

MANUAL DE GESTIÓN FORTIANALYZER SERIE F

VERSIÓN: 1.0

OBJETIVO: el usuario podrá descargar los informes preconfigurados, visualizar los LOGS y agregar filtros.

SISTEMA SOBRE EL QUE APLICA EL MANUAL – FortiAnalyzer Serie F Versión v6.0 – 6.4.

PROCEDIMIENTO:

ACCESO AL SISTEMA

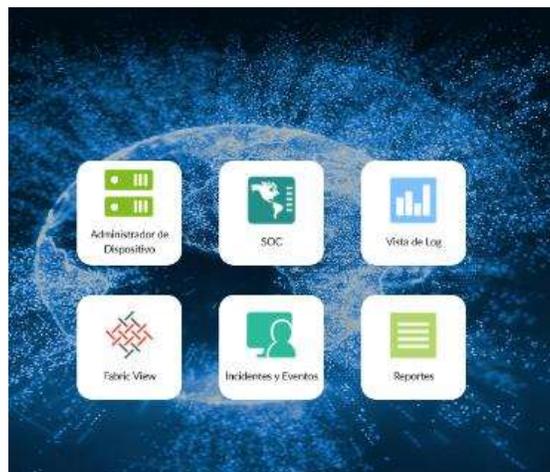
Se accede al dispositivo desde la IP Publica por el puerto 4446,

NOTA: la IP publica a ingresar ha sido enviada al correo de contacto registrado.



Diagnóstico

1. una vez que ya hallamos ingresado a nuestra consola principal con nuestras credenciales, en el panel principal encontramos la opción a las de dispositivos, Vista de logs, reportes, incidentes y eventos.



Administración de dispositivo

En este módulo se puede ver el estado de nuestros equipos sincronizados y su almacenamiento.



Vista de logs.

En este módulo se puede ver todos los LOGS de los equipos, configurar filtros por fecha, dispositivos, IP de origen, IP de destino, usuario, servicio, aplicación, protocolo, trafico.



Reportes.

En este módulo se pueden:

- ver los reportes preconfigurados.



- Descargar los informes existentes en el formato deseado.



Incidentes y eventos.

En este módulo se puede ver todos los eventos de seguridad reportados por los firewalls, y aplicar filtros de búsqueda personalizados.



#	Evento	Estatus del	Tipo de Event	Cont	Severidad	Primera Aparicion	Ultima Actualizacion	Informacion Adic	Gestor
1	> SupVis.RB-1...	Mitigado	IPS	1	Alta	4 days ago	4 days ago	OS Command ...	IPS - High Sev...
2	> SSLFatalAL...	Mitigado	Event	261	Medium	4 days ago	4 days ago	SSL Alert rece...	FOS Event Log...
3	> PHPStudy.W...	Mitigado	IPS	19	Alta	5 days ago	3 days ago	Code Injection...	IPS - High Sev...
4	> vRUBeh.Ra...	Mitigado	IPS	30	Critico	5 days ago	3 days ago	Code Injection...	IPS - Critical S...
5	> PHPCGI.Arg...	Mitigado	IPS	22	Alta	5 days ago	3 days ago	Code Injection...	IPS - High Sev...
6	> ThinkPHPH...	Mitigado	IPS	6	Alta	5 days ago	3 days ago	Code Injection...	IPS - High Sev...
7	> ThinkPHRR...	Mitigado	IPS	5	Alta	5 days ago	3 days ago	Code Injection...	IPS - High Sev...
8	> Joomla!Cor...	Mitigado	IPS	44	Critico	5 days ago	3 days ago	Code Injection...	IPS - Critical S...
9	> Desaru.CPO...	Mitigado	IPS	1	Critico	3 days ago	3 days ago	OS Command ...	IPS - Critical S...
10	> LinuxMir...	Mitigado	IPS	2	Critico	4 days ago	2 days ago	OS Command ...	IPS - Critical S...
11	> D-Lini.DevL...	Mitigado	IPS	2	Critico	4 days ago	2 days ago	OS Command ...	IPS - Critical S...
12	> Admin login ...		Event	2	Medium	2 days ago	2 days ago	Administrator ...	FOS Event Log...
13	> Gandm.Botn...	No Manejado	IPS	7	Critico	5 days ago	A day ago	General	IPS - Critical S...
14	> XorODOS.B...	No Manejado	IPS	2	Critico	5 days ago	A day ago	General	IPS - Critical S...
15	> Nitol.Botnet...	No Manejado	IPS	2	Critico	5 days ago	A day ago	General	IPS - Critical S...
16	> Admin perfo...		Event	1	Medium	A day ago	A day ago	System config...	FOS Event Log...
17	> JAWS.DVR...	Mitigado	IPS	8	Alta	4 days ago	A day ago	OS Command ...	IPS - High Sev...