Hardening

Hardening

Hardening monitoring

The recommendations of the Center for Internet Security (CIS) have been merged with Pandora FMS monitoring technology to offer an integrated assurance audit system. This allows the evolution of hardening measures (security strengthening) to be tracked and evaluated over time in the environments used and monitored.

System hardening is a process used to improve the security of a computer system by reducing its attack surface and strengthening its defenses. It consists of making it more difficult for potential attackers to explore configuration errors, whether due to default configurations, bad configurations or improper configurations.

System hardening is an ongoing process as security threats and vulnerabilities evolve over time. It requires constant monitoring, risk assessments, and adjustments to security configurations to adapt to changing circumstances. Additionally, organizations often follow industry-specific standards and best practices, such as CIS controls or National Institute of Standards and Technology (NIST) guidelines, to ensure integral hardening system.

Pandora FMS uses several CIS categories to group the checks it performs.

CIS Categories Audited by Pandora FMS

We have taken the CIS recommendations a step further by implementing more than 1,500 individual checks across a variety of safety-critical categories.

Inventory and control of hardware and software assets: Monitor and manage all devices and software in your organization. Maintain an up-to-date inventory of your technology assets and use authentication to block unauthorized processes.

Device inventory and control: Identify and manage your hardware devices so that only authorized ones have access, blocking others. Maintaining proper inventory minimizes internal risks, organizes your environment, and provides clarity to your network.

Vulnerability Management: Analyze your assets continuously over time to detect potential vulnerabilities and fix them before they become the gateway to an attack. Strengthen network security by ensuring that software and operating systems in the organization are always up-to-date with the latest security measures and patches. Help manage your software to ensure that

only authorized software is installed and running. Avoid vulnerabilities and risks by maintaining accurate inventory and managing your software.

Controlled use of administrative privileges: Closely monitor access controls and the behavior of users with privileged accounts to prevent any unauthorized access to critical systems. Ensure that only authorized people have the appropriate privileges to avoid any misuse of administrative privileges. Establish strict policies to prevent misuse of privileges.

Secure hardware and software configuration: Establish and maintain security configurations based on standards approved by your organization. Create a rigorous configuration management system that detects and alerts about any bad configuration, and establishes a change control process to prevent attackers from exploiting vulnerable services and configurations.

Log and audit log maintenance, monitoring, and analysis: Collect, manage, and analyze event audit logs to identify potential anomalies. Maintain detailed logs to fully understand attacks and respond effectively to security incidents.

Malware Defenses: Monitor and control the installation and execution of malicious code at different points in your organization to prevent attacks. Configure and use anti-malware software and leverage automation to ensure fast defense updates and prompt corrective action in the event of attacks.

Email and Web Browser Protection: Protect and manage your web browsers and email systems from online threats to reduce your attack surface. Disable unauthorized email plugins and ensure that users only access trusted websites using web-based URL filters. Keep common entry doors safe from attacks.

Data recovery capabilities: Establish processes and tools to ensure your organization's critical information is properly backed up. Ensure you have a reliable data recovery system to restore information in the event of attacks that compromise critical data. Prepare your organization to deal with data loss effectively.

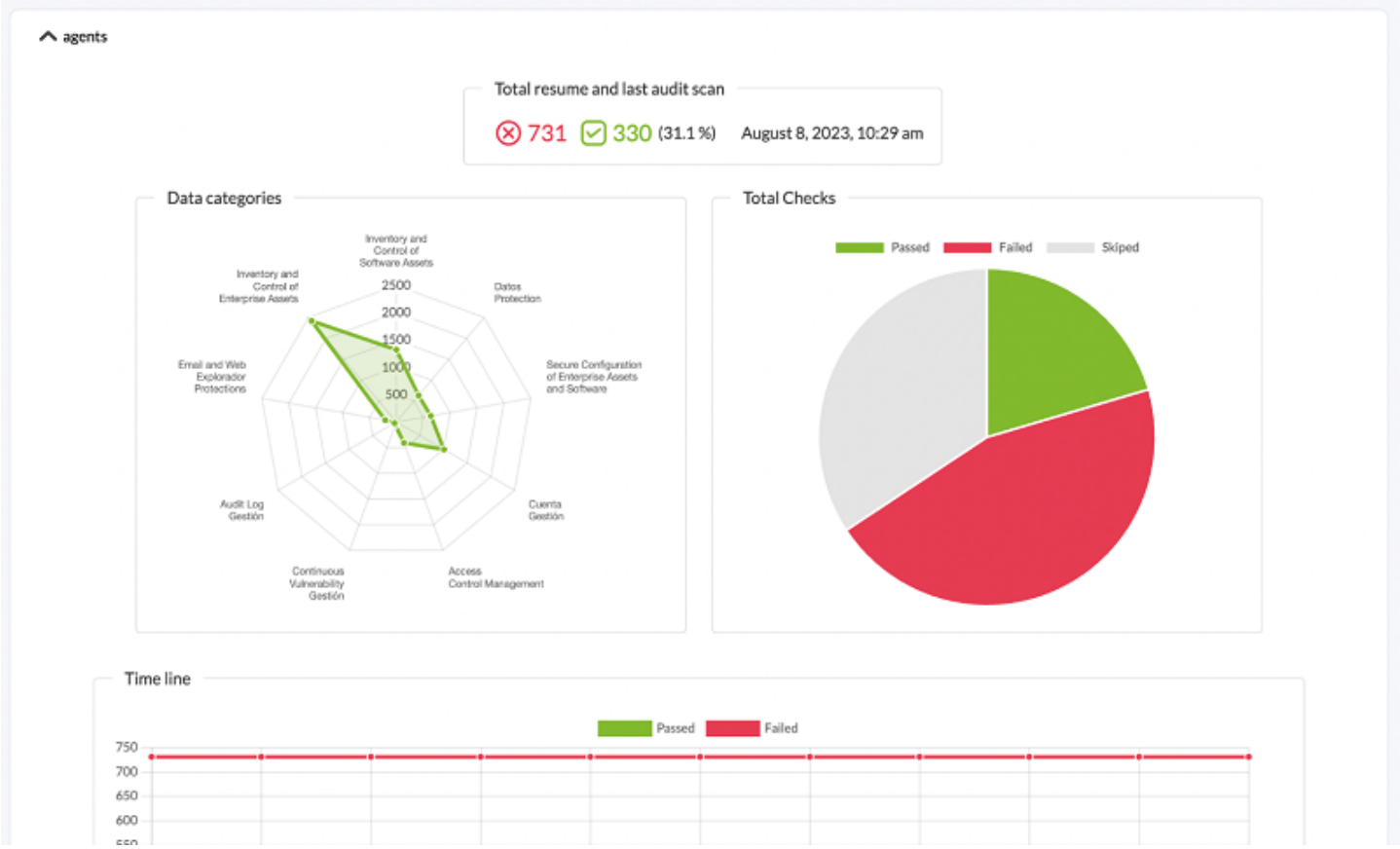
Boundary defense and data protection: Identify and separate sensitive data, and establish a series of processes that include encryption, data infiltration protection plans, and data loss prevention techniques. Establish strong barriers to prevent unauthorized access.

Monitoring and Account Control: Closely monitors the entire life cycle of your systems and application accounts, from creation to deletion, usage and inactivity. This active management prevents attackers from exploiting legitimate but inactive user accounts for malicious purposes and allows you to maintain constant control over the accounts and their activities.

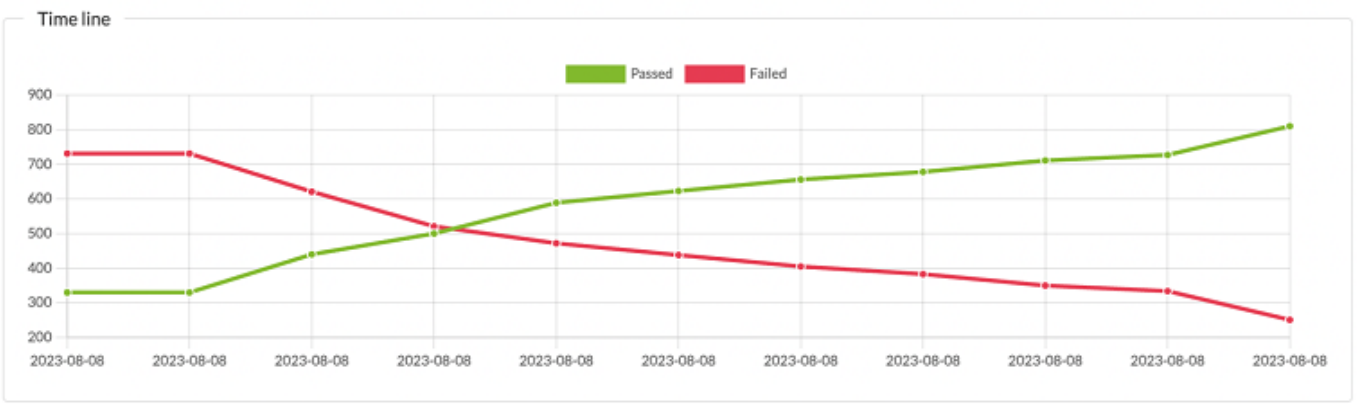
Detailed hardening audits of each machine

The checks are performed by the EndPoint that runs on each machine. Usually an audit takes place every week, but that period can be set to a longer period, such as a month. That way you can take a snapshot of the security of the system, calculate and assign a security index (a numerical rating, defined as the percentage of checks carried out and approved versus checks that do not pass the tests) and see the evolution of that safety index over time.

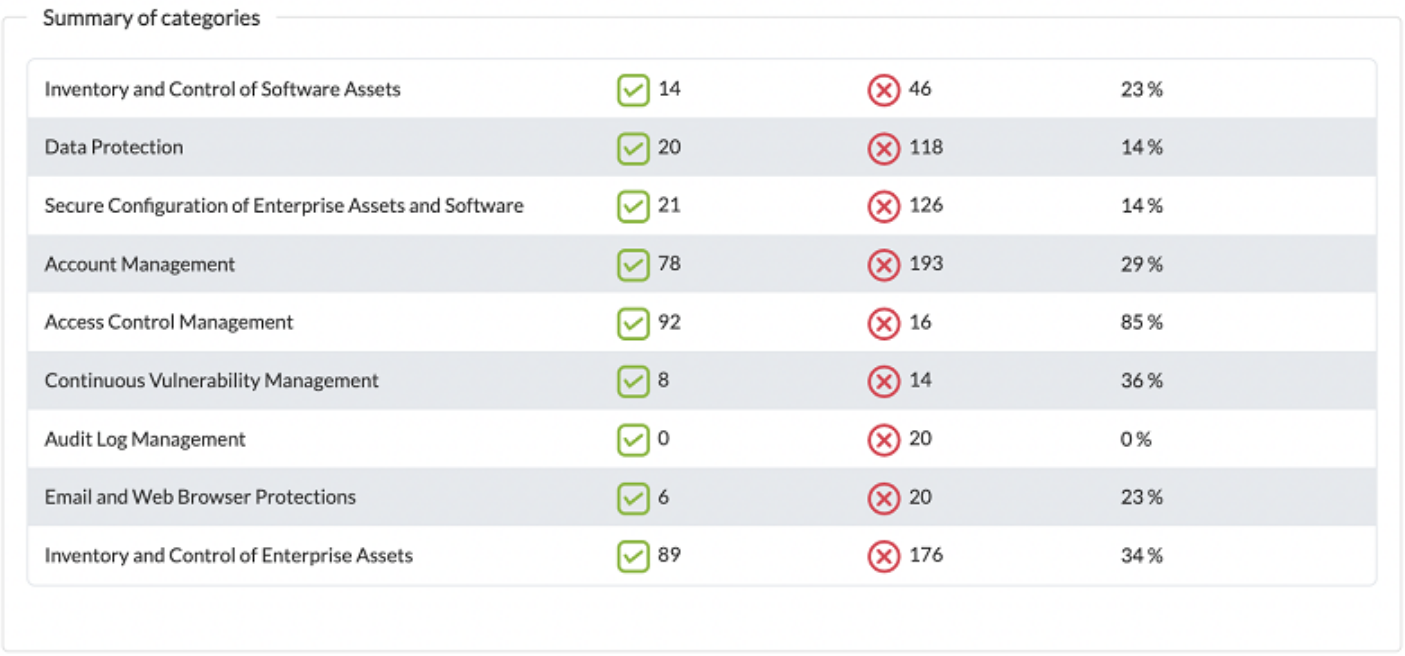
Example of a “snapshot” of the hardening status of a system:



Example of the evolution of hardening of a system over time:



The system allows us to see, broken down by category, the checks that have been executed:


Summary of categories

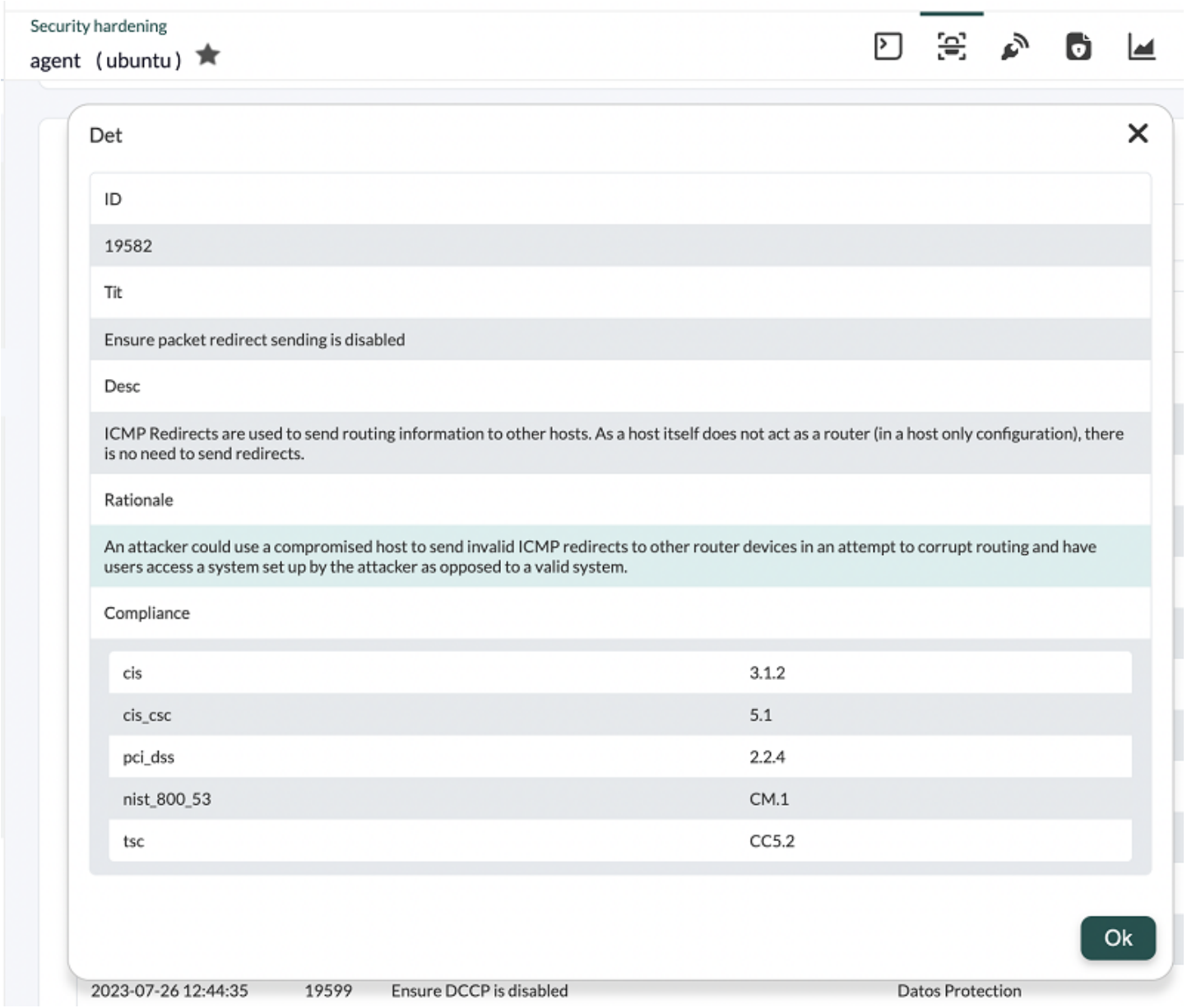
Inventory and Control of Software Assets	14	46	23 %
Data Protection	20	118	14 %
Secure Configuration of Enterprise Assets and Software	21	126	14 %
Account Management	78	193	29 %
Access Control Management	92	16	85 %
Continuous Vulnerability Management	8	14	36 %
Audit Log Management	0	20	0 %
Email and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

And for each group of elements, see the detail, to be able to work on its correction:

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		



Hardening monitoring configuration

Controls have been developed, depending on each system if applicable, that will help determine if they are relevant for the environment to be monitored. Currently this feature is available for MS Windows® and Linux® servers.

This feature is available with 773 EndPoints or later. If the EndPoints belong to a version prior to 773, they must be updated.

For that, activate the corresponding plugin in the EndPoint configuration. It can be done manually or through monitoring policies on machine groups.

On 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
```

In these examples, the hardening audit will be executed every 7 days, with a timeout of 150 seconds for each command launched during the audit. You may increase this value to 30 days, but we do not recommend doing it every few days, as it will generate unnecessary inventory data.

Hardening data monitoring

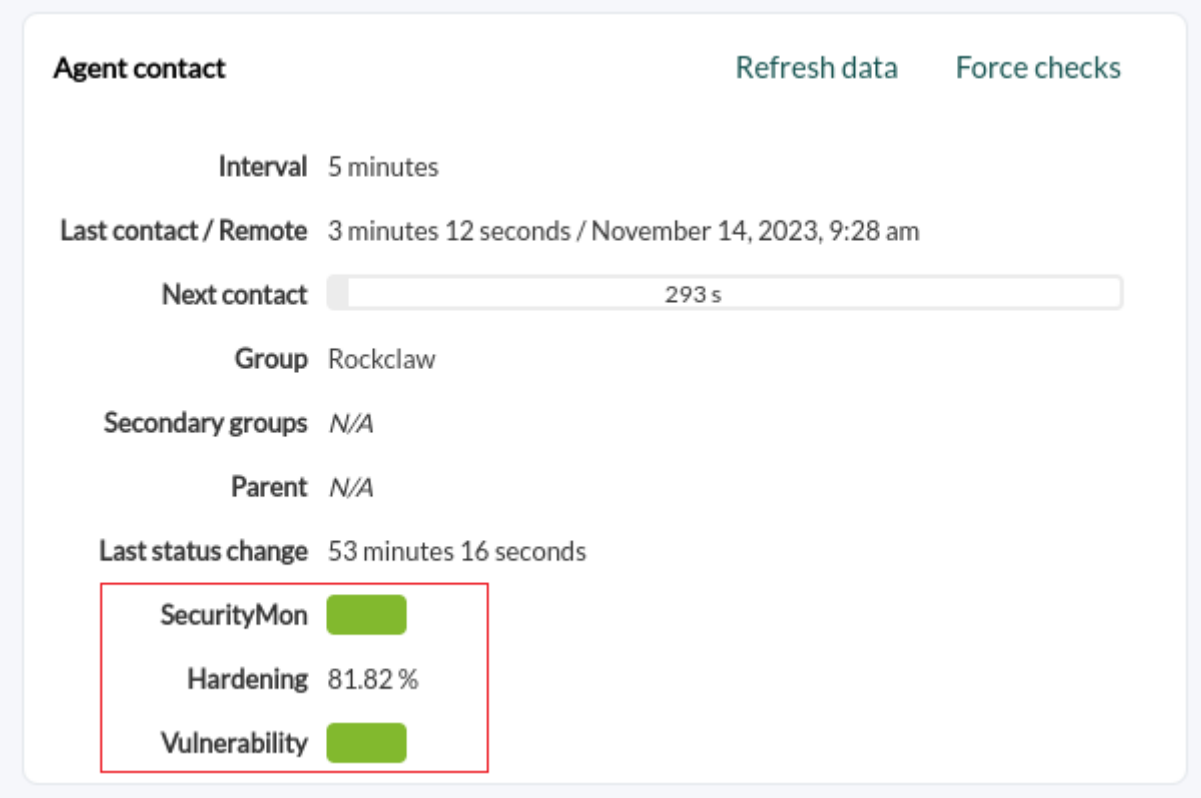
In addition to the dashboard and specific views to be able to analyze this data in specific systems or at a global level, there are some modules generated by the hardening system that will allow the hardening evaluation data to be processed like other Pandora FMS data, to establish alerts, generate graphics or any other use that is needed. These modules are generated or updated automatically each time a hardening audit is run and belong to the Module group called Security.

- Hardening - Failed checks: It shows the total number of checks that did not pass the securing test.
- Hardening - Not applied checks: It shows the total number of checks that were not run because they do not apply (for example, checks for another version of your Linux distribution or Windows version, or because they look for a certain component that is not installed).
- Hardening - Passed checks: It shows the total number of checks that passed the securing test.
- Hardening - Score: It shows the percentage of checks that passed. A threshold can be set here to show when the system is in `Warning` or `Critical` state regarding securing.

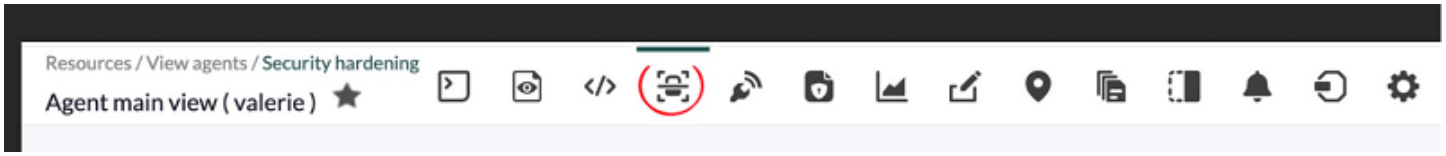
Hardening - Failed checks	Number of failed checks across policies.		N/A - N/A	2
Hardening - Not applied checks	Number of checks that did not apply across policies.		N/A - N/A	192
Hardening - Passed checks	Number of passed checks across policies.		N/A - N/A	10
Hardening - Score	% of passed checks (0 to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

Hardening data display

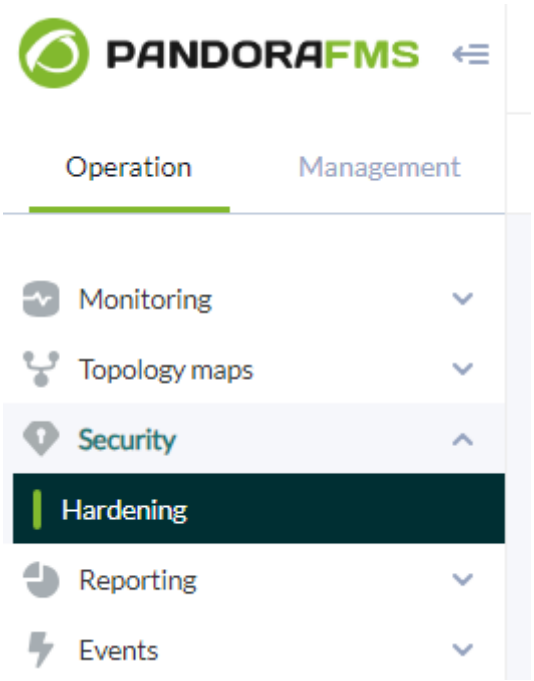
Once the EndPoints run the hardening module for the first time, the information will arrive and you may see in the detail of each EndPoint (Operation → Monitoring views → Agent detail → Agent main view) in the Agent Contact box three elements summarizing the security status (SecurityMon, hovering the pointer over it will show the number of security modules), the security percentage achieved (Hardening) and the vulnerability status (Vulnerability, hovering the pointer over it will show the score achieved):

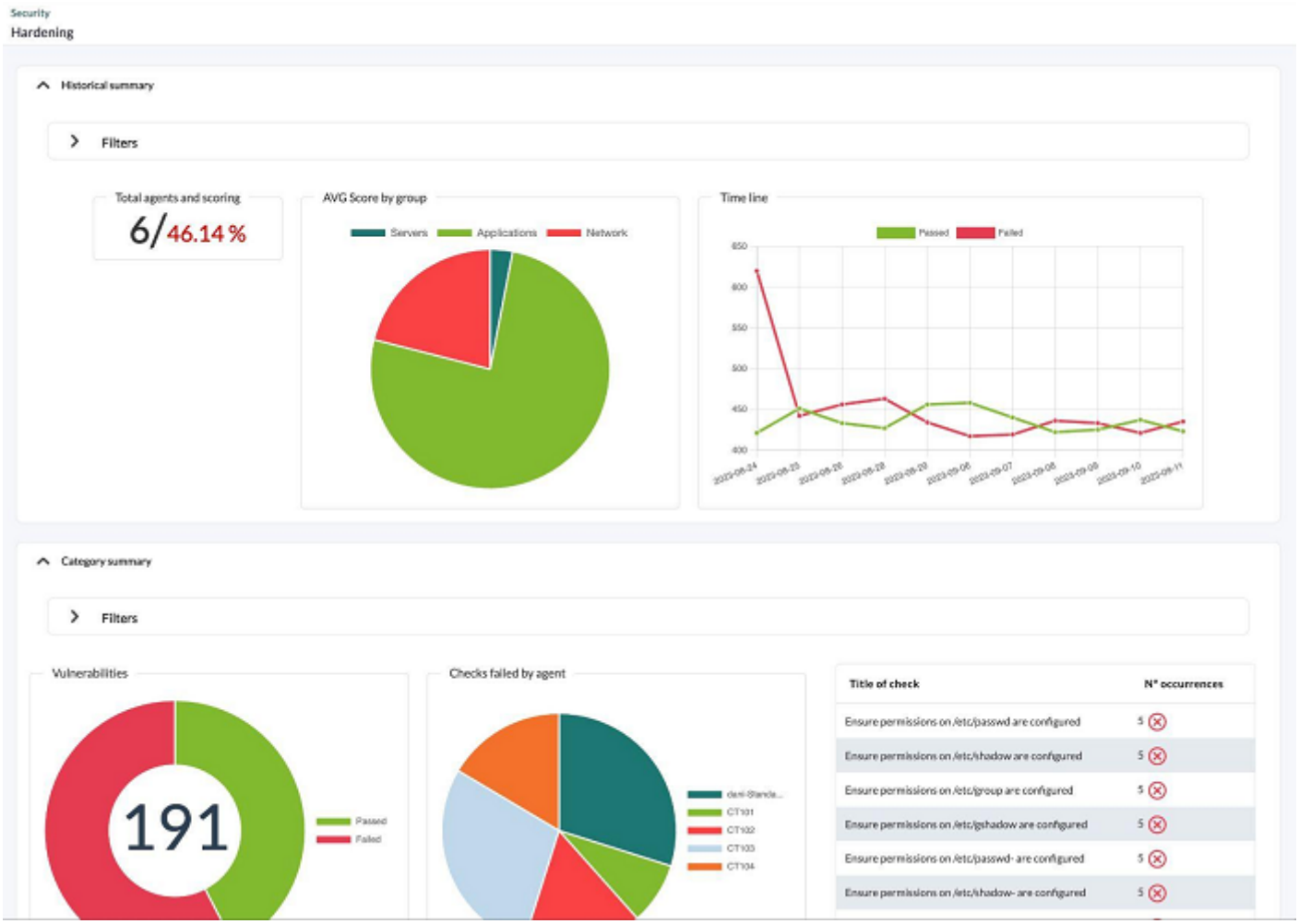


A specific section will also be enabled for the hardening of these agents:



In addition, you will be able to see a section in the operation menu called Security, where there is a specific dashboard for Hardening data where you may filter by groups, agents, CIS categories and other details.





Hardening reports

New report types have been created to display hardening information:

- Top N agents with the worst score. Filtered by groups.
- Top N of checkups that fail most frequently. Filtered by groups.
- Pie chart with Vulnerabilities by type. Choosing a CIS category, the fails, passed and skipped (optional) of all agents are grouped (or only the group selected) by category.
- Top N of checks that fail by category, the latest data from all agents (or only the selected group) is grouped by hardening categories and the categories with the highest number of fails among all agents are listed.
- List of security checks is a technical and exhaustive report with all the details, the latest checks of an agent are listed, filtered by group, category and status.
- Scoring, the latest scoring of the agents of the selected group or of all within the time range selected in the default filter of the reports is shown. The last scoring of each agent within the temporal range is always taken, that is, if a range of one month is set, the last scoring of the agents within that month will be searched.
- Evolution, a global evolution of hardening is shown by averaging the tests that passed and those that failed, grouped by day, for all agents or those within the selected group.

Here are some examples of PDF reports:

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

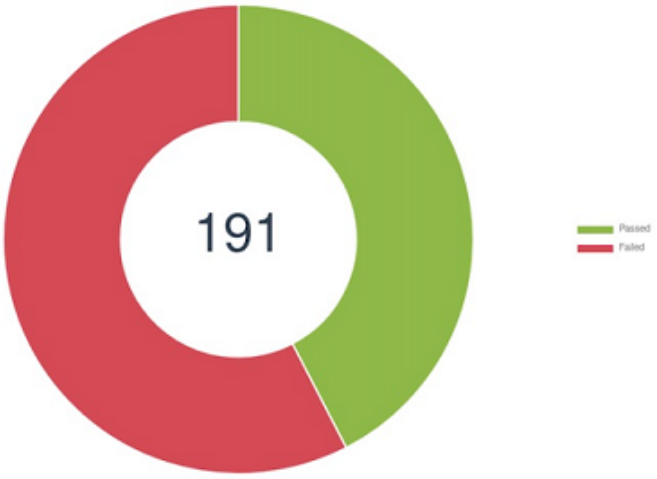
PANDORAFMS ENTERPRISE

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*

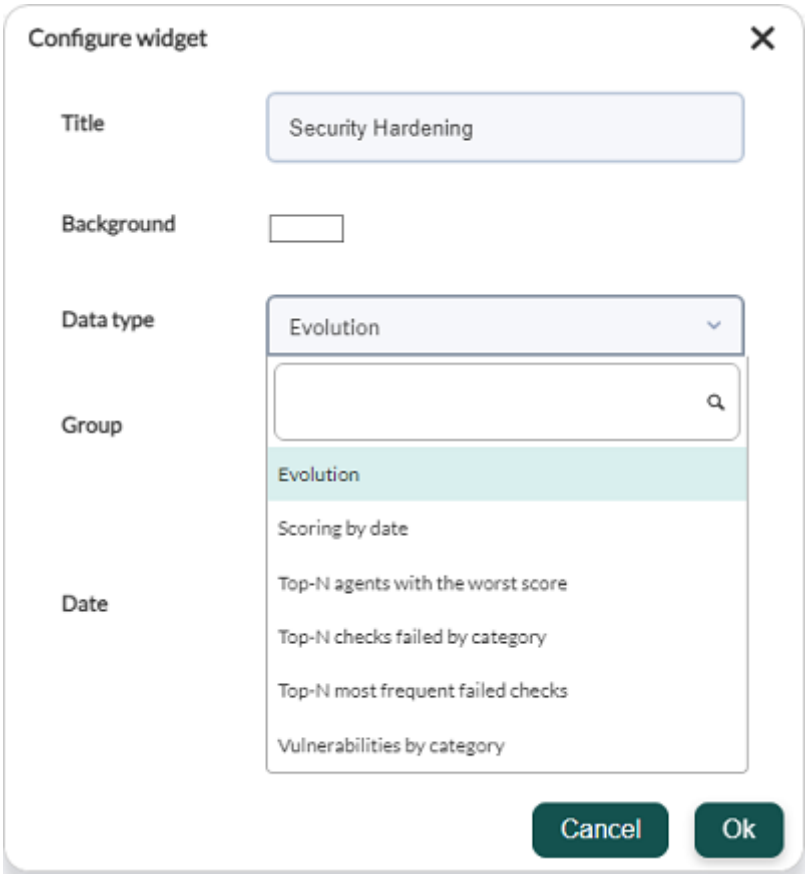
List of checks

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

Hardening Dashboard

A new widget in the Pandora FMS Dashboard groups most hardening reports:

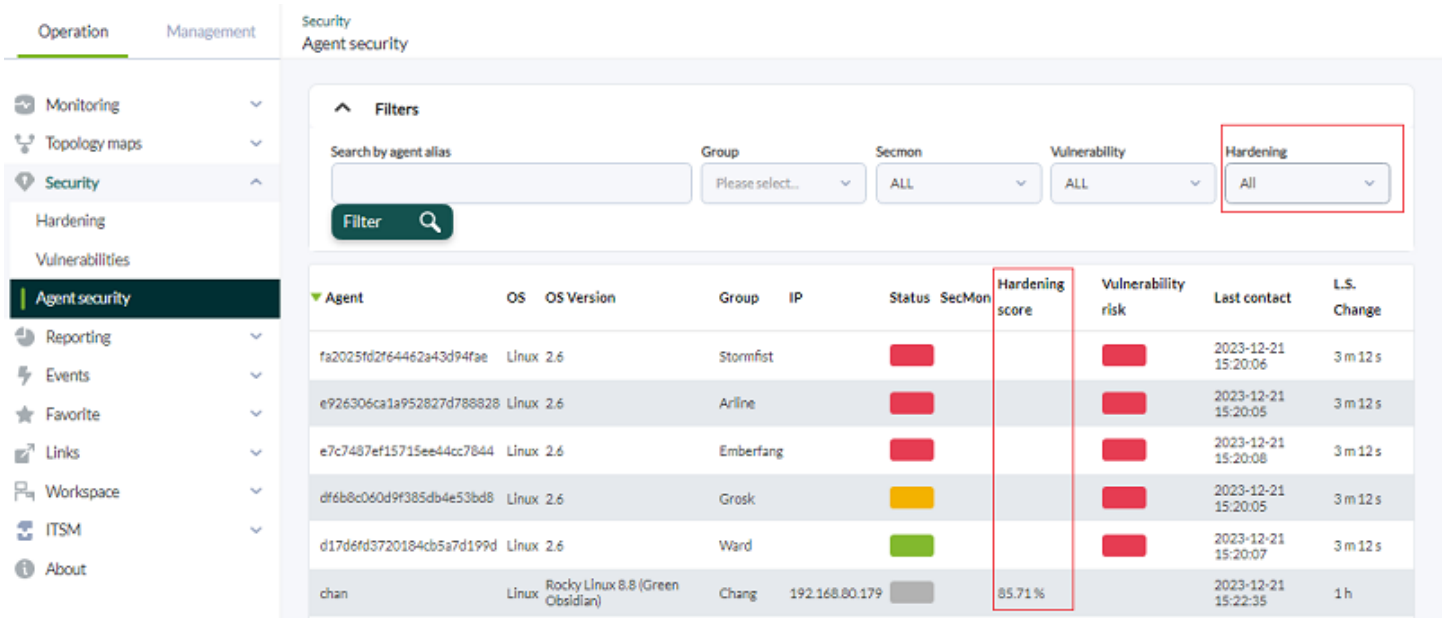
Configuration options:



Security view of the agents

Operation → Security → Agent security menu.

In the agents' security view, Hardening column, you will be able to see the score of each agent, among other data. You may filter by hardening score percentage and include other additional fields. To show the agents without hardening score, use the All option.



Return to Pandora FMS documentation index