File integrity monitoring report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
003	Win10	192.168.2.101	Wazuh v4.11.2	mail.strayerraptors.com	Microsoft Windows 10 Education 10.0.19045.5796	May 2, 2025 @ 23:41:10.000	May 7, 2025 @ 21:59:30.000

Group: default

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

2025-05-06T21:59:37 to 2025-05-07T21:59:37

manager.name: mail.strayerraptors.com AND rule.groups: syscheck AND agent.id: 003

Last file integrity monitoring scan was executed from 2025-05-07T19:02:45+00:00 to 2025-05-07T19:04:14+00:00.

Last 10 deleted files

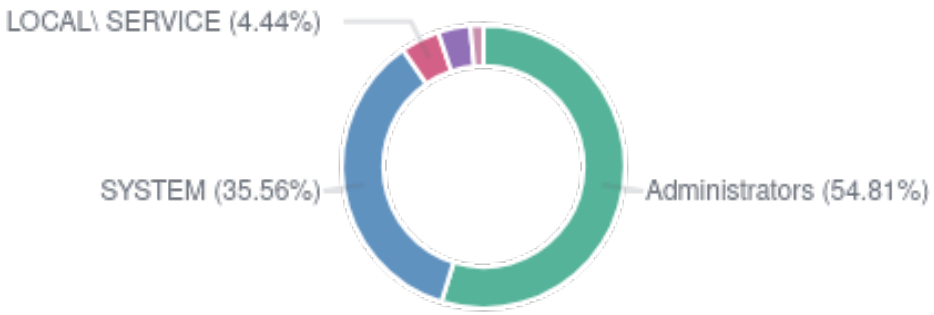
Path	Date
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter	2025-05-07T19:06:31.585Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	2025-05-07T19:06:31.585Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\BootTime\Filter	2025-05-07T19:05:50.451Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cbdhsvc_337879\Security	2025-05-07T02:44:19.162Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cbdhsvc_337879	2025-05-07T02:44:19.146Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WpnUserService_337879\Security	2025-05-07T02:44:19.131Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WpnUserService_337879	2025-05-07T02:44:19.115Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\UserDataSvc_337879\Security	2025-05-07T02:44:19.099Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\UnistoreSvc_337879	2025-05-07T02:44:19.084Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\UnistoreSvc_337879\Security	2025-05-07T02:44:19.084Z

Last 10 modified files

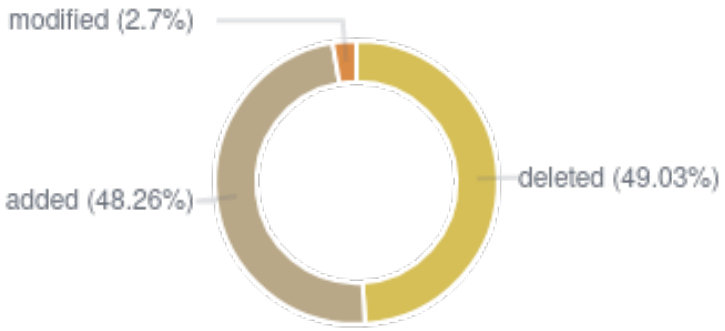
Path	Date
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	2025-05-07T19:03:49.173Z
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\VolatileUserMgrKey	2025-05-07T19:03:49.142Z
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\Win32kWPP\Parameters	2025-05-07T19:03:48.590Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services	2025-05-07T19:03:47.302Z

Path	Date
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	2025-05-07T19:03:45.711Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime	2025-05-07T19:03:45.642Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\Config	2025-05-07T19:03:45.595Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\Config\Status	2025-05-07T19:03:45.574Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{27ca38dd-e1d5-4f4e-b646-ca397da0893d}	2025-05-07T19:03:43.636Z
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{27ca38dd-e1d5-4f4e-b646-ca397da0893d}	2025-05-07T19:03:43.549Z

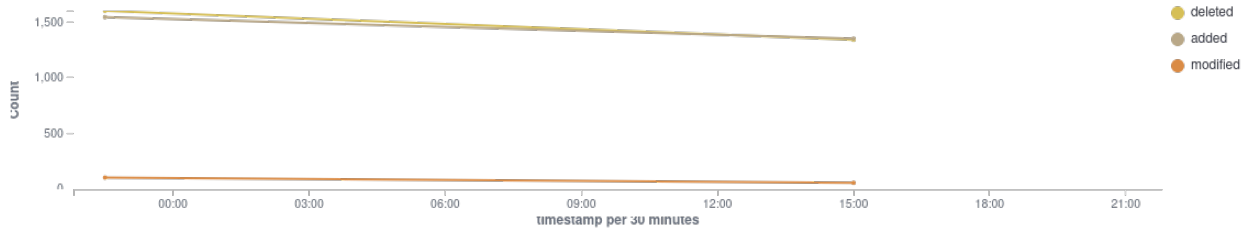
Most active users



Actions



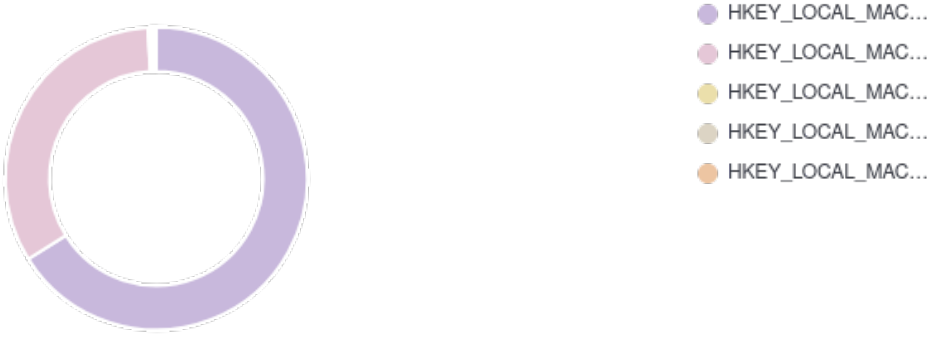
Events



Files added

Files modified

Files deleted



Alerts summary

Path	Description
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\BootTime\Filter	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\BootTime\Filter	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2339272666-3457689461-1411455609-1111	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{27ca38dd-e1d5-4f4e-b646-ca397da0893d}	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AarSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BcastDVRUserService_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDPUserSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ConsentUxUserSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CredentialEnrollmentManagerUserSvc_337879	Registry Value Entry Deleted.

Path	Description
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DeviceAssociationBrokerSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DevicePickerUserSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DevicesFlowUserSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MessagingService_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PrintWorkflowUserSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\UdkUserSvc_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WpnUserService_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CaptureService_337879	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2339272666-3457689461-1411455609-1111	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2339272666-3457689461-1411455609-1104	Registry Value Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2339272666-3457689461-1411455609-1104	Registry Value Entry Added to the System
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BFE\Parameters\Policy\BootTime\Filter	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\AppIso\FirewallRules	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2339272666-3457689461-1411455609-1111	Registry Key

Path	Description
	Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{27ca38dd-e1d5-4f4e-b646-ca397da0893d}	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules	Registry Value Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2339272666-3457689461-1411455609-1104	Registry Key Integrity Checksum Changed
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AarSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BcastDVRUserService_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDPUserSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ConsentUxUserSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CredentialEnrollmentManagerUserSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DeviceAssociationBrokerSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DevicePickerUserSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DevicesFlowUserSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MessagingService_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PrintWorkflowUserSvc_337879	Registry Key Entry Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\UdkUserSvc_337879	Registry Key Entry

Path	Description
	Deleted.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WpnUserService_337879	Registry Key Entry Deleted.