observe IT
a proofpoint® company

Integration Guide

ObserveIT Extension for IBM Resilient

Version 1.0.2 – April 19, 2019

Table of Contents

ObserveIT Introduction

Your biggest asset is also your biggest risk. Whether it is trusted third parties, privileged users, or business users, insiders present a massive risk to organizations because they have been given access to critical applications, systems and data to do their jobs. With over 1,700 global customers across all major verticals, ObserveIT is the only insider threat management solution that empowers security teams to detect insider threats, streamline the investigation process, and prevent data exfiltration.

ObserveIT's software agents monitor and capture key data about insider threats. ObserveIT records user sessions (including screen, mouse, and keyboard activity, as well as local and remote logins) and transmits captured data to the application server in real time.

To learn more, visit https://www.observeit.com/product/highlights/

Extension Overview

ObserveIT's Insider Threat Management solution and IBM Resilient now work together to streamline insider threat response and investigations, resulting in increased efficiency for both incident response and the greater security team.

The ObserveIT extension for Resilient brings your ObserveIT alerts into the Resilient incident response platform. Your Insider Threat alerts are now immediately actionable! Leverage the power of Resilient's workflows to drive your ObserveIT Insider Threat response plan and react quickly to the threats on your network.

Bring ObserveIT's unmatched user investigation tools to augment your existing incident response workflows. Quickly learn which users were logged in and what they were doing before, during and after an event. ObserveIT reconstructs the users session for a visual playback of the incident.

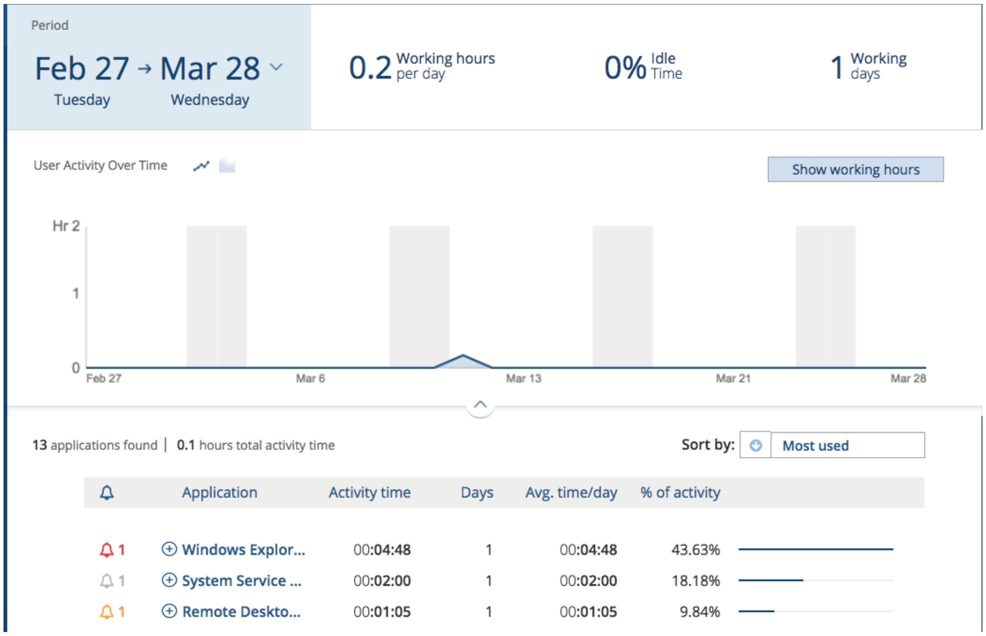
The partnership addresses the growing complexity of insider threat response, incorporating all the needed technologies and involved parties – Security, Legal & HR.

Use Cases

Detecting and Responding to Insider Threats

Not only are ObserveIT's alert rules fully customizable, it also comes equipped with a library of expertly crafted rules to identify hundreds of Insider Threat scenarios out of the box. The ObserveIT extension for IBM Resilient will escalate the critical alerts into the Resilient platform, automatically triggering an Insider Threat response workflow to help analyze and mitigate the threat.

Third Party Activity Monitoring: Monitor and review the actions of third parties (consultants, vendors, contractors, etc.) with access to your organization's environment. Enable rules to detect time fraud or unauthorized access following or during completion of job.



Period

Feb 27 → Mar 28
Tuesday Wednesday

0.2 Working hours per day

0% Idle Time

1 Working days

13 applications found | 0.1 hours total activity time

Sort by: Most used

🔔	Application	Activity time	Days	Avg. time/day	% of activity
1	⊕ Windows Explor...	00:04:48	1	00:04:48	43.63%
1	⊕ System Service ...	00:02:00	1	00:02:00	18.18%
1	⊕ Remote Deskto...	00:01:05	1	00:01:05	9.84%

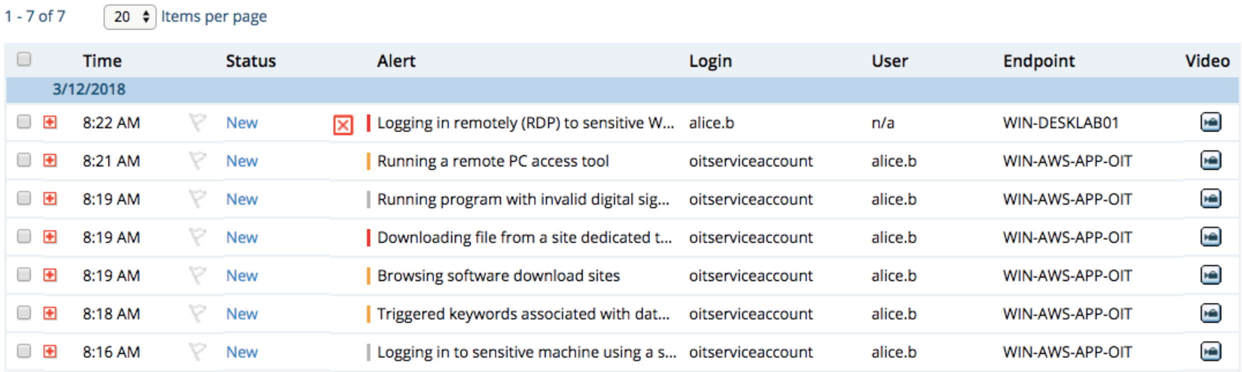
Image 1: Review applications used and time active for employee and third parties

ObserveIT as an Investigation Tool

The average SOC has alerts coming in from multiple sources, overwhelming analysts with security incidents that need to be investigated. ObserveIT provides unique user context around insider threats, regardless of which tool originally highlighted the threat. While other tools will leave you sifting through log files, or querying your SIEM to piece together what happened, ObserveIT lets you quickly and thoroughly investigate insider threat incidents with complete visibility into user activity. ObserveIT simplifies and streamlines insider threat investigations by offering granular details of user activity via visual capture, precise activity trails, and easy to search and understand metadata.

Phished User Verification: ObserveIT can be used in a Resilient workflow following a phishing attempt to identify users' actions before, during and after receiving the email. Include the ObserveIT "Investigate Endpoint Activity" function in your Resilient Phishing playbook to investigate user's involvement in the phishing attempt.

Data Exfiltration Investigation: Following an identification or suspicion that data has exited an organizations environment, investigate user activity (including key strokes, mouse clicks, drag and drops, etc.) in connection with the lost data.



1 - 7 of 7 20 Items per page

□	Time	Status	Alert	Login	User	Endpoint	Video
3/12/2018							
□	8:22 AM	New	Logging in remotely (RDP) to sensitive W...	alice.b	n/a	WIN-DESKLAB01	
□	8:21 AM	New	Running a remote PC access tool	oitserviceaccount	alice.b	WIN-AWS-APP-OIT	
□	8:19 AM	New	Running program with invalid digital sig...	oitserviceaccount	alice.b	WIN-AWS-APP-OIT	
□	8:19 AM	New	Downloading file from a site dedicated t...	oitserviceaccount	alice.b	WIN-AWS-APP-OIT	
□	8:19 AM	New	Browsing software download sites	oitserviceaccount	alice.b	WIN-AWS-APP-OIT	
□	8:18 AM	New	Triggered keywords associated with dat...	oitserviceaccount	alice.b	WIN-AWS-APP-OIT	
□	8:16 AM	New	Logging in to sensitive machine using a s...	oitserviceaccount	alice.b	WIN-AWS-APP-OIT	

Image 2: Insider threat alerts flagged with severity and paired with video of the reconstructed session

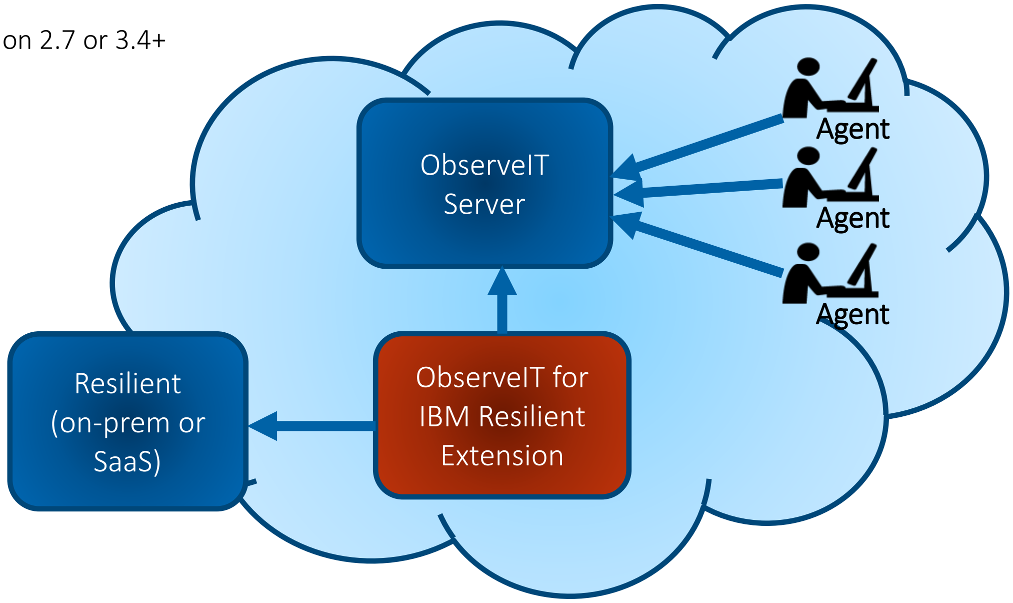
Prerequisites

The ObserveIT extension for IBM Resilient is a resilient-circuits based Python application and can run on Linux or Windows. It will need to be able to connect directly to both your Resilient and ObserveIT APIs.

Minimum supported ObserveIT version is 7.5

Minimum supported Resilient version is 30.0.0

Python 2.7 or 3.4+


ObserveIT Server
Agent
Agent
Agent
Resilient (on-prem or SaaS)
ObserveIT for IBM Resilient Extension

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.

Download Trial License

Download Your Trial License

Request a Demo

Request a demo of ObserveIT user activity monitoring solution. An ObserveIT representative will be in touch soon to schedule a live demo.

Request Pricing

Want a price quote for ObserveIT in your environment? Simply fill out the form and a specialist will contact you shortly.

Installation

Install Python Package

Unzip the extension and install the included python package. This will install the ObserveIT extension and pull all required dependencies from PyPi.

```
> pip install resilient_observeit-1.0.0-py2.py3-none-any.whl
```

If the extension is being installed in an **offline** environment, then you will need to use the included packages in the "deps" directory rather than pulling from PyPi.

```
> pip install --no-index --find-links deps
 resilient_observeit-1.0.0-py2.py3-none-any.whl
```

To verify that the installation was successful, run the resilient-circuits list command to see that the components are registered.

```
>        resilient-circuits list
The following packages and components are installed:
resilient-observeit (1.0.0) installed components:
     ObserveitAlertComponent
     ObserveitEndpointActivityComponent
```

Generate Config File

Once successfully installed, you will need to generate the observeit configuration settings for the extension. If updating an existing app.config file, use the "-u" option and if creating a new app.config file, use the "-c" option.

```
> resilient-circuits config -u
UPDATING config file /Users/jdoe/.resilient/app.config
Adding new section 'observeit' for 'resilient-observeit 1.0.0'
Update finished.  New sections may require manual edits with your
specific configuration values.
```

Create Resilient Application

In order to authenticate with ObserveIT, we will need to register a Resilient application with ObserveIT. The "observeit_create_application" utility was installed along with the extension for this purpose. Run, passing in the URL for your ObserveIT Web Server.

```
> observeit create application -o http://oit.example.com:4884
Enter your ObserveIT Username: admin
Enter your ObserveIT Password:
Application created
Please update the [observeit] section of your Resilient
app.config file to contain the following:
client_id = 3f0844fd-a22a-489f-8e5b-b27af5444b9c
client secret =
80bc7b466e29d83de167b2304437343b0acf697438bccabacca42476c9df99cff
ced03cf22d05440f278e35f67fdd391
```

You can now update the [observeit] configuration section that was generated in your app.config file. Open the app.config file in the editor of your choice and update the configuration with your ObserveIT server URL and the generated Client ID and Secret. Example:

```
[observeit]
host = http://oit.example.com:4884
client_id = 3f0844fd-a22a-489f-8e5b-b27af5444b9c
client_secret =
80bc7b466e29d83de167b2304437343b0acf697438bccabacca42476c9df99cff
ced03cf22d05440f278e35f67fdd391
```

Customization/Configuration

The [observeit] section of the app.config file also controls which alerts in ObserveIT will be automatically selected for escalation to a Resilient incident.

The “min_severity” setting will indicate to the extension the minimum severity level to look for when considering an alert. For example, if you set min_severity to Medium, then all Medium, High, and Critical alerts will be escalated to Resilient as new incidents.

The “rules” setting is a csv list of alert rule names to look for. If an alert is created with a ruleName that matches one of the values on this list, then it will be escalated to Resilient as a new incident, regardless of its severity level.

Example:

```
[observeit]
host = http://oit.example.com:4884
client_id = 3f0844fd-a22a-489f-8e5b-b27af5444b9c
client_secret =
80bc7b466e29d83de167b2304437343b0acf697438bccabacca42476c9df99cff
ced03cf22d05440f278e35f67fdd391
min_severity = High
```

```
rules = "Running CD or DVD burning tools", "Copying sensitive
file"
```

Configure Resilient

There are various configuration items that will need to be generated in Resilient (message destinations, functions, layouts, etc.).   Some of these can be created automatically with the resilient-circuits customize utility and others will need to be created manually with the Resilient console.

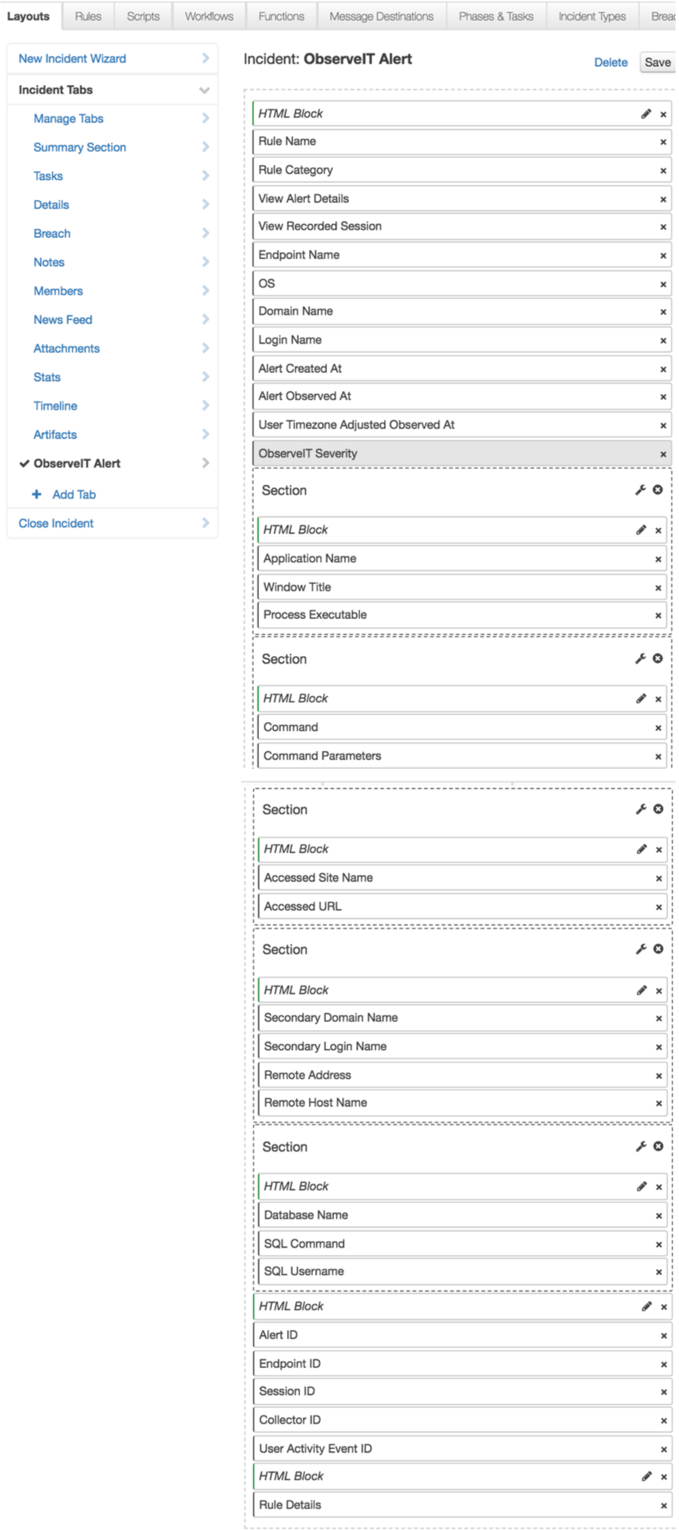
Install Packaged Configuration Elements

To create the packaged customizations in Resilient, run the “resilient-circuits customize” command, entering “y” to create each element as prompted.

```
resilient-circuits customize
Package 'resilient-observeit 1.0.0':
    OK to create type 'observeit_recorded_sessions'? (y/n):y
…
Package 'resilient-observeit 1.0.0' done.
```

Creating a Layout for ObserveIT Alerts

Once the custom fields and data tables have been created with the customize tool, we can create a layout to display ObserveIT alerts. This is a manual process in Resilient, but the following screen shots give a suggested Layout tab for displaying ObserveIT Alert data. The sections in the layout can be configured to be visible only when the relevant fields are populated, thus ensuring your ObserveIT tab only shows the data relevant to that particular type of alert rather than empty fields.

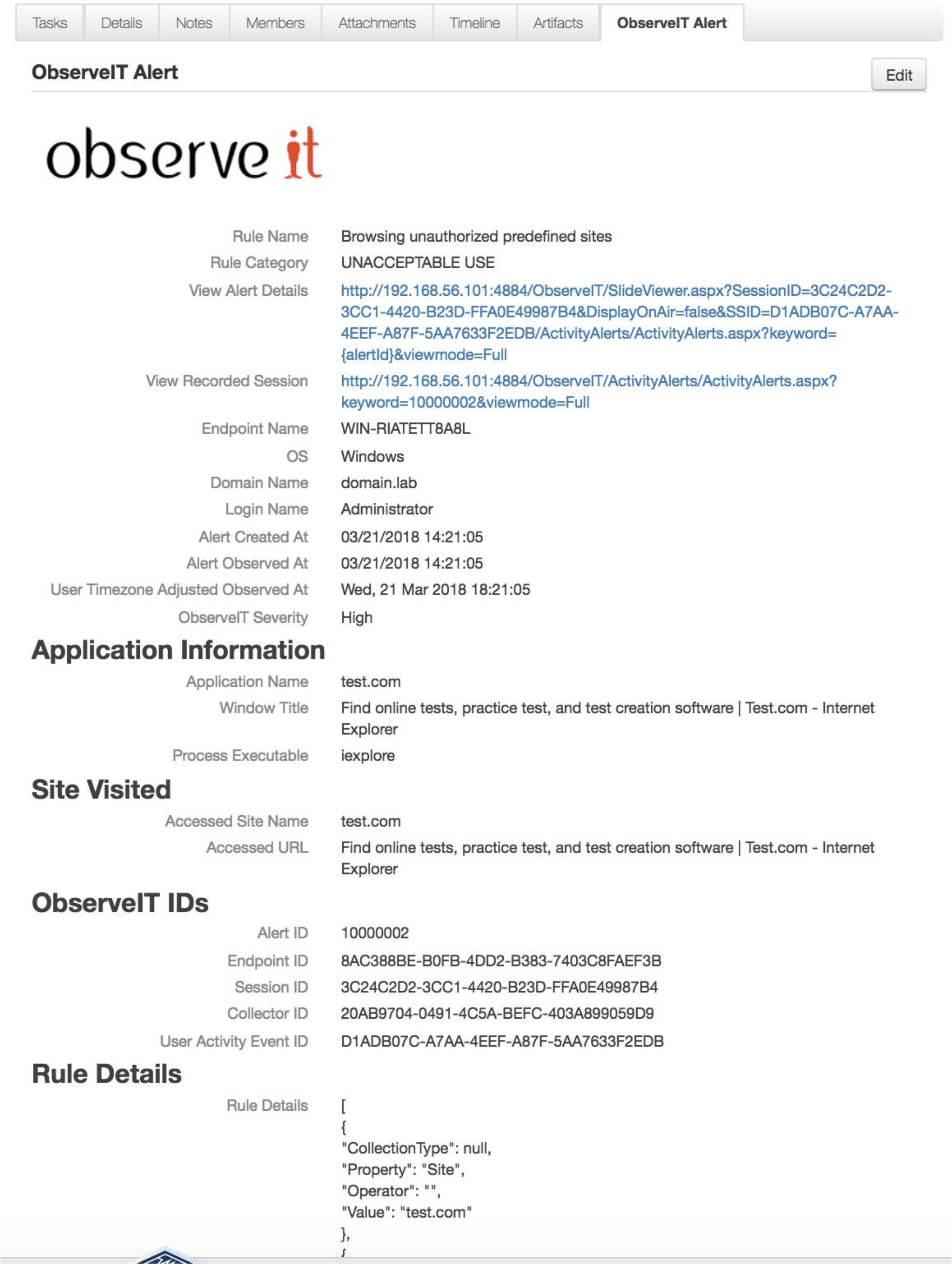


Layouts | Rules | Scripts | Workflows | Functions | Message Destinations | Phases & Tasks | Incident Types | Brea

- New Incident Wizard
- Incident Tabs
  - Manage Tabs
  - Summary Section
  - Tasks
  - Details
  - Breach
  - Notes
  - Members
  - News Feed
  - Attachments
  - Stats
  - Timeline
  - Artifacts
  - ✓ ObserveIT Alert
  - + Add Tab
- Close Incident

Incident: **ObserveIT Alert** Delete Save

- *HTML Block*
- Rule Name
- Rule Category
- View Alert Details
- View Recorded Session
- Endpoint Name
- OS
- Domain Name
- Login Name
- Alert Created At
- Alert Observed At
- User Timezone Adjusted Observed At
- ObserveIT Severity
- Section
  - *HTML Block*
  - Application Name
  - Window Title
  - Process Executable
- Section
  - *HTML Block*
  - Command
  - Command Parameters
- Section
  - *HTML Block*
  - Accessed Site Name
  - Accessed URL
- Section
  - *HTML Block*
  - Secondary Domain Name
  - Secondary Login Name
  - Remote Address
  - Remote Host Name
- Section
  - *HTML Block*
  - Database Name
  - SQL Command
  - SQL Username
- *HTML Block*
- Alert ID
- Endpoint ID
- Session ID
- Collector ID
- User Activity Event ID
- *HTML Block*
- Rule Details



ObserveIT Alert

Rule Name	Browsing unauthorized predefined sites
Rule Category	UNACCEPTABLE USE
View Alert Details	http://192.168.56.101:4884/ObserveIT/SlideViewer.aspx?SessionID=3C24C2D2-3CC1-4420-B23D-FFA0E49987B4&DisplayOnAir=false&SSID=D1ADB07C-A7AA-4EEF-A87F-5AA7633F2EDB/ActivityAlerts/ActivityAlerts.aspx?keyword={alertId}&viewmode=Full
View Recorded Session	http://192.168.56.101:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?keyword=10000002&viewmode=Full
Endpoint Name	WIN-RIATETT8A8L
OS	Windows
Domain Name	domain.lab
Login Name	Administrator
Alert Created At	03/21/2018 14:21:05
Alert Observed At	03/21/2018 14:21:05
User Timezone Adjusted Observed At	Wed, 21 Mar 2018 18:21:05
ObserveIT Severity	High

Application Information

Application Name	test.com
Window Title	Find online tests, practice test, and test creation software | Test.com - Internet Explorer
Process Executable	iexplore

Site Visited

Accessed Site Name	test.com
Accessed URL	Find online tests, practice test, and test creation software | Test.com - Internet Explorer

ObserveIT IDs

Alert ID	10000002
Endpoint ID	8AC388BE-B0FB-4DD2-B383-7403C8FAEF3B
Session ID	3C24C2D2-3CC1-4420-B23D-FFA0E49987B4
Collector ID	20AB9704-0491-4C5A-BEFC-403A899059D9
User Activity Event ID	D1ADB07C-A7AA-4EEF-A87F-5AA7633F2EDB

Rule Details

Rule Details

```
[
{
"CollectionType": null,
"Property": "Site",
"Operator": "",
"Value": "test.com"
},
{
```

Customizing Incident Creation

When alerts are escalated from ObserveIT to Resilient, only the custom ObserveIT fields and a few other required fields will be populated. Any remaining desired fields can be populated using a script in Resilient. The included "ObserveIT: Incident Fields From Alert" script will map a value for Incident Type and Severity, but should be customized after installation for your needs. A good first update would be updating the Incident Type mapping rules to use any custom types defined in your system.

The included "ObserveIT: Get Insider Threat Artifacts" script will create several artifacts based on the contents of the ObserveIT alert. It can be customized after installation as well.

RUNNING THE EXTENSION

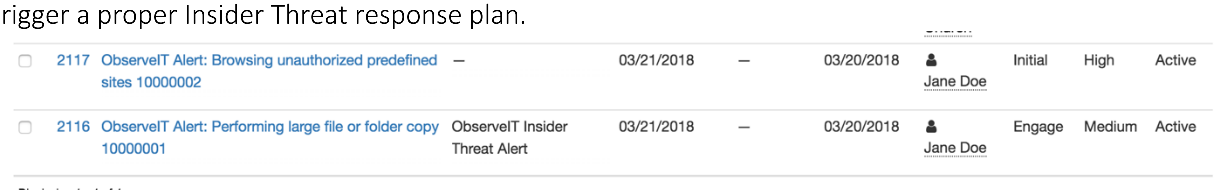
The extension is started using the resilient-circuits run command. For more advanced usage, such as running as a service, please refer to IBM Resilient's documentation.

```
> resilient-circuits run
```

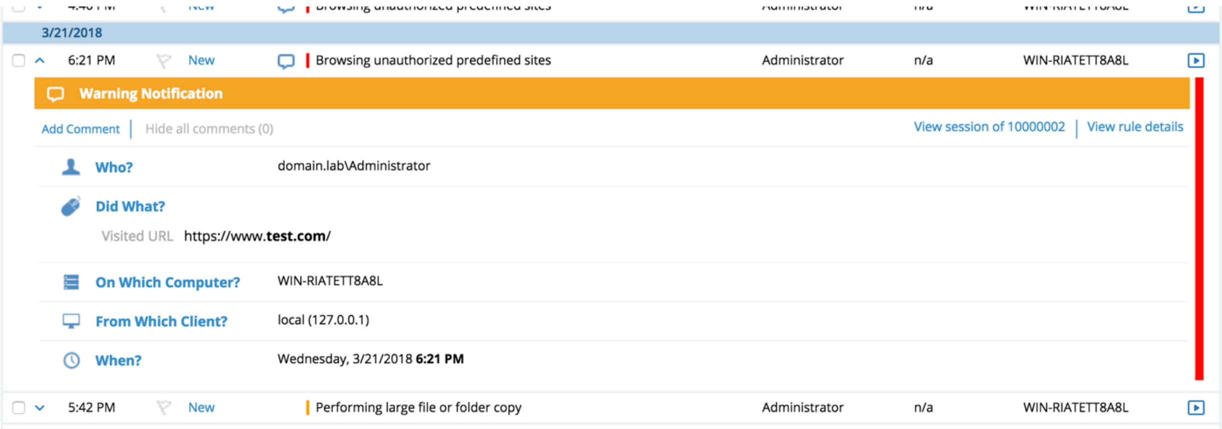
Usage

ESCALATING ALERTS

While the integration is running, it will regularly poll ObserveIT for any new alerts that match the criteria specified in the app.config file. As long as this has been configured everything as described above, all your critical alerts should now be generating incidents in Resilient. The polling interval can be adjusted in the app.config file if desired. Once ObserveIT alerts are coming into Resilient, a rule can be configured to trigger a proper Insider Threat response plan.



□	2117	ObserveIT Alert: Browsing unauthorized predefined sites 10000002	—	03/21/2018	—	03/20/2018	Jane Doe	Initial	High	Active
□	2116	ObserveIT Alert: Performing large file or folder copy 10000001	ObserveIT Insider Threat Alert	03/21/2018	—	03/20/2018	Jane Doe	Engage	Medium	Active



4:40 PM New Browsing unauthorized predefined sites Administrator n/a WIN-RIATETT8A8L

3/21/2018

6:21 PM New Browsing unauthorized predefined sites Administrator n/a WIN-RIATETT8A8L

Warning Notification

Add Comment | Hide all comments (0) View session of 10000002 | View rule details

Who? domain.lab\Administrator

Did What?
Visited URL https://www.**test.com**/

On Which Computer? WIN-RIATETT8A8L

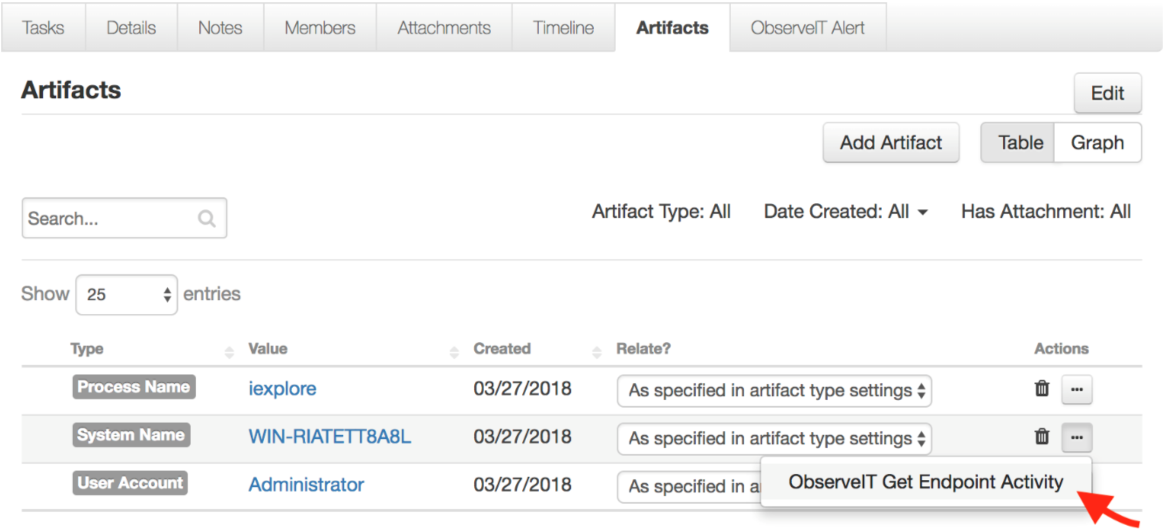
From Which Client? local (127.0.0.1)

When? Wednesday, 3/21/2018 **6:21 PM**

5:42 PM New Performing large file or folder copy Administrator n/a WIN-RIATETT8A8L

Investigating Artifacts

Even if your Resilient incident was not initiated from an ObserveIT alert, getting the user context about an alert from the affected endpoint is still valuable. The included “ObserveIT: Get Endpoint Activity” function can be used in your workflows to automatically bring this valuable information into Resilient. You can trigger it out-of-the-box from any “System Name” or “User Account” artifacts. Take a look at the included “ObserveIT Investigate Endpoint” workflow for an example of how to use it.

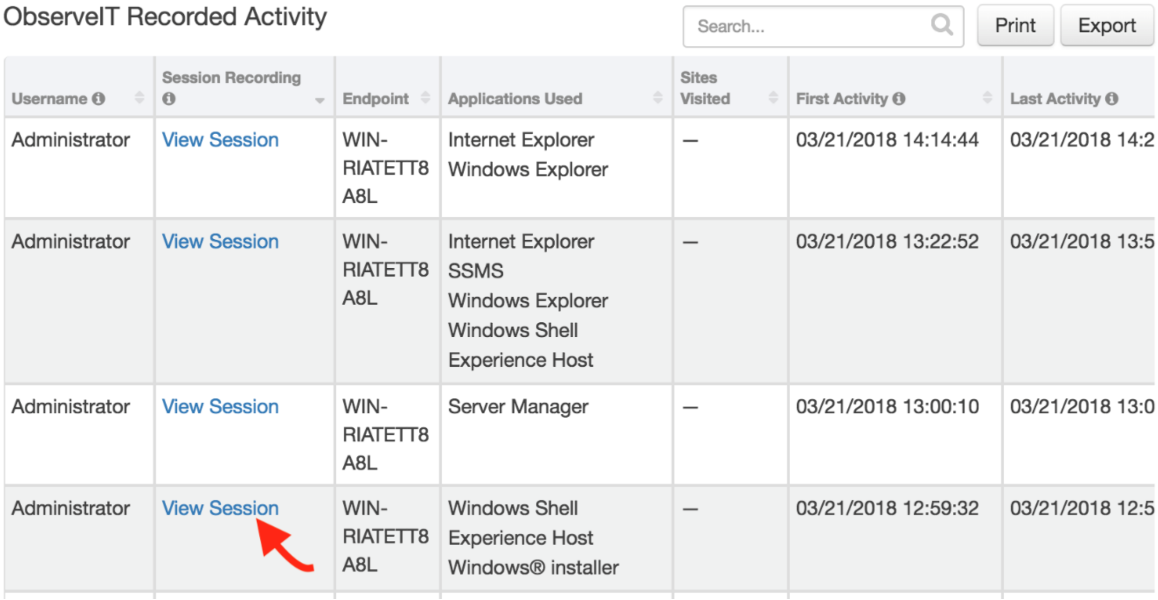


Artifacts

Artifact Type: All Date Created: All Has Attachment: All

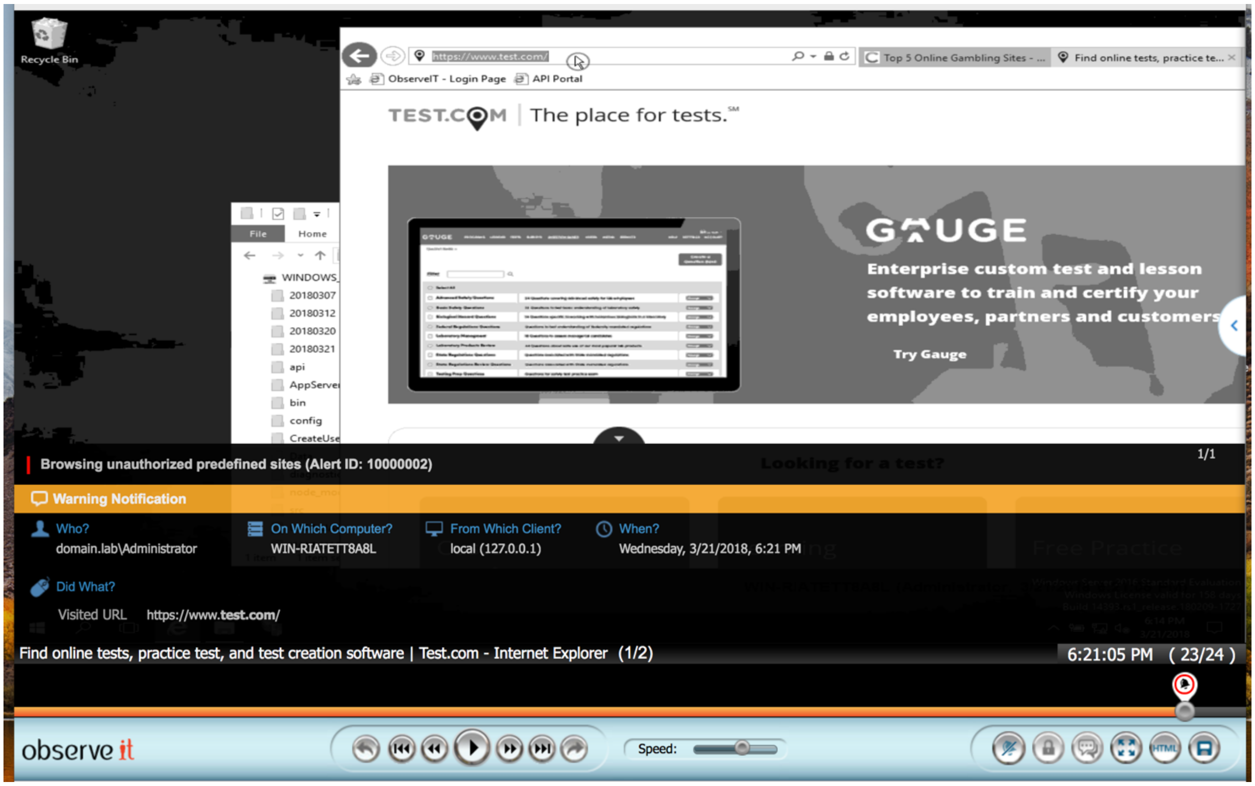
Show 25 entries

Type	Value	Created	Relate?	Actions
Process Name	iexplore	03/27/2018	As specified in artifact type settings	
System Name	WIN-RIATETT8A8L	03/27/2018	As specified in artifact type settings	
User Account	Administrator	03/27/2018	As specified in a	ObserveIT Get Endpoint Activity



ObserveIT Recorded Activity

Username	Session Recording	Endpoint	Applications Used	Sites Visited	First Activity	Last Activity
Administrator	View Session	WIN-RIATETT8A8L	Internet Explorer Windows Explorer	—	03/21/2018 14:14:44	03/21/2018 14:2
Administrator	View Session	WIN-RIATETT8A8L	Internet Explorer SSMS Windows Explorer Windows Shell Experience Host	—	03/21/2018 13:22:52	03/21/2018 13:5
Administrator	View Session	WIN-RIATETT8A8L	Server Manager	—	03/21/2018 13:00:10	03/21/2018 13:0
Administrator	View Session	WIN-RIATETT8A8L	Windows Shell Experience Host Windows® installer	—	03/21/2018 12:59:32	03/21/2018 12:5



Recycle Bin
https://www.test.com/
Top 5 Online Gambling Sites - ...
Find online tests, practice te...
ObserveIT - Login Page
API Portal
TEST.COM | The place for tests.℠
GAUGE
Enterprise custom test and lesson software to train and certify your employees, partners and customers
Try Gauge
File
Home
WINDOWS_
20180307
20180312
20180320
20180321
api
AppServe
bin
config
CreateUse

Browsing unauthorized predefined sites (Alert ID: 10000002) 1/1

Warning Notification

Who? domain.lab\Administrator

On Which Computer? WIN-RIATETT8A8L

From Which Client? local (127.0.0.1)

When? Wednesday, 3/21/2018, 6:21 PM

Did What?

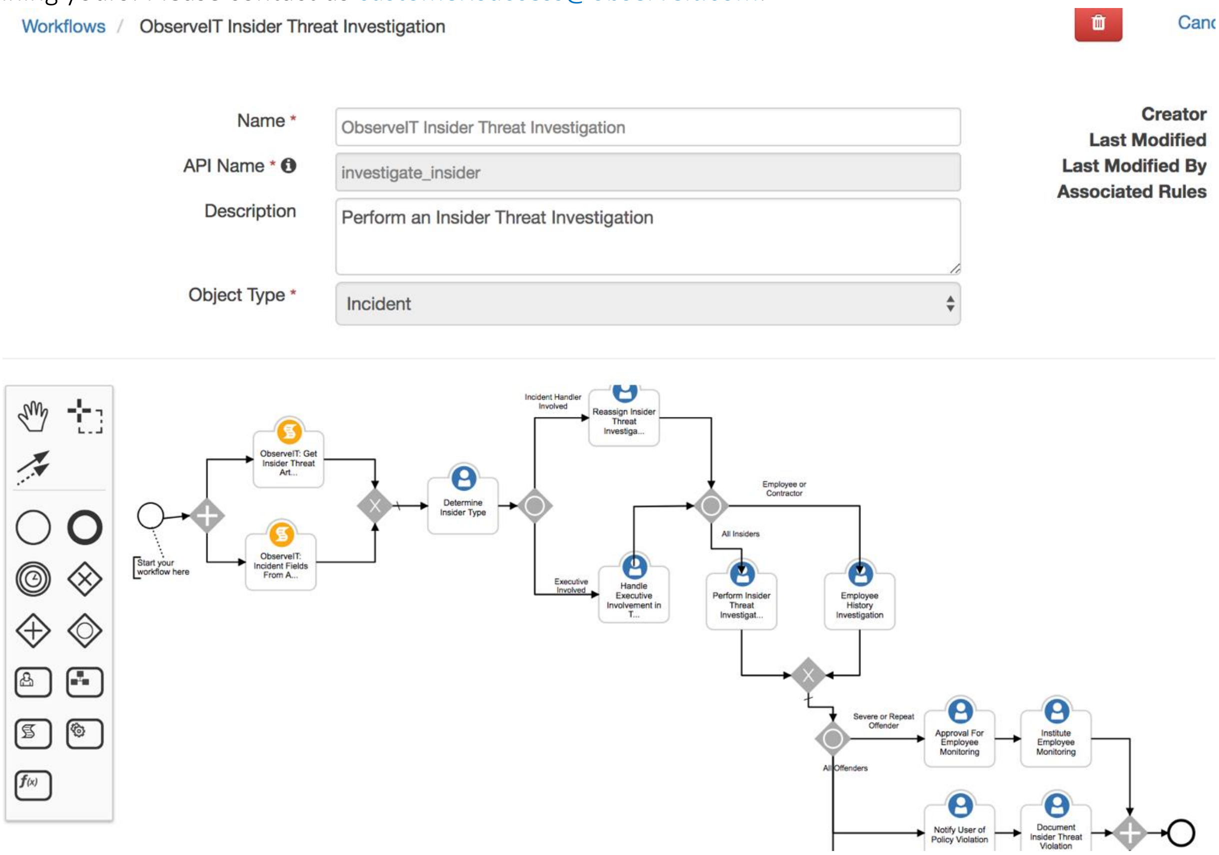
Visited URL https://www.test.com/

Find online tests, practice test, and test creation software | Test.com - Internet Explorer (1/2)

6:21:05 PM (23/24)

ObserveIT Insider Threat Playbook

Designing a playbook to guide your Insider Threat response is a critical part of your organization's overall Insider Threat Program. The Services group at ObserveIT is ready to help you get started building or refining yours! Please contact us customer.success@observeit.com.



Workflows / ObserveIT Insider Threat Investigation

Name * ObserveIT Insider Threat Investigation

API Name * investigate_insider

Description Perform an Insider Threat Investigation

Object Type * Incident

Creator
Last Modified
Last Modified By
Associated Rules

Canc
Start your workflow here
ObserveIT: Get Insider Threat Art...
ObserveIT: Incident Fields From A...
Determine Insider Type
Incident Handler Involved
Reassign Insider Threat Investiga...
Executive Involved
Handle Executive Involvement in T...
Employee or Contractor
All Insiders
Perform Insider Threat Investigat...
Employee History Investigation
Severe or Repeat Offender
Approval For Employee Monitoring
Institute Employee Monitoring
All Offenders
Notify User of Policy Violation
Document Insider Threat Violation

Support

For additional support configuring the ObserveIT extension or using the ObserveIT platform, please contact the ObserveIT support organization.
https://www.observeit.com/support/

Release notes

Version	Date	Notes
1.0.0	2018-03-29	• Initial Release • New: ○ Automatically create Resilient incidents from new ObserveIT alerts ○ Function to investigate endpoint activity • Fixed: • Improved:
1.0.1	2018-08-15	• New: • Fixed: ○ authentication token refresh. • Improved:
1.0.2	2019-04-19	• New: • Fixed: ○ Datatable display in Resilient v32 ○ Observeit 7.7 API Compatibility • Improved: