

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

Whitepaper



## Contents

How Snare helps with FIM, FAM, RIM and RAM	3 3
FIM, FAM, RIM and RAM General Overview	
FIM, FAM, RIM and RAM Settings for Snare Enterprise Agent for Windows	6
FAM and FIM Settings for Snare Enterprise Agent for Linux	10
FAM Settings for Snare Enterprise Agent for Solaris and OSX	13
Reporting on FIM, FAM, RIM and RAM Log Activity	17
Example FIM, FAM, RIM and RAM Monitoring	19
FIM About	23



## 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.

SNARE ENTERPRISE AGENT FOR	RWINDOWS	
> Audit Service Status	> Objectives Configuration	
> Latest Events	The following parameters of the Snare objective may be set:	
> Destination Configuration	Identify the high level event	Clegon or Legoff
> General Configuration		Account Administration     Access a file or directory
> Access Configuration		Change the security policy     Start or stop a process
<ul> <li>Objectives Configuration</li> </ul>		<ul> <li>Restart, shutdown and system</li> <li>Use of user rights</li> </ul>
> Log Configuration		Filtering platform events     USB event
> Log Filter Configuration		Any event(s)
<ul> <li>File Integrity Monitoring</li> </ul>	Event ID Search Term Optional, Comma separated: only used by the Vary Event' setting above	Include     Exclude
> Registry Integrity Monitoring	Optional, Comma separated, only used by the Arty Event second above	· -
> HeartBeat & Agent Log	General Search Term	Include
> Audit Service Statistics	Used for event string match, file auditing is c1payroll, registry auditing is MACHINElkeyname Wildcards or regest functions only valid on event string match and not for file or registry auditing	C Exclude
<ul> <li>Security Certificates</li> </ul>	model of ingenie releases only hand on chain any model on the relief of regions booking.	c:tauditme Regular expression
> Users And Members	User Search Term	® Include
> License	Usernames, comma separated, Wildoards accepted	© Exolude
Ø Restart Service		
	Source Names, comma separated. Wildcards accepted	Include     Exclude
? Knowledge Base		•
User Guide (2)	Identify the event types to be captured	Booless Audit     de Jalver Audit     de Jalver Audit     Monte     Monneg     Grove     Cross     Active Sea
	Identify the event logs ignores if any solutions other than 'Any event(s)' is selected	X Security
OS Windows	Select the Alert Level	<ul> <li>Critical</li> <li>Principy</li> <li>Vataming</li> <li>Information</li> <li>Clear</li> </ul>
Build 5.3.0-10a4ca012 © Intersect Alliance Pty Ltd 1999-2019	Change Configuration Reset Form	



Audit Service Status	> Objectives Configuration	
Latest Events		
Destination Configuration	A Notice Changes have been updated but not yet applied	
General Configuration	The following parameters of the Snare objective may be set:	
Access Configuration	Identify the high level event	O Logon or Logoff
Objectives Configuration		<ul> <li>Account Administration</li> <li>Access a file or directory</li> <li>Change the security policy</li> </ul>
Log Configuration		Start or stop a process
Log Filter Configuration		<ul> <li>Restart, shutdown and system</li> <li>Use of user rights</li> </ul>
File Integrity Monitoring		<ul> <li>Filtering platform events</li> <li>USB event</li> </ul>
Registry Integrity Monitoring		Any event(s)
HeartBeat & Agent Log	Event ID Search Term Optional, Comma separated: only used by the 'Any Event' setting above	Include Exclude
Audit Service Statistics		
Security Certificates	General Search Term	(® Include
Users And Members	Used for event string match, file auditing is c/payroll, registry auditing is MACHINE\keyname Wildcards or regex functions only valid on event string match and not for file or registry auditing	Exclude     MACHINEVInterSect Alliance/Confid
License		Regular expression
Apply Configuration & Restart Service	User Search Term	Include
	Usernames, comma separated. Wildcards accepted	C Exclude
Knowledge Base		
User Guide	Source Search Term	Include     Exclude
	Source Names, comma separated. Wildcards accepted	- Exclude
	Identify the event types to be captured	Success Audit
	Identity the event types to be captured	Subbess Aubit     Failure Audit
		Information
		☑ Warning
		Error
		Critical
		Verbose
		Activity Tracing
	Identify the event logs	Security
	Ignored if any objective other than 'Any event(s)' is selected	System
		Application
		Directory Service
		DNS Server
		DFS Replication
		Legacy FRS
		Custom Event Log
	Select the Alert Level	Critical
Windows 8		Priority
		Warning
uld 5.3.0-16a4ca0f2		Information
Intersect Alliance Pty Ltd 1999-2019		© 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 dropdown 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.



SNARE ENTERPRISE AGENT	FOR WINDOWS	
> Audit Service Status	> File Integrity Monitor Configuration	
Latest Events		
> Destination Configuration	A Notee Charges have been updated but not yet applied	
General Configuration	The following monitor inputs may be set:	
<ul> <li>Access Configuration</li> </ul>	Salaet the Schudula	Custom
> Objectives Configuration	Custom schedules are supported by selecting the "Custom" option. Custom options are in crem format. For example, 15 10 **** defines a schedule that runs at 10*16am daily.	*****
> Leg Configuration		© Critical
Log Filler Configuration	Severity Level Marka all event generated with this severity level	O Priority
File Integrity Monitoring		Warning     Information
<ul> <li>Registry Integrity Monitoring</li> </ul>		® Clear
<ul> <li>HeartBeat &amp; Agent Log</li> </ul>	File or Directory An absolute path to the file or directory to monitor: Wildcards are supported. Recursion is supported using the * wildcard.	o./windows/system32/*
Audit Service Statistics	Inclusion Fermat	*.exe
Security Certificates	For example, 1 eve motiones on all evecutable files	(Drily used with 'File or Directory')
Users And Members		
> License	Exclusion Format For example. Two metobes on all generated top files	
<ul> <li>Apply Configuration &amp; Restart Service</li> </ul>	N CONTRACTOR OF CONT	(Dnly used with 'File or Directory')
# User Guide	About Policies     Remole Remole Remole Remole Management SGP Super Group Policy AGP Agent Group Policy LR Local Registry ID Default Value	
	Remote Perform management gas medicing and can only be easily and a special concertaging of beauty to beauty to beauty to be a set of the set o	



SNARE ENTERPRISE AGEN	T FOR WINDOWS							
Audit Service Status	> Latest Events							
- Latest Events								
Destination Configuration	A Notice Changes have be	en updated but not yet applied						
General Configuration	Destinations	Jestinations						
Access Configuration	Destination				Status	Average Per Second		
Objectives Configuration	10.1.5.7.0104 (TLS_AUTH TO	(9)			Connected	17.648, 33.1695		
Leg Configuration	10.1.8.1.0101 (TCP)				Connected	17.8x8, 33.16PS		
Log Filter Configuration	Last Heartbeat Sent							
File Integrity Monitoring	Heartbeats are daabled							
Registry Integrity Monitoring	Heartoesis are disabled							
HeartBeal & Agent Log	Event Logn Log Audit	File Integrity Registry Integrit	×					
Audit Service Statistics	File Integrity Monitoring	Events						
Security Certificates	Date/Time	System	Severity	File Name	Modifications			
Users And Members	2010-04-04 13 42 57	sharetest05 share ia	CLEAR	o windows lavstem 32 Nocad Wan Helper ere		4 43 40. Size 74552 bries. Owner: BUILTIN Administrators. Attributes. 0:20		
Licerse	2010-04-04 13 42 57	provedep 05 prove la	CLEAR	el windows agstern32 Npcap Nicos Haber era		4.43.40. Size 110550 bytes. Owner: BUILTIN/Administrators. Adminutes 0120		
Apply Configuration & Restart Serv		STATEMENTS STOLEN	ULEAR	-c. who was all seems 2 up to bring the part was	THE M PILE, CREAKE, 2010-341-25 C	A 2.40, Size 110030 Syles, Carrer, BUILTINGASHINGSSIST, ASTRONES 0120		
Knowledge Base	<i>a</i>							

SNARE ENTERPRISE AGEN	T FOR MINDOWS									# Replaned To: Svetana Shepty
> Aust Device Status	> Registry Integrity	Monster Confe	guration							
> Latest Events	The following registry is	cast and values	are being membered	by Snare						
> Destination Configuration	Acture	Policy	Schedule	Seventir Level	Registry Root Key	Registry Key or Value	inclusiona	Enclosiona	Lest Scen	Sieko
> General Configuration	Usiala Nodly	LR.	080911111	CLEAR	HEY LOCAL MACHINE	SOFTWARENINGSST	*		2018-Apr-08 07 56 00, 105652 Heal/Wave(s), Time 32 30 23	Scheduler: 2018-Jpr-08 11-44-00
> Access Configuration	Cease Koony									
> Olçantivas Configuration	Osiele Rodry	LB	CRONP****	CLEAR	HERY_LOCAL_MACHINE	SOFTWATE INterSect Allerce AudiService/Config?	*	82	2018-8p-02 11:45 00, 27 Key/Velle(#), 1Wel 00 00:14	Schedules: 2018-Apr-05 11:44:00
> Log Configuration	Benefit this buttern to an	97 9905								
> Log Filter Configuration		a new Konto	A44							
> File Integrity Monitoring	About Policies		2 1 12 2		tor UR Local Reports D Defect					
> Registry Integrity Monitoring	Remote Remote Mana Remote 50P and 40P r					Anthe				
> HeartBeat & Agent Log										
> Auck Service Statistics										
> Security Certificates										
> Users And Members										
> Literae										
Ø Restert Service										
7 Knowledge Base	a									
E User Guise	al a									

N1 FOR WINDOWS		· Registered To Southern Sheriff	
3 Registry Integrity Monton Configuration			
Custom antestises are supported by selecting the "Custom" option.			
Severity Level Marie al every personal with the severy level	O Charles		
	Q interview		
	# Clar		
Registry Root Key Vinteen Registry Root Vey	NKEY_LOCAL_MACHINE	2	
Restativ Sec or Value			
An advalute part to the Velue or Registry Key to monitor. Wildcards are supported. Recursion is supported using the Y wildcard.	SCHTWARE Mensols"		
Inclusion Format A more for the value research into the same Tale To match on all values	1		
	(Only used with Registry Key or Velue)		
Exclusion Parman A format for the value names to evaluate from the scan. Wildowsta are supported.	(One used with Review Key of Volum)		
Charge Configuration Read Fant			
27 About Polices     Bonne Monopolerer 507 Fuer Decip Faces Add Agent Decip Policy 18 Lises Regimy, 30 Debut Voles     Revues, 107 Mol Of the Index researching and and the Second Deputy addresses			

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:

SNARE ENTERPRISE AGENT F	OR LINUX							# Registered To:
> Audit Service Status	> Objectives Configur	ration						
> Latest Events	Objectives							
> Destination Configuration		ectives are active. Filtering object	tives allow a user to define whi	ich system calls (syscalls) are	rapped by the Snare age	ant These can be defined below:		
> General Configuration	Action	Criticality	Event Source Match			Filters Match	Regex Match	
> Access Configuration	Delate Modify	INFO	execute fork, exit kill tidl.	rgkill				Down
> Objectives Configuration		PRIORITY	februard chemod februards	at chown Johown februar februar	nat			
> Log Configuration	Delete Modily				nan.			Up Down
Log Filter Configuration	Delete Modify	WARNING	Ink,linkat.mknod.unlink.	unlinkat,symlink,symlinkat				Up Down
File Integrity Monitoring     HeartBeat & Agent Log	Dolete Modify	PRIORITY	mount,umount2					Up Down
Audit Service Statistics		PRIORITY	setfouid setuid setrouid.	setfsgid,setregid,setgid,setres	ad			
<ul> <li>Security Certificates</li> </ul>	Delete Modily							Up Down
> Users And Mombers	Delete Modity	CRITICAL	reboot, settimeolday, doi	ck_settime.setdomainname.se	thostname			Up Down
> License	Dalete Modify	INFO	login_start,login_auth.lo	gout				Up Down
Ø Restart Service	Add							
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1							
	File Watches The following file watche				211100000000000000000000000000000000000	10010-012-01-01-00		
Ciser Oulde	Action	s are active. File watches allow a	Criticality	n activity on a directory or life. Path	Permissions	Regex Match		
	-		INFO	ren	wa	Kegex Match		
	Delete Modfy		ini v	100			Up Dawn	
06 Linx Build 5.2.2-38acte12 © <u>Internet: Allence Pty Ltd</u> 1999-2019	ar. 14							
Audit Service Status     Latest Events	> File W	Atcher Objective Configu						
> Destination Configuration	I he follow	ving parameters of the Sna	ire hie watcher objective	may be set				
> General Configuration	File wat	ch path				/etc		
	Permiss	sions to trigger an event				wa		
> Access Configuration								
<ul> <li>Objectives Configuration</li> </ul>	Regular	Expression Match Type				Include     Exclude		
<ul> <li>Log Configuration</li> </ul>						- Licitite		
<ul> <li>Log Filter Configuration</li> </ul>	Option, is	* Expression Match s: .*root.*						
> File Integrity Monitoring	Select t	he Alert Level				Critical		
> HeartBeat & Agent Log						Priority		
> Audit Service Statistics						Warning     Information		
<ul> <li>Security Certificates</li> </ul>						Clear		
Users And Members	Change	Configuration Reset Fo	orm					
> License								
2 Restart Service								
? Knowledge Base	C <sup>a</sup>							
User Guide	$\mathbb{C}^n$							
OS Build 5.2.2 © <u>Intersect Alliance Pty Ltd</u> 1999-20	Linux 2-38acfe124 019							

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

- $\cdot$  Select the Add button
- $\cdot$  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 t's the path to that location. If you require a recursive search from that location, then enter /\* at the end asper 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

 $\cdot$  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

	ENT FOR LINUX									
Audit Service Status	> File Inte	grity Monitor C	onfiguration							
Latest Events										
Destination Configuration		The following monitor inputs may be set:								
General Configuration	Select the	Schedule wrt.es are sum	orted by selectio	a the "Custom" online	n			Ho	utly	
Access Configuration	Custom opt	ions are in cron	format. For exam	nple, 15 10 *** defin	n. es a schedule that runs at	10:15am daily:				
Objectives Configuration	Severity L	Soverity Levol Maris all event generated with this severity level							ritical	
Log Configuration	Marks all er	rent generated w	ith this severity i	evel				ev	nonty /aming	
								0 k 0 c	formation lear	
Log Filter Configuration	File or Dir	ectory						/et		
File Integrity Monitoring	An absolute	path to the file o	r directory to mo	mitor. Wildcards are :	supported. Recursion is su	ported using the /*	wildcard.	/et	c	
HeartBeat & Agent Log	Inclusion	Format e, *.exe matches								
Audit Service Statistics	Forexample	e, "lexe matches	on all executabl	e files				(Onl	y used with 'File or Directory')	
Security Certificates										
Users And Members	Exclusion For example	Format e, *Jog matches	on all generated	log files						
License				-				(Onl	y used with 'File or Directory')	
7 Restart Service	_	_								
		onliguration	Reset Form							
Knowledge Base	About Po	licies								
8 User Gulde	SGP Super SGP and AG	P settings are rea	ad-only and can	only be edited by gro	al Registry D Default Va up policy administrator	ue				
										P Registered To: Stave C
Audit Service Status	> File Integrity Mon	itor Configuration	1							
Lalesi Events	The following files are	boing monitored b	y Seare:							
Destinution Configuration	Actions		Schedule	Severity Level	File or Directory	File Format	Exclusions		Status	
Access Configuration	Dalete Modily	LR	Bhourly	CRITICAL	/etc			2019-Apr-08 11:59:59, 86 Files, Time: 00:00:01	Scheduled 2019	Apr-08 13:00:00
Objectives Configuration	Dakte Modily	LR	ghourly	CLEAR	/eto/bind			2019-Apr-08 11:59:59, 13 Files, Time: 00:00:01	Scheduled: 2019	Apr-08 13:00:00
Log Configuration		UR	Ghourly	CRITICAL	/ver/lib/bind			2015-Apr-08 11:59:59, 1 Files, Time: 00:00:01	Scheduled 2015	Law-08 13/00 00
Log Filter Configuration	Dalcto Notify		di nord	Charlon.					0.100.000.2010	
File Integrity Monitoring	Select this button to ad	id a new Monitor.	Add							
HeartBeat & Agent Log	About Policies									
Audit Service Statistics	About Policies SGP Super Group Pol	loy AGP Agent G	roup Policy LR I	.ocal Registry D Defa	ult Value					
Audit Service Statistics Security Certificates	About Policies SGP Super Group Pol SOP and AOP settings of	icy AGP Agent G are read-cety and ca	roup Policy LR I an only be edited by	.ocal Registry D Defa group policy administra	ult Value tor					
Audit Service Statistics Security Contilicates Usars And Members	About Policies SGP Super Group Pol DOP and AOP settings of	icy AGP Agent G menead-only and ca	roup Policy LR I in only be edited by	.ocal Registry D Defa group policy administra	nult Value for					
Audit Service Statistics Security Cottilicates Users And Members	About Policies SGP Super Group Pol SOP and AOP settings (	icy AGP Agent G ne read-only and ca	roup Policy LR I in only be edited by	.ocal Registry D Defa group policy administra	uit Value for					
HeartBest & Agent Leg     Audit Service Statistics     Society Cartificates     Users And Members     Liberte     Context	About Policies SGP Super Group Pol SOP and AOP settings of	icy AGP Agent G ne read-only and ca	roup Policy LR I in only be edited by	.ocal Registry D Dela	sult Value for					
Audit Service Statistics     Socurity Certificates     Uears And Members     License	About Policies SGP Super Group Pol GOP and AOP settings of	icy AGP Agent G	roup Policy LR I in only be edited by	.ocal Registry D Dela	sult Value for					
Audit Service Statistics Security Certificates Usars And Members Lionne 2 Restart Service	About Policies SGP Super Group Pol GOP and AOP settings (	icy AGP Agent G	roup Policy LR I in only be edied by	.ocel Registry D Data	ull Value					
Audi Sunica Statistics Socially Certificates Usans And Members Usanse Prestart Senice Keronledge Dase (2)	About Policies SGP Super Group Pol SGP and AOP antilige of SGP and AOP antilige of	icy AGP Agent G	roup Policy LR I in only be edited by	.ocal Registry D Defa	u II Vahue for					
Auft Service Statistics Security Contractes Users And Wombers Users  Protect Service  Noronkoge Dave  Der Guide  C	SGP Super Group Pol OOP and AOP settings a	loy AGP Agent G	roup Policy LR I in only be edited by	.coal Registry D Defa	uð Valus					
Andt Dervice Statistics Security Contractures Ubares And Wombers Ubares And Wombers Recording Ease () Police Guide ()	SGP Super Group Pol OOP and AOP settings a		reup Policy LR I	.coal Registry ID Data	ell Value for					
Andi Barvice Butatics Security Contractans Ubars And Wombers Ubars And Wombers Breaket Service Des Cause Contractant Service Status	SCP Stops Oraci Pad 30P and AOP settings of 20 20 20 20 20 20 20 20 20 20 20 20 20	vents	reup Policy LR I en only be edited by	.coal Registry ID Data	nil Value for					
Add Tarvis Statutos Sacaty Cottacas Usars Add Mathems Usars Add Mathems Pastart Starks Neokolgo Base (C) Der Galde C) Der Galde Add Skrivice Status Latest Events	SCP Stops Outp Pd SCP stops Outp Pd SCP and ACP settings of CO CO CO CO CO CO CO CO CO CO	vents	reup Policy LR II en only be edited by	.coal Registry ID Deta	vit Value for					
Auft Barvice Statutes Sacarity Contratuan Usans Auft Warbers Usans Penter Service Penter Service Contratus Service Auft Service Status Destination Configuration	SCP Stops Oraci Pad 30P and AOP settings of 20 20 20 20 20 20 20 20 20 20 20 20 20	vents	ince Poloy LR I	.coti Pogitery D Dete	nil Value for		Status	۸	verage Par Second	
Add Bavke Bateles Sacaity Collitation Sacaity Collitation Users Add Workers Users Add Workers Resolution Resolutio Resolu	SCP Stops Outp Pd SCP stops Outp Pd SCP and ACP settings of CO CO CO CO CO CO CO CO CO CO	vents ns	irous Policy LR I en esty be edited by	.codi Registry D Data	vil Value tor		Status Connected		verage Per Second 18 - 18 EPS	
Audi Raveke Statutes Saunity Contratante Uteres Auf Membres Uteres Auf Membres Vere Grade Audit Service Status Latest Events Dastanation Configuration General Centigrantion Access Configuration	SCP Steps One PM SOP and ADP willings of PM ENT FOR LINUX ENT FOR LINUX Destination Destination 10.11.316	vents ins n 161 (TCP)	roup Policy LR I no only be edited by	.coli Registry. D Dati s	në Valua For					
Auft Reves Ratatics Saunty Contrature Users Auft Mehres Users Rested Service Revelacing S	ENT FOR LINUX ENT FOR LINUX ENT FOR LINUX Linux Destinatio Last Hear	vents ns 1161 (TCP) tbeat Sent	roup Policy LR I on only be edited by	.codi Registry. D Defa	në Vahan Ke					
Auft Revek Ruters Security Contracture Uters Auft Werkers Uters Workloge Das Uters Workloge Das Workloge Das Worklog	SCP Exer One hit SCP ex	vents ins n 161 (TCP) tbeat Sent re disabled			në Vahan Ke					
Add Barvke Statutes Sandry Celtatute Users Add Wankes Users Add Wankes Users Add Wankes View Celtatu Add Sarvke Statute Add Sarvke Statute Label Events Dastination Configuration Access Configuration Ling Configuration Ling Configuration	SCP Exer One hit SCP ex	vents ns 1161 (TCP) tbeat Sent			në Valua Ke					
Aufi Ravke Statutes Sauti Contraute Sauti Contraute Utares Aufi Manhas Utares Result Savide Aufi Savide Status Latest Events Dastanation Configuration Colpactives Configuration Colpactives Configuration Lag Configuration Lag Tither Configuration File Inspirity Montoring	SCP Speer Ones Md SCP seer Ones Md SCP and SCP wellow EXAMPLE Destination Units Hear Units Hear Units Astronomics	vents n 161 (TCP) tbeat Sent re disabled it Log Audi	1 File integ		në Vahan Ke					
Aufi Ravke Statutes Sauti Contraute Sauti Contraute Utares Aufi Manhas Utares Result Savide Aufi Savide Status Latest Events Dastanation Configuration Colpactives Configuration Colpactives Configuration Lag Configuration Lag Tither Configuration File Inspirity Montoring	EXT FOR LINUX EXT File Integr	vents n 161 (TCP) tbeat Sent tre disabled ti Log Aad	1 File Integ	19			Connected	K		
Aufi farvis fautors Sauti Contrauto Sauti Contrauto Uters Aufi Methes Uters Aufi Methes Contrauto Readed Service Contrauto Con	SCP Speer Ones hit SCP Speer Ones hit SCP Speer Ones hit SCP seeby one school webger of SCP Speer Ones hit S	vents n 1651 (TCP) tibeat Sent it Log Audi tit Log Audi	: File integ ing Events Syst	10	Severity	File Name	Connected	< Medifications	18. «1 EPS	
Auft Rovice Statutes Saunity Contraute Uters Auft Weiters Uters Woolndge Das  Perter Statute Configuration Auft Savice Statute Configuration C	SCP Speer Orace Ma SOP and AD wellow CP CP CP CP CP CP CP CP CP CP CP CP CP	vents ins n 1161 (TCP) tbeat Sent rer disabled It Log Audi ty Monitorin 2 15.17.46	s File Inneg ng Events Syst VMU	eyr enn buntut 804464	Severity CHITICAL	/etc/mtab	Connected	Kodifications ChANGE FILE: Modified 2018 Sup-26 11 40	18. <1 EPS 15	
Adh Barvis Subaics Subaics Subaics Subaics Unava Instant Subaics Instant Subaics Instant Subaics Audi Sarvis Cathyana Ca	SCP Gaser Ones Pd 50P each Ones Pd 50P each Ones Pd 50P each Ones Pd 50P each One Pd 5	vents ins infifi (TCP) iteat Sent ite disabled it Log Audi ity Monitorins 2 15.17.46 2 15.17.45	t File integ ng Events Syst VMU VMU	riv em burtu 1884;44	Severity CRATICAL CRATICAL	/etc/mtab /etc/mtab	Connected	Kodifications CHANGE FILE, Modified 2018-Sep-06 11 40 CHANGE FILE, Modified 2018-Sep-06 11 40	18. <1 EPS 15 15	
Aufi Ravke Satalics Sauti/ Cathatai Uario Aufi Manis Satalics Itario Satalics Result Savice Satalics Cathatis Savice Satalics Cathatis Configuration Caperties Configuration C	SCP Speer Orace Ma SOP and AD wellow CP CP CP CP CP CP CP CP CP CP CP CP CP	vents ins infifi (TCP) iteat Sent ite disabled it Log Audi ity Monitorins 2 15.17.46 2 15.17.45	t File integ ng Events Syst VMU VMU	eyr enn buntut 804464	Severity CHITICAL	/etc/mtab	Connected	Kodifications ChANGE FILE: Modified 2018 Sup-26 11 40	18. <1 EPS 15 15	
Audi Savice Statutes Saunty Cathatas Usars dat Manhas Usars dat Manhas Usars dat Manhas Usars dat Manhas Audi Savice Statutes Audit Savice Statutes Capacities Configuration General Configuration General Configuration Lag Configuration Lag Configuration Lag Configuration Lag Configuration Lag Configuration Lag Configuration File Integrity Monitoring File Integrity File Fil	SCP Gaser Ones Pd 50P each Ones Pd 50P each Ones Pd 50P each Ones Pd 50P each One Pd 5	vents           ins           n           1651 (TCP)           tibbalt Sent           ing disabled           it           Log Aud           it           15.17.46           2 15.17.45	r File Integ Syst VMU VMU VMU	riv em burtu 1884;44	Severity CRATICAL CRATICAL	/etc/mtab /etc/mtab	Connected	Kodifications CHANGE FILE, Modified 2018-Sep-06 11 40 CHANGE FILE, Modified 2018-Sep-06 11 40	18, <1 EPS 15 15 15	
Audi Savice Statutes Saunty Cathatas Usars dat Manhas Usars dat Manhas Usars dat Manhas Usars dat Manhas Audi Savice Statutes Audit Savice Statutes Capacities Configuration General Configuration General Configuration Lag Configuration Lag Configuration Lag Configuration Lag Configuration Lag Configuration Lag Configuration File Integrity Monitoring File Integrity File Fil	SCP Speer Ones hit SCP and OP webger SCP SCP SCP SCP SCP SCP SCP SCP SCP SCP	vents ins iffi (TCP) itbeat Sent itc Log Audi it Log Audi itg Monitorin - - 2 15 17 45 2 15 17 45 2 15 17 45 2 15 17 45	t TBe Integer Ing Events VMULU VMULU VMULU	em buntus 104464 buntus 104464	Severity CRITICAL CRITICAL CRITICAL	/etc/mtab /etc/mtab /etc/mtab	Connected	Kodifications CHANGE FILE, Modified 2018 Sep 26 11 40 CHANGE FILE, Modified 2018 Sep 26 11 40 CHANGE FILE, Modified 2018 Sep 26 11 40	18 <1 EPS 15 15 15 15	
Audi Sarvice Statutes Saunity Cathatas Usars dat Manis Saunity Restart Sarvice Audit Sarvice Statutes Cathatas	SCP Speer Orace Ma SCP acted Orace Ma SCP action to web years Destination Dest	with           I           1161 (TCP)	t File more ing Events System Value Valu	em em bantu 1804.054 bantu 1804.054 bantu 1804.054	Severity CRATICAL CRATICAL CRATICAL CRATICAL	/etc/mtab /etc/mtab /etc/mtab /etc/mtab	Connected	Kotffeetions CHANGE FILE, Modified, 2018-Sep-06 11 40 CHANGE FILE, Modified, 2018-Sep-06 11 40 CHANGE FILE, Modified, 2018-Sep-06 11 40	18. «1 EPS 19. 15. 15. 15.	
Auft Barvice Statutes Sacarity Contratuan Usans Auft Warbers Usans Pended Service User Cells Contra Status Auft Service Status Destination Configuration	SCP Exer Orace Ma SCP Exer Orace Ma SCP exer Orace Ma SCP exer Orace Ma Destination Units A Exer File Integr 2015-660 20	www.sec.           ns           1           1681 (TCP)           2016 (TCP)     <	1 <b>File house</b> <b>Systems</b> VAUU VAUU VAUU VAUU VAUU	etv m burtu 1884x64 burtu 1884x64 burtu 1884x64 burtu 1884x64 burtu 1884x64 burtu 1884x64	<b>Sevetity</b> СКИТСАЦ СКИТСАЦ СКИТСАЦ СКИТСАЦ СКИТСАЦ СКИТСАЦ СКИТСАЦ	/etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab	Cennecled	Modifications           CHANGE FILE, Modified 2018-Sep-06 1140	18. «1 EPS 19. 15. 15. 15.	
Aufi Ravke Statutes Sauti Contraute Users Aufi Mentes Users Aufi Mentes Users Aufi Mentes Contrautes Research Contrautes	SCP Speer Owen Hall SCP asser Owen Hall SCP and SCP seebyon EXP FOR LUNUX EXP FOR LUNU	www.switchild	1 File houge by Events Value V	199 em buntus 804/064 buntus 804/064 buntus 804/064 buntus 804/064 buntus 804/064 buntus 804/064	Severity CRATICAL CRATICAL CRATICAL CRATICAL CRATICAL CRATICAL CRATICAL CRATICAL	/etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab	Cennecled	Modifications           CHANGE FILE, Modified 2018 Sup 26 11 40           CHANGE FILE, Modified 2018 Sup 61 140	18 «1 EPS 15 15 15 15 15 15 15 15 15	
Aufi Ravke Statutes Sauti Contraute Users Aufi Mentes Users Aufi Mentes Users Aufi Mentes Contrautes Research Contrautes	SCP Speer Orace Ma SCP Speer Orace Ma SCP and SCP seeby or selection Destinati	www.s           rs           i <td>া Fab rouge ng Events গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে</td> <td>em buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054</td> <td>Severity           CRATICAL           CRATICAL</td> <td>/etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab</td> <td>Connected</td> <td>Modifications           CHANGE FILE, Modified 2018-sep-66 11 40           CHANGE FILE, Modified 2018-sep-66 11 40</td> <td>18 «1 EPS 15 15 15 15 15 15 15 15 15 15</td> <td></td>	া Fab rouge ng Events গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে গমানে	em buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054 buntu 1804.054	Severity           CRATICAL	/etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab	Connected	Modifications           CHANGE FILE, Modified 2018-sep-66 11 40	18 «1 EPS 15 15 15 15 15 15 15 15 15 15	
Aufi Ravke Statutes Sauti Contraute Users Aufi Mentes Users Aufi Mentes Users Aufi Mentes Contrautes Research Contrautes	SCF Speer Orase Ma SOF asset Orase Ma SOF asset Orase Ma Destination Units of the Units Destination Units of the Units Destination Units of the Units Destination Units of the Units Destination Desti	www.sets           m           1           1           1           1           1           1           1           1           1           1           1           2           1           2      2 <tr tr="">          2&lt;</tr>	হ <b>Feb rengy</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Systems</b> <b>Syst</b>	em buntus 804/64 buntus 804/64 buntus 804/64 buntus 804/64 buntus 804/64 buntus 804/64	Severity           CRITICAL	/etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab	Connected	Modifications           CHANGE FILE, Modified, 2015-Sep-06 11 40	15 15 15 15 15 15 15 15 15 15 15 15 15 1	
Aufi Ravke Statutes Sauti Contraute Users Aufi Mentes Users Aufi Mentes Users Aufi Mentes Contrautes Research Contrautes	SCP Exer Orace hit SCP exer Orace hit SCP exer Orace hit SCP exer Orace hit SCP exer Orace hit Destination I 11 131 Last Hear Hear Beats 2015-460 2	www.sets           r<	1 <b>File more</b> Systems VARU VARU VARU VARU VARU	rty Burtu 1884;64 Burtu 1884;64 Burtu 1884;64 Burtu 1884;64 Burtu 1884;64 Burtu 1884;64 Burtu 1884;64 Burtu 1884;64 Burtu 1884;64 Burtu 1884;64	Severby           СКИТСАL           СВИТСАL	/etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab /etc/mtab	Centected	Modifications           CHANGE FILE, Modified 2018-Sep-66 1140	18. «1 EPS 19. 15. 15. 15. 15. 15. 15. 15. 15. 15. 15	
Aufi Ravke Statutes Sauti Contraute Users Aufi Mentes Users Aufi Mentes Users Aufi Mentes Contrautes Research Contrautes	SCP Speer Orace hild needs of the series of	ns	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ety ety buttus 1064/c4 buttus 1064/c4 butt	Severity           CRITICAL	Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab	Centected	Modifications           CHANGE FILE, Modified 2018-Sep-06 11 40           CHANGE FILE, Modified 2018-Sep-06 11 40	18 «1 EPS 15 15 15 15 15 15 15 15 15 15	
Aufi Ravke Statutes Sauti Contraute Users Aufi Mentes Users Aufi Mentes Users Aufi Mentes Contrautes Research Contrautes	SCP Speer Orace hit SSP and CP seeks or seeks or seeks or or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or seeks or	www.s           rs           s           isit (TCP)	Fail Integration           System           VALUE	em burut 1864/4 burut 1864/4	Severity           CRITICAL           CRITICAL	Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab Astcimtab	Connected	Modifications           CHANGE FILE, Modified 2018-Sep-661 140	18 «1 EPS 15 15 15 15 15 15 15 15 15 15	
Audi Savoka Subatoka Savahi'y Cantibatan Umari Gali Mambal Umari Gali Mambal Kasata Savoka Audit Savoka Satata Labet Events Dastanatin Configuration Colpectives Cantiguration Colpectives Cantiguration	SCP Speer Orace hild needs of the series of	www.s           rs           s           isit (TCP)	Fail Integration           System           VALUE	ety and a second secon	Severity           CRITICAL	Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab Asterntab	Connected	Modifications           CHANGE FILE, Modified 2018-Sep-06 11 40           CHANGE FILE, Modified 2018-Sep-06 11 40	18 «1 EPS 15 15 15 15 15 15 15 15 15 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,sym link

- In the Search Term field enter the file(s) to be monitored. ie <a href="https://etc/(passwd/shadow">https://etc/(passwd/shadow</a>)\$
- 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:

		Ŷ
		Snare Enterprise for Solaris
Latest Events Network Configuration		Objective Configuration
Objectives Configuration Remote Control Configuration	Identify the high level event	© Login/Logout events © Open a file/dir for reading only © Witte 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 outoping network connection © Any Event(s)
View Audit Service Status Apply the Latest Audit Configuration	Search Term	open_rc,open_rt,open_rtc,open_rw open_rwc.open_rwt.open_rwtc,creat,mkdir,mknod.link,symlink
Display a list of Users Display a list of Groups	Select the General Match Type	Include      Exclude
Display a list of GroupMembers	General Search Term (regular expression)	//etc/(passwd shadow)\$
	Select the User Match Type	O Include ® Exclude
	Term	root
	Identify the event types to be captured	🕄 Success Audit 🛑 Failure Audit
	Select the Alert Level	Critical O Priority O Warning O Information O Clear
	Change Configu	(c) Intersect Alliance Pty Ltd 1999-2014. This site is powered by <u>Snare Externise for Solaris</u>
		(c) annexes mining evolution approach, this are is powered by an exemption of access to access to a solution.

The v5 OSX agent has the following configuration settings.



	MACOS		# Registered To: xxx_Custemer	Alpha_xe
> Audit Service Statue	> Objectives Configuration			
> Latest Events				
> Destination Configuration	A Notice Changes have been updated but not yet applied			
> Access Configuration	identify the high level event			
> Objectives Configuration		Change user or group identity Establish an outgoing network connection		
> Log Configuration		Login/Logost events Modify system, file or directory attributes		
> Log Filter Configuration		Open a file/dr for reading only O Remove a file or directory		
> File Integrity Monitoring		<ul> <li>Start or stop program execution</li> <li>White or create a file or directory</li> </ul>		
> HeartBeat & Agent Log		Any Event(s)		
> Audit Service Statistics	Event ID Search Term			-
> Security Certificates			pan_wt.open_wto.open_wv.open_rwt.spen_rwt.creat.mkclit.mkned.ymkned.link.cyminicumdrumink.raname.tumcate.ftruncate	(h)
> License	Salact the General Match Type	B thoude Exclude		
✓ Apply Configuration & Rostart Service	General Search Tenn (regulær expression)	*/elc/(passwd)shadww/8		
? Knowledge Base □	Select the User Match Type	8 Include Exclude		
🖉 Usar Gulda 🛛 🖓	User Search Term			
	User Search Term	2		
	Identify the event types to be captured	R Success Audit	10 Falue Audi	
	Solect the Alert Level	Critical Critical Warning Sinformation Clear		
CÓ Davie	Change Configuration Reset Form			
Build S3.0-RC1-00880e33				

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:

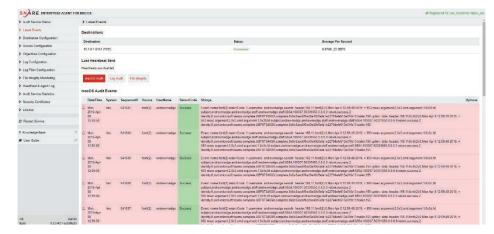
- Access a file or directory.
- These can be combined with other system calls for open\_rc,open\_rt,open\_rtc,open\_w,open\_wc,open\_ wt,open\_wtc,open\_rw,open\_rwt,open\_rwtc,creat,mkdir,mknod,xmknod,link,symlink, rmdir,unlink,r ename,truncate,ftruncatet

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.



SNARE ENTERPRISE AGENT FOR	R MACO S	
> Audit Service Status	> File Integrity Monitor Configuration	
> Latest Events	The following monitor inputs may be set:	
> Destination Configuration	The rolewing monitor inputs may up set: Select the Schedule	
> Access Configuration	Custem schedules are supported by selecting the "Custom" option.	Custom
> Objectives Configuration	Custom options are in cron format. For example, 15 10 * * * defines a schedule that runs at 10: tSam daily.	*****
> Log Configuration	Severity Level Maria all event constaled with this severity level	Critical Priority
Log Filter Configuration		© Warning © Information
> File Integrity Monitoring		© Clear
> HeartBeat & Agent Log	File or Directory An abselute path to the tile or directory to monitor, Wildcards are supported. Recursion is supported using the # wildcard	/Users/andrewmadge/Documents/FIM/
> Audit Service Statistice	Inclusion Format	
> Security Certificates	For example, " eve matches on all executable files	".log (Oely used with 'File or Directory')
> License		(Cerry Liced went Pille of Linescory )
C Restart Service	Exclusion Format	
C Restart Dervice	For example, "tog matches on all generated log files	(Only used with 'File or Directory')
? Knowledge Base		
🖉 User Guide 🛛 🖄	Change Cartiguration Reset Form	
	About Palicies Renos Fences Unsequence: SOP Sign: Group Folicy: ACP Agent Group Policy: LR Local Registry: D Debuit Value Randot, SOP end ACP-relative are read-only and can only be estible by show policy administrative	

	ENT FOR MACOS				# Registered To	. xxx_Contorner Alpha_xxx				
> Audit Service Status	> Latest Events	> Latest Events								
> Latost Events	Destinations	Destinations								
> Destination Configuration	Destination			Stetus	Average Par Second					
> Access Canilguration	10.1.6.1.6161 (TCP)			Connected	32.540, 87.4EPG					
> Objectives Configuration										
> Log Configuration	Last Heartbeat Sent									
> Log Filter Configuration	Heartbeats are disabled									
> File Integrity Monitoring	macOS Audit Log	Audit Elle Integrity								
> HeartBeat & Agent Log										
HeartBeat & Agent Log     Audit Service Statistics	File Integrity Monitor									
	File Integrity Monitor Date/Time		Severity	File Name	Medifications					
> Audit Service Statistics		ing Events System Nice	Severity INFO	File Name Alternated actually=Documents=FM/act90 log	Modifications CREPTE PLR Modified 2419-40-42 11 36 36					
Audit Service Statistics     Security Certificates     License	Date/Time	ing Events System								
Audit Service Statistics     Security Certificates	Date/Time 2015-04-06 84 13:00	ing Events System Nice	INFO	Aberta'end extractive Documents F Mideat 99 log	DELETE FILE, ModBed 2019-Ap-02 11 36 38					
Audit Service Statistics     Security Certificates     License	Date/Time 2015-04-06 84 13:00	ing Events System Nice	INFO	Aberta'end extractive Documents F Mideat 99 log	DELETE FILE, ModBed 2019-Ap-02 11 36 38					



# 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.

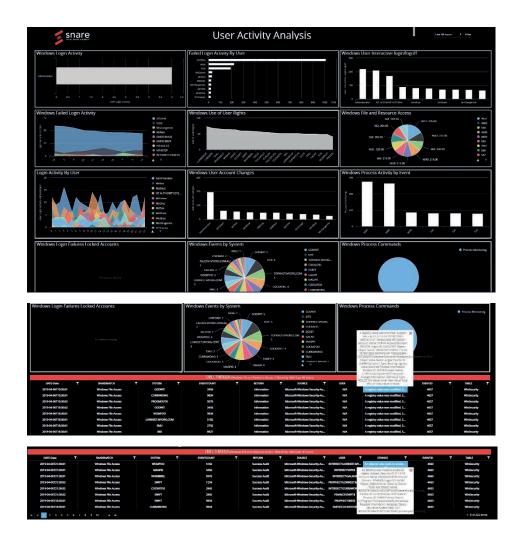
These reports can be run interactively or scheduled to run overnight to report on specific time periods.

2	Query the G	Beneric Log for events of intere	ast				Generated: 03 May 2018 12:43:11 [Duration: 00:00:0
allem Map	1	Tabular Dolaile Pie Grep	sh Patiern Mag	>2			
attern	n map of	events over time					
		2 X 41 4	, Me	ve mouse cursor over a squar	Query Results e to display the value, and click t	he square to view the raw logs	a a a a a a a
Key 1		a, a a a					
oorts : O	perating Syst	tems : File and Resource Acce	ess : Windows : Snare FIN	lactivity			
	Query the 0	Generic Log for events of inte	erest				Generated: 03 May 2018 12:43:11 [Duration: 00:00:03
0-	-						
tern Map		Tabular Details Pie G	iraph Patter	n Map 2			
DATE	prev 1 n	ext > last >> SYSTEM	CRITICALITY	DIGESTTYPE	EVENTACTION	OBJECTTYPE	OBJECTNAME
018- 5-03	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:\windows\system32\xwizard.exe
018- 5-03	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:\windows\system32\xcopy.exe
018- 5-03	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:\windows\system32\wusa.exe
018- 5-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:/windows/system32/WUDFHost.exe
018-	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:/windows/system32/wuaucit.exe
018- 5-03	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:\windows\system32\wuapp.exe
018-	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:\windows\system32\wsgmcons.exe
5-03 018-	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:/windows/system32/wsmprovhost.exe
5-03 018-	10:50:20	10.1.4.6		SHA-512	NEW	FILE	c:/windows/system32/WSManHTTPConfig.exe
5-03 018-							
5-03	10:50:20	10.1.4.6	-	SHA-512	NEW	FILE	c:\windows\system32\wscript.exe
2018-	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	Horizontal Graph Line Graph PDF Dutput RealTime Alter Pie Graph 2 Threshold Reporting Annotations							
	Drop Components Here to add them to the objective output							
	📖 🔜 🥌 📖 🧇							
	Pattern Map Tabular Details Pie Graph Pattern Map 2 Access Flags							
Access Flags	Select the desired actions to report on. If no options are selected, all file operations are reported.							
	<ul> <li>New folder added</li> <li>Modify a file</li> <li>Directory Listing</li> <li>File or directory query</li> </ul>							
	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.





## 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

 ${\sf HKEY\_LOCAL\_MACHINE\Software\Classes\batfile}$ 

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

 ${\sf HKEY\_LOCAL\_MACHINE\Software\Classes\Protocols}$ 

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

 ${\sf HKEY\_LOCAL\_MACHINE}\ Software \verb|Microsoft|Windows|CurrentVersion|Run|$ 

 ${\sf HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current\Version\RunOnce}$ 

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.snaresolutiions.com

