

McAfee Integration Guide

Table of Contents

OVERVIEW	1
Prerequisites Deployment Architecture	1 2
OBSERVEIT CONFIGURATION	3
MCAFEE ESM CONFIGURATION	5
MCAFEE SIEM COLLECTOR CONFIGURATION	6
VIEWING EVENTS	9
CREATING ALARMS	10
Alarm Examples	11
SUPPORT	12
RELEASE NOTES	12



Overview

This document describes the ObserveIT integration with McAfee Enterprise Security Management (ESM),

McAfee ESM is a security information and event management (SIEM) solution used to prioritize, investigate, and respond to threats.

This integration provides security analysts and security investigation teams with powerful user-activity metadata and smart user behavior alerts.

Prerequisites

The ObserveIT integration is generally available in ESM. If you don't see the ObserveIT data source available, you will need to update your rule signatures.

- ObserveIT (Minimum supported version: 7.4)
- McAfee ESM (Minimum supported version: 11)
- McAfee SIEM Collector installed alongside ObserveIT Application Server



DEPLOYMENT ARCHITECTURE

This diagram shows how ObserveIT and McAfee ESM integrate.





- 1. Software agents capture user activity data and send it to the ObserveIT Application server.
- 2. ObserveIT Application server sends the user activity logs in an ArcSight Common Event Format (CEF) file to McAfee SEIM Collector.
- 3. McAfee SIEM Collector forwards the events from the ObserveIT SIEM logs into McAfee ESM.

ObserveIT Configuration

To configure ObserveIT configuration for integration with McAfee:

• Enable the integrated SIEM logs by selecting the logs you want McAfee to ingest. Windows and Unix Activity, Activity Alerts, System Events and Audit logs are supported.

NDPOINT DIARY USER DIARY	FILE DIARY	DBA ACTIVITY	ALERTS	CONFIGURATION	SEARCH
Admin Dashboard					
Console Users	ObservelT Logs	SIEM Log I	ntegration		
Identification	SIEM Log Integr	ation			
Endpoints	Activate SIEM log in	ntegration			
Endpoint Groups	Enable export to i	ArcSight format			
Recording Policies	Log data				
Security & Privacy	All selected types of I	og data will be stored in	the same file.		
Alert & Prevent Rules	Windows and Un	ix Activity			
Lists	Activity Alerts				
	DBA Activity				
In-App Elements (Beta)	System Events				
System Events	In-App element				
Identity Theft Detection	🛃 Audit				
Messages	Audit Sessi	ons			
Call Center Integration	Audit Logir	15			
Convice Deck Integration	Audit Confi	iguration changes			
Service Desk Integration	 Log file properties 				
License	The Folder location d	isplays the path to the c	urrent log files. To cha	ange the location, enter a new	path, and click "S
SMTP Settings	Folder location: C:\	Program Files\ObserveIT\N	otificationService\LogF	iles\ArcSight	
Integrated SIEM	File name: Oh	serveit activity log.cef		-	

• Enabling the file clean-up process to run every hour. This prevents the log file from becoming too large by deleting the older events and leaving the newer ones.



1	Log file cleanup		_
	Enable log file clean u	p.	
	Run daily at: Run every:	6:00 AM	
		Save Cancel	4



McAfee ESM Configuration

To configure McAfee ESM:

• Make sure you have a Local Receiver configured in McAfee ESM to receive the events being sent by the SIEM collector.



• Add an ObserveIT Data Source, configured as shown below. Specify the IP Address or Host ID with the location of the ObserveIT application server where the SIEM Log Collector runs.

Add Data Source	×
Use System Profiles:	No Profiles Defined
Data Source Vendor:	ObserveIT
Data Source Model:	ObserveIT
Data Format:	Default
Data Retrieval:	MEF
Enabled:	Parsing ELM SNMP Trap
Name:	ObserveIT CEF Logs
IP Address:	172.31.2.171
Host ID:	EC2AMAZ-18L6TVS
Use encryption:	
Time Zone:	(GMT,00:00) Greenwich Mean Time
Support Generic Syslogs:	Log "unknown syslog" event
Generic Rule Assignment:	User Defined 1
Interface Manage the	network interface for the parent Receiver.
Advanced	OK Cancel



Note: If ObserveIT Data Source type is not available, make sure you have updated your ESM to include the latest rule signature updates.

• Roll out the policy to all devices when the Data Source is created and you are prompted.

McAfee SIEM Collector Configuration

The McAfee SIEM Collector is used to forward the events from the ObserveIT SIEM logs into McAfee ESM.

- To configure McAfee SIEM Collector:
- Install the McAfee SIEM Collector Management Utility on your ObserveIT application server(s).
- Configure the collector to communicate with the ESM Receiver. Enter the receiver's IP address and port (default is 8082).

Note: **Receiver: Connecte**d in the bottom- left indicates a successful connection.

Receiver	Receiver Configuration			
SIEM Collector	The SIEM Collector is configured to send lo following IP address, on the specified McAf	g events to the R ee Event Format (eceiver locate (MEF) Port:	ed at the
	Receiver IP Address:	172.31.143.230		
	MEF Port:	8082		
	Selected Network Adapter	: 172.31.2.171	-	
	NOTE: To find the Receiver IP address and MEF P target Receiver in the System device tree, dick or select Receiver Configuration, then select the Int	ort, log on to the Mc n the Properties icon erface button.	Afee ESM dien	it, select the tree toolbar,



- Create a new host group and enable it.
- Add a new host to the host group.



- Configure the new host to read the ObserveIT SIEM log file.
- Enter the Host Name of the ObserveIT Application server. Under Clients, select Generic log tail from the drop down and click Add Client
 - The Host ID must match the Host Name you entered previously on the Host Configuration.
 - The Directory must match what you have configured in the Integrated SIEM log screen in ObservelT.
 - Use *.cef as the log file name and select **End of file** for tail mode. Other items can be left as default.



+ -		
Receiver BIEM Collector Mew Host Group We EctAMAZ-18L6TVS EC2AMAZ-18L6TVS	Host Configuration Host Name/IP: EC2AMAZ-18L6TVS	Enabled
Observer CEr	Credentials: Local System (From Parent)	
	🖓 Generic Log Tail Client 🛛 🗙	ľ
	Identification	
	Name": ObserveI CEF	
	Host ID: EC2AMAZ-18L6TVS	Enable All
	Configuration	Enabled
	Directory*: EIT/WotificationService/LogFiles/ArcSight 0	gFiles\ArcSight
	Log File*: *.cef	
	Tail Mode: End of file 🔻	× 0
	Delmiter:	
	Delimiter is a RegEx:	
	Max Lines Per Event: 1	
	OK Cancel	u bi ta

- Set both the Client and the Host to **Enabled**.
- Click on **SIEM Collector** on the left and click the **Validate** button to ensure successful configuration.



+ -	
 Receiver SIEM Collector Image: New Host Group 	Host Group Configuration These settings are to be used when host settings are in can be left blank. Name: New Host Group Credentials: Local System (From Parent) Log Level: Info (From Parent) Validation Results ×
	Validation Results

Viewing Events

When is configured properly, you will see events flowing into ESM, as shown in the example.



Events							Q. K.
Q Search c	urrent table data					Displaying	100 of 128 Row
Aver	Rule Message	E	Source IP	Destinatio	Prot	Last Time	Event Subtyp
80	Opening root shell using SUDO command	1	172.31.2.171	::	n/a	12/20/2018 1	alert
80	Running SU command to open root shell w	vitł 1	172.31.2.171	::	n/a	12/20/2018 1	alert
80	Running Command Line Shell programs	4	172.31.2.171	::	n/a	12/20/2018 1	alert
100	Running Command Line Shell programs as	A 4	172.31.2.171		n/a	12/20/2018 1	alert
10	UserAc Running Command Line Shell programs	as Admin	istrator 31.2.171	**	n/a	12/20/2018 1	alert
(+n)	Heartetists	٦	171 21 2 171		n/-	10/00/0010 1	alast
DETAILS	GEOLOCATION DESCRIPTION	ľ	NOTES CL	JSTOM TYPES	PA	CKET	
Message	Opening root shell using SUDO co	mmand					
Description							
Description	Indicates a miscellaneous suspicio	ous event	. Belongs to				
	Suspicious Activity: The Suspicious	s Activity	category indicates				

Creating Alarms

You can configure alarms in ESM for certain ObserveIT alerts.

To configure an alarm:

- In the configuration menu in ESM, select **Local ESM** and open the properties menu.
- Configure an alarm to fire for the ObserveIT device based on field match.



System	Properties									
System	Informatio	n	(Alarms	Settings					
Alarms					_					
Clusterii	ng			Name		Condition	Sta	itus		Add
Content	Alarm Set	tings								X
Custom	Summary	Condition	Devices	Actions	Escalation					?
Custom	Type:	ield Match								
Cyber T										
Data En									AND	
Databas									•	
Databas Email S										
Databas Email S ESM Ma										
Databas Email S ESM Ma Event F			[Filters	s -> Device Tyj	pe (In) [ObserveIT]				
Databas Email S ESM Ma Event F File Mai		— : <i>4</i>		Filters	s -> Device Tyj s -> Event Sub	pe (In) [ObserveIT] type (In) [alert]				
Databas Email S ESM Ma Event F File Mai Hosts		-: /		Filters Filters Filters	s -> Device Tyj s -> Event Sub s -> Severity (?	pe (In) [ObserveIT] type (In) [alert] In) [100]				
Databas Email S ESM Ma Event F File Mai Hosts Login S		-: /		Filters Filters	s -> Device Tyj s -> Event Sub s -> Severity (;	pe (In) [ObserveIT] type (In) [alert] In) [100]				
Databas Email S ESM Ma Event F File Mai Hosts Login S Profile I		-: /		Filters Filters Filters	s -> Device Tyj s -> Event Sub s -> Severity (;	pe (In) [ObserveIT] type (In) [alert] In) [100]				
Databas Email S ESM Ma Event F File Mai Hosts Login S Profile I Reports		-: /		Filters Filters Filters	s -> Device Tyj s -> Event Sub s -> Severity (;	pe (In) [ObserveIT] type (In) [alert] In) [100]				
Databas Email S ESM Ma Event F File Mai Hosts Login S Profile I Reports SNMP C	Maxim	- : A	n Trigger	Filters Filters Filters	s -> Device Tyj s -> Event Sub s -> Severity (:	pe (In) [ObserveIT] type (In) [alert] In) [100]				
Databas Email S ESM Ma Event F File Mai Hosts Login S Profile I Reports SNMP C System	Maxim Hours:	- : 4	n Trigger dinutes:	Filters Filters Filters	s -> Device Tyj s -> Event Sub s -> Severity (;	pe (In) [ObserveIT] type (In) [alert] In) [100]				
Databas Email S ESM Ma Event F File Mai Hosts Login S Profile I Reports SNMP C System Users a	Maxim Hours:	um Conditio 0 ► ►	n Trigger finutes:	Filters Filters Frequency	s -> Device Tyj s -> Event Sub s -> Severity (;	pe (In) [ObserveIT] type (In) [alert] In) [100]				

ALARM EXAMPLES

You can automatically create a case for each alert with High or Critical severity level.

Configuration X	No	rmalized	Dashb 🗙				
	O Local ESM - Local Receiver-ELM						
३४:0२⊜₽	🗸 🌒 🖓 🗸 Triggered Alarms 🛛 💿 🖓 🏠 🖓 🗡 🗄						
Physical Display	:						
	Ŗ	Alarm N:	Summary	Assignee	Severity	Trigger Date	Acknowledge Date
∋ 🛅 📕 Physical Display		Observel	Field match alarm triggered	NGCP	70	12/31/2018 19:40:05	12/31/2018 19:41:32
\ominus 📰 🏓 Local ESM		Observe	Field match alarm trigge	NGCP	70	12/31/2018 19:40:05	
💷 📕 (Local ESM		Observe	Field match alarm trigge	NGCP	50	12/31/2018 19:30:05	
ා 🍋 🔁 Local Recei	- n	 .					
📄 🛤 (Local R	Deta	ils Trigge	aring Event Actions				
∖ > ObserveIT C	- <u>Crea</u>	ited case Ob	serveIT Alert: Logging in rer	notely (RDP) to s	ensitive Workstatic	on during irregular hours for NC	<u>;CP</u>

If you have the Advanced Correlation Engine Appliance, you can create a rule to group ObserveIT alerts by user. This will then allow you to correlate multiple alerts for the same user into a single alarm.



Support

- For help configuring McAfee ESM or the McAfee SIEM Collector: Consult McAfee Support.
- For help using or configuring the ObserveIT platform: Contact the ObserveIT support organization. <u>https://www.observeit.com/support/</u>

You can also send an email to <u>integrations@observeit.com</u> with questions about this and other ObserveIT integrations.

Not a customer yet? Start your Free Trial of ObserveIT today!

Free Trial

Start your free trial with ObserveIT today. Detect and prevent insider threats in minutes. Reduce your risk, speed up investigations, and streamline compliance.

Release notes

Version	Date	Notes
1.0.0	2018-12-18	• New:
		 Load ObserveIT logs into McAfee ESM
		• Fixed: N/A
		Improved: N/A