How **Snare** helps with FIM, FAM, RIM and RAM

snare

Contents

How Snare helps with FIM, FAM, RIM and RAM

This document is designed to assist a systems / security administrator with managing the File Integrity Monitoring (FIM), File Activity Monitoring (FAM), Registry Integrity Monitoring (RIM) and Registry Activity Monitoring (RAM) with Snare Enterprise Agents, Snare Central Server, Snare Advanced Analytics and Snare Advanced Threat Intelligence.

FIM, FAM, RIM and RAM General Overview

For many years systems have used various third-party software to monitor the systems files and data. Third party software features to perform a checksum on a selected group of files and directories has been one method to track file changes. This has been known as File Integrity Monitoring also known as FIM.

This software would keep a master database repository of the checksum data of the selected files and directories store and keep the log information locally or send the data to a central server. It would then run periodic checks of all the files again to compare the current state to the master copy or baseline of information. These software checks would typically be performed once a week or daily depending on the business needs. The principal behind the checksum approach was to detect a change to a file or directory, this would then trigger an alert and report to administrator to highlight the file or contents of a directory had changed from the master copy. The report would show the details of the file including the change time, file size, or owner information along with the before and after details. The administrator would then have to determine who, how and what data had actually changed, if it was of concern and if any action was required. The Who, What and How questions are answered by using File Activity Monitoring or FAM. These events will track all the user based activity performed on the system that traditional FIM can't do.

While the traditional FIM solutions are very good for detecting that a change has occurred they are limited and don't allow the administrator to know who did the change, how many times they changed the files and what they used to make the change. This is where FAM or File Activity Monitoring compliments the traditional FIM solutions.

The Snare Enterprise agents for Windows, Linux, OSX and Solaris have the ability to monitor all file-based activity and provide a much greater depth of information than traditional FIM solutions. The reporting ability of the Enterprise agents includes all read, write, change and delete activity on a file or directory. The Snare Enterprise agents can track and report on these changes in near real time. If unauthorised activity is occurring the events are captured and sent to the central SIEM system as they are occurring.

These events can then be processed, and real time alerts initiated to warn security staff that changes are occurring on sensitive files or data. If the SIEM system is the Snare Central Server or Snare Advanced Analytics, then it can generate these alerts as the events are received or be based on specific threshold levels before being reported on. The events provide much greater detail than traditional FIM solutions in that it will show the specific userid, commands used to change or view the file (ie text editor, script, programs that was run). If they were to make multiple changes to the file, each instance of the change is recorded logged and sent to the central SIEM system and provides more detail than when, compared to only a single summary that a change occurred with traditional FIM solutions. Additionally, the Snare Enterprise agent will also report on any attempted access to files or directories that were not successful as failure events. This can also capture potential malicious activity on systems and may give early warning to a potential data breach.

For customers that also require the specific feature of FIM capability the all of our current v5 agents support the checksum (SHA512) feature for monitoring files, directories, and on Windows platforms, the registry keys. The agents will report on all changes, additions and deletes of files or registry keys, along with the relevant file systems permissions and file ownership changes. The full delta of the changes can be tracked with both the before baseline details and the state after any changes being reported on. This data can also be correlated with the FAM activity as detailed above to assist with any forensic investigation.

Why the need for FIM or FAM?

So why the need for file activity monitoring such as FIM and FAM? There can be many business reasons and can be a mixture of the following:

- Compliance such as PCI DSS for requirements 11.5 and 12.9 where it is a must for compliance activity
- Tracking changes for hacker or unauthorised activity
- Malware outbreaks for system changes. This can be useful for where there is a day zero vulnerability that normal malware detection does not block and the exploit allows access to the system, now the malware or hacker starts to make changes to gain additional privilege or plant Trojans on the network.
- Intruder detection where the hacker is gaining access to systems and making changes as they move laterally around the network. Knowing what they change and access is critical to any incident investigation and remediation activity.
- Data theft such as disgruntled employees copying data, changing data, or sending internal corporate information out of the network.

Monitoring of all types of files and user data

All critical files need to be monitored. The question is, though, what is critical?

Most staff can point to files that they can't lose or are very sensitive in nature that others should not see or tamper with. These can be any system files or user data such as:

- Operating system binary exe's, DLL files, configuration files and application registry keys
- Third party application binaries, DLL files, configuration files, and application registry keys, many vendors can advise on critical parts of their applications that should be monitored and the integrity of the data is paramount to its operation.
- User data files such as spreadsheets, text files, MS Word documents, PowerPoint files etc
- Sensitive documentation and files that should be restricted to staff that have a need to know.
- Application database files are generally not a good fit for FIM and FAM monitoring as they constantly change. Unless the application data files are generally static they are not a good candidate for monitoring.
- Log files for key systems, while some log files can be highly active, archived log files should never change as they are a record of what has occurred.

What systems should be monitored

Most systems will benefit from being monitored. The critical nature and value of the data that system contains is usually the key factor to help determine what should monitored. If management of the business, business operations or users can't live without the system or data then it's often critical. System such as:

- Domain Controllers
- Application Servers
- Database Servers
- Web Servers
- Key desktops that perform critical business functions for key staff.
- POS systems, these usually have a PCI DSS requirement to be monitored.
- All systems in scope for any PCI DSS network including servers and desktops.

The Snare Solution – Continuous Monitoring of Files

With the Snare file activity monitoring solution, you will collect the audit log data and can then be notified when files are created or key files are viewed, deleted, modified, or when user or group ownership is changed.

You can selectively monitor with granular controls and filters that can pinpoint specific files and either perform scans at desired intervals or operate in near real-time for continuous monitoring. Correlate file-level behaviour to enhance security and audit activities. Easily pivot from a file access or change to a specific user, then view a full timeline of user activity, containing both FIM, FAM, RIM or RAM along with other user activity information. With the Snare Enterprise agent policy-based FIM, FAM, RIM and RAM features, you can assign multiple policies to the same endpoint, reducing ongoing management overhead as policies are updated.

Policies can also be managed from our Agent Management Console (AMC). For example, individual policies can be created for Windows, Linux or MAC OSX operating system files and directories. Domain Controllers, Application Servers, File Servers, Web Application Servers, and DNS Servers. FIM and FAM multi-policy support simplifies management, ensuring that the policies are assigned to the appropriate system assets and that changes to those policies are centrally managed via the AMC and propagated across the environment.

In addition, using our Snare Advanced Threat Intelligence suite the FIM, FAM, RIM and RAM activity can be correlated and detect changes to systems outside of authorised change control windows when linked with the customers change tracking systems. Snare detects these changes by monitoring production servers for changes that occur outside normal operating windows which can be defined using our Key Performance Indicator (KPI) feature or changes that don't precede an authorised change request from the customers change tracking system. With the addition of this file monitoring features and the data it generates, Snare can monitor for and alert on a variety of malicious behaviours, from improper user access of confidential files to botnet-related breaches and transmittal of sensitive data as detailed above.

Easy to Deploy

Snare agents are easy to deploy

- Pre-configure your agent using your custom configurations including file policies for the operating systems you need. For Windows platforms using our smart MSI packing makes deployment easy and can be deployed using GPO, Microsoft SCCM and other software deployment tools.
- Simplified policy administration with the ability to assign multiple FIM, FAM, RIM and RAM policies to the same host so you can monitor different directories, specific files, and applications as needed
- Centralised Policy Management with the Snare Agent Management Console (AMC) for all v5 Snare agents
- Available for deployment on both desktops and servers

All of the Snare Enterprise agents support FAM and the latest v5.2.x agents all support FIM and on Windows RIM and RAM. There are several Snare Enterprise agents for different operating systems that include:

- Snare Enterprise Agent for Windows
- Snare Enterprise Agent for Linux
- Snare Enterprise Agent for Solaris
- Snare Enterprise Agent for OS X

To see the feature set of the Enterprise Agents, go to the Snare Solutions website at

https://www.snaresolutions.com/products/snare-agents/

The nest section of this document instructs users of the Snare Enterprise Agent on how to use it for FIM, FAM, RIM and RAM based on your operating system platform.

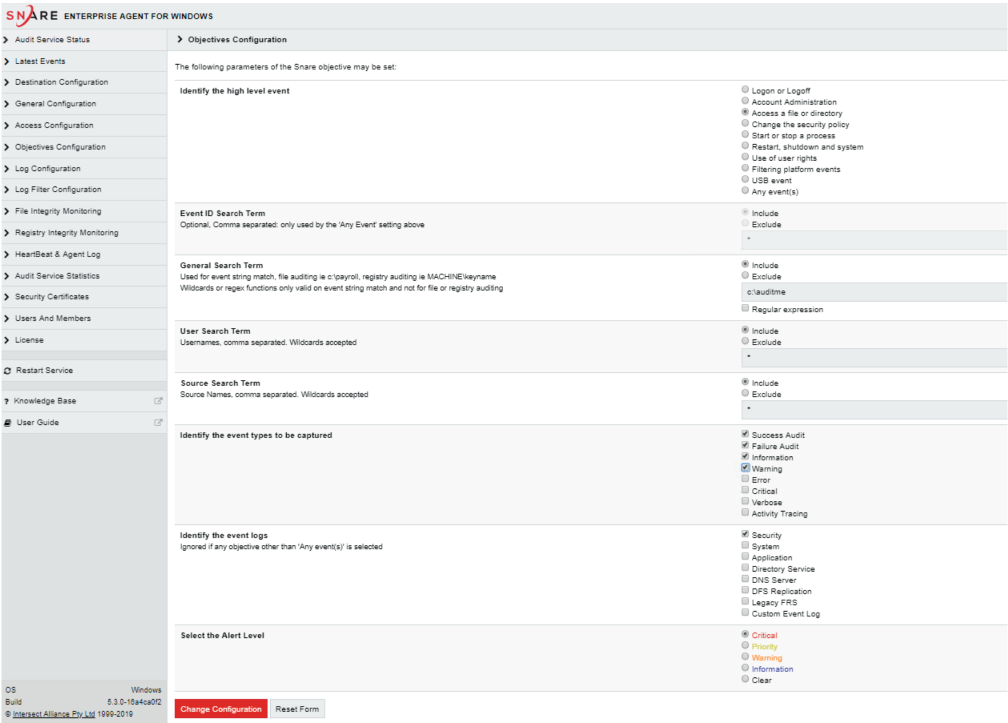
FIM, FAM, RIM and RAM Settings for Snare Enterprise Agent for Windows

To configure the Snare Enterprise Windows agent to perform File Integrity Monitoring (FIM), File Activity Monitoring (FAM), Registry Integrity Monitoring (RIM) and Registry Activity Monitoring (RAM) perform the following basic steps.

- Review the critical parts of the operating system and applications that need to be monitored. In general, there will be many files, directories and registry keys that need to be monitored. This should form your baseline or core monitoring
- Document the baseline of these parts of the system that need to be audited and monitored.
- Create Snare objectives in the agents to match the configuration that you documented. You may require different policies for different systems. You can use the Snare Agent Management Console to manage different polices on different systems based on operational needs.
- Ensure that all the systems have the correct date and time and are using NTP settings to keep accurate time.
- In the reporting system such as Snare Central or Snare Advanced Analytics ensure that the events are being monitored and alerts are configured to notify the relevant staff of the system changes.

The FAM and RAM features use the host operating systems audit function. For Windows this is driven by audit policy of the system. The events produced relate to the activity being performed which can include reads, changes, additions or deletions of files or registry keys. The Windows platform can generate many events related to file changes on a system. These events will need to be correlated together to determine what the user has done. The events will show what application was used for the relevant activity – for example used MSWord to open the file and saved it back with some changes or deleted a file from a command prompt. For registry activity these events will show the "before" and "after" changes to any registry keys in the single event. As with other windows events the events will show the data and time of the activity, details of the user performing the operation and all the related commands they used along with any success or failure status. The basic process to configure a FAM and RAM monitoring objective is as follows:

- Allow Snare to automatically set file audit configuration on the destination configuration screen. If this is not set in the agent then all of the objective settings will need to be set manually or via group policy. Using this setting enables the file system auditing to be controlled by the Snare objective settings. In order for Windows to collect file and registry access records, not only must the correct audit category be selected, but also the correct object auditing parameters must be set. Setting this field will automatically set these parameters, based on the objectives which have been set. It is highly recommended that this checkbox setting be selected.
- Open the objective screen and select "Access to a file or directory" radio button.
- For file auditing, enter the target file or directory into the General Search Term of the objective, e.g. c:\auditme\.
- For RAM registry auditing (HKEY_LOCAL_MACHINE only), enter "MACHINE\keyname" into the General Search Term of the objective, e.g. MACHINE\SOFTWARE\InterSect Alliance\AuditService\Config
- Select the event types to be collected ie Success, Failure, Informational, Warning.
- The source of these logs will generally be from the Security event log location.
- If applicable, set the criticality of the event so it can be tracked in Snare Central Server if events are being tracked in this way. Some events may be more critical than others so this feature allows events to be grouped in ways to make its more applicable for reporting.



Objectives Configuration

The following parameters of the Snare objective may be set:

Identify the high level event
○ Logon or Logoff
○ Account Administration
● Access a file or directory
○ Change the security policy
○ Start or stop a process
○ Restart, shutdown and system
○ Use of user rights
○ Filtering platform events
○ USB event
○ Any event(s)

Event ID Search Term
Optional, Comma separated: only used by the 'Any Event' setting above
● Include
○ Exclude
*

General Search Term
Used for event string match, file auditing ie c:\payroll, registry auditing ie MACHINE\keyname
Wildcards or regex functions only valid on event string match and not for file or registry auditing
● Include
○ Exclude
c:\auditme
□ Regular expression

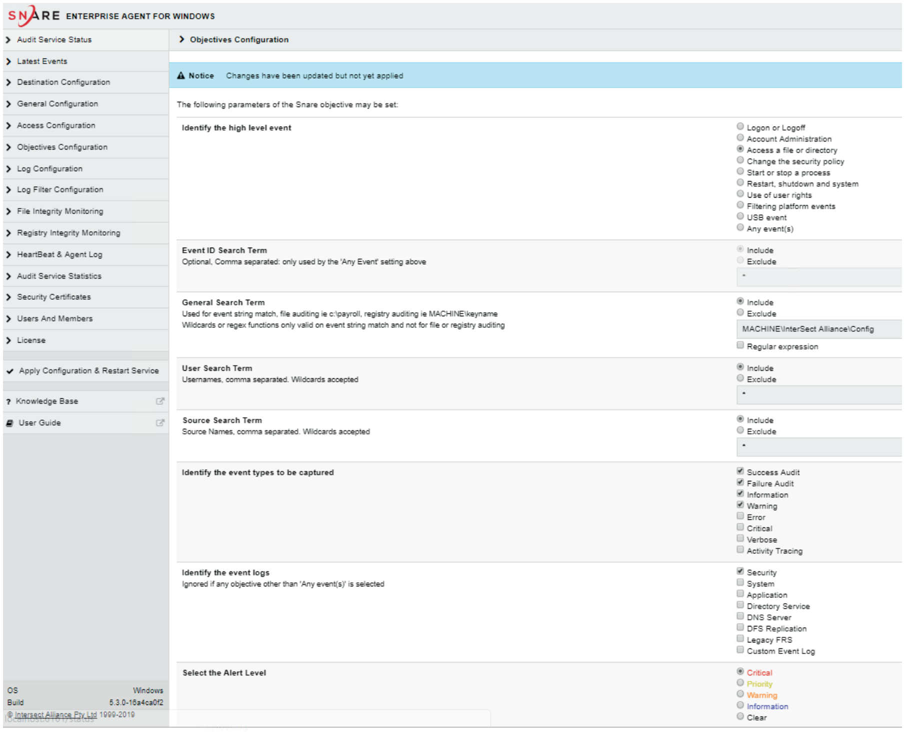
User Search Term
Usernames, comma separated. Wildcards accepted
● Include
○ Exclude
*

Source Search Term
Source Names, comma separated. Wildcards accepted
● Include
○ Exclude
*

Identify the event types to be captured
☑ Success Audit
☑ Failure Audit
☑ Information
☑ Warning
□ Error
□ Critical
□ Verbose
□ Activity Tracing

Identify the event logs
Ignored if any objective other than 'Any event(s)' is selected
☑ Security
□ System
□ Application
□ Directory Service
□ DNS Server
□ DFS Replication
□ Legacy FRS
□ Custom Event Log

Select the Alert Level
● Critical
○ Priority
○ Warning
○ Information
○ Clear



Objectives Configuration

Notice Changes have been updated but not yet applied

The following parameters of the Snare objective may be set:

Identify the high level event
○ Logon or Logoff
○ Account Administration
● Access a file or directory
○ Change the security policy
○ Start or stop a process
○ Restart, shutdown and system
○ Use of user rights
○ Filtering platform events
○ USB event
○ Any event(s)

Event ID Search Term
Optional, Comma separated: only used by the 'Any Event' setting above
● Include
○ Exclude
*

General Search Term
Used for event string match, file auditing ie c:\payroll, registry auditing ie MACHINE\keyname
Wildcards or regex functions only valid on event string match and not for file or registry auditing
● Include
○ Exclude
MACHINE\InterSect Alliance\Config
□ Regular expression

User Search Term
Usernames, comma separated. Wildcards accepted
● Include
○ Exclude
*

Source Search Term
Source Names, comma separated. Wildcards accepted
● Include
○ Exclude
*

Identify the event types to be captured
☑ Success Audit
☑ Failure Audit
☑ Information
☑ Warning
□ Error
□ Critical
□ Verbose
□ Activity Tracing

Identify the event logs
Ignored if any objective other than 'Any event(s)' is selected
☑ Security
□ System
□ Application
□ Directory Service
□ DNS Server
□ DFS Replication
□ Legacy FRS
□ Custom Event Log

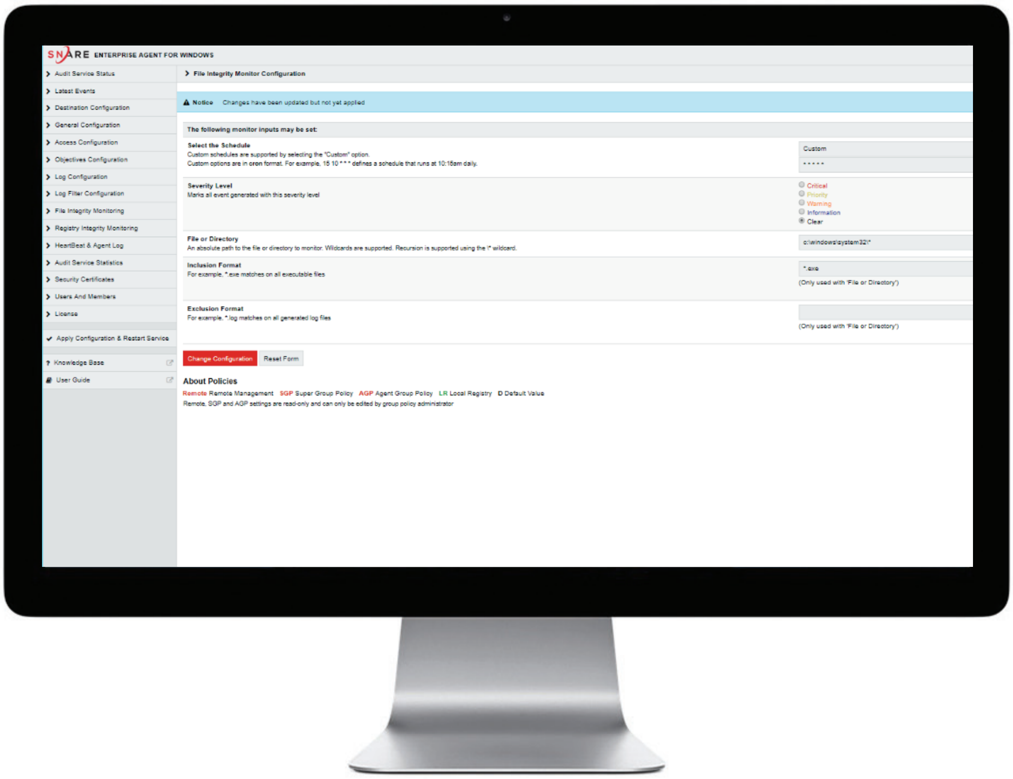
Select the Alert Level
● Critical
○ Priority
○ Warning
○ Information
○ Clear

Once the all the settings are set as desired then press the Change Configuration button to save the objective. Repeat this approach for all desired files or folders that require auditing enabled. Once all the objectives have been made then select “Apply the latest audit configuration” button and restart the agent. The events will show up in the latest events screen using the standard Windows Event IDs. The events can be any of the following:

- Access a file or directory.
- for Windows 2003 and XP based systems 560, 561, 562, 563, 564, 565, 566, 567, 594, 595
- For Windows 2008, 2012, 2016, 2019, windows 7,8,10 based systems they will use any of these event ids 4656, 4657, 4658, 4659, 4660, 4661, 4662, 4663, 4690, 4691

There are various standards that call for the usage of FIM and RIM such as PCI DSS. The technology compliments the FAM and RAM features with looking at some details of the file and registry changes performed on the systems. However, the events will show the results of the change and not who made the change. The "who" activity monitoring comes as part of the FAM and RAM monitoring as detailed above. The FIM and RIM features use a checksum approach along with file system details to determine changes made to files. The Snare Enterprise agents can perform these file system checks based on a schedule of the customers choosing. In general, this change detection process would be run either daily or weekly depending on the granularity required. These system checks can be system intensive as the agent has to perform a lot of disk IO to read all the files and then perform the checksum (SHA512) operations so they would generally be performed out of hours or when the system has low user activity. The basic process to configure FIM and RIM for the windows agent is as follows.

- Select the File Integrity Monitoring or Registry Integrity Monitoring menu item on the left
- Select the Add button
- Select the schedule the FIM/RIM checks will be performed
- Select the critically levels of these events
- Enter the file or Directory path. A file will be the absolute path to that file to be monitored. For a directory it's the path to that location. If you require a recursive search from that location, then enter * at the end as per the agent instructions.
    - for Registry Monitoring enter the KEY path details ie HKEY_LOCAL_MACHINE from the drop-down menu. Then select the registry Key or Value to be monitored. This is the absolute path of the Registry Key. As with the FIM wild card searching and recursive monitoring can also be performed.
- Enter the inclusion format ie *.exe to just select .exe files, Others such as *.dll or *.* can be used for all files in a location.
    - for Registry Monitoring enter the registry key or path that is to be monitored. The inclusion format is generally just a single * unless only specific keys are being monitored
- If there are files that you need to exclude then enter them in the exclusion section.
- Save the agent settings by selecting the Change Configuration button and then run the Apply Configuration to restart the agent
- The events will now show up in the latest events in the FIM section when the schedule kicks in showing the type of the event being New File, Change or Delete operations.



File Integrity Monitor Configuration

Notice Changes have been updated but not yet applied

The following monitor inputs may be set:

Select the Schedule
Custom schedules are supported by selecting the "Custom" option.
Custom options are in cron format. For example, 15 10 * * * defines a schedule that runs at 10:15am daily.
Custom
* * * * *

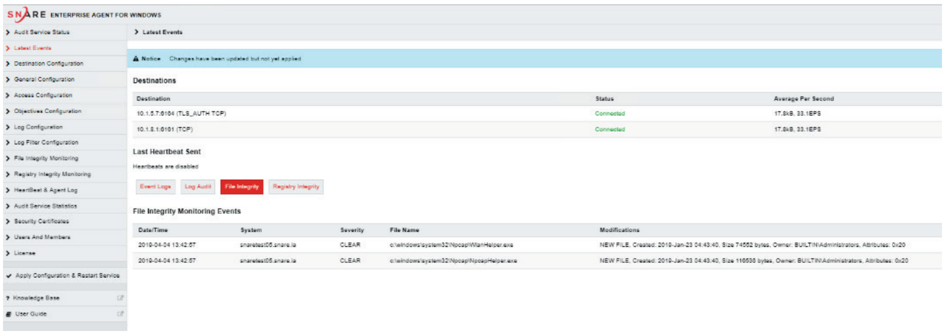
Severity Level
Marks all event generated with this severity level
○ Critical
○ Priority
○ Warning
○ Information
● Clear

File or Directory
An absolute path to the file or directory to monitor. Wildcards are supported. Recursion is supported using the * wildcard.
c:\windows\system32\*

Inclusion Format
For example, *.exe matches on all executable files
*.exe
(Only used with 'File or Directory')

Exclusion Format
For example, *.log matches on all generated log files
(Only used with 'File or Directory')

About Policies
Remote Remote Management SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value
Remote, SGP and AGP settings are read-only and can only be edited by group policy administrator



Latest Events

Notice Changes have been updated but not yet applied

Destinations

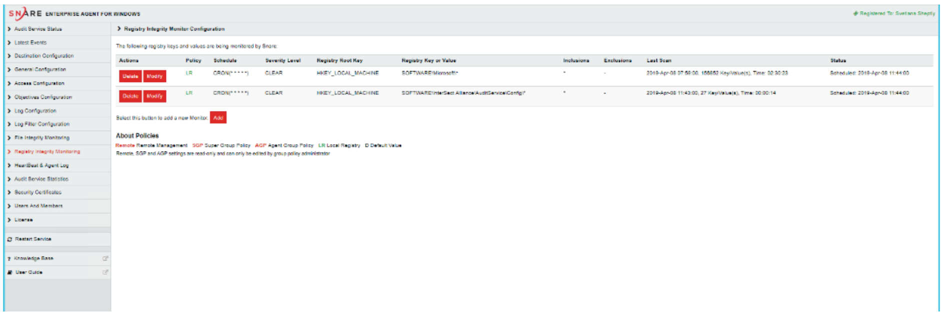
Destination	Status	Average Per Second
10.1.5.7:6164 (TLS_AUTH TCP)	Connected	17.8kB, 33.1EPS
10.1.8.1:6161 (TCP)	Connected	17.8kB, 33.1EPS

Last Heartbeat Sent

Heartbeats are disabled

File Integrity Monitoring Events

Date/Time	System	Severity	File Name	Modifications
2019-04-04 13:42:57	snaretest05.snare.ia	CLEAR	c:\windows\system32\Npcap\WlanHelper.exe	NEW FILE, Created: 2019-Jan-23 04:43:40, Size 74562 bytes, Owner: BUILTIN\Administrators, Attributes: 0x20
2019-04-04 13:42:57	snaretest05.snare.ia	CLEAR	c:\windows\system32\Npcap\NpcapHelper.exe	NEW FILE, Created: 2019-Jan-23 04:43:40, Size 116536 bytes, Owner: BUILTIN\Administrators, Attributes: 0x20



Registry Integrity Monitor Configuration

The following registry keys and values are being monitored by Snare:

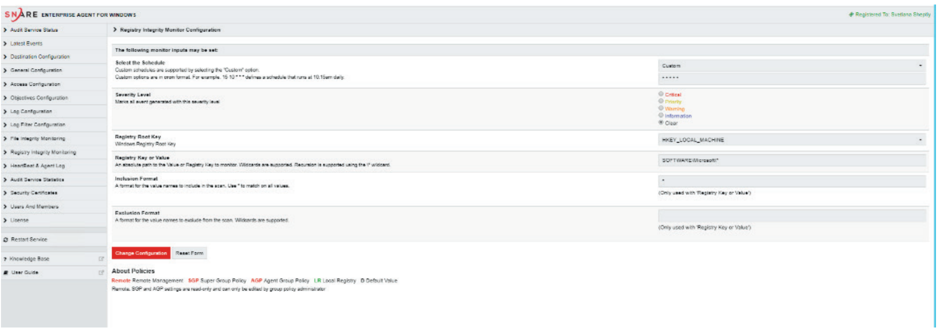
Actions	Policy	Schedule	Severity Level	Registry Root Key	Registry Key or Value	Inclusions	Exclusions	Last Scan	Status
Delete Modify	LR	CRON(* * * * *)	CLEAR	HKEY_LOCAL_MACHINE	SOFTWARE\Microsoft\*	*	-	2019-Apr-08 07:59:00, 156652 Key/Value(s), Time: 02:30:23	Scheduled: 2019-Apr-08 11:44:00
Delete Modify	LR	CRON(* * * * *)	CLEAR	HKEY_LOCAL_MACHINE	SOFTWARE\InterSect Alliance\AuditService\Config\*	*	-	2019-Apr-08 11:43:00, 27 Key/Value(s), Time: 00:00:14	Scheduled: 2019-Apr-08 11:44:00

Select this button to add a new Monitor. Add

About Policies

Remote Remote Management SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value

Remote, SGP and AGP settings are read-only and can only be edited by group policy administrator



Registry Integrity Monitor Configuration

The following monitor inputs may be set:

Select the Schedule
Custom schedules are supported by selecting the "Custom" option.
Custom options are in cron format. For example, 15 10 * * * defines a schedule that runs at 10:15am daily.
Custom
* * * * *

Severity Level
Marks all event generated with this severity level
○ Critical
○ Priority
○ Warning
○ Information
● Clear

Registry Root Key
Windows Registry Root Key
HKEY_LOCAL_MACHINE

Registry Key or Value
An absolute path to the Value or Registry Key to monitor. Wildcards are supported. Recursion is supported using the * wildcard.
SOFTWARE\Microsoft\*

Inclusion Format
A format for the value names to include in the scan. Use * to match on all values.
*
(Only used with 'Registry Key or Value')

Exclusion Format
A format for the value names to exclude from the scan. Wildcards are supported.
(Only used with 'Registry Key or Value')

About Policies

Remote Remote Management SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value

Remote, SGP and AGP settings are read-only and can only be edited by group policy administrator

Registry Integrity Monitoring will show up

FAM and FIM Settings for Snare Enterprise Agent for Linux

The approach for enabling File Activity Monitoring for Linux is similar to Windows however the directory structure and options available are slightly different due to the operating system. The Unix / Linux agents have a separate file watch section in the objective screen that allows objectives to be created on files or directories. To configure the Snare Enterprise Linux agent to perform File Integrity Monitoring and File Activity Monitoring perform the following basic steps.

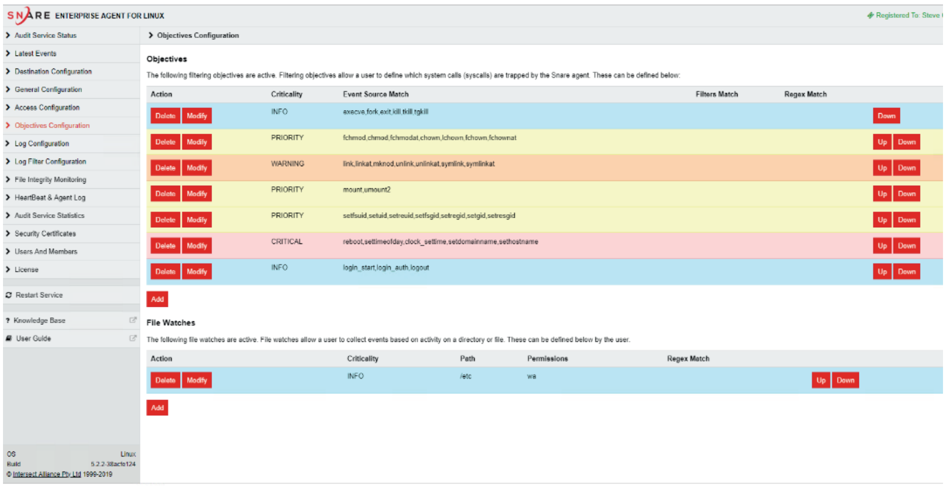
- Review the critical parts of the operating system and applications that need to be monitored. In general, there will be many files, directories and registry keys that need to be monitored. This should form your baseline or core monitoring
- Document the baseline of these parts of the system that need to be audited and monitored.
- Create Snare objectives in the agents to match the configuration that you documented. You may require different policies for different systems. You can use the Snare Agent Management Console to manage different polices on different systems based on operational needs.
- Ensure that all the systems have the correct date and time and are using NTP settings to keep accurate time.
- In the reporting system such as Snare Central or Snare Advanced Analytics ensure that the events are being monitored and alerts are configured to notify the relevant staff of the system changes.

The FAM features use the host operating systems **auditd** function which is part of Linux. For Linux based systems this is driven by **auditd** policy of the system which is managed by the Snare for Linux agent. The events produced relate to the activity being performed which can include reads, changes, adding or deletions of files on the system. The Linux platform can generate many events related to file changes on a system which can come from user actions or activities performed by CRON, these events will need to be correlated together to determine what the user has done. The events will show what application was used for the relevant activity - ie used vi to open the file and saved it back with some changes, or deleted a file from a shell command prompt. The basic process to configure a FAM objective is as follows:

To configure a file watch objective in Linux:

1. Allow Snare to automatically set audit configuration on the general configuration screen. If this is not set in the agent then all of the objective settings will need to be set manually or via manual updates to the audit.rules configuration file. Using this setting enables the file system auditing to be controlled by the Snare objective settings. In order for Linux to collect file and directory access logs, not only must the correct audit category be selected, but also the correct audit rules be applied to the auditing system. Setting this field will automatically set these parameters, based on the objectives which have been set. It is highly recommended that this checkbox be selected.
2. Open the objective screen and select “Add” for a new file watch radio button.
3. For file auditing, enter the target file or directory into the File watch path of the objective, e.g. /auditme/. There is a default objective that watches the /etc directory location. You can add many locations either specific directories or mount points that are in use on the Linux host.
4. Select the event permissions to watch ie “wa” for all writes and accesses to files
5. Enter a regex to match events of a specific type or user ie “”.*root.*”
6. If applicable, set the alert level of the event so it can be tracked in Snare Server, if events are being tracked in this way. Some events may be more critical than others, so this feature allows events to be grouped in ways to make its more applicable for reporting.
7. Once complete press the “Change Configuration” button and apply the latest audit configuration to restart the agent.

The figure below displays a file watch objective for the Snare Enterprise Linux agent:



> Objectives Configuration

Objectives

The following filtering objectives are active. Filtering objectives allow a user to define which system calls (syscalls) are trapped by the Snare agent. These can be defined below:

Action	Criticality	Event Source Match	Filters Match	Regex Match	
Delete Modify	INFO	execve,fork,exit,kill,tkill,tgkill			Down
Delete Modify	PRIORITY	fchmod,chmod,fchmodat,chown,lchown,fchown,fchownat			Up Down
Delete Modify	WARNING	link,linkat,mknod,unlink,unlinkat,symlink,symlinkat			Up Down
Delete Modify	PRIORITY	mount,umount2			Up Down
Delete Modify	PRIORITY	setfsuid,setuid,setreuid,setfsgid,setregid,setgid,setresgid			Up Down
Delete Modify	CRITICAL	reboot,settimeofday,clock_settime,setdomainname,sethostname			Up Down
Delete Modify	INFO	login_start,login_auth,logout			Up Down

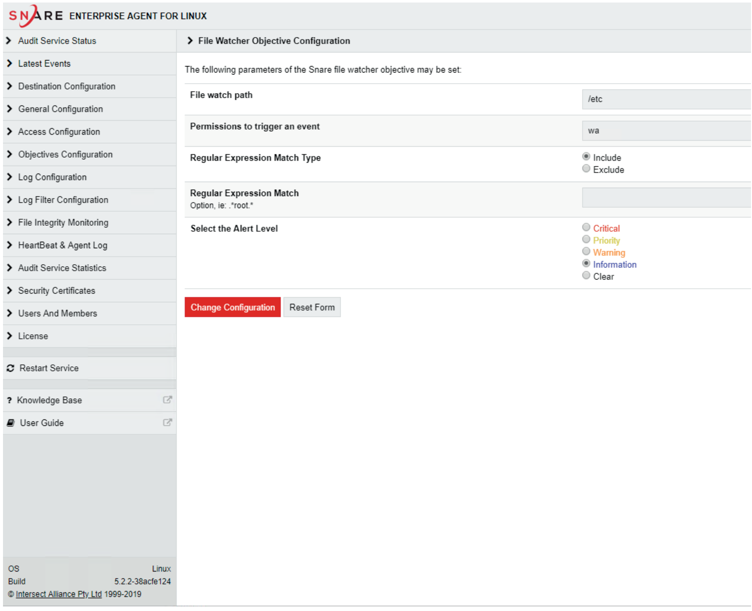
Add

File Watches

The following file watches are active. File watches allow a user to collect events based on activity on a directory or file. These can be defined below by the user.

Action	Criticality	Path	Permissions	Regex Match	
Delete Modify	INFO	/etc	wa		Up Down

Add



> File Watcher Objective Configuration

The following parameters of the Snare file watcher objective may be set:

File watch path	/etc
Permissions to trigger an event	wa
Regular Expression Match Type	● Include ○ Exclude
Regular Expression Match Option, ie: .*root.*	
Select the Alert Level	○ Critical ○ Priority ○ Warning ● Information ○ Clear

Change Configuration Reset Form

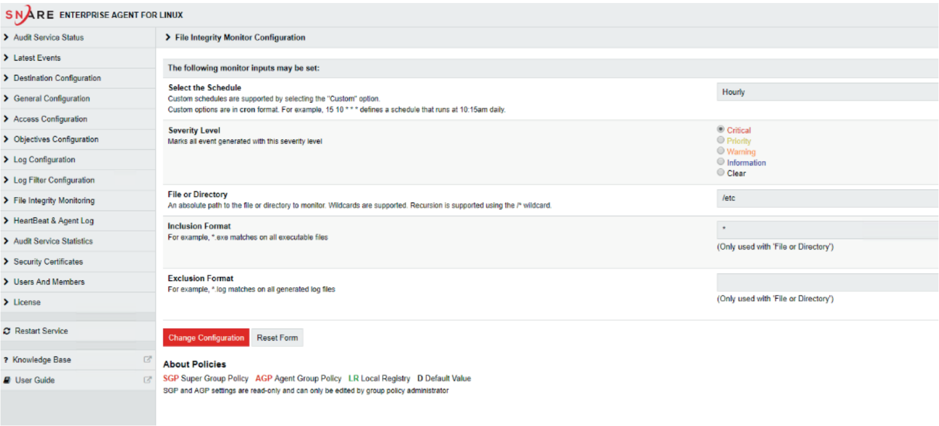
Once the all the settings are set as desired then press the Change Configuration button to save the objective. Repeat this approach for all desired files or directories that require file watch auditing enabled. Once all the objectives have been made then select “Apply the latest audit configuration” button and restart the agent. The events will show up in the latest events screen using the standard Linux events. The events can be any of the following:

- Access a file or directory.
- execve calls showing the command run on the system to perform the file operation. These can be combined with other system calls for fchmod, chmod, fchmoda, chown, kchown, fchownat, link, linkat, mkmod, unlink, unlinkat, symlink, symlinkat

There are various standards that call for the usage of FIM such as PCI DSS. This technology compliments the FAM features by looking at some details of the file and directory changes performed on the systems. However, the events will show the results of the change and not who made the change. The “who” activity monitoring comes as part of the FAM monitoring as detailed above. The FIM features use a checksum approach along with file system details to determine changes made to files. The Snare Enterprise agents can perform these file system checks based on a schedule of the customers choosing. In general, these change detection process would be run either daily or weekly depending on the granularity required. These system checks can be system intensive as the agent has to perform a lot of disk IO to read all the files and then perform the checksum (SHA512) operations so they would generally be performed out of hours or when the system has low user activity.

The basic process to configure FIM for the Snare Enterprise Linux agent is as follows.

- Select the File Integrity Monitoring menu item on the left
- Select the Add button
- Select the schedule the FIM checks will be performed
- Select the critically levels of these events
- Enter the file or Directory path. A file will be the absolute path to that file to be monitored. For a directory it's the path to that location. If you require a recursive search from that location, then enter /* at the end as per the agent instructions. Note that this forward slash on Linux.
- Enter the inclusion format ie * to just select .all files, Others such as *.config can be used for just config files in a location.
- If there are files that you need to exclude then enter them in the exclusion section.
- Save the agent settings by selecting the Change Configuration button and then run the Apply Configuration to restart the agent
- The events will now show up in the latest events in the FIM section when the schedule kicks in showing the type of the event being New File, Change or Delete operations.



File Integrity Monitor Configuration

The following monitor inputs may be set:

Select the Schedule Hourly
Custom schedules are supported by selecting the "Custom" option.
Custom options are in cron format. For example, 15 10 * * * defines a schedule that runs at 10:15am daily.

Severity Level ● Critical ○ Priority ○ Warning ○ Information ○ Clear
Marks all event generated with this severity level

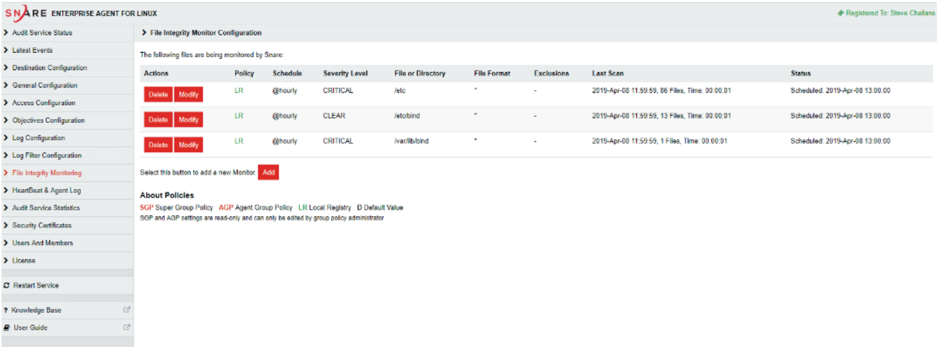
File or Directory /etc
An absolute path to the file or directory to monitor. Wildcards are supported. Recursion is supported using the /* wildcard.

Inclusion Format *
For example, *.exe matches on all executable files
(Only used with 'File or Directory')

Exclusion Format
For example, *.log matches on all generated log files
(Only used with 'File or Directory')

Change Configuration Reset Form

About Policies
SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value
SGP and AGP settings are read-only and can only be edited by group policy administrator



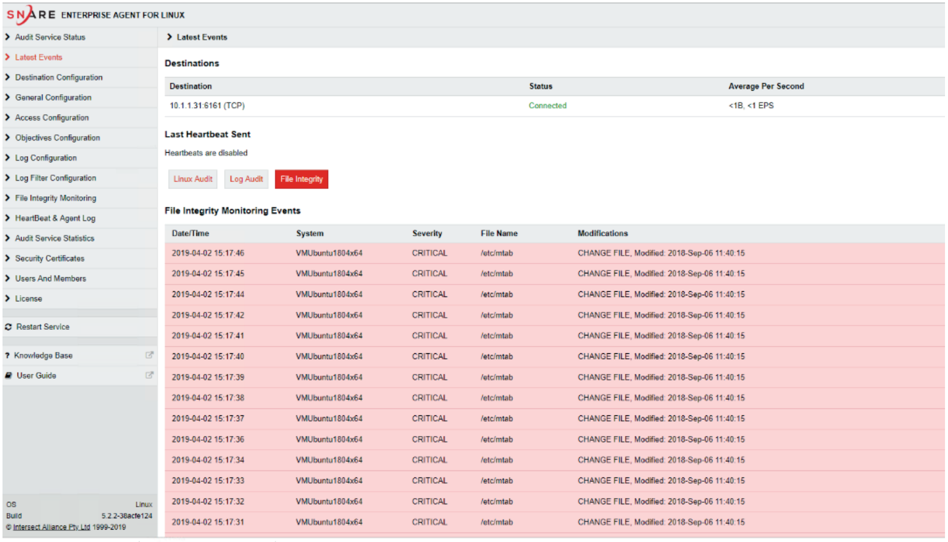
File Integrity Monitor Configuration

The following files are being monitored by Snare:

Actions	Policy	Schedule	Severity Level	File or Directory	File Format	Exclusions	Last Scan	Status
Delete Modify	LR	@hourly	CRITICAL	/etc	*	-	2019-Apr-08 11:59:59, 86 Files, Time: 00:00:01	Scheduled: 2019-Apr-08 13:00:00
Delete Modify	LR	@hourly	CLEAR	/etc/bind	*	-	2019-Apr-08 11:59:59, 13 Files, Time: 00:00:01	Scheduled: 2019-Apr-08 13:00:00
Delete Modify	LR	@hourly	CRITICAL	/var/lib/bind	*	-	2019-Apr-08 11:59:59, 1 Files, Time: 00:00:01	Scheduled: 2019-Apr-08 13:00:00

Select this button to add a new Monitor. Add

About Policies
SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value
SGP and AGP settings are read-only and can only be edited by group policy administrator



OS Linux
Build 5.2.2-38acfe124
© Intersect Alliance Pty Ltd 1999-2019

Latest Events

Destinations

Destination	Status	Average Per Second
10.1.1.31:6161 (TCP)	Connected	<1B, <1 EPS

Last Heartbeat Sent

Heartbeats are disabled

Linux Audit Log Audit File Integrity

File Integrity Monitoring Events

Date/Time	System	Severity	File Name	Modifications
2019-04-02 15:17:46	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:45	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:44	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:42	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:41	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:40	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:39	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:38	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:37	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:36	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:34	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:33	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:32	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15
2019-04-02 15:17:31	VMUbuntu1804x64	CRITICAL	/etc/mtab	CHANGE FILE, Modified: 2018-Sep-06 11:40:15

FAM Settings for Snare Enterprise Agent for Solaris and OSX

The approach for enabling File Activity Monitoring for Solaris and Mac OSX is similar to Linux however the objective settings are slightly different due to the operating system audit differences. The Solaris and OSX agents need to use filtering options on the objectives to select the files or directories. For Sun Solaris and Mac OSX agents the operating system does not have the same facility as Linux so the events have to be selected based on the search term parameters.

To configure the Snare Enterprise Solaris and OSX agent to perform File Integrity Monitoring perform the following basic steps.

- Review the critical parts of the operating system and applications that need to be monitored. In general, there will be many files, directories and registry keys that need to be monitored. This should form your baseline or core monitoring
- Document the baseline of these parts of the system that need to be audited and monitored.
- Create Snare objectives in the agents to match the configuration that you documented. You may require different policies for different systems. You can use the Snare Agent Management Console to manage different polices on different systems based on operational needs.
- Ensure that all the systems have the correct date and time and are using NTP settings to keep accurate time.
- In the reporting system such as Snare Central or Snare Advanced Analytics ensure that the events are being monitored and alerts are configured to notify the relevant staff of the system changes.

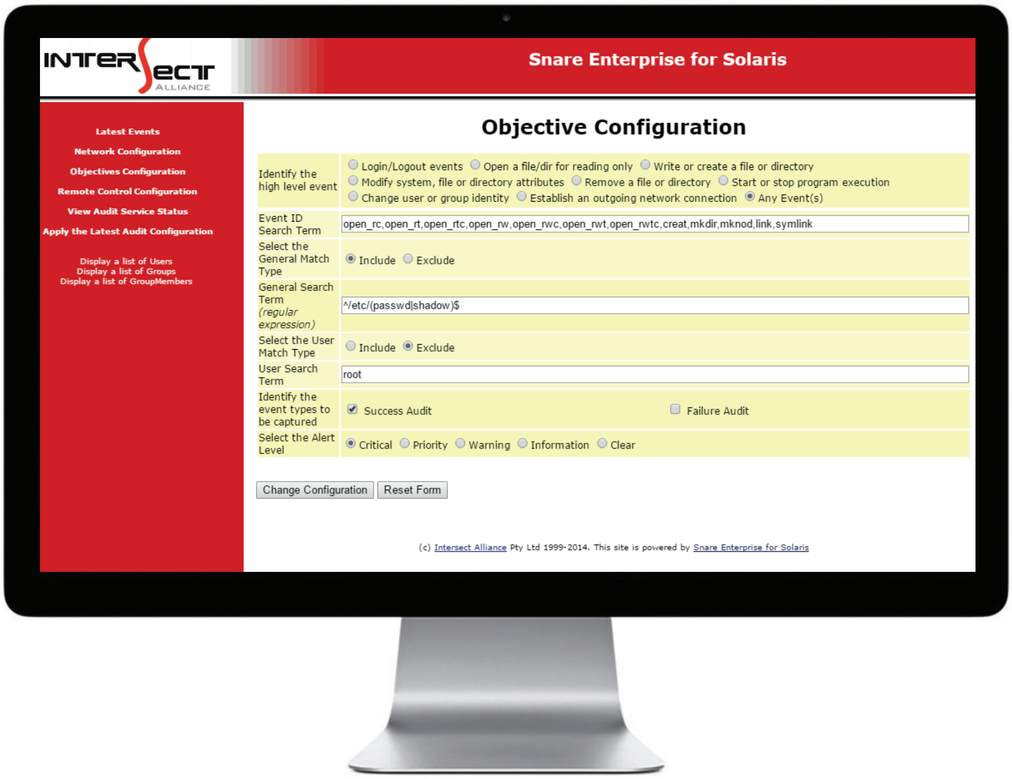
The FAM features use the host operating systems BSM audit function which is part of Solaris and OSX platforms. For these systems this is driven by BSM audit policy of the system which is managed by the Snare Enterprise agent. The events produced relate to the activity being performed which can include reads, changes, adding or deletions of files on the system. The BSM platform can generate many events related to file changes on a system which can come from user actions or activities performed by CRON. These events will need to be correlated together to determine what the user has done. The events will show which application was used for the relevant activity ie used vi to open the file and saved it back with some changes or deleted a file from a shell command prompt. The basic process to configure a FAM objective is as follows:

The basic process to configure an objective to capture file auditing events is as follows:

- Allow Snare to automatically set audit configuration on the destination configuration screen. If this is not set in the agent, then all of the objective settings will need to be set manually or via manual updates to the audit.rules configuration file. Using this setting enables the file system auditing to be controlled by the Snare objective settings. For Solaris or OSX to collect file and directory access logs, not only must the correct audit category be selected, but also the correct audit rules auditing parameters must also be set. Setting this field will automatically set these parameters, based on the objectives which have been set. It is highly recommended that this checkbox be selected.
- Open the objective screen and select “Add” for a new objective button
- Select the any event radio button
- Enter the event id to be monitored ie the following example will monitor all file opens, changes and writes to the file:
    - *open_rc,open_rt,open_rtc,open_rw,open_rwc,open_rwt,open_rwtc,creat,mkdir,mknod,link,symlink*
- In the Search Term field enter the file(s) to be monitored. ie ^/etc/(*passwd*|*shadow*)$
- Adjust the user Search Term to match or exclude users as desired.
- Select the type of event to be collected being success or failure or both.
- If applicable set the alert level of the event so it can be tracked in Snare Central Server if events are being tracked in this way. Some events may be more critical than others, so this feature allows events to be grouped in ways to make its more applicable for reporting.

- Once complete press the “Change Configuration” button and apply the latest audit configuration to restart the agent.

In the v4 Snare Enterprise Solaris agent the screen is as follows:


INTERSECT ALLIANCE
Snare Enterprise for Solaris
Latest Events
Network Configuration
Objectives Configuration
Remote Control Configuration
View Audit Service Status
Apply the Latest Audit Configuration
Display a list of Users
Display a list of Groups
Display a list of GroupMembers

Objective Configuration

Identify the high level event: ○ Login/Logout events ○ Open a file/dir for reading only ○ Write or create a file or directory ○ Modify system, file or directory attributes ○ Remove a file or directory ○ Start or stop program execution ○ Change user or group identity ○ Establish an outgoing network connection ● Any Event(s)

Event ID Search Term: open_rc,open_rt,open_rtc,open_rw,open_rwc,open_rwt,open_rwtc,creat,mkdir,mknod,link,symlink

Select the General Match Type: ● Include ○ Exclude

General Search Term *(regular expression)*: ^/etc/(passwd|shadow)$

Select the User Match Type: ○ Include ● Exclude

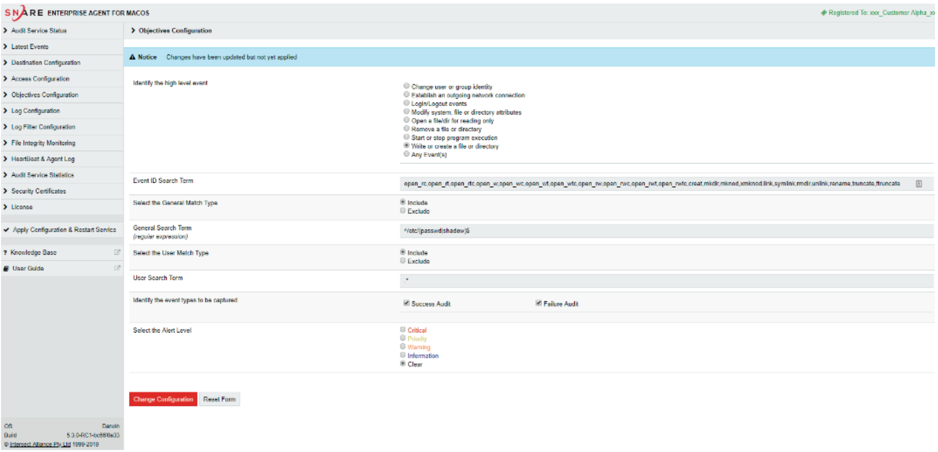
User Search Term: root

Identify the event types to be captured: ☑ Success Audit □ Failure Audit

Select the Alert Level: ● Critical ○ Priority ○ Warning ○ Information ○ Clear

(c) Intersect Alliance Pty Ltd 1999-2014. This site is powered by Snare Enterprise for Solaris

The v5 OSX agent has the following configuration settings.



Notice Changes have been updated but not yet applied

Identify the high level event:
○ Change user or group identity
○ Establish an outgoing network connection
○ Login/Logout events
○ Modify system, file or directory attributes
○ Open a file/dir for reading only
○ Remove a file or directory
○ Start or stop program execution
● Write or create a file or directory
○ Any Event(s)

Event ID Search Term: open_rc,open_rt,open_rtc,open_w,open_wc,open_wt,open_wtc,open_rw,open_rwc,open_rwt,open_rwtc,creat,mkdir,mknod,xmknod,link,symlink,rmdir,unlink,rename,truncate,ftruncate

Select the General Match Type: ● Include ○ Exclude

General Search Term *(regular expression)*: ^/etc/(passwd|shadow)$

Select the User Match Type: ● Include ○ Exclude

User Search Term: .*

Identify the event types to be captured: ☑ Success Audit ☑ Failure Audit

Select the Alert Level:
○ Critical
○ Priority
○ Warning
○ Information
● Clear

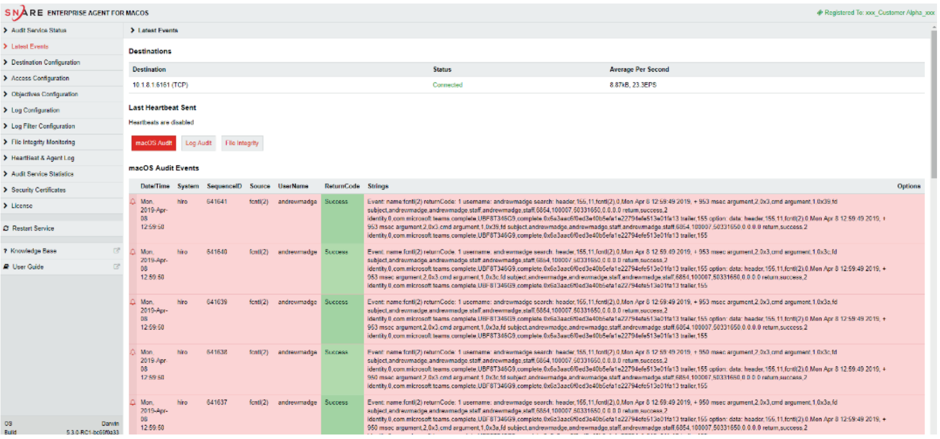
OS Darwin
Build 5.3.0-RC1-bc680a33
© Intersect Alliance Pty Ltd 1999-2019

Once the all the settings are set as desired then press the Change Configuration button to save the objective. Repeat this approach for all desired files or directories that require file watch auditing enabled. Once all the objectives have been made then select "Apply the latest audit configuration" button and restart the agent. The events will show up in the latest events screen using the standard Linux events. The events can be any of the following:

- Access a file or directory.
- These can be combined with other system calls for open_rc,open_rt,open_rtc,open_w,open_wc,open_wt,open_wtc,open_rw,open_rwc,open_rwt,open_rwtc,creat,mkdir,mknod,xmknod,link,symlink,rmdir,unlink,rename,truncate,ftruncatet

There are various standards that call for the usage of FIM such as PCI DSS. The technology compliments the FAM features by looking at some details of the file and directory changes performed on the systems. However, the events will show the results of the change and not who made the change. The "who" activity monitoring comes as part of the FAM monitoring as detailed above. The FIM features use a checksum approach along with file system details to determine changes made to files. The V5 Snare Enterprise agents can perform these file system checks based on a schedule of the customers choosing. In general, these change detection process would be run either daily or weekly depending on the granularity required. These system checks can be system intensive as the agent has to perform a lot of disk IO to read all the files and then perform the checksum (SHA512) operations so they would generally be performed out of hours or when the system has low user activity. The basic process to configure FIM for the Snare Enterprise Linux agent is as follows.

- Select the File Integrity Monitoring menu item on the left
- Select the Add button
- Select the schedule the FIM checks will be performed
- Select the critically levels of these events
- Enter the file or Directory path. A file will be the absolute path to that file to be monitored. For a directory it's the path to that location. If you require a recursive search from that location, then enter /* at the end as per the agent instructions. Note that this forward slash on Linux.
- Enter the inclusion format ie * to just select .all files, Others such as *.config can be used for just config files in a location.
- If there are files that you need to exclude then enter them in the exclusion section.
- Save the agent settings by selecting the Change Configuration button and then run the Apply Configuration to restart the agent
- The events will now show up in the latest events in the FIM section when the schedule kicks in showing the type of the event being New File, Change or Delete operations.



OS Darwin
Build 5.3.0-RC1-bc66f0a33

Latest Events

Destinations

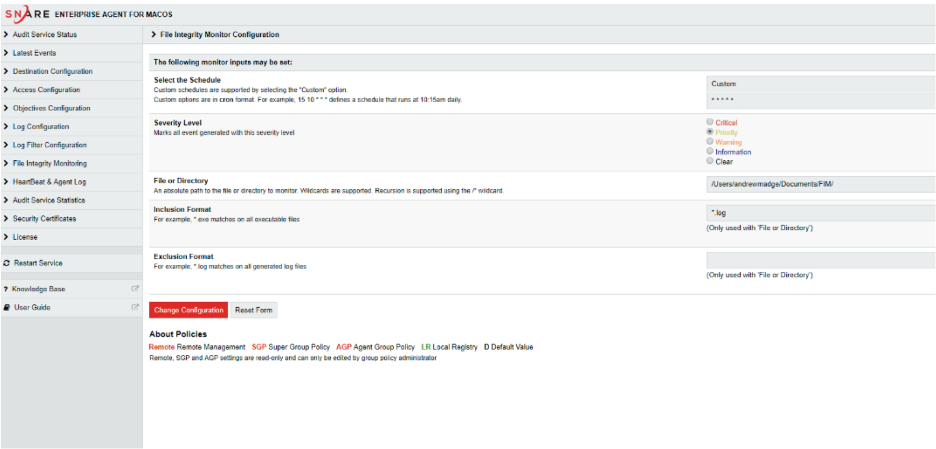
Destination	Status	Average Per Second
10.1.8.1:6161 (TCP)	Connected	8.87kB, 23.3EPS

Last Heartbeat Sent

Heartbeats are disabled

macOS Audit Events

Date/Time	System	SequenceID	Source	UserName	ReturnCode	Strings	Options
Mon, 2019-Apr-08 12:59:50	hiro	641641	fcntl(2)	andrewmadge	Success	Event: name:fcntl(2) returnCode: 1 username: andrewmadge search: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 953 msec argument,2,0x3,cmd argument,1,0x39,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155 option: data: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 953 msec argument,2,0x3,cmd argument,1,0x39,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155	
Mon, 2019-Apr-08 12:59:50	hiro	641640	fcntl(2)	andrewmadge	Success	Event: name:fcntl(2) returnCode: 1 username: andrewmadge search: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 953 msec argument,2,0x3,cmd argument,1,0x3c,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155 option: data: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 953 msec argument,2,0x3,cmd argument,1,0x3c,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155	
Mon, 2019-Apr-08 12:59:50	hiro	641639	fcntl(2)	andrewmadge	Success	Event: name:fcntl(2) returnCode: 1 username: andrewmadge search: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 953 msec argument,2,0x3,cmd argument,1,0x3a,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155 option: data: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 953 msec argument,2,0x3,cmd argument,1,0x3a,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155	
Mon, 2019-Apr-08 12:59:50	hiro	641638	fcntl(2)	andrewmadge	Success	Event: name:fcntl(2) returnCode: 1 username: andrewmadge search: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 950 msec argument,2,0x3,cmd argument,1,0x3c,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155 option: data: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 950 msec argument,2,0x3,cmd argument,1,0x3c,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155	
Mon, 2019-Apr-08 12:59:50	hiro	641637	fcntl(2)	andrewmadge	Success	Event: name:fcntl(2) returnCode: 1 username: andrewmadge search: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 950 msec argument,2,0x3,cmd argument,1,0x3a,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2 identity,0,com.microsoft.teams.complete,UBF8T346G9,complete,0x6a3aac6f0ed3e40b5efa1e22794efe513e01fa13 trailer,155 option: data: header,155,11,fcntl(2),0,Mon Apr 8 12:59:49 2019, + 950 msec argument,2,0x3,cmd argument,1,0x3a,fd subject,andrewmadge,andrewmadge,staff,andrewmadge,staff,6854,100007,50331650,0.0.0.0 return,success,2	



File Integrity Monitor Configuration

The following monitor inputs may be set:

Select the Schedule
Custom schedules are supported by selecting the "Custom" option.
Custom options are in cron format. For example, 15 10 * * * defines a schedule that runs at 10:15am daily.

Custom
* * * * *

Severity Level
Marks all event generated with this severity level

○ Critical
● Priority
○ Warning
○ Information
○ Clear

File or Directory
An absolute path to the file or directory to monitor. Wildcards are supported. Recursion is supported using the /* wildcard.

/Users/andrewmadge/Documents/FIM/

Inclusion Format
For example, *.exe matches on all executable files

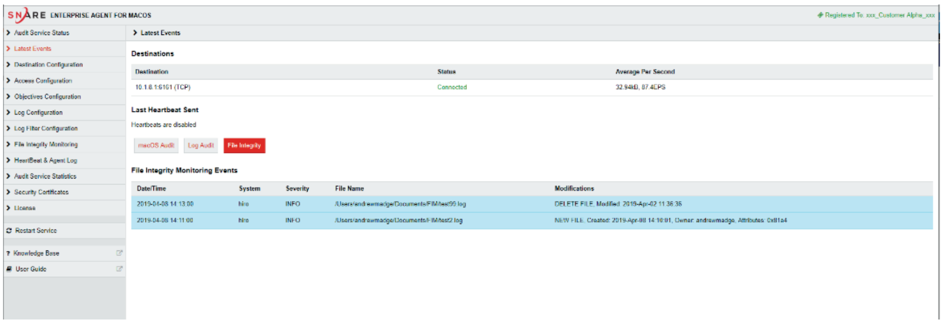
*.log
(Only used with 'File or Directory')

Exclusion Format
For example, *.log matches on all generated log files

(Only used with 'File or Directory')

About Policies

Remote Remote Management SGP Super Group Policy AGP Agent Group Policy LR Local Registry D Default Value
Remote, SGP and AGP settings are read-only and can only be edited by group policy administrator



Latest Events

Destinations

Destination	Status	Average Per Second
10.1.8.1:6161 (TCP)	Connected	32.94kB, 87.4EPS

Last Heartbeat Sent

Heartbeats are disabled

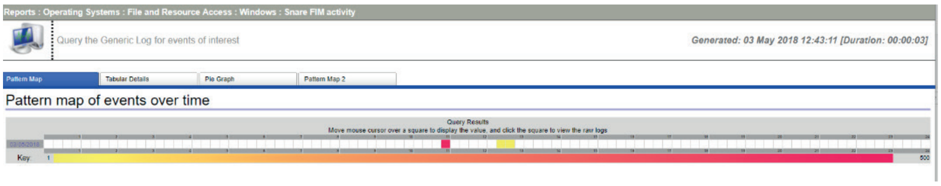
File Integrity Monitoring Events

Date/Time	System	Severity	File Name	Modifications
2019-04-08 14:13:00	hiro	INFO	/Users/andrewmadge/Documents/FIM/test99.log	DELETE FILE. Modified: 2019-Apr-02 11:36:36
2019-04-08 14:11:00	hiro	INFO	/Users/andrewmadge/Documents/FIM/test2.log	NEW FILE. Created: 2019-Apr-08 14:10:01, Owner: andrewmadge, Attributes: 0x81a4

Reporting on FIM, FAM, RIM and RAM Log Activity

Snare has two systems that can help with reporting on FIM, FAM, RIM and RAM log activity.

- **Snare Central Server** - Out of the box Snare Central contains objective for various platforms including Windows, Linux, and Solaris objective reports that can show the activity occurring on the systems. These reports can be run interactively or scheduled to run overnight to report on specific time periods.



Reports : Operating Systems : File and Resource Access : Windows : Snare FIM activity

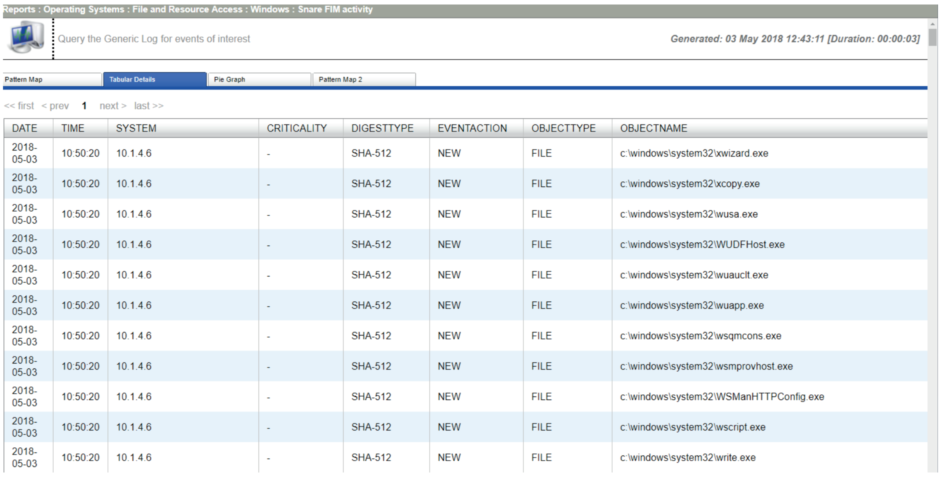
Query the Generic Log for events of interest

Generated: 03 May 2018 12:43:11 [Duration: 00:00:03]

Pattern map of events over time

Query Results

Move mouse cursor over a square to display the value, and click the square to view the raw logs

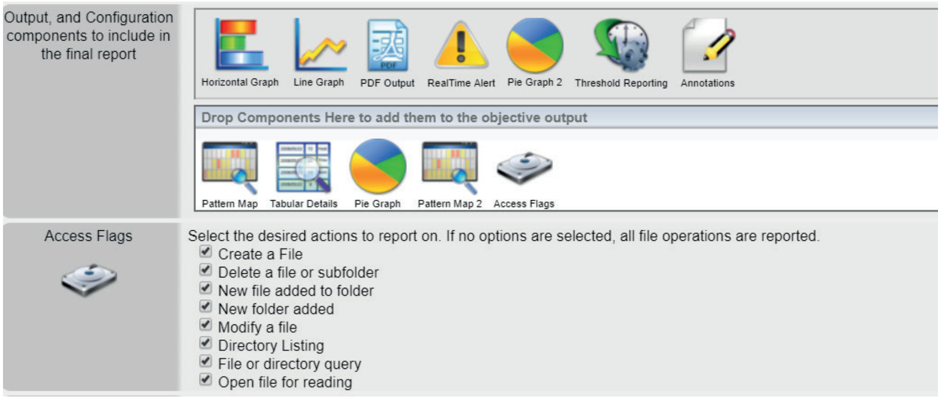


Reports : Operating Systems : File and Resource Access : Windows : Snare FIM activity

Query the Generic Log for events of interest

Generated: 03 May 2018 12:43:11 [Duration: 00:00:03]

DATE	TIME	SYSTEM	CRITICALITY	DIGESTTYPE	EVENTACTION	OBJECTTYPE	OBJECTNAME
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\xwizard.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\xcopy.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\wusa.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\WUDFHost.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\wuauclt.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\wuapp.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\wsqmcons.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\wsmprovhost.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\WSManHTTPConfig.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\wscript.exe
2018-05-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\write.exe



Output, and Configuration components to include in the final report

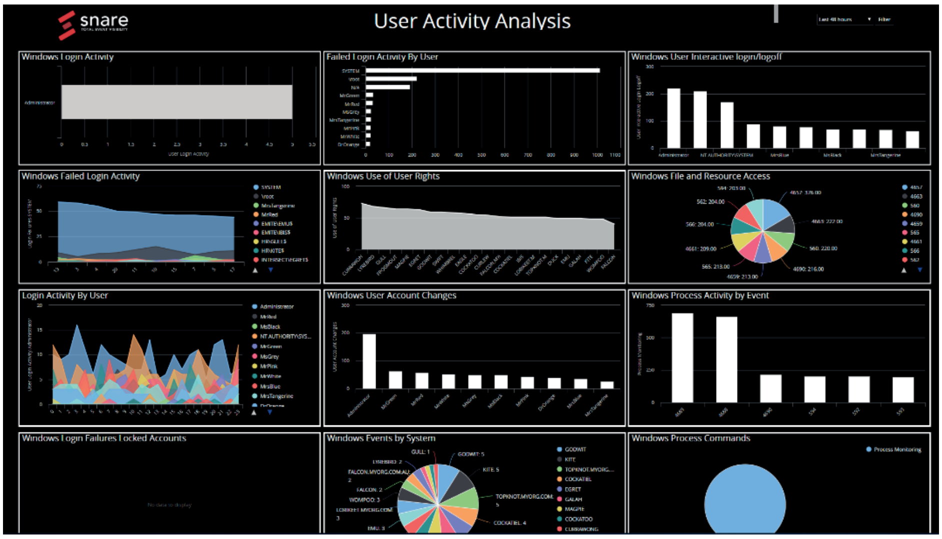
Drop Components Here to add them to the objective output

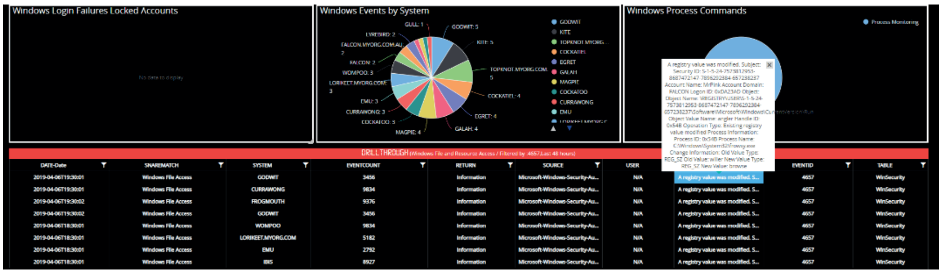
Access Flags

Select the desired actions to report on. If no options are selected, all file operations are reported.

- ☑ Create a File
- ☑ Delete a file or subfolder
- ☑ New file added to folder
- ☑ New folder added
- ☑ Modify a file
- ☑ Directory Listing
- ☑ File or directory query
- ☑ Open file for reading

- **Snare Advanced Analytics Plus** and **Snare Advanced Threat Intelligence** screen shots are below. Data can be viewed in a variety of ways, and customised dashboards created to link and correlate data on a single page to suit the needs of the user. Data can be linked to third party CMDB and ticketing systems to assist with tracking the activities and if authorisation was obtained for the detected system changes.

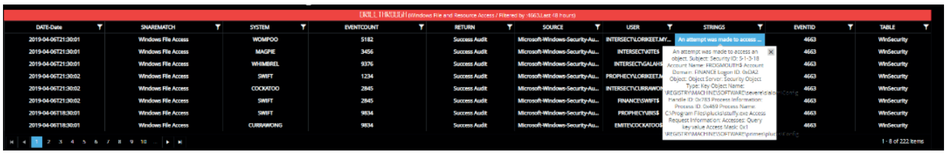




A registry value was modified. Subject: Security ID: S-1-5-24-7573812953-8687472147-7896292384-657238237 Account Name: MrPink Account Domain: FALCON Logon ID: 0xDA23AD Object: Object Name: \REGISTRY\USER\S-1-5-24-7573812953-8687472147-7896292384-657238237\Software\Microsoft\Windows\CurrentVersion\Run Object Value Name: angler Handle ID: 0x548 Operation Type: Existing registry value modified Process Information: Process ID: 0x548 Process Name: C:\Windows\System32\frowsy.exe Change Information: Old Value Type: REG_SZ Old Value: willer New Value Type: REG_SZ New Value: browse

DRILL THROUGH (Windows File and Resource Access / Filtered by :4657,Last 48 hours)

DATE-Date	SNAREMATCH	SYSTEM	EVENTCOUNT	RETURN	SOURCE	USER		EVENTID	TABLE
2019-04-06T19:30:01	Windows File Access	GODWIT	3456	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity
2019-04-06T19:30:01	Windows File Access	CURRAWONG	9834	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity
2019-04-06T19:30:02	Windows File Access	FROGMOUTH	9376	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity
2019-04-06T19:30:02	Windows File Access	GODWIT	3456	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity
2019-04-06T18:30:01	Windows File Access	WOMPOO	9834	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity
2019-04-06T18:30:01	Windows File Access	LORIKEET.MYORG.COM	5182	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity
2019-04-06T18:30:01	Windows File Access	EMU	2792	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity
2019-04-06T18:30:01	Windows File Access	IBIS	8927	Information	Microsoft-Windows-Security-Au...	N/A	A registry value was modified. S...	4657	WinSecurity



DRILL THROUGH (Windows File and Resource Access / Filtered by :4663,Last 48 hours)

DATE-Date	SNAREMATCH	SYSTEM	EVENTCOUNT	RETURN	SOURCE	USER	STRINGS	EVENTID	TABLE
2019-04-06T21:30:01	Windows File Access	WOMPOO	5182	Success Audit	Microsoft-Windows-Security-Au...	INTERSECT\LORIKEET.MY...	An attempt was made to access ...	4663	WinSecurity
2019-04-06T21:30:01	Windows File Access	MAGPIE	3456	Success Audit	Microsoft-Windows-Security-Au...	INTERSECT\KITE$		4663	WinSecurity
2019-04-06T21:30:01	Windows File Access	WHIMBREL	9376	Success Audit	Microsoft-Windows-Security-Au...	INTERSECT\GALAH$		4663	WinSecurity
2019-04-06T21:30:02	Windows File Access	SWIFT	1234	Success Audit	Microsoft-Windows-Security-Au...	PROPHECY\LORIKEET.M		4663	WinSecurity
2019-04-06T21:30:02	Windows File Access	COCKATOO	2845	Success Audit	Microsoft-Windows-Security-Au...	INTERSECT\CURRAWON		4663	WinSecurity
2019-04-06T21:30:02	Windows File Access	SWIFT	2845	Success Audit	Microsoft-Windows-Security-Au...	FINANCE\SWIFT$		4663	WinSecurity
2019-04-06T18:30:01	Windows File Access	SWIFT	9834	Success Audit	Microsoft-Windows-Security-Au...	PROPHECY\IBIS$		4663	WinSecurity
2019-04-06T18:30:01	Windows File Access	CURRAWONG	9834	Success Audit	Microsoft-Windows-Security-Au...	EMITE\COCKATOO$		4663	WinSecurity

An attempt was made to access an object. Subject: Security ID: S-1-3-18 Account Name: FROGMOUTH$ Account Domain: FINANCE Logon ID: 0xDA2 Object: Object Server: Security Object Type: Key Object Name: \REGISTRY\MACHINE\SOFTWARE\severe\slalom\Config Handle ID: 0x783 Process Information: Process ID: 0x469 Process Name: C:\Program Files\plucks\stuffy.exe Access Request Information: Accesses: Query key value Access Mask: 0x1 \REGISTRY\MACHINE\SOFTWARE\primer\plucks\Config

1 - 8 of 222 items

Example FIM, FAM, RIM and RAM Monitoring

The following tables are some examples of what can or should be monitored on systems. The exact list may vary from customer to customer and system to system but there are many baseline configurations that are common for most systems. Sometimes the settings can require tuning as different systems or customers use systems differently. What can work fine for one customer may cause a lot of noise for another. So try the settings and monitor for a few hours or days then tune out files that change to frequently if that's is normal activity. Sometimes implementing the new monitoring can uncover some bad behaviour that also needs remediation. So be very careful with removing what looks like noise as it could be some malicious activity going on.

Example for Windows systems that various security professionals have mentioned over time.

The list covers core part of Windows.

FIM and FAM monitoring for the following areas.

%WINDIR%/win.ini
%WINDIR%/system.ini
%WINDIR%\System32\*.exe
C:\Windows\System32\*.dll
C:\autoexec.bat
c:\Config.sys
C:\boot.ini
%WINDIR%\System32
%WINDIR%\regedit.exe
%WINDIR%\System32\drivers\etc\hosts
C:\Documents and Settings/All Users/Start Menu/Programs/Startup
C:\Users/Public/All Users/Microsoft/Windows/Start Menu/Startup

Examples for Windows Registry RIM and RAM monitoring

On Windows, the registry contains many useful locations that can also be monitored by Snare

HKEY_LOCAL_MACHINE\Software\Classes\batfile
HKEY_LOCAL_MACHINE\Software\Classes\cmdfile
HKEY_LOCAL_MACHINE\Software\Classes\comfile
HKEY_LOCAL_MACHINE\Software\Classes\exefile
HKEY_LOCAL_MACHINE\Software\Classes\piffile
HKEY_LOCAL_MACHINE\Software\Classes\AllFilesystemObjects
HKEY_LOCAL_MACHINE\Software\Classes\Directory
HKEY_LOCAL_MACHINE\Software\Classes\Folder
HKEY_LOCAL_MACHINE\Software\Classes\Protocols
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_LOCAL_MACHINE\Security
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\URL
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\Security\Policy\Secrets
HKEY_LOCAL_MACHINE\Security\SAM\Domains\Account\Users\Enum$

Areas that can be noisy and may be excluded

HKEY_LOCAL_MACHINE\Security\Policy\Secrets
HKEY_LOCAL_MACHINE\Security\SAM\Domains\Account\Users

The following Windows files can be ignored using the exclude feature in the Snare agents as they change too often and will create a lot of noise.

C:\WINDOWS/System32/LogFiles
C:\WINDOWS/Debug
C:\WINDOWS/WindowsUpdate.log
C:\WINDOWS/iis6.log
C:\WINDOWS/system32/wbem/Logs
C:\WINDOWS/system32/wbem/Repository
C:\WINDOWS/Prefetch
C:\WINDOWS/PCHEALTH/HELPCTR/DataColl
C:\WINDOWS/SoftwareDistribution
C:\WINDOWS/Temp
C:\WINDOWS/system32/config
C:\WINDOWS/system32/spool
C:\WINDOWS/system32/CatRoot

For Unix systems these examples can apply.

/etc
/boot
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/etc
/usr/local/bin
/usr/local/sbin
/usr/local/etc
/opt
/var/opt
/lib
/usr/lib
/var/lib
/usr/local/lib
/lib64

Specific files from other locations can also be monitored.

- Executable files in /tmp ,/usr/local/tmp, /var/tmp
- Plain files in /dev, other device files may not be suitable for monitoring as they will change to often

Locations that can sometimes be ignored as some of them can cause a lot of noise with many changes per second.

/etc/mtab
/etc/mnttab
/etc/mail/statistics
/etc/random-seed
/etc/adjtime
/etc/httpd/logs
/var/log/apache2/logs
/etc/utmpx
/var/log

About

Snare Solutions, part of the Prophecy International Holdings Group, is a team of leading information technology security specialists. In particular, the Snare Solutions team are noted leaders in key aspects of IT Security, including host intrusion detection. Our solutions have and continue to be used in the most sensitive areas of Government, Banking, Finance, Retail and commercial business sectors.

Prophecy International intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying security administration by abstracting the complexity away and/or solving complex security problems.

Prophecy International welcomes and values your support, comments, and contributions. For more information on the Enterprise Agents, Snare Central Server, Snare Advanced Analytics or Snare Advanced Threat Intelligence and licensing options, please contact us as follows:

The Americas	+1 (800) 834 1060 Toll Free +1 (303) 771 2666 Denver
Asia Pacific	+61 8 8213 1200 Adelaide Australia
Europe and the UK	+0 (800) 368 7423
Email	snaresales@prophecyinternational.com
Visit	www.snaresolutions.com

snare