Hardening

Hardening

Monitorización de hardening

Se han fusionado las recomendaciones del Center for Internet Security (CIS) con la tecnología de monitorización de Pandora FMS para ofrecer un sistema de auditoría de aseguramiento integrado. Esto permite rastrear y evaluar a lo largo del tiempo la evolución de las medidas de *hardening* (fortalecimiento de la seguridad) en los entornos utilizados y monitorizados.

El *system hardening* (o endurecimiento del sistema) es un proceso que utilizado para mejorar la seguridad de un sistema informático al reducir su superficie de ataque y fortalecer sus defensas. Consiste en hacer más difícil que posibles atacantes exploren fallos de configuración, ya sea por configuraciones por defecto, malas configuraciones o configuraciones indebidas.

El *system hardening* es un proceso continuo ya que las amenazas de seguridad y las vulnerabilidades evolucionan con el tiempo. Requiere un monitoreo constante, evaluaciones de riesgos y ajustes en las configuraciones de seguridad para adaptarse a las circunstancias cambiantes. Además, las organizaciones a menudo siguen estándares y mejores prácticas específicas de la industria, como los controles del CIS o las pautas del National Institute of Standards and Technology (NIST), para garantizar un *system hardening* integral.

Pandora FMS utiliza varias categorías del CIS para agrupar los chequeos que realiza.

Categorías CIS Auditadas por Pandora FMS

Hemos llevado las recomendaciones del CIS un paso más allá al implementar más de 1500 comprobaciones individuales en una variedad de categorías cruciales para la seguridad.

Inventario y control de activos hardware y software: Supervise y gestione todos los dispositivos y software en su organización. Mantenga un inventario actualizado de sus activos tecnológicos y use la autenticación para bloquear los procesos no autorizados.

Inventario y control de dispositivos: identificar y gestionar sus dispositivos de hardware para que solamente los autorizados tengan acceso, bloqueando los demás. Mantener un inventario adecuado minimiza riesgos internos, organiza su entorno y brinda claridad a su red.

Gestión de vulnerabilidades: Analice sus activos de forma continua en el tiempo para detectar vulnerabilidades potenciales y solucionelas antes de que se conviertan en la entrada a un ataque. Refuerce la seguridad de red asegurándose de que el software y los sistemas operativos en la

organización estén siempre actualizados con las últimas medidas de seguridad y *parches*. Ayude a gestionar su software para asegurar que solamente el software autorizado esté instalado y sea ejecutado. Evite vulnerabilidades y riesgos al mantener un inventario preciso y gestionar su software.

Uso controlado de privilegios administrativos: Supervise de cerca los controles de acceso y el comportamiento de los usuarios con cuentas privilegiadas para evitar cualquier acceso no autorizado a sistemas críticos. Asegúrese de que solamente las personas autorizadas tengan privilegios elevados para evitar cualquier mal uso de los privilegios administrativos. Establece políticas estrictas para prevenir el uso indebido de privilegios.

Configuración segura de hardware y software: Establezca y mantenga configuraciones de seguridad basadas en los estándares aprobados por su organización. Crea un sistema de gestión de configuraciones riguroso que detecte y alerte sobre cualquier configuración incorrecta, y establece un proceso de control de cambios para evitar que los atacantes se aprovechen de servicios y configuraciones vulnerables.

Mantenimiento, supervisión y análisis de *logs* y registros de auditoría: Recopile, administre y analice los *logs* de auditoría de eventos para identificar posibles anomalías. Mantenga registros detallados para comprender a fondo los ataques y poder responder de manera eficaz a los incidentes de seguridad.

Defensas contra *malware* : Supervise y controle la instalación y ejecución de código malicioso en varios puntos de su organización para prevenir ataques. Configure y utiliza *software antimalware* y aproveche la automatización para garantizar actualizaciones rápidas de defensas y una acción correctiva ágil en caso de ataques.

Protección del correo electrónico y los navegadores web: Proteja y administre sus navegadores web y sistemas de correo electrónico contra amenazas en línea para reducir su superficie de ataque. Desactive complementos de correo electrónico no autorizados y asegúrese de que los usuarios solo accedan a sitios web de confianza mediante filtros de URL basados en la red. Mantenga seguras las puertas de entrada más comunes para ataques.

Capacidades de recuperación de datos: Establece procesos y herramientas para asegurar que la información crítica de tu organización esté respaldada adecuadamente. Asegúrese de contar con un sistema de recuperación de datos confiable para restaurar la información en caso de ataques que pongan en peligro los datos críticos. Prepare su organización para hacer frente a la pérdida de datos de manera efectiva.

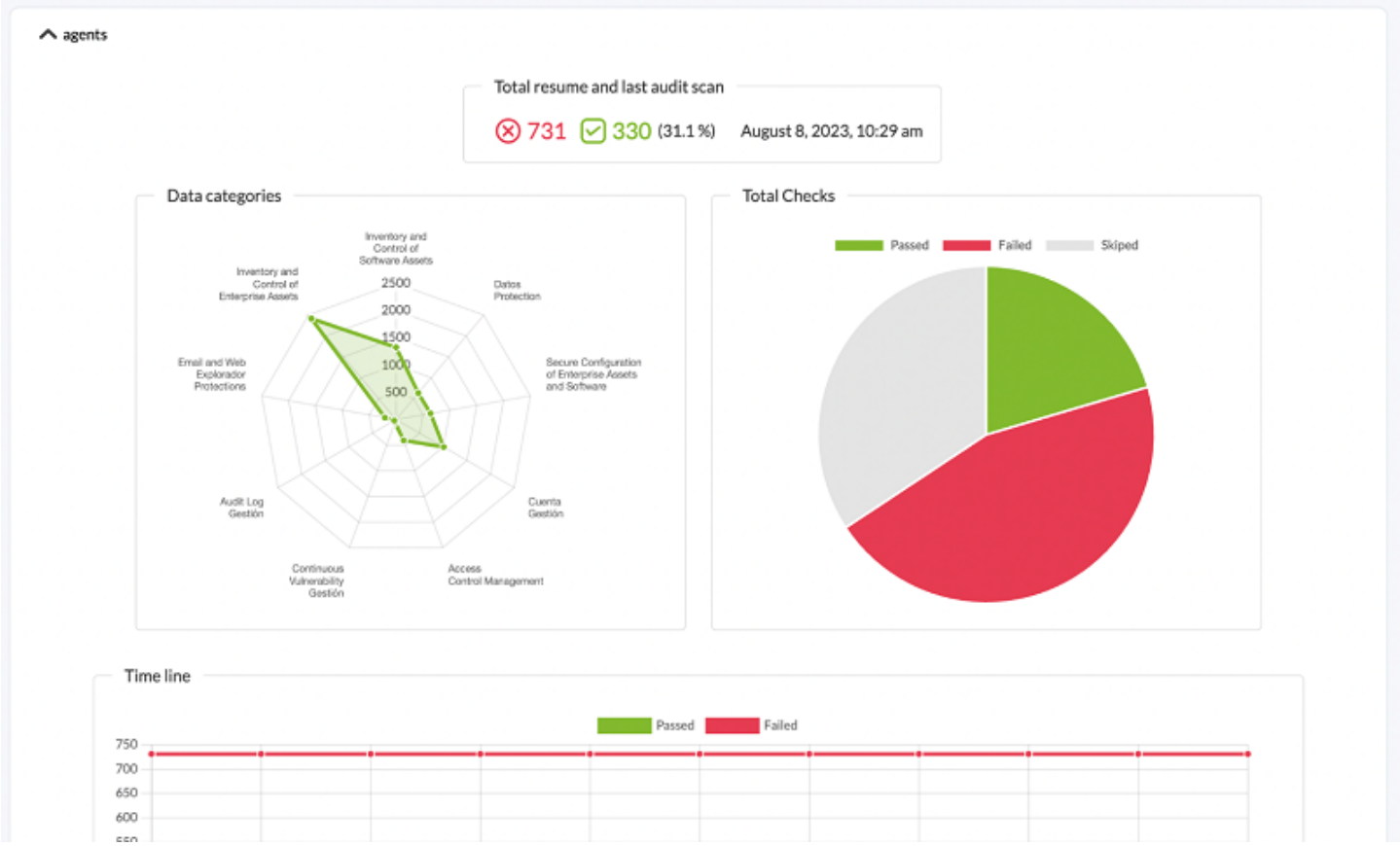
Defensa de límites y protección de datos: Identifica y separa los datos sensibles, y establece una serie de procesos que incluyan la codificación, planes de protección contra la infiltración de datos y técnicas de prevención de pérdida de datos. Establece barreras sólidas para prevenir el acceso no autorizado.

Supervisión y control de cuentas: Supervisa de cerca todo el ciclo de vida de sus sistemas y cuentas de aplicaciones, desde su creación hasta su eliminación, pasando por su uso e inactividad. Esta gestión activa previene que los atacantes se aprovechen de cuentas de usuarios legítimos pero inactivos para fines maliciosos y permite mantener un control constante sobre las cuentas y sus actividades.

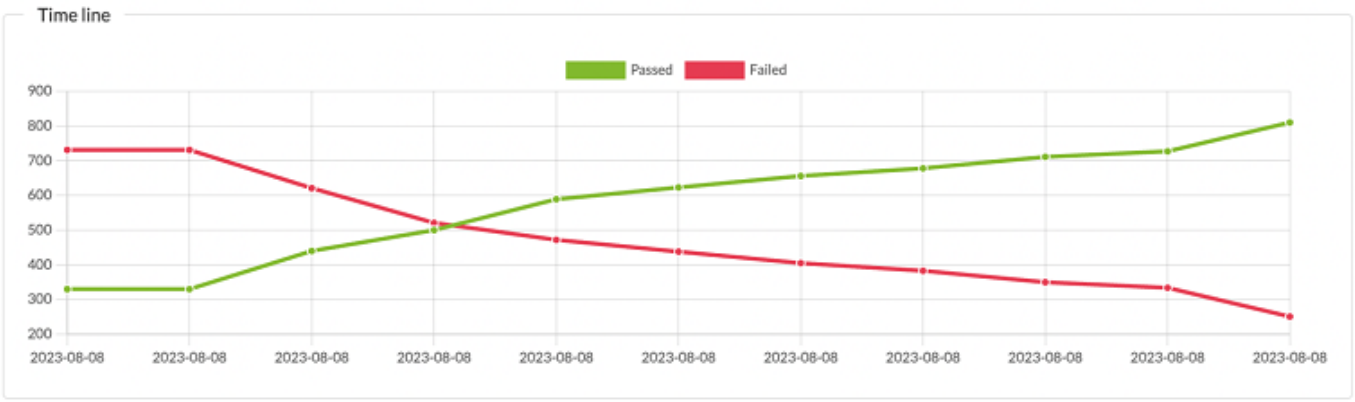
Auditorías de hardening detalladas de cada máquina

Los chequeos son realizados por el EndPoint que corre en cada máquina. Habitualmente toma una auditoría cada semana, pero ese período puede ser configurado a más tiempo, por ejemplo un mes. De esta forma se puede tomar una *fotografía del aseguramiento* del sistema, calcular y asignar un índice de seguridad (una valoración numérica, definida como el porcentaje de chequeos realizados y aprobados versus los chequeos que no pasan las pruebas) y ver la evolución de ese índice de seguridad a lo largo del tiempo.

Ejemplo de una “fotografía” del estado del *hardening* de un sistema:



Ejemplo de evolución del *hardening* de un sistema a lo largo del tiempo:



El sistema nos permite ver, desglosado por categorías, los chequeos que se han ejecutado:

Summary of categories

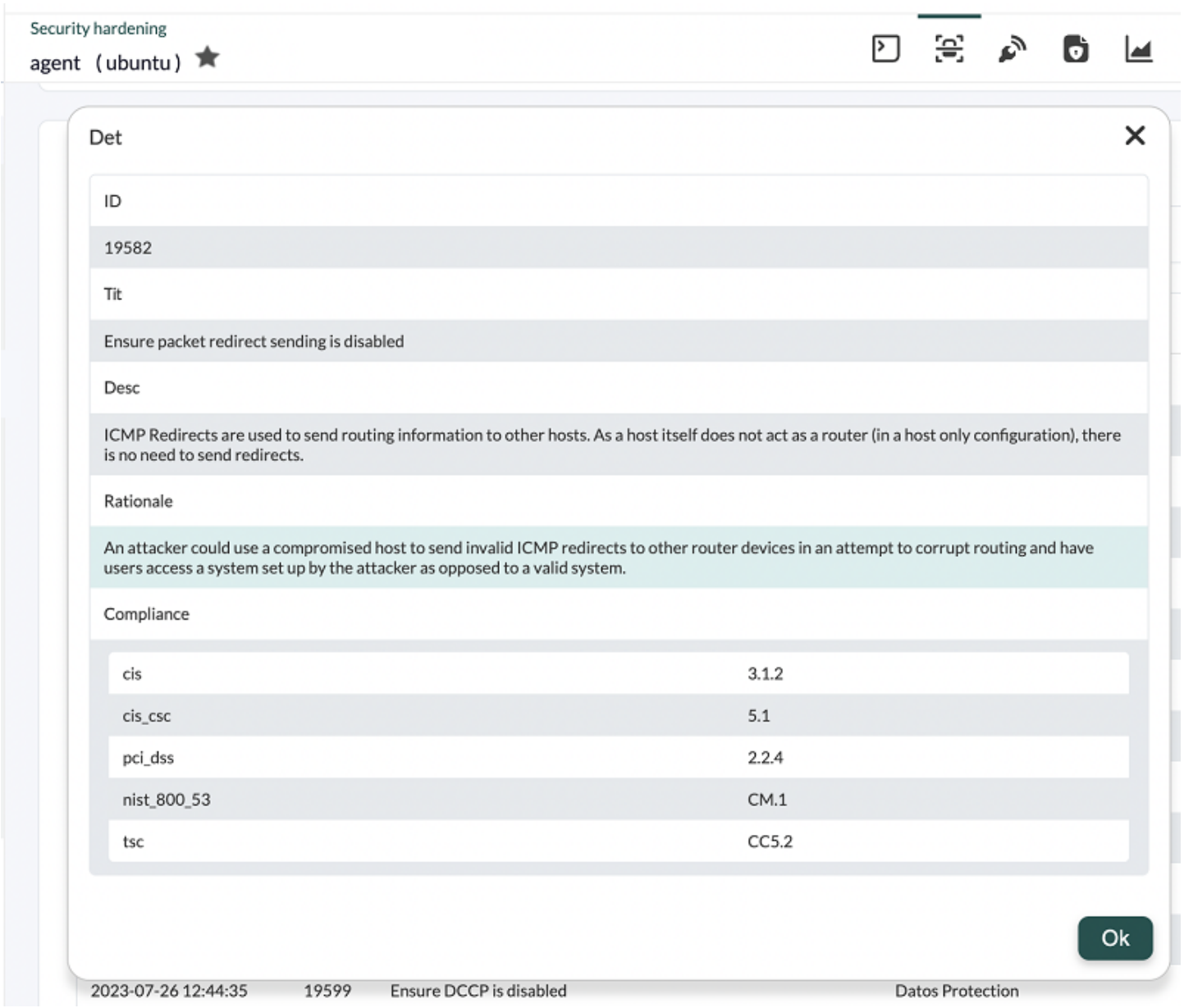
Inventory and Control of Software Assets	14	46	23 %
Data Protection	20	118	14 %
Secure Configuration of Enterprise Assets and Software	21	126	14 %
Account Management	78	193	29 %
Access Control Management	92	16	85 %
Continuous Vulnerability Management	8	14	36 %
Audit Log Management	0	20	0 %
Email and Web Browser Protections	6	20	23 %
Inventory and Control of Enterprise Assets	89	176	34 %

Y de cada grupo de elementos, ver el detalle, para poder trabajar sobre su corrección:

Results for audit on 2023-07-26 12:44:35

Filters

Date	ID	Title	Category	Status	Details
2023-07-26 12:44:35	19581	Ensure IP forwarding is disabled	Datos Protection		
2023-07-26 12:44:35	19582	Ensure packet redirect sending is disabled	Datos Protection		
2023-07-26 12:44:35	19583	Ensure source routed packets are not accepted	Datos Protection		
2023-07-26 12:44:35	19584	Ensure ICMP redirects are not accepted	Datos Protection		
2023-07-26 12:44:35	19585	Ensure secure ICMP redirects are not accepted	Datos Protection		
2023-07-26 12:44:35	19586	Ensure suspicious packets are logged	Datos Protection		
2023-07-26 12:44:35	19589	Ensure Reverse Path Filtering is enabled	Datos Protection		
2023-07-26 12:44:35	19590	Ensure TCP SYN Cookies is enabled	Datos Protection		
2023-07-26 12:44:35	19591	Ensure IPv6 router advertisements are not accepted	Datos Protection		
2023-07-26 12:44:35	19592	Ensure IPv6 redirects are not accepted	Datos Protection		
2023-07-26 12:44:35	19593	Ensure IPv6 is disabled	Datos Protection		
2023-07-26 12:44:35	19596	Ensure /etc/hosts.deny is configured	Datos Protection		
2023-07-26 12:44:35	19599	Ensure DCCP is disabled	Datos Protection		



Configuración de la monitorización de hardening

Se han desarrollado controles, dependiendo de cada sistema si son aplicables, que ayudarán a determinar si son relevantes en el entorno a monitorizar. Actualmente esta funcionalidad está disponible para servidores MS Windows® y Linux®.

Está funcionalidad está disponible con los EndPoints 773 o posteriores. Si los EndPoints son de una versión anterior a 773 se deberán de actualizar.

Para ello se tendrá que activar el *plugin* correspondiente en la configuración del EndPoint. Se podrá realizar manualmente o a través de políticas de monitorización en grupos de máquinas.

En MS Windows®:

```
module_begin
module_plugin "%PROGRAMFILES%\Pandora_Agent\util\pandora_hardening.exe -t 150"
module_absoluteinterval 7d
module_end
```

Linux®:

```
module_begin
module_plugin /usr/share/pandora_agent/plugins/pandora_hardening -t 150
module_absoluteinterval 7d
module_end
```

En estos ejemplos se ejecutará la auditoría de *hardening* cada 7 días, con un *timeout* de 150 segundos para cada comando que se lance durante la auditoría. Puede incrementar este valor a 30 días, pero no recomendamos que lo haga cada menos días pues generará datos innecesarios de inventario.

Monitorización de los datos de hardening

Además de *dashboard* y vistas específicas para poder analizar esos datos en sistemas concretos o a nivel global, se dispone de algunos módulos generados por el sistema de *hardening* que permitirán tratar los datos de la evaluación del *hardening* como otros datos de Pandora FMS, para establecer alertas, generar gráficas o cualquier otro uso que se necesite. Estos módulos son generados o actualizados automáticamente cada vez que se ejecuta una auditoría de *hardening* y pertenecen al Module group denominado Security.

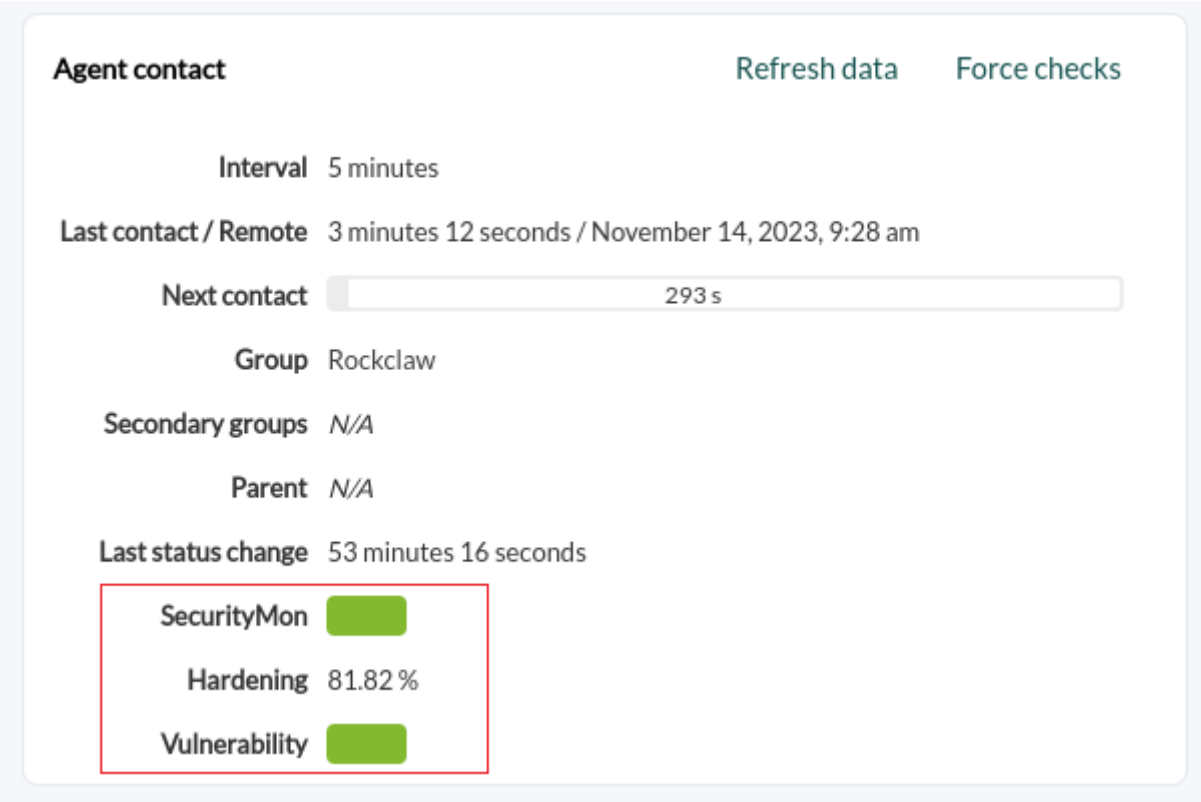
- Hardening - Failed checks: Muestra el número total de chequeos que no han aprobado la prueba de *aseguramiento*.
- Hardening - Not applied checks:Muestra el número total de chequeos que no se han ejecutado porque no aplican (por ejemplo, chequeos para otra versión de su distribución Linux o versión Windows, o porque buscan un determinado componente que no está instalado).
- Hardening - Passed checks: Muestra el número total de chequeos que han aprobado la prueba de *aseguramiento*.
- Hardening - Score: Muestra el porcentaje de los chequeos que han pasado. Se puede establecer un umbral aquí para mostrar cuando el sistema está en estado `Warning` o `Critical` respecto a la *aseguramiento*.

Hardening - Failed checks	Number of failed checks across policies.		N/A - N/A	2
Hardening - Not applied checks	Number of checks that did not apply across policies.		N/A - N/A	192
Hardening - Passed checks	Number of passed checks across policies.		N/A - N/A	10
Hardening - Score	% of passed checks (0 to 100).		N/A - N/A	83.3

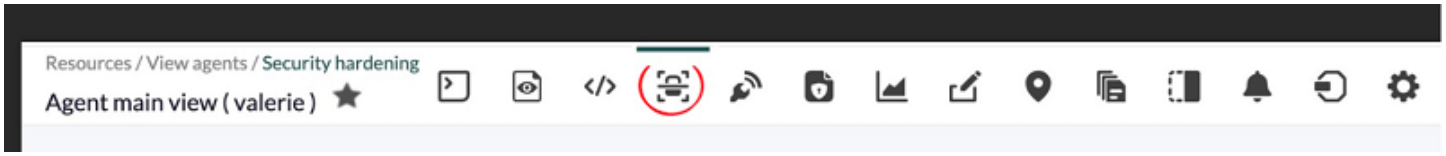
Visualización de los datos de hardening

Menú Operation → Monitoring → Views → Agent detail

Una vez que los EndPoints ejecuten por primera vez el módulo de *hardening*, la información llegará y se podrá ver en el detalle de cada EndPoint haciendo clic en su nombre respectivo. Luego en Agent main view, en el cuadro Agent Contact, tres elementos resumen el estado de la seguridad (SecurityMon, al colocar el puntero encima mostrará el número de módulos de seguridad), el porcentaje de seguridad alcanzado (Hardening) y el estado de la vulnerabilidad (Vulnerability, al colocar el puntero encima mostrará el puntaje alcanzado):

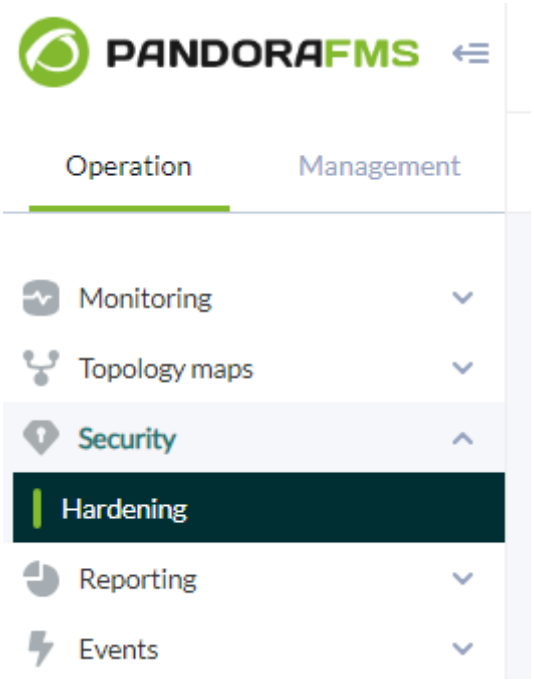


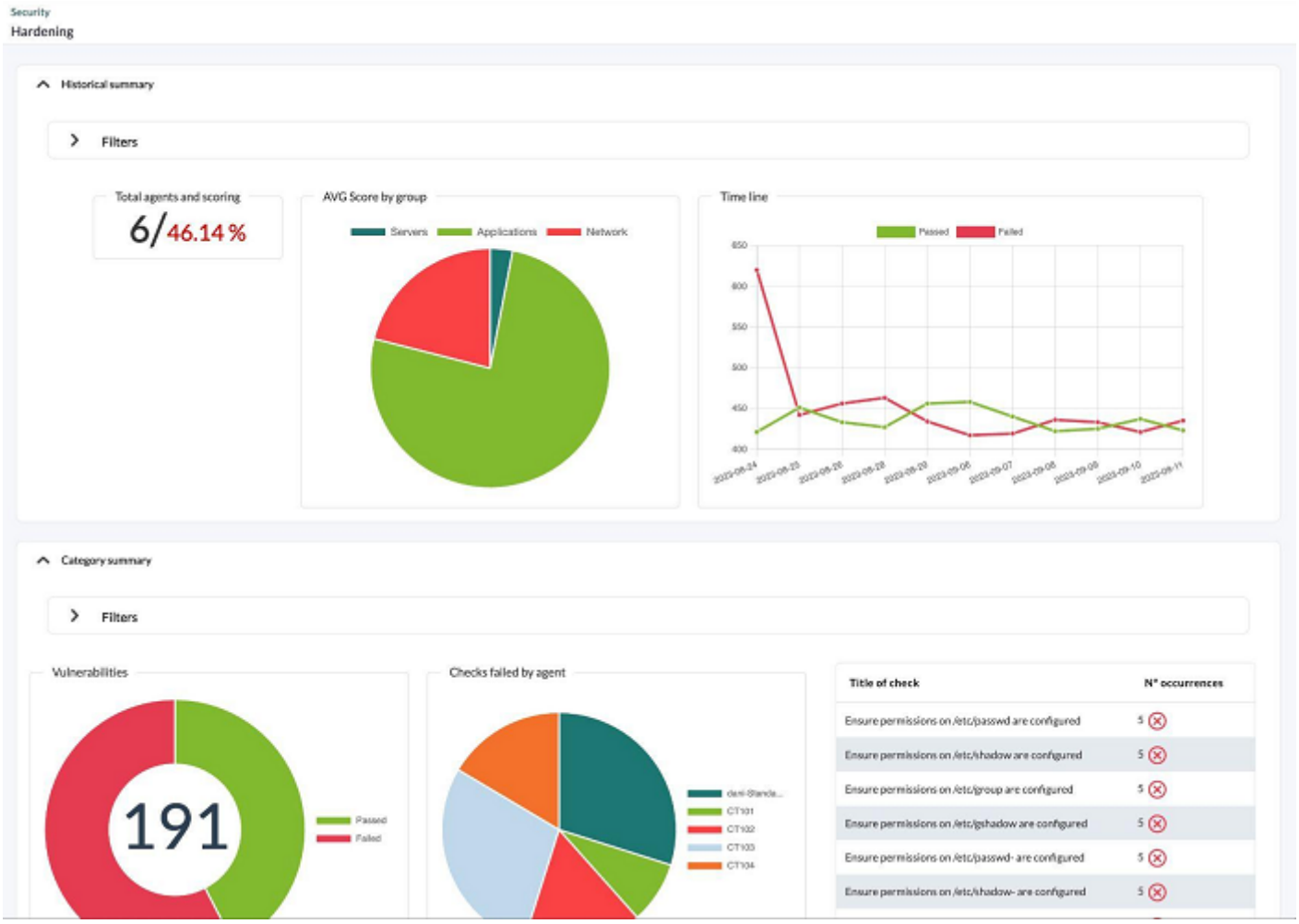
También se habilitará una sección específica para el *hardening* de dichos EndPoints:



Además, podrá ver una sección en el menú de operación llamada “Seguridad” (Security), donde

existe un *dashboard* específico para los datos de Hardening donde podrá filtrar por grupos, EndPoints, categorías del CIS y otros detalles.





Informes de hardening

Se han creado nuevos tipos de informe para mostrar la información de *hardening*:

- Top N EndPoints con peor puntuación. Filtrada por grupos.
- Top N de chequeos que no pasan más frecuentes. Filtrada por grupos.
- Gráfica de tarta con Vulnerabilidades por tipo. Eligiendo una categoría CIS, se agrupan los *fails*, *passed* y *skipped* (opcional) de todos los EndPoints (o solo el grupo seleccionado) por categoría.
- Top N de chequeos que no pasan por categoría, se agrupan los últimos datos de todos los EndPoints (o solo el grupo seleccionado) por categorías del *hardening* y se listan las categorías con mayor número de *fails* entre todos los EndPoints.
- Listado de chequeos de *securización*, es un informe técnico y exhaustivo con todos los detalles, se listan los últimos chequeos de un EndPoint filtrado por grupo, categoría y estado.
- Scoring, se muestran los últimos *scoring* de los EndPoints del grupo seleccionado o de todos dentro del rango de tiempo seleccionado en el filtro por defecto de los informes. Siempre se coge el último scoring de cada EndPoint dentro del rango temporal, es decir si se coloca un rango de un mes, se buscará el último scoring de los EndPoints dentro de ese mes.
- Evolution, se muestra una evolución global del *hardening* haciendo la media de los *test* que han pasado y los que han fallado agrupando por día, de todos los EndPoints o de los que estén dentro del grupo seleccionado.

Estos son algunos ejemplos de informes en PDF:

PANDORAFMS ENTERPRISE

Test

T n agents Hardening: Top number of agents with the worst score

T n agents

Agent	Last audit scan	Score
DESKTOP-UUKUE87	September 21, 2023, 11:25 am	0.7 %
dani-Standard-PC-i440FX-PIIX-1996	September 21, 2023, 9:24 am	4.19 %
CT103	September 21, 2023, 9:24 am	17.06 %
CT104	September 21, 2023, 9:24 am	48.48 %
CT102	September 21, 2023, 9:23 am	54.21 %
CT101	September 21, 2023, 9:26 am	82.02 %

T most frequent Hardening: Top number most frequent failed checks

T most frequent

Title	Total Failed	Description
Ensure /etc/hosts.deny is configured	5	The /etc/hosts.deny file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.allow file.
Verify permissions on /etc/hosts.allow	5	The /etc/hosts.allow file contains network information that is used by many system applications and therefore must be readable for these applications to operate.
Verify permissions on /etc/hosts.deny	5	The /etc/hosts.deny file contains network information that is used by many system applications and therefore must be readable for these applications to operate.
Ensure default deny firewall policy	5	A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Ensure loopback traffic is configured	5	Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).
Ensure audit log storage size is configured	5	Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.
Ensure system is disabled when audit logs are full	5	The auditd daemon can be configured to halt the system when the audit logs are full.
Ensure audit logs are not automatically deleted	5	The max_log_file_action setting determines how to handle the audit log file reaching the max file size. A value of keep_logs will rotate the logs but never delete old logs.
Ensure events that modify date and time information are collected	5	Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier "time-change"
Ensure rsyslog default file permissions configured	5	rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Top n checks Hardening: Top number most frequent failed checks by category

Top n checks

Id	Category	Total Failed
1	Inventory and Control of Enterprise Assets	991
5	Account Management	777

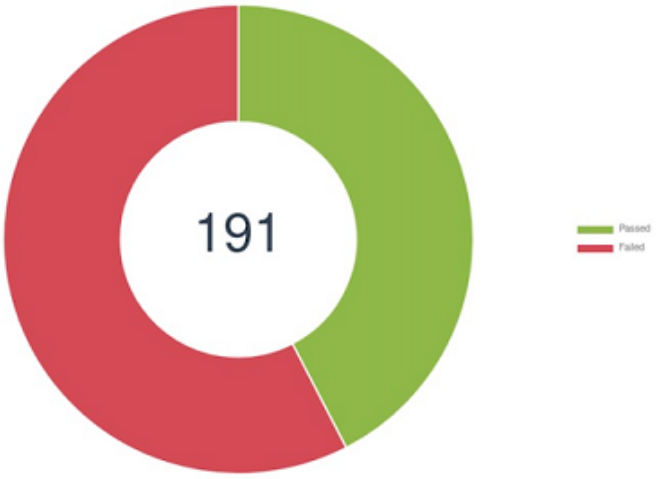
PANDORAFMS ENTERPRISE

Test

Top n checks

Id	Category	Total Failed
4	Secure Configuration of Enterprise Assets and Software	422
3	Data Protection	403
6	Access Control Management	328
2	Inventory and Control of Software Assets	261
9	Email and Web Browser Protections	104
8	Audit Log Management	45
7	Continuous Vulnerability Management	44

Vulnerabilities Hardening: Vulnerabilities of Access Control Management



List of checks Hardening: Checks of agent DESKTOP-UUKUE87 *September 21, 2023, 11:25 am*

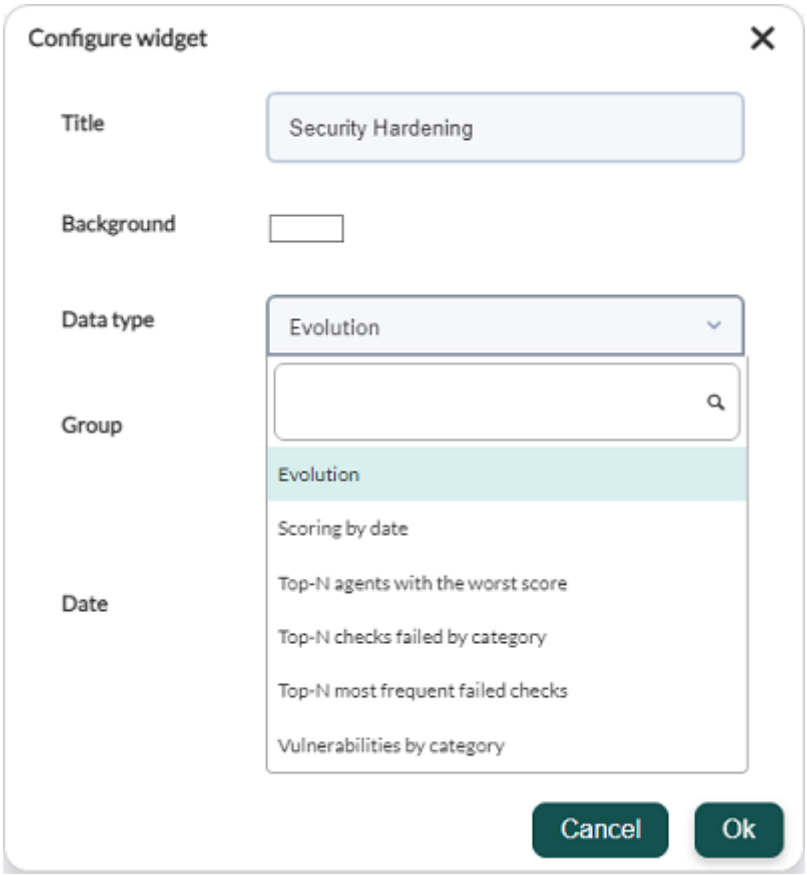
List of checks

Id	Title	Category	Status
12522	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
13521	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
12022	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
11522	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
13022	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
24533	Ensure 'EXECUTE' is revoked from 'PUBLIC' on File System Packages.	Access Control Management	Skiped
24536	Ensure 'EXECUTE' is revoked from 'PUBLIC' on Job Scheduler Packages.	Access Control Management	Skiped
24561	Ensure the 'USER' Audit Option Is Enabled.	Access Control Management	Skiped
24562	Ensure the 'ROLE' Audit Option Is Enabled.	Access Control Management	Skiped
24563	Ensure the 'SYSTEM GRANT' Audit Option Is Enabled.	Access Control Management	Skiped
24564	Ensure the 'PROFILE' Audit Option Is Enabled.	Access Control Management	Skiped
24565	Ensure the 'DATABASE LINK' Audit Option Is Enabled.	Access Control Management	Skiped
24566	Ensure the 'PUBLIC DATABASE LINK' Audit Option Is Enabled.	Access Control Management	Skiped
24567	Ensure the 'PUBLIC SYNONYM' Audit Option Is Enabled.	Access Control Management	Skiped

Dashboard de hardening

Un nuevo *widget* en los Dashboard de Pandora FMS agrupa la mayoría de informes de *hardening*:

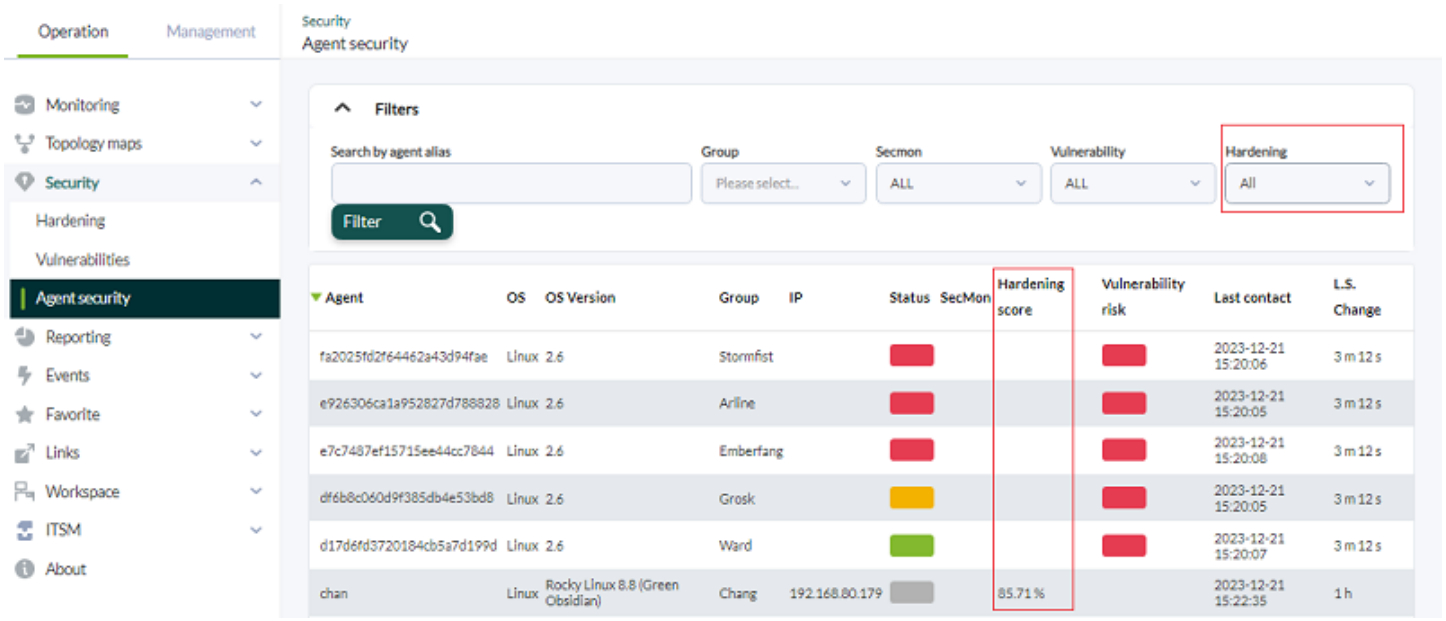
Opciones de configuración:



Vista de seguridad de los agentes

Menú Operation → Security → Agent security.

En la vista de seguridad de los agentes, columna Hardening, se podrá observar la puntuación de cada agente, entre otros datos. Se puede filtrar por porcentaje de puntuación de *hardening* e incluir otros campos adicionales. Para mostrar los agentes sin puntuación de *hardening* se utiliza la opción All.



Volver al índice de documentación de Pandora FMS