info@wazuh.com
https://wazuh.com

File integrity monitoring report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	victima-windows	192.168.1.73	Wazuh v4.9.1	instance-20241026-022758	Microsoft Windows 10 Pro 10.0.19041.450	Oct 28, 2024 @ 03:39:10.000	Nov 5, 2024 @ 17:55:26.000

Group: default

Alerts related to file changes, including permissions, content, ownership and attributes.

2024-11-04T10:00:00 to 2024-11-04T23:00:00

manager.name: instance-20241026-022758 AND rule.groups: syscheck AND agent.id: 002

File integrity monitoring scan is currently in progress for this agent (started on 2024-11-05T17:55:09+00:00).

Last 10 deleted files

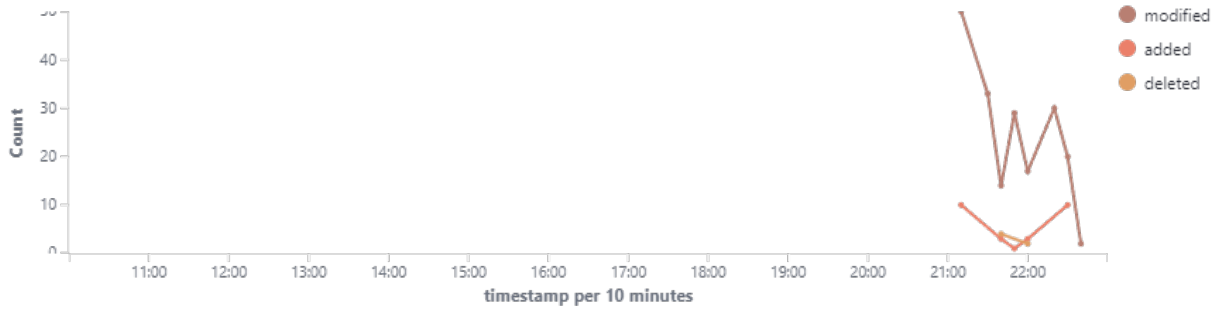
Path	Date
c:\users\sears\documents\textito.txt	2024-11-05T04:00:32.472Z
c:\users\sears\documents\pdfcito.pdf	2024-11-05T04:00:32.353Z
c:\users\sears\documents\nuevo documento de texto.txt	2024-11-05T03:49:19.455Z
c:\users\sears\documents\pdfcito.pingu	2024-11-05T03:47:48.583Z
c:\users\sears\documents\piplup.pingu	2024-11-05T03:47:48.583Z
c:\users\sears\documents\textito.pingu	2024-11-05T03:47:48.482Z

Last 10 modified files

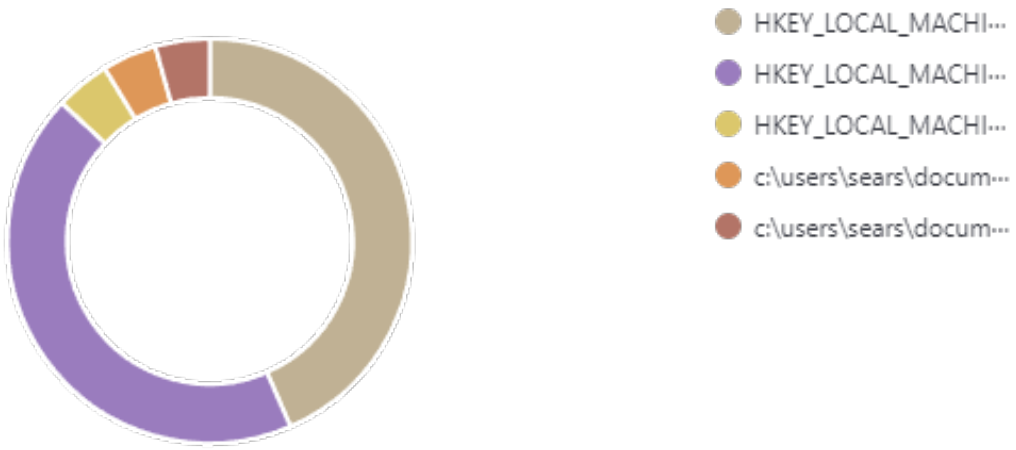
Path	Date
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1722412146-1496493419-2419464286-1001	2024-11-05T04:41:39.451Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	2024-11-05T04:38:50.027Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	2024-11-05T04:38:49.963Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services	2024-11-05T04:37:21.010Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters	2024-11-05T04:28:04.743Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	2024-11-05T04:28:04.671Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{888283b4-	2024-11-05T04:28:04.411Z

Path	Date
d781-48c7-bf3c-07404d912de8}	
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch	2024-11-05T04:28:02.137Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch2	2024-11-05T04:28:02.137Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\dam\PowerEvents	2024-11-05T04:27:51.202Z

Events



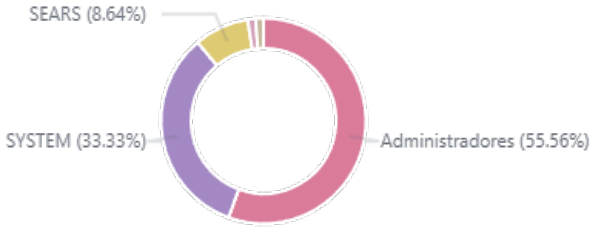
Files added



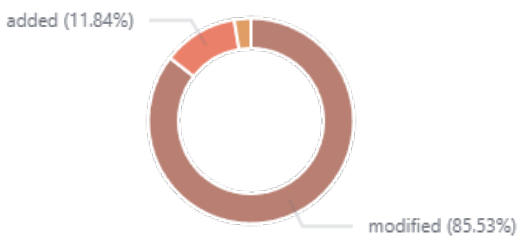
Files modified

Files deleted

Most active users



Actions



Alerts summary

Path	Description
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1722412146-1496493419-2419464286-1001	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1722412146-1496493419-2419464286-1001	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\dam\PowerEvents	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\GoogleUpdaterInternalService131.0.6776.2	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\GoogleUpdaterService131.0.6776.2	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	Registry Key Integrity Checksum

Path	Description
	Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\dam\PowerEvents	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch2	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch2	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1722412146-1496493419-2419464286-1001	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\GoogleUpdaterInternalService131.0.6776.2	Registry Key Entry Added to the System

Path	Description
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\GoogleUpdaterService131.0.6776.2	Registry Key Entry Added to the System
c:\users\sears\documents\textito.txt	File added to the system.
c:\users\sears\documents\textito.txt	File deleted.
c:\users\sears\documents\textito.txt	Integrity checksum changed.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ACPI\Parameters\WakeUp	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ACPI\Parameters\WakeUp	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18	Registry Value Integrity Checksum Changed
c:\users\sears\documents\nuevo documento de texto.txt	File added to the system.
c:\users\sears\documents\nuevo documento de texto.txt	File deleted.
c:\users\sears\documents\pdfcito.pdf	File added to the system.
c:\users\sears\documents\pdfcito.pdf	File deleted.
c:\users\sears\documents\pdfcito.pingu	File added to the system.
c:\users\sears\documents\pdfcito.pingu	File deleted.
c:\users\sears\documents\piplup.pingu	File added to the system.
c:\users\sears\documents\piplup.pingu	File deleted.
c:\users\sears\documents\textito.pingu	File added

Path	Description
	to the system.
c:\users\sears\documents\textito.pingu	File deleted.