



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
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

FortiSandbox 1000F



Instalación FortiSandbox

EDICIÓN 1

Tipo de Documento:

IMPLEMENTACIÓN

Versión: 1.0 / 2023

Página 4 de 10

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.

The dashboard provides a high-level overview of the system's status and performance. It includes sections for System Information, Connectivity and Services, and Scan Performance - Last 4 Hours. The Scan Performance section displays various statistics such as total scanned files, processing times, and security detections.

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.

The interface includes a sidebar for managing licenses and a main area for monitoring system activity. The 'Scan Statistics - Last 24 Hours' table highlights a significant number of pending tasks (14) for Device sources. The 'File Scan - Last 24 Hours' chart shows a single major event occurring around the 8-hour mark.

Inputs	Pending	Processing	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	0	0	0	0	0	0	14	0	14
Adapter	0	0	0	0	0	0	0	0	0
On Demand	0	0	0	0	0	0	0	0	0
Network Share	0	0	0	0	0	0	0	0	0
Sniffer	0	0	0	0	0	0	0	0	0
URL	0	0	0	0	0	0	0	0	0
All Sources	0	0	0	0	0	0	0	14	0

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

The screenshot shows the FortiSandbox interface. On the left, under 'Basic Information', details about a job are listed: Job ID: 6644624392907112598, Status: Done, Received: 2023-06-14 18:40:42, Started: 2023-06-14 18:40:44, Rated By: Static Scan Engine, Submit Type: On-Demand, Digital Signature: No, AI Mode: ON, SIMNET: OFF, Timeout Value: 60 seconds, and Virus Total: [?Q](#). On the right, under 'Details Information', specific analysis results are shown: Filename: audit_01-06-2023_to_14-06-2023_5941367670704199176.csv, Downloaded From: audit_01-06-2023_to_14-06-2023_5941367670704199176.csv, Scan Start Time: 2023-06-14 18:40:44, Scan End Time: 2023-06-14 18:40:46, Total Scan Time: 2 seconds, File Type: csv, File Size: 35701 (bytes), Embedded URL: 0, MD5: d48b0f7fe228ff54721d011a3a0aa53d, SHA1: e15e5a1588af655610318de74687e86f3ab3238a, and SHA256: 158f12d269977dd781f6a44b7260dd13eb765e9898b36ef425b8f80afc44ef4. A red box highlights the SHA1 and SHA256 fields.

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.

The screenshot shows the FortiSandbox interface with a focus on URL On-Demand analysis. The table displays two entries: one for 'scan_of_secure.eicar.org' (Status: Done, Rating: Clean) and another for 'scan_of_mail.policiafederal.gov.ar' (Status: Done, Rating: Malicious). A red arrow points from the 'URL On-Demand' section in the sidebar to the first row of the table.

Action	Detection	URL	Rating	Status	URL Cou...	Comments
Jun 14 2023 18:52:01	scan_of_secure.eicar.org	Clean	Done	4		
Jun 14 2023 18:48:25	scan_of_mail.policiafederal.gov.ar	Malicious	Done	1	Análisis URL de prueba	

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.

The screenshot shows the FortiSandbox interface with a focus on URL On-Demand analysis. The table displays four entries, all of which are marked as 'Malicious'. A red arrow points from the 'URL On-Demand' section in the sidebar to the second row of the table.

Action	Detection	URL	Rating	Status	Submitted Filename
Jun 14 2023 18:53:06	https://secure.eicar.org/eicarcom2.zip	Clean	Done	1	scan_of_secure.eicar.org
Jun 14 2023 18:52:02	https://secure.eicar.org/eicarcom2.zip	Malicious	Done	1	scan_of_secure.eicar.org
Jun 14 2023 18:52:02	https://secure.eicar.org/eicarcom2.zip/eicar_com.zip	Malicious	Done	1	scan_of_secure.eicar.org
Jun 14 2023 18:52:02	https://secure.eicar.org/eicarcom2.zip/eicar_com.zip/...	Malicious	Done	1	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

Job ID:	6644636027480961054
Status:	Done
Received:	2023-06-14 18:51:57
Started:	2023-06-14 18:52:01
Rated By:	AV Scan Engine
Submit Type:	On-Demand
AI Mode:	ON
SIMNET:	OFF
Depth:	0
Timeout Value:	60 seconds
Virus Total:	Q
URL and Payloads	eicar_com.zip

Details Information

URL:	https://secure.eicar.org/eicarcom2.zip/eicar_com.zip
Scan Start Time:	2023-06-14 18:52:01
Scan End Time:	2023-06-14 18:52:02
Total Scan Time:	1 second
File Type:	zip
Embedded URL:	0
MDS:	6ce6f415d8475545be5ba114f208b0ff
SHA1:	d27265074c9eac2e2122ed69294dbc4d7cce9141
SHA256:	2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad
Submitted By:	[REDACTED]
Submitted Filename:	scan_of_secure.eicar.org
Scan Unit:	FSA1KFT622000091

① 3 security vendors flagged this URL as malicious

3 / 93

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
Default VMs (1/1) ✖							
	WIN7X64SP1O16Z	activated	✓	1	1	OriginalDefault	doc docm docx dot dotm dotx eml iqy msg onetoc pot potm potx pps ppsm ppsx ppt pptm pptx rtf sldm sldm slk thmx xlam xls xlsm xltx xltx xltx swf WEBLink
Optional VMs (1/7)							
	WIN10X64VM	activated	✓	1	1	OriginalDefault	bat cmd dll exe jar jse ms1 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
Remote MAC OSX							

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.

Scan Profile		
Pre-Filter	VM Association	Advanced
+ WIN10X64VM		
- WIN7X64SP1O16Z		
Installed Applications		
Adobe Flash Player 17 ActiveX 17.0.0.134 Adobe Reader X (8.1.2) Google Chrome 47.0.2526.73 Microsoft .NET Framework 4.5.1 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 4.6.810		
Scanned File Types		
doc	docm	docx
dotx	eml	iqy
pot	potm	potx
ppsm	ppsx	ppt

Select Extensions ✖

- Executables(12)
 - bat
 - cmd
 - dll
 - exe
 - jar
 - jse
 - msi
 - ps1
 - scr
 - upx
 - vbs
 - wsf



Instalación FortiSandbox

EDICIÓN 1

Tipo de Documento:

IMPLEMENTACIÓN

Versión: 1.0 / 2023

Página 9 de 10

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

Scan Profile

Pre-Filter VM Association Advanced

Process the following selected file types.

Executables PDF documents Office documents Flash files Web pages
Compressed archives Android files Mac files Linux files URL detection
User defined extensions

Notes: The file type prefiltering applies to submission via sniffer, adapters and Fabric devices (except FortiMail). Files from OnDemand, FortiMail and Network Share are always processed.

Check for Active Content on the selected file types during VM Scan pre-filter.

office dll htm js pdf swf url archive

Notes: Active Content are embedded codes that can be executed (e.g. macros scripts). When enabled, the overall system throughput is improved by only processing files with active content. Otherwise, forward all files. All executable files are forwarded.

Operation Center

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

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.

Action
✓ ✗ ⚡

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.



Instalación FortiSandbox

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.



Revisiones y Modificaciones:

- 04/07/24