión	Si	
Sistema de Detección Comand & Control	Si	
Filtros Web, AV, IPS	Si	
Rendimiento efectivo (archivos/h)	1400	
Rendimiento Análisis Estático (archivos/h)	10.000	
Rendimiento Análisis Dinámico (archivos/h)	500	
Rendimiento FortiMail (emails/h)	14.000	
Máquinas Virtuales por defecto	2	
Máquinas Virtuales totales posibles de desplegar	+ 12	
Sistema Operativo Soportado	Windows	
Sistema Operativo Soportado	Linux	
Sistema Operativo Soportado	Android	
Sistema Operativo Soportado	Personalizado	
Sistema Operativo Soportado (limitado)	macOS	

Dashboard

Muestra un resumen del estado general del sistema, como el estado de funcionamiento, la disponibilidad de recursos, la capacidad de almacenamiento y servicios utilizados.



Asimismo, proporciona una visión general de las amenazas analizadas, incluyendo la cantidad de archivos analizados y las estadísticas de detección de malware. Esto puede incluir información sobre el tipo de amenazas, como virus, troyanos, ransomware, etc.



A continuación, se detalla el método “manual” de utilización de la herramienta nombrada de forma simple.

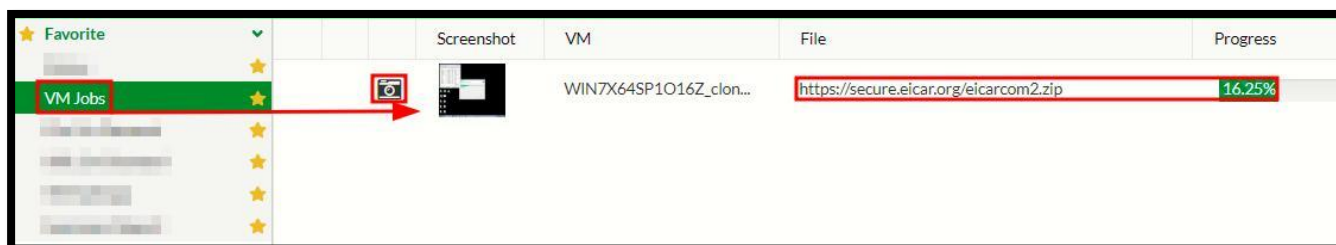


Instalación FortiSandbox

EDICIÓN 1
Tipo de Documento: IMPLEMENTACIÓN
Versión: 1.0 / 2023
Página 5 de 10

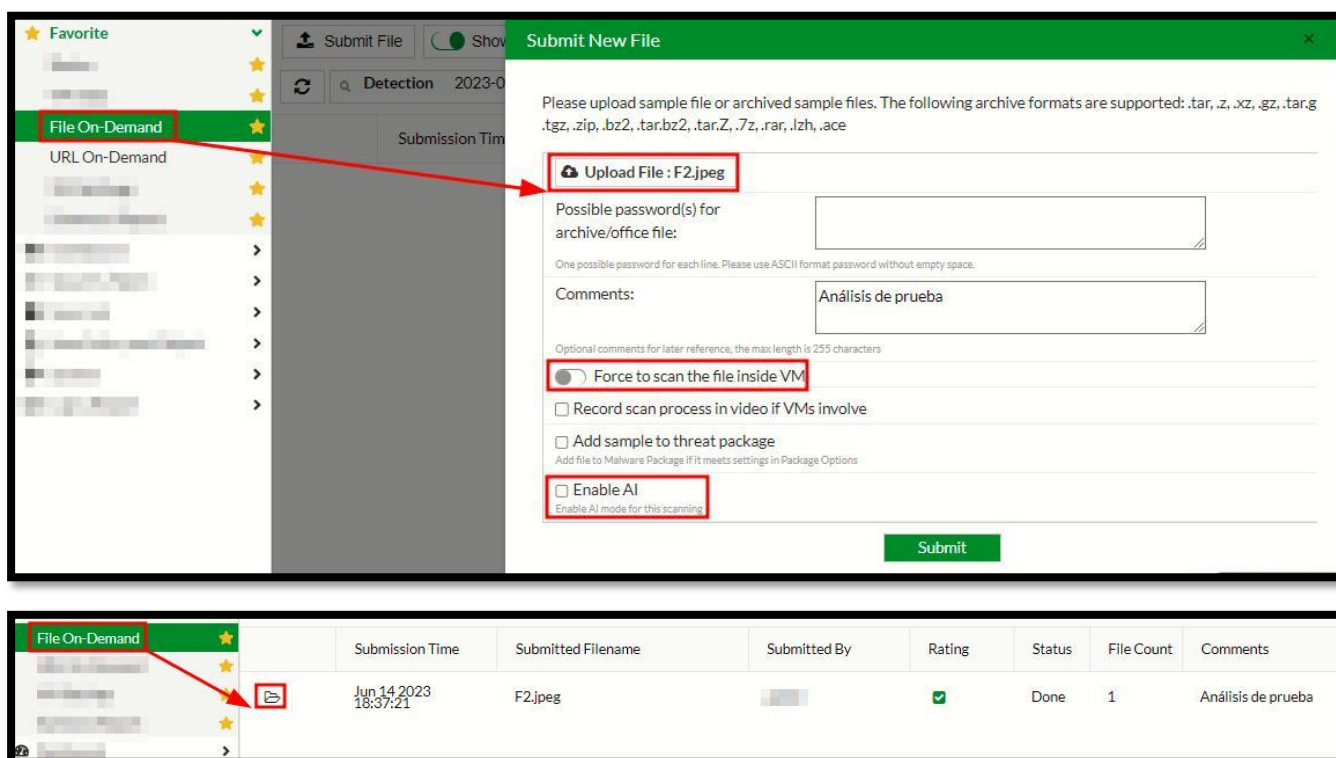
VM Jobs

Se puede obtener información sobre el estado actual del VM Job, como si está en cola de ejecución, en progreso, completado o fallido. Esto permite realizar un seguimiento de las tareas en ejecución y su estado.



File On-Demand

Se puede indicar a la herramienta que archivo específico analizar, esto puede incluir el veredicto del análisis, que indica si el archivo es limpio, sospechoso o malicioso. Además, se puede obtener información detallada sobre las características y comportamiento del archivo analizado.



Una vez finalizado el análisis, FortiSandbox nos permitirá visualizar detalles específicos del archivo analizado, como su nombre, tamaño, fecha de envío y hash. Estos detalles ayudan a identificar y distinguir el archivo en cuestión.



Instalación FortiSandbox

EDICIÓN 1

Tipo de Documento:
IMPLEMENTACIÓN

Versión: 1.0 / 2023

Página 6 de 10

Clean File csv		Overview	Tree View
Basic Information		Details Information	
Job ID:	6644624392907112598	Filename:	audit_01-06-2023_to_14-06-2023_5941367670704199176.csv
Status:	Done	Downloaded From:	audit_01-06-2023_to_14-06-2023_5941367670704199176.csv
Received:	2023-06-14 18:40:42	Scan Start Time:	2023-06-14 18:40:44
Started:	2023-06-14 18:40:44	Scan End Time:	2023-06-14 18:40:46
Rated By:	Static Scan Engine	Total Scan Time:	2 seconds
Submit Type:	On-Demand	File Type:	csv
Digital Signature:	No	File Size:	35701 (bytes)
AI Mode:	ON	Embedded URL:	0
SIMNET:	OFF	MD5:	d48b0f7fe228ff54721d011a3a0aa53d
Timeout Value:	60 seconds	SHA1:	e15e5a1588af655610318de74687e86f3ab3238a
Virus Total:		SHA256:	158f12d269977dd781f6a44b7260dd13ebe765e9898b36ef425b8f80afc44ef4

URL On-Demand

El análisis de URL proporciona el veredicto del análisis, que indica si la URL es segura, sospechosa o maliciosa, también obtener información detallada sobre el contenido y comportamiento de la URL analizada.

Favorite

<

Además, puede incluir información sobre el dominio de la URL, su confiabilidad o reputación conocida, y si se han encontrado registros de esta URL en otras fuentes de inteligencia de seguridad.

Favorite		<	↺	🔍		
Action	Detection	URL		Rating ↑	Submitted Filename	
	Jun 14 2023 18:53:06	https://secure.eicar.org/eicarcom2.zip		Clean	scan_of_secure.eicar.org	
	Jun 14 2023 18:52:02	https://secure.eicar.org/eicarcom2.zip		Malicious	scan_of_secure.eicar.org	
	Jun 14 2023 18:52:02	https://secure.eicar.org/eicarcom2.zip/eicar_com.zip		Malicious	scan_of_secure.eicar.org	
	Jun 14 2023 18:52:02	https://secure.eicar.org/eicarcom2.zip/eicar_com.zip/...		Malicious	scan_of_secure.eicar.org	

Si la URL enviada muestra un comportamiento sospechoso o malicioso durante el análisis, FortiSandbox puede registrar y mostrar información sobre las actividades realizadas por la URL. Esto puede incluir la descarga de archivos, la comunicación con dominios maliciosos, la presencia de contenido no seguro o cualquier otro comportamiento detectado.



Instalación FortiSandbox

EDICIÓN 1

Tipo de Documento:
IMPLEMENTACIÓN

Versión: 1.0 / 2023

Página 7 de 10

Malware EICAR_TEST_FILE (clean WEblink Payload) Overview

Basic Information		Details Information	
Job ID:	6644636027480961054	URL:	https://secure.eicar.org/eicarcom2.zip/eicar_com.zip
Status:	Done	Scan Start Time:	2023-06-14 18:52:01
Received:	2023-06-14 18:51:57	Scan End Time:	2023-06-14 18:52:02
Started:	2023-06-14 18:52:01	Total Scan Time:	1 second
Rated By:	AV Scan Engine	File Type:	zip
Submit Type:	On-Demand	Embedded URL:	0
AI Mode:	ON	MD5:	6ce6f415d8475545be5ba114f208b0ff
SIMNET:	OFF	SHA1:	d27265074c9eac2e2122ed69294dbc4d7cce9141
Depth:	0	SHA256:	2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad
Timeout Value:	60 seconds	Submitted By:	
Virus Total:		Submitted Filename:	scan_of_secure.eicar.org
URL and Payloads	eicar_com.zip	Scan Unit:	FSA1KFT622000091

3 / 93

3 security vendors flagged this URL as malicious

https://secure.eicar.org/eicarcom2.zip/eicar_com.zip
secure.eicar.org
[text/html; charset=UTF-8](#)



Instalación FortiSandbox

EDICIÓN 1

Tipo de Documento:
IMPLEMENTACIÓN

Versión: 1.0 / 2023

Página 8 de 10

VM Settings

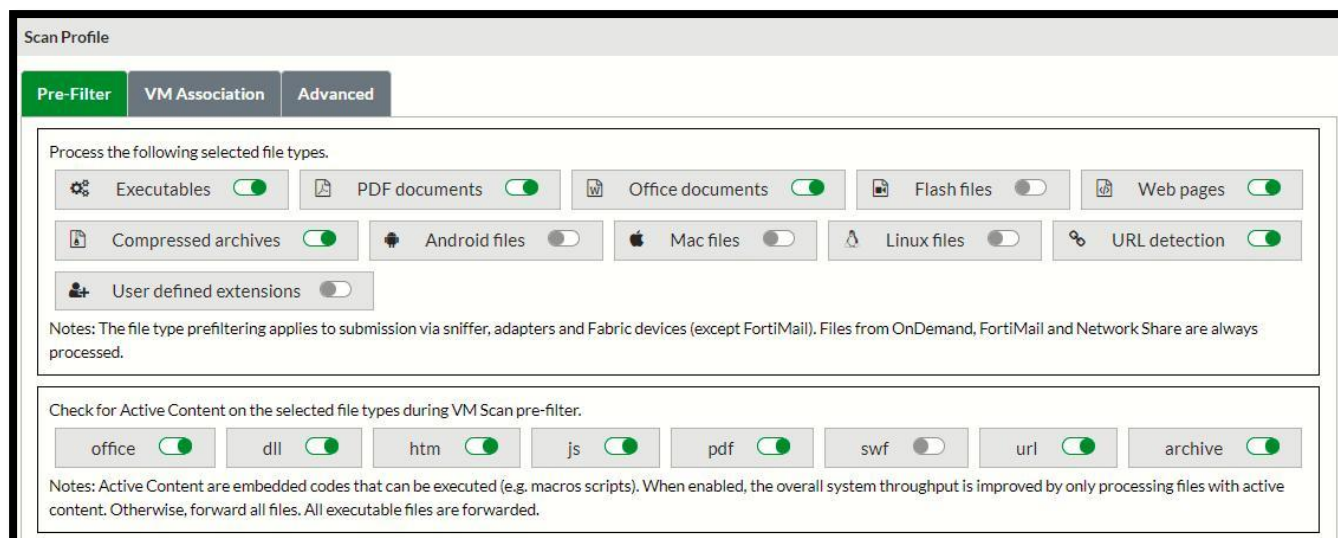
En la sección VM Settings, permite personalizar y configurar las opciones relacionadas con las máquinas virtuales utilizadas para el análisis de malware y pruebas de seguridad, como así también observar cuantas VM se tienen habilitadas.

Actions	Name	Status	Enabled	Clone #	Load #	Browser	Extensions
	WIN7X64SP1O16Z	activated	✓	1	1	OriginalDefault	doc docm docx dot dotm dotx eml iqy msg onetoc pot potm potx ppsm ppsx ppt pptm pptx rtf sldm sldx thmx xlam xls xlsx xism xlsx xlt xltm xlsx swf WVEBLink
	WIN10X64VM	activated	✓	1	1	OriginalDefault	bat cmd dll exe jar jse msi ps1 scr upx vbs wsf pdf
	WIN7X64VM	3 GB	✗	0	0		N/A
	WIN7X64SP1	4 GB	✗	0	0		N/A
	WIN7X86VM	4 GB	✗	0	0		N/A
	WIN10O19V1	✗	✗	0	0		N/A
	AndroidVM	1 GB	✗	0	0		N/A
	Ubuntu18	4 GB	✗	0	0		N/A

Es posible configurar parámetros específicos de la máquina virtual utilizada en FortiSandbox. Esto puede incluir detalles sobre el tipo de máquina virtual utilizada (por ejemplo, VMware, Hyper-V), la versión del sistema operativo huésped y otros aspectos relacionados con la configuración de la máquina virtual.

Installed Applications	Scanned File Types
Adobe Flash Player 17 ActiveX 17.0.0.134	doc docm docx
Adobe Reader X (8.1.2)	dotx eml iqy
Google Chrome 47.0.2526.73	pot potm potx
Microsoft .NET Framework 4.5.1	ppsm ppsx ppt
Microsoft .NET Framework 4.5.1 4.5.50938	
Microsoft .NET Framework 4.5.2 4.5.51209.34209	
Microsoft .NET Framework 4.6.4 6.8.1.0	

Por último, también permite asignar y controlar las extensiones y tipos de archivos habilitados en la VM.



Operation Center

En esta sección se encuentran aquellas alertas que la herramienta no puede dar un veredicto específico y requiere acción del operador.

<ul style="list-style-type: none"> Dashboard Status Scan Performance Operation Center Threats by Topology Threats by Hosts Threats by Files Threats by Device Security Fabric Scan Job Scan Policy and Object 	Detection 2024-07-03 15:20:19 to 2024-07-04 15:32:53				
	Source	Incident Time	Threat Name	File Name	Action
	1.220.166.1...	Jul 04 2024 07:13:04	Suspicious - Low	NOTICIAS DE INTERES 04JUL24.docx	Action Required
	7.136.85.60	Jul 03 2024 21:22:27	Suspicious - Low	EXPLOTACION DE PRENSA 3-7 GNA A LEY 23737.pdf	Action Taken
	7.136.85.60	Jul 03 2024 21:22:33	Suspicious - Low	EXPLOTACION DE PRENSA 3-7 GNA A LEY 23737.docx	Action Taken

Luego de analizar cada caso, del lado derecho se encuentra la columna "Action" donde podemos ver las opciones a elegir para el veredicto.



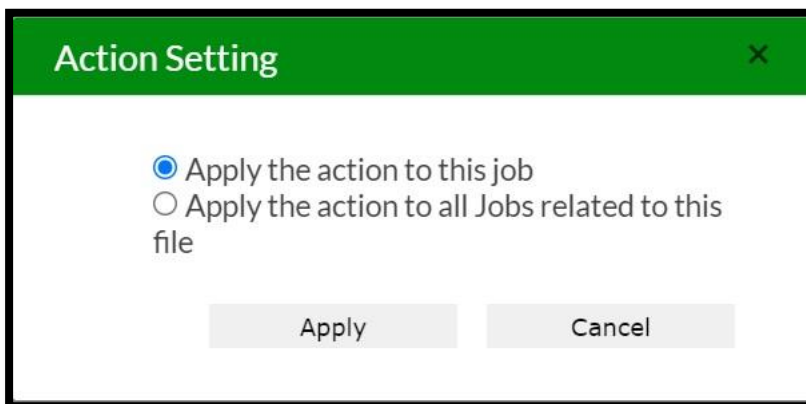
Check Verde/ action taken: Para indicar que el archivo es malicioso y que la acción de retenerlo fue correcta.

X Rojo/ Ignore: Para indicar que la alerta es un Falso Positivo.

Block rojo: No toma ninguna acción, en este caso se utilizaría si el analista no logra definir un veredicto y queda a la espera de que se defina.

	<h1>Instalación FortiSandbox</h1>	EDICIÓN 1
		Tipo de Documento: IMPLEMENTACIÓN
		Versión: 1.0 / 2023
		Página 10 de 10

Luego, el analista puede marcar una acción para un solo trabajo o para todos los trabajos del mismo archivo.



Action Setting ✕

☒ Apply the action to this job
☐ Apply the action to all Jobs related to this file

Apply Cancel

Revisiones y Modificaciones:

➤ 04/07/24