Inventario

Inventario

Introducción

Pandora FMS permite mantener un inventario de los dispositivos monitorizados por Pandora FMS. Con dicho inventario es posible mantener listados e informes (disponibles en la versión Enterprise) de:

-  Modelo y velocidad del procesador (MS Windows®, GNU/Linux®).
-  Almacenamiento y *filesystems*.
-  Versión de *firmware* (hardware de red).
-  Configuración del dispositivo (hardware de red).
-  Números de serie y licencias (p.e: MS Office®, MS Windows®).
-  Aplicaciones instaladas en el equipo (MS Windows®, Android Linux®, GNU/Linux®).
-  Tarjetas de red y sus MAC asociadas a direcciones IP.
-  Módulos de memoria RAM y su capacidad (MS Windows®, GNU/Linux®).
-  Rutas instaladas.
-  Servicios en ejecución.
-  Dispositivos de almacenamiento (MS Windows®, GNU/Linux®).
-  Usuarios del sistema.

Recogida de datos para el inventario

El inventario es independiente de la monitorización y puede ser obtenido:

- De forma remota, mediante Módulos de inventario, a través de *scripts* integrados en Pandora FMS que ejecutan *queries* WMI, o *scripts* ejecutados a través de SSH con Expect o métodos similares.
- De forma local, con el Agente Software de Pandora FMS, mediante *plugins* en el Agente.

Módulos de inventario

Los Módulos de inventario son Módulos remotos que ejecutan un comando contra una máquina

remota. Dichos Módulos funcionan de forma similar a un *plugin*. Los mismos módulos se pueden definir como *locales* cuando obtienen los datos a través de un Agente Software.

En los parámetros de Usuario y Contraseña se pueden usar las siguientes macros: `_agentcustomfield_n_` (campo personalizado número *n* del agente).

Inventario remoto

Con Pandora FMS Enterprise vienen instalados por defecto una buena cantidad de módulos de inventario y también permite construir nuevos módulos de inventario, modificar, borrar y personalizar los que ya existen por medio del editor de módulos de inventario.

Creación de módulos remotos

En el menú Management → Configuration → Inventory Modules podrá ver dicha lista, y con el botón Create añadir uno nuevo.

Algunos campos de importancia:

- Interpreter: *Déjelo en blanco si es un Módulo local*. Campo donde se pone el intérprete de comandos que se usa en el módulo. Puede ser Shell Script, Perl u otro intérprete válido para el servidor de inventario que se ejecuta sobre un sistema GNU/Linux.
- Code: *Déjelo en blanco si es un Módulo local*. Código del Módulo; generalmente es código Perl o Shell Script. Si fuera código binario necesitaría un procedimiento de carga diferente que ha de ser introducido mediante *scripts* auxiliares.
- Block mode: Muestra y detecta cambios en la configuración.
- Format: Escriba los campos separados por `;` que devolverá el módulo.

- En Format asegúrese de colocar todos y cada uno de los campos separados por punto y coma. Si omite este campo no podrá crear o guardar un módulo de inventario y perderá los cambios realizados.
- Es muy importante elegir el sistema operativo correspondiente porque al añadir módulos de inventario en un agente solo aparecerán aquellos módulos en los que coincide el sistema operativo del módulo con el sistema operativo del agente.

Asignar módulos remotos

La asignación de Módulos de Inventario se realiza en el propio Agente, en la pestaña de administración del Agente, se pulsa sobre la pestaña Inventory.

- Module: Elija el módulo de inventario que se necesita añadir. *Solo aparecerán los módulos cuyo Sistema Operativo coincide con el del Agente*.
- Target: Dirección IP o nombre del servidor del que se quiere sacar el inventario.
- Interval: Elija el intervalo de tiempo en que se ejecutará el módulo de inventario.

Es posible definir campos en lugar de los de usuario y contraseña que existen normalmente, para ello es necesario activar el campo Use custom fields. Tras hacer esto, aparecerá un control para agregar campos nuevos (Add field).

- En este control habrá que introducir el nombre deseado antes de añadirlo.
- Si indica que el campo va a contener una contraseña maque It`s a password y el valor se guardará en base de datos de forma ofuscada.
- Tras crear los campos, se les puede dar un valor y añadir finalmente el Módulo.
- Estos campos serán aplicados en orden de creación en la ejecución del *script* de inventario remoto.

Inventario local a través de los Agentes Software

Mediante los Agentes Software es posible obtener los datos de inventario de una máquina. Bastará con aplicar los módulos de inventario correspondiente en la configuración del Agente Software.

Al igual que en los módulos remotos, también es necesario añadir estos módulos como módulo de inventario en Management → Configuration → Inventory modules.

Creación de Módulos locales

Para crear un Módulo local vaya a Management → Configuration → Inventory modules donde aparecen todos los módulos de inventario que han sido creados. Se deben crear aquí todos los módulos que se definirán en la configuración del Agente; también debe coincidir el sistema operativo asignado al Agente en la consola con el del Módulo creado.

El procedimiento es el mismo utilizado para el caso remoto, *exceptuando el rellenar los campos* Interpreter y Code. Para editar el módulo de inventario recién creado (así como todos los demás) haga clic bien sea en el nombre o en el icono de llave inglesa.

Configuración de inventario local para Agentes Software

Estos *plugins* vienen por defecto con la instalación del agente software, aunque vienen *comentados* en el archivo de configuración, para utilizarlos descomente tales líneas y reinicie el agente software (en la versión Enterprise se pueden reiniciar los agentes software por su configuración remota).

Ejemplo para MS Windows®:

```
#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\cpuinfo.vbs"
#module_crontab * 12-15 * * 1
```

```
#module_end
```

Se pueden descargar más elementos de la colección de *scripts* en la biblioteca de Pandora FMS. Cada uno tiene sus instrucciones de uso y se debe configurar la ejecución programada de *scripts* de inventario local en el archivo `pandora_agent.conf` agregando la información al final del fichero.

Módulo de Inventario en sistemas Unix mediante Agente Software

El módulo del Agente Software de Unix, usa, de forma local, un *plugin* para recoger información sobre diferentes aspectos de la máquina, tanto de software como de hardware.

El *plugin* que recoge el inventario está en el directorio `/etc/pandora/plugins`

La sintaxis del Módulo es la siguiente:

```
module_plugin inventory 1 cpu ram video nic hd cdrom software init_services
filesystem users route
```

El Módulo se compone de una línea con los siguientes parámetros:

- Activación del Módulo:

```
"module_plugin inventory" 1 cpu ram video nic hd cdrom software init_services
filesystem users route
```

- Campo donde se establece cada cuántos días se ejecutará el Módulo. Si es cero (0) el inventario es devuelto en cada ejecución del Agente.

```
module_plugin inventory "1" cpu ram video nic hd cdrom software init_services
filesystem users route
```

- Campo donde se definen los objetos de inventario que se recogen.

```
module_plugin inventory 1 "cpu ram video nic hd cdrom software init_services
filesystem users route"
```

También se puede especificar simplemente que recoja toda la información disponible. En este ejemplo, recogerá diariamente toda la información de inventario:

```
 # Plugin for inventory on the agent (Only Enterprise)
 module_plugin inventory 1
```

Para activar el Módulo de inventario se copia el código descrito anteriormente y se agrega en el fichero `pandora_agent.conf` del Agente Software y se reinicia el servicio.

Asignar módulos locales

Es innecesario activar los Módulos en los Agentes definidos en la Consola:

- Si los módulos se han creado en Configuration → Inventory modules.
- Si el sistema operativo coincide y está definida la ejecución en el archivo de configuración del Agente Software.
- *Los datos recolectados aparecerán directamente* en la sección View → Inventory del Agente en la Consola.

Creación de módulos de inventario locales con Agente Software

Además de los sistemas de inventario que vienen preconfigurados en el Agente, se pueden crear Módulos de inventario para sistemas Unix® y MS Windows®. Básicamente tiene que crear un *script* que genere un XML con la siguiente estructura:

```
<inventory>
    <inventory_module>
        <name>INVENTORY_MODULE_NAME</name>
        <type>generic_data_string</type>
        <datalist>
            <data>DATA1;DATA2;DATA3....</data>
        </datalist>
    </inventory_module>
</inventory>
```

- INVENTORY_MODULE_NAME: Se debe colocar el mismo nombre del Módulo que registró en los módulos de inventario en la Consola de Pandora FMS.
- DATA1;DATA2... : Son los datos a sacar y que se han definido en el Módulo de inventario.
- En el fichero `pandora_agent.conf` se debe ejecutar el *script* que genera el XML.
- Para que la ejecución del *script* local pueda almacenar información de inventario, debe tener definido un Módulo de inventario en la Consola, especificando el sistema operativo, nombre del Módulo y los datos a almacenar separados por `;` .
- Por lo anterior se debe crear el Módulo de inventario en Pandora FMS antes de reiniciar el agente de Pandora FMS.

Visualización de datos para el inventario

Los datos de inventario que se han recogido de un sistema, ya sea de forma local o de forma remota, se pueden ver desde el propio Agente o desde el menú de Inventario de la Consola.

Ver datos de Inventario en el menú de Inventario

Desde Operation → Monitoring → Inventory es posible ver los datos de inventario de todos los agentes, realizar búsquedas y exportar los datos a un fichero de tipo CSV.

De manera predeterminada se muestran todos los agentes pero es posible ver los módulos de todos los agentes que tienen inventario eligiendo All en las opciones de búsqueda y pulsando en Search. En todo caso de búsqueda (grupo, módulo, etcétera) podrá agrupar por agente si marca la opción Order by agent.

En la vista detallada del inventario de Agente, a través de un selector, se puede escoger la fecha del informe de inventario concreto a visualizar (por defecto Last).

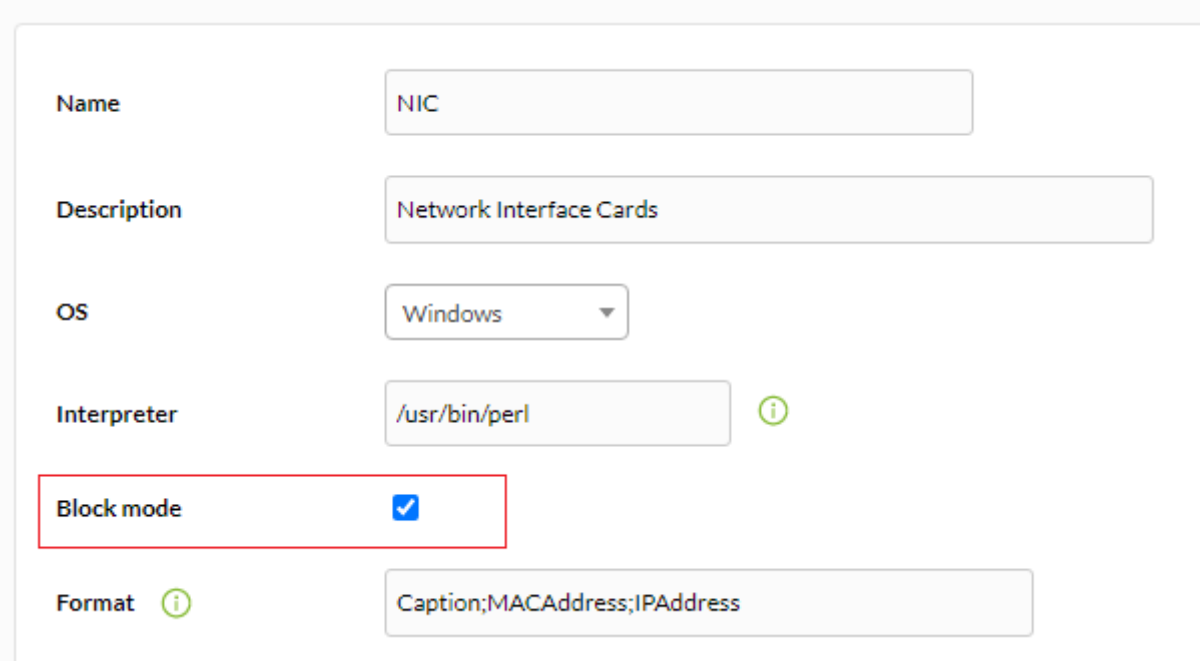
Si observa que faltan fechas será probablemente porque no hay cambios en los datos respecto a la última ejecución de inventario. *Es decir, Pandora FMS solamente almacena datos de inventario cuando estos cambian respecto a la última ejecución.*

Exportar los datos de inventario a CSV

Desde Operation → Monitoring → Inventory es posible exportar los datos del inventario, resultado de un filtro, a un archivo CSV utilizando el botón Export this list to CSV. Se creará y descargará un fichero con los datos de inventario separados por el caracter configurado en Setup → Visual styles → CSV divider.

Diferencias entre versiones de inventario

Pandora FMS puede mostrar visualmente las diferencias entre dos configuraciones, visualizándolo en dos columnas para ver las diferencias. El Block mode especifica que el resultado de un módulo de inventario es un único elemento, en vez de interpretar cada línea como elementos diferentes del mismo tipo, como se ha hecho en los módulos de inventario vistos anteriormente. Se configura al definir un Módulo de inventario local o remoto:



Alertas de inventario

Versión 751 NG o posterior.

Las alertas de inventario sirven para lanzar alertas específicas sobre el contenido de inventario de un grupo de agentes. Al igual que las alertas SNMP o a las alertas sobre eventos, no se aplican agente por agente si no que son globales, en este caso, se aplican por grupos.

Para configurar las alertas, se debe ir a la sección Management → Alerts → Inventory alerts.

Las alertas de inventario tienen campos similares a otras alertas como nombre, descripción, *time threshold* y acción y con las siguientes diferencias:

- El grupo en este caso actúa como condición de alerta, de manera que se evaluarán las alertas para cualquier dato que venga de un Agente de dicho grupo.
- Estas alertas disponen además de la opción desactivar evento que sirve para que cuando se dispare la alerta, no se genere un evento de alerta. Es útil ya que es posible que con la aplicación de alertas de inventario salten o se disparen muchas alertas en una sola ejecución.

Condición de disparado de alerta

Coincidencia de cadena de texto

De este modo, cuando llegue una cadena concreta en un módulo de inventario específico (por ejemplo “software”) se disparará la acción establecida. Los Módulos de inventario tienen campos dinámicos; por ejemplo en el módulo de inventario *software*, existen los campos *nombre*, *versión* y *descripción* que pueden ser utilizados. Así se puede establecer una alerta para cualquiera de los tres campos dinámicos, como por ejemplo para monitorizar un paquete de una versión concreta:

En estos campos puede introducir expresiones regulares para hacer búsquedas mas complejas. Si un campo se queda vacío cuenta como `.*` (hará coincidencia en cualquier valor).

Lista restringida

En este caso (Condition, Black list) se debe especificar solamente un campo del tipo de Módulo de inventario, y establecer una lista de cadenas (una por línea) de manera que si el Agente contiene un elemento de esa lista, saltará la alerta

Lista permitida

Similar al caso anterior: Se especifica una lista de elementos (Condition, White list) para uno de los campos de inventario, salvo que en este caso, el valor del Módulo de inventario debe encontrarse siempre en uno de los elementos de la lista, *en caso de no ser así, saltará la alerta.*

Usos de las alertas de inventario

Esta funcionalidad es realmente útil para detectar versiones vulnerables de dispositivos, usuarios no autorizados en máquinas o software de uso no autorizado en los equipos.

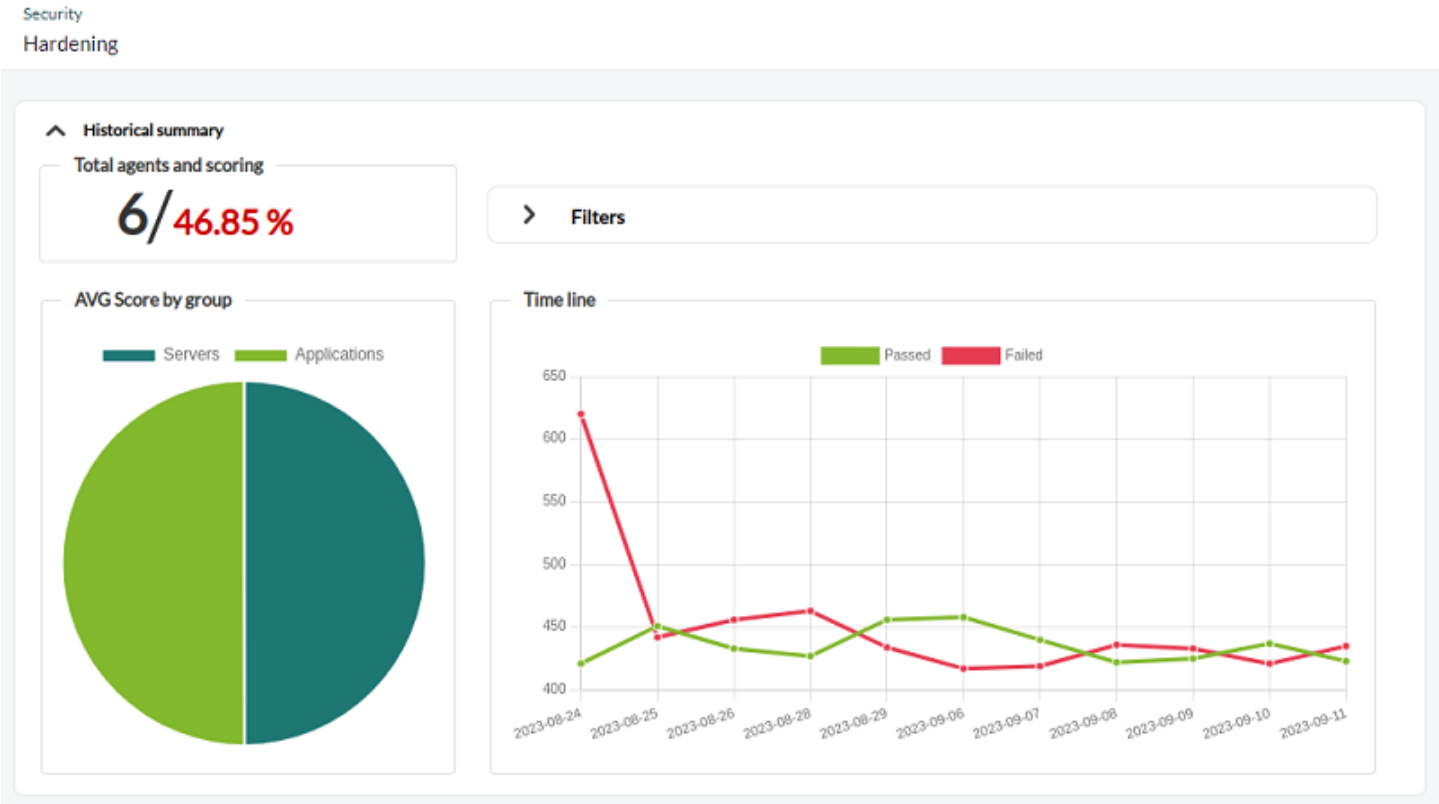
Monitorización de la seguridad

Pandora FMS permite recoger, además de los datos de inventario, otros valores importantes de cada sistema operativo monitorizado por medio de los agentes software. Todo esto está centralizado en la sección Operation → Security → Hardening.

Con esta herramienta se busca fortalecer la seguridad de cada uno de los dispositivos monitorizados y se presenta la información en tres secciones principales.

Historical summary

En el Resumen histórico se presenta el total de agentes que monitorizan los módulos destinados a la seguridad y con la media total de puntuación (cuadro Total agents and scoring).

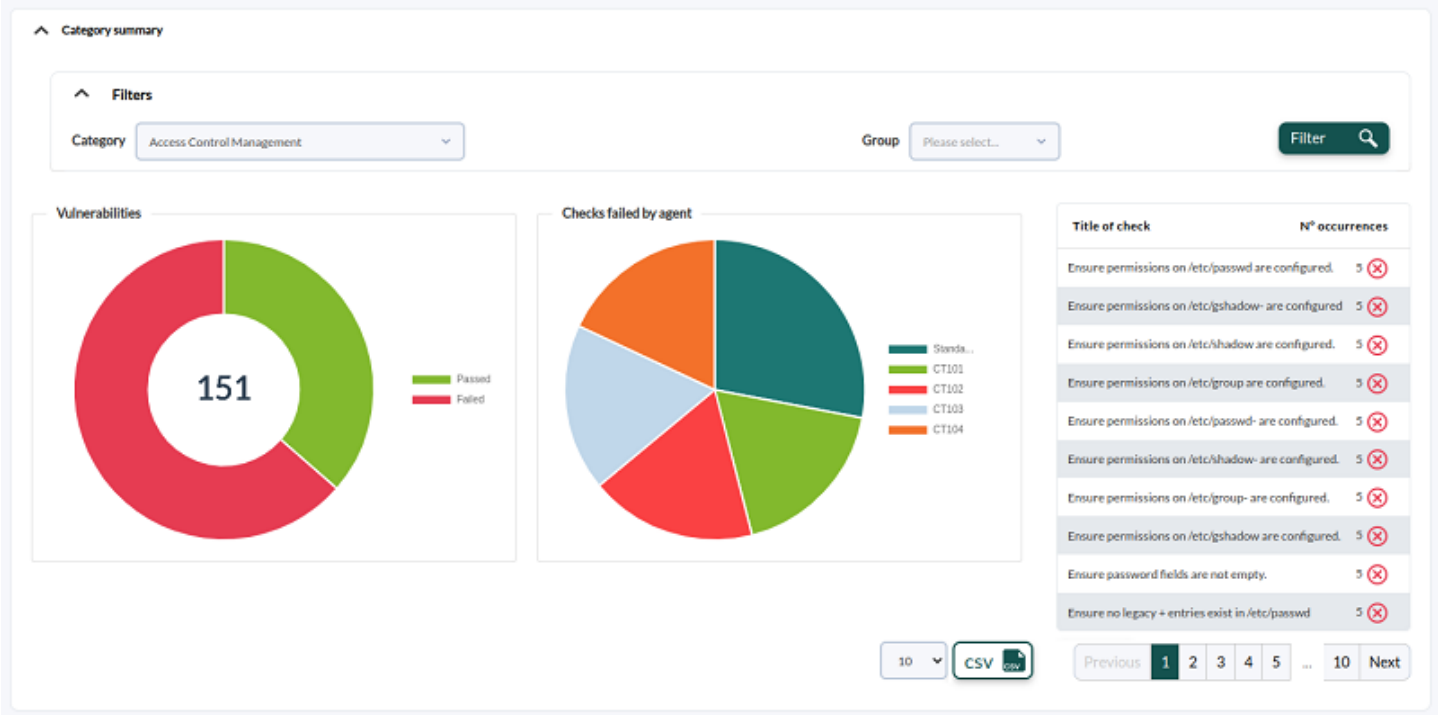


En el cuadro AVG Score by group se presenta la puntuación media por cada grupo definido en PFMS.

Se cuenta también con la gráfica histórica (cuadro Time line) con el promedio de los chequeos de seguridad fallidos y aprobados agrupados por días (máximo los últimos once días) independientemente del periodo de tiempo seleccionado. En Filters se puede selecciona un periodo de tiempo personalizado o por valores comunes (última semana, último mes, etcétera).

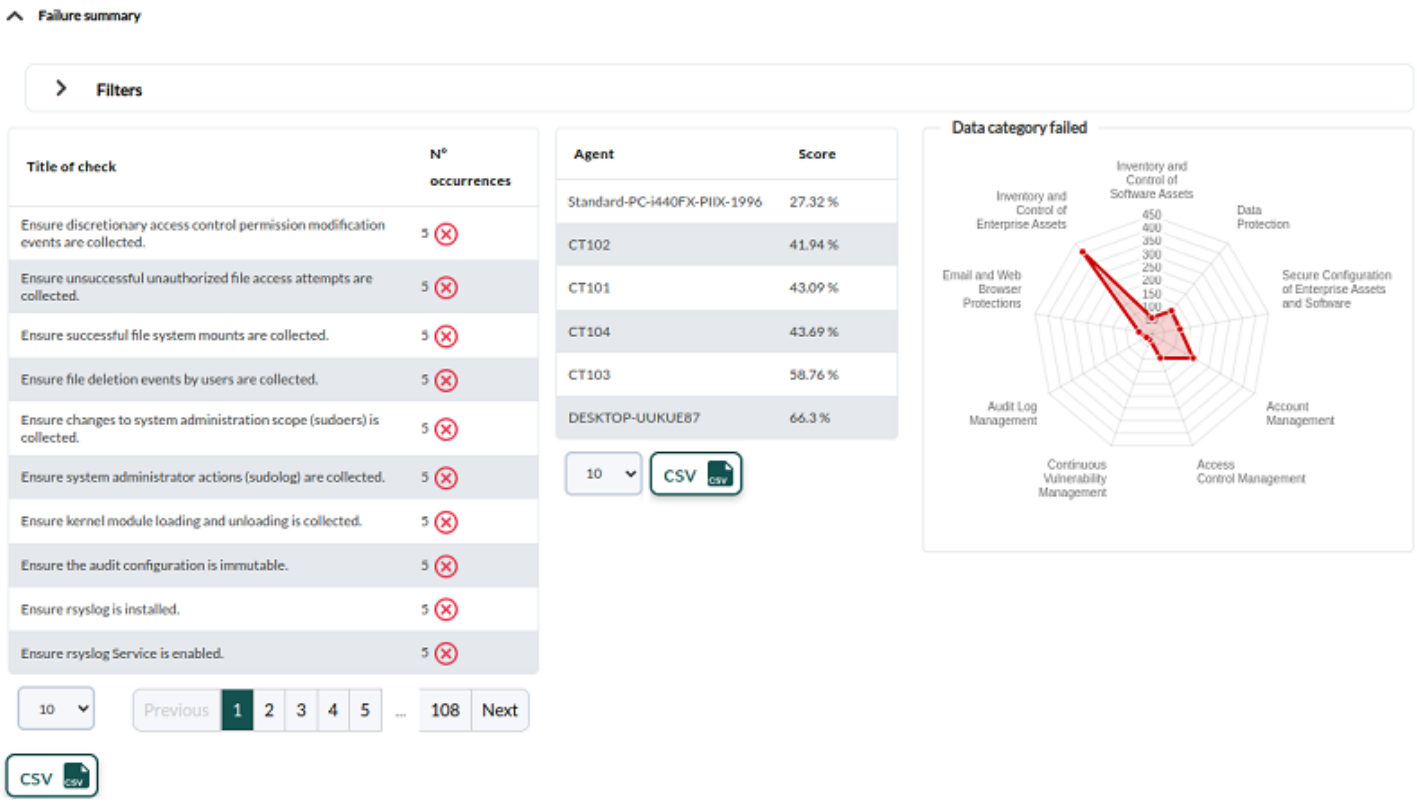
Category summary

En el Resumen por categorías se deberá filtrar obligatoriamente por categoría y opcionalmente por grupo para visualizar. Por defecto se muestra seleccionada la categoría Access Control Management.



* En el cuadro Vulnerabilities se mostrarán el total de vulnerabilidades fallidas y vulnerabilidades superadas. * En Checks failed by agent el listado de chequeos fallidos de la categoría seleccionada, al pulsar en cada sector del gráfico se listarán los detalles del chequeo seleccionado y los agentes afectados.

Failure summary



Se presenta el resumen de fallos (Tittle of check): El listado de chequeos fallidos filtrados por

grupo y el número de incidencias. Utilice el cuadro Filters para definir nuevos parámetros de búsqueda y visualización.

También el listado de los agentes con peor puntuación de seguridad, con la opción de visualizar la vista de seguridad de cada agente al hacer clic en los mismos.

Por último se presenta un gráfico de radar con la distribución de fallos por categoría.

Volver al índice de documentación de Pandora FMS