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 @ 17:53:25.000

Group: default

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

🕘 2024-11-04T09:00:00 to 2024-11-04T22:00:00

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

Last file integrity monitoring scan was executed from 2024-11-05T17:52:07+00:00 to 2024-11-05T17:52:37+00:00.

Last 10 deleted files

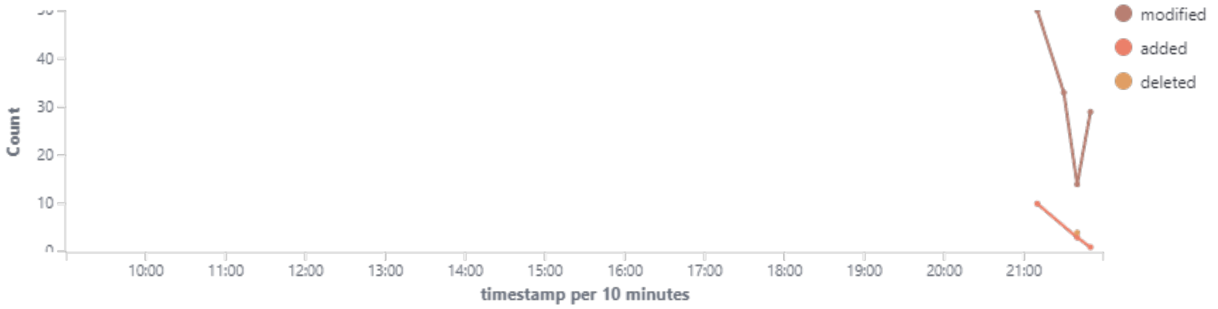
Path	Date
c:\users\sears\documents\nuevo documento de texto.txt	2024-11-05T03:49:19.455Z
c:\users\sears\documents\pdfcito.pingu	2024-11-05T03:47:48.583Z
c:\users\sears\documents\piplup.pingu	2024-11-05T03:47:48.583Z
c:\users\sears\documents\textito.pingu	2024-11-05T03:47:48.482Z

Last 10 modified files

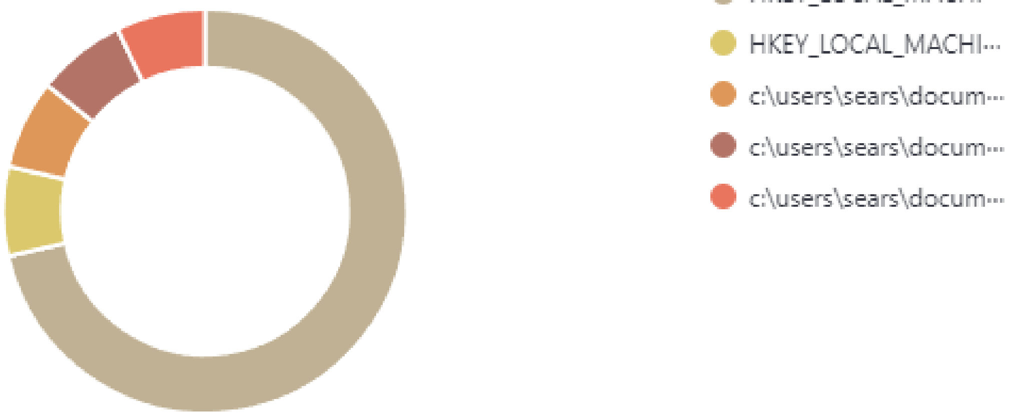
Path	Date
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	2024-11-05T03:57:49.368Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	2024-11-05T03:57:49.309Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1722412146-1496493419-2419464286-1001	2024-11-05T03:57:34.962Z
c:\users\sears\documents\textito.txt	2024-11-05T03:49:30.983Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters	2024-11-05T03:36:49.026Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	2024-11-05T03:36:48.965Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	2024-11-05T03:36:48.714Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch	2024-11-05T03:36:45.917Z

Path	Date
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Epoch2	2024-11-05T03:36:45.917Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\dam\PowerEvents	2024-11-05T03:36:33.967Z

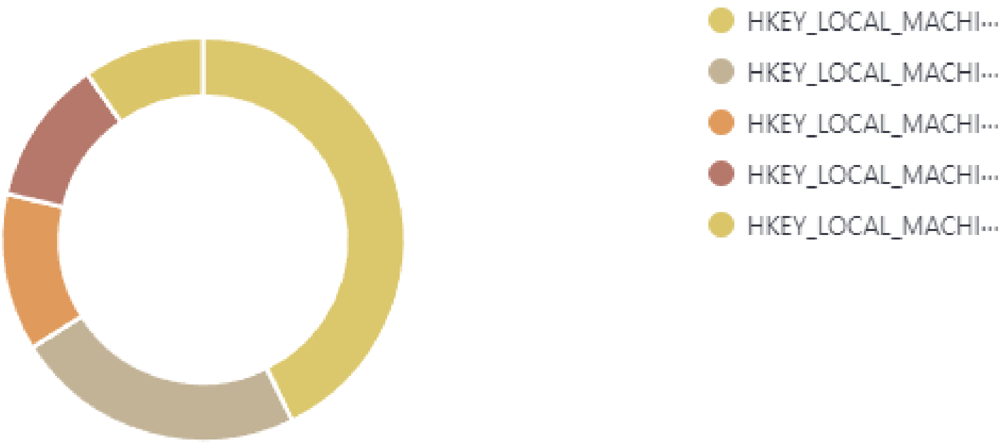
Events



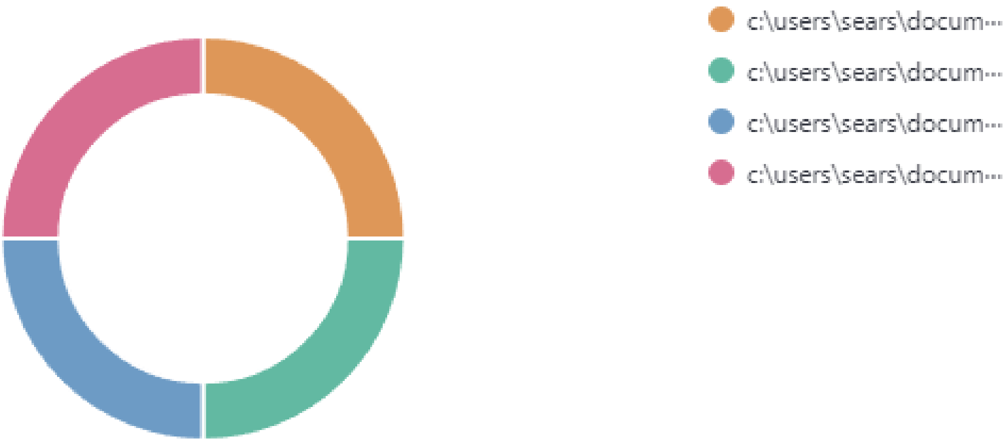
Files added



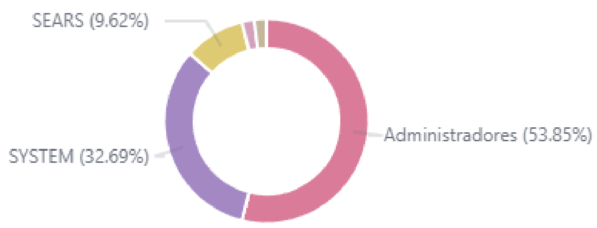
Files modified



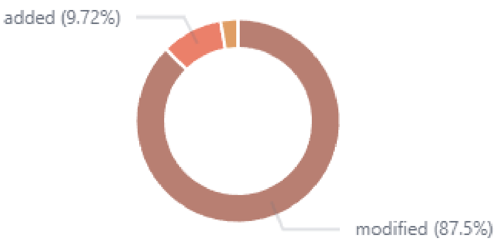
Files deleted



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\GoogleUpdaterInternalService131.0.6776.2	Registry Value Entry Added to the System
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\Tcpip\Parameters\Interfaces\{888283b4-d781-48c7-bf3c-07404d912de8}	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\dam\PowerEvents	Registry Key Integrity

Path	Description
	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\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
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

Path	Description
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\textito.txt	File added to the system.
c:\users\sears\documents\textito.txt	Integrity checksum changed.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ACPI\Parameters	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsActiveIfs	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsActiveIfs\INFINITUM3444_5_9	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NativeWifiP\State\Parameters\Adapters\{888283b4-d781-48c7-bf3c-07404d912de8}	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NativeWifiP\State\Parameters\Adapters\{888283b4-d781-48c7-bf3c-07404d912de8}\ExtSTAMib	Registry Key Integrity Checksum Changed
c:\users\sears\documents\pdfcito.pdf	File added to the system.