Netsurion | EventTracker®

Integrate StealthINTERCEPT

EventTracker v9.2 and above

Publication Date: August 4, 2020

Abstract

This guide helps you in configuring **StealthINTERCEPT** with EventTracker to receive **StealthINTERCEPT** events. In this guide, you will find the detailed procedures required for monitoring **StealthINTERCEPT.**

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.2 or above and **StealthINTERCEPT.**

Audience

Administrators, who are assigned the task to monitor and manage **StealthINTERCEPT** events using **EventTracker.**

Table of Contents

1. Overview

StealthINTERCEPT monitors and prevents unwanted and unauthorized activities in real-time for active directory security and compliance. It inspects all active directory, exchange, and file system traffic at the source, it detects malicious and unintended changes in real-time to safeguard organizations' credentials and unstructured data.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

NOTE: Currently EventTracker supports only active directory monitoring by StealthINTERCEPT.

2. Prerequisites

- **EventTracker v9.2** or **above** should be installed.
- **Port 514** should be open.

3. Integrating StealthINTERCEPT with EventTracker

1. Log in to StealthINTERCEPT.
2. Open the **Administration** Console.
3. From the menu bar, select **Configuration → Alerts**.
4. Click **the SIEM tab**.
5. Click the button in front of **Disabled** to toggle the setting to **Enabled**.

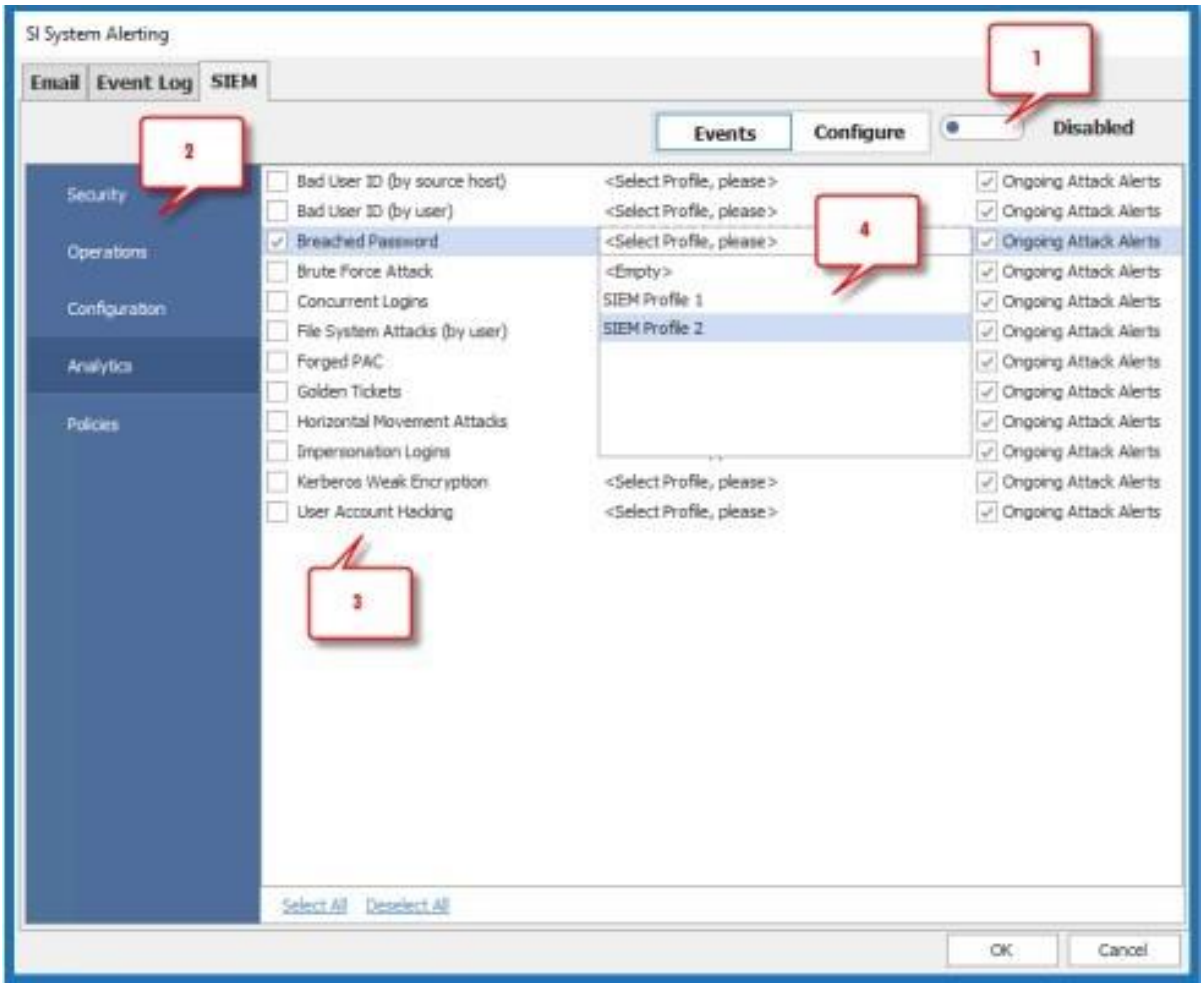

Figure 1

6. Click **Configure** in the SI System Alerting window.
7. Enter the **Protocol**.
8. Enter the **IP address** of the EventTracker in the Host Address field.
9. In the **Port** field, enter **514**.
10. From the Mapping File drop-down lists, select the "**Generic CEF format**".
11. Click **Events** and select the event types that you want for SIEM reporting.
12. Select the event category (Security, Operations, Configuration, Analytics, Policies) from the list on the left.
13. Check the event/incident/policy that triggers SIEM notifications from the center list.
14. Select the new Configured SIEM Profile to send alerts to.
15. Click OK to apply the new configuration.

4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support StealthINTERCEPT.

4.1 Category

- **StealthINTERCEPT: Authentication Failed-** This category provides information related to user authentication failure detected in StealthINTERCEPT.
- **StealthINTERCEPT: Authentication Success –** This category provides information related to authentication success in StealthINTERCEPT.
- **StealthINTERCEPT: Active Directory Activites –** This category provides information related to active directory activites in StealthINTERCEPT.
- **StealthINTERCEPT: LSASS Guardian Events–** This category provides information related to LSASS guardian events in StealthINTERCEPT.
- **StealthINTERCEPT: AD Replication Monitoring Events -** This category provides information related to AD replication monitoring events in StealthINTERCEPT.

4.2 Alert

- **StealthINTERCEPT - Login Failed -** This alert is generated when any user authentication failure is detected in StealthINTERCEPT.
- **StealthINTERCEPT - User Account Locked Out -** This alert is generated when locked user account is detected in StealthINTERCEPT.
- **StealthINTERCEPT - User Password Changes -** This alert is generated when any user password change is detected in StealthINTERCEPT.

4.3 Report

- **StealthINTERCEPT: User Authentication Failure -** This report gives information regarding all the user authentication failure detected in StealthINTERCEPT. Reports contains IP address, session ID, username, email and other useful information for further analysis.

LogTime	Computer	Destination User	Object Class	Policy Name	Source Domain	Source User Info	Source User	Source Address
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	cn\=healthmailbox38f36bfa0bd345c6aa4158999f8f7bd0,cn\=monitoring mailboxes,cn\=microsoft exchange system objects,dc\=rowanads,dc\=rowan,dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=healthmailbox38f36bfa0bd345c6aa4158999f8f7bd0,cn\=monitoring mailboxes,cn\=microsoft exchange system objects,dc\=rowanads,dc\=rowan,dc\=edu	healthmailbox38f36bfa0bd345c6aa4158999f8f7bd0	[::ffff:150.250.75.9]
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	cn\=ashton\, holly a,ou\=employees,ou\=accounts,dc\=rowanads,dc\=rowan,dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=ashton\, holly a,ou\=employees,ou\=accounts,dc\=rowanads,dc\=rowan,dc\=edu	ashton\	ADS02
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	cn\=irons\, al,ou\=affiliates,ou\=accounts,dc\=rowanads,dc\=rowan,dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=irons\, al,ou\=affiliates,ou\=accounts,dc\=rowanads,dc\=rowan,dc\=edu	irons\	CLEARPASS-03
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	Othe2-jo305\User	user	StealthDEFEND for AD	ROWANADS	Othe2-jo305\User		OTHE2-JO305
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	cn\=miller\, kevin,ou\=employees,ou\=accounts,dc\=rowanads,dc\=rowan,dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=miller\, kevin,ou\=employees,ou\=accounts,dc\=rowanads,dc\=rowan,dc\=edu	miller\	172.25.64.115
07/24/2020 12:33:29 PM	R1S5-VM30\172.27.100.40-SYSLOG	cn\=fusco\, catherine m,ou\=wellness,ou\=som,ou\=som,ou\=med,dc\=rowanads,dc\=rowan,dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=fusco\, catherine m,ou\=wellness,ou\=som,ou\=som,ou\=med,dc\=rowanads,dc\=rowan,dc\=edu	fusco\	[::ffff:10.84.128.211]
07/24/2020 12:33:29 PM	R1S5-VM30\172.27.100.40-SYSLOG	CN\=HealthMailboxce823841dd344a99b67d594541483411,CN\=Monitoring Mailboxes,CN\=Microsoft Exchange System Objects,DC\=rowanads,DC\=rowan,DC\=edu	user	StealthDEFEND for AD	ROWANADS	CN\=HealthMailboxce823841dd344a99b67d594541483411,CN\=Monitoring Mailboxes,CN\=Microsoft Exchange System Objects,DC\=rowanads,DC\=rowan,DC\=edu	HealthMailboxce823841dd344a99b67d594541483411	[::ffff:150.250.75.123]
07/24/2020 12:33:29 PM	R1S5-VM30\172.27.100.40-SYSLOG	CN\=Millennium Proxy,OU\=Proxies,DC\=rowanads,	user	StealthDEFEND for AD	ROWANADS	CN\=Millennium Proxy,OU\=Proxies,DC\=rowanads,	Millennium Proxy	[::ffff:150.250.64.139]

Figure 2

- **StealthINTERCEPT: User Authentication Success -** This report gives information regarding all the user authentication success detected in StealthINTERCEPT. Reports contains IP address, session ID, username, IP and other useful information for further analysis.

LogTime	Computer	Object Class	Policy Name	Source Domain	Source Address	Source User Info	Source User
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	SWONPM04	cn\=swappwinproxy,ou\=proxies,dc\=rowanads,dc\=rowan,dc\=edu	swappwinproxy
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	BITVISESSH02	cn\=goetz\, shauna r,ou\=gradmeded,ou\=som,ou\=som,ou\=med,dc\=rowanads,dc\=rowan,dc\=edu	goetz\
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	SWONPM04	cn\=swappwinproxy,ou\=proxies,dc\=rowanads,dc\=rowan,dc\=edu	swappwinproxy
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	CLEARPASS-01	cn\=zimmerman\, keith t,ou\=students,ou\=accounts,dc\=rowanads,dc\=rowan,dc\=edu	zimmerman\
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	[::ffff:10.64.188.183]	cn\=kathleen benasutti,ou\=cbo,ou\=som,ou\=som,ou\=med,dc\=rowanads,dc\=rowan,dc\=edu	kathleen benasutti
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	[::ffff:10.84.128.211]	cn\=fusco\, catherine m,ou\=wellness,ou\=som,ou\=som,ou\=med,dc\=rowanads,dc\=rowan,dc\=edu	fusco\
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	[::ffff:150.250.75.9]	cn\=healthmailbox7a6696c1448b46cea7a0c4a71b5dfecd,cn\=monitoring mailboxes,cn\=microsoft exchange system objects,dc\=rowanads,dc\=rowan,dc\=edu	healthmailbox7a6696c1448b46cea7a0c4a71b5dfecd
07/24/2020 12:33:28 PM	R1S5-VM30\172.27.100.40-SYSLOG	user	StealthDEFEND for AD	ROWANADS	[::ffff:150.250.75.9]	cn\=healthmailbox7a6696c1448b46cea7a0c4a71b5dfecd,cn\=monitoring mailboxes,cn\=microsoft exchange system	healthmailbox7a6696c1448b46cea7a0c4a71b5dfecd

Figure 3

- **StealthINTERCEPT: Active Directory Activites –** This report gives information regarding all the active directory activites detected in StealthINTERCEPT. Reports contains IP address, username, Object modified, IP and other useful information for further analysis.

LogTime	r	Attribute Name	Blocked	Destination User	Object Class	Policy Name	Source Domain	Source Address	Source User Info	Source User	Operation	Event Type	New Value	Value	Success
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	lastLogon	False	CN\=Studdell0020, OU\=QBORO,OU\=Managed,OU\=Workstations,DC\=row	computer	StealthDEFEND for AD	ROWANADS	AUTH:Studdell0020	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	Anonymous Logon	Change Attribute	Active DirectorycomputerObject Modified	{ 2020-07-17 07:52:50.335361 Z UTC }		True
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	logonCount	False	CN\=Millennium Proxy,OU\=Proxies,DC\=rowanads,DC\=rowan,DC\=ed	user	StealthDEFEND for AD	ROWANADS	AUTH:MILLENNIUM7	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	65535		True
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	lastLogon	False	CN\=Millennium Proxy,OU\=Proxies,DC\=rowanads,DC\=rowan,DC\=ed	user	StealthDEFEND for AD	ROWANADS	AUTH:MILLENNIUM7	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	{ 2020-07-17 07:52:50.163017 3Z UTC }		True
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	logonCount	False	CN\=Millennium Proxy,OU\=Proxies,DC\=rowanads,DC\=rowan,DC\=ed	user	AD: Successful Account Logons	ROWANADS	AUTH:MILLENNIUM7	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	65535		True
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	lastLogon	False	CN\=Millennium Proxy,OU\=Proxies,DC\=rowanads,DC\=rowan,DC\=ed	user	AD: Successful Account Logons	ROWANADS	AUTH:MILLENNIUM7	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	{ 2020-07-17 07:52:50.163017 3Z UTC }		True
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	logonCount	False	CN\=Martin Mischa Forsberg,OU\=Cfa,OU\=SOM,OU\=SOM,OU\=Med,DC\=ro	user	AD: Successful Account Logons	ROWANADS	AUTH:CTXICON001	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	12636		True
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	lastLogon	False	CN\=Martin Mischa Forsberg,OU\=Cfa,OU\=SOM,OU\=SOM,OU\=Med,DC\=ro	user	StealthDEFEND for AD	ROWANADS	AUTH:CTXICON001	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	{ 2020-07-17 07:53:05.949323 1Z UTC }		True
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-	logonCount	False	CN\=Martin Mischa Forsberg,OU\=Cfa,OU\=SOM,OU\=SO	user	StealthDEFEND for AD	ROWANADS	AUTH:CTXICON001	CN\=Anonymous Logon,CN\=WellKnown Security Principals,CN\=Configuration,DC\=r	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	12636		True

Figure 4

- **StealthINTERCEPT: LSASS Guardian Events–** This report provides information related to LSASS guardian events in StealthINTERCEPT.

LogTime	Computer	Attribute Name	Destination User	New Value	Object Class	Policy Name	Source Domain	Source Address	Event Type	Success	Source User Info	Source User
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-SYSLOG	Process	lsass.exe	vmtoolsd.exe	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	System
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-SYSLOG	Desired	lsass.exe	PROCESS_QUERY_LIMITED_INFORMATION	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	System
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-SYSLOG	Desired	lsass.exe	PROCESS_QUERY_INFORMATION	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	System
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-SYSLOG	Desired	lsass.exe	PROCESS_VM_WRITE	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	System
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-SYSLOG	Desired	lsass.exe	PROCESS_VM_READ	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	System
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-SYSLOG	Desired	lsass.exe	PROCESS_VM_OPERATION	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	System
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-SYSLOG	Desired	lsass.exe	PROCESS_CREATE_THREAD	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=rowanads,DC\=rowan,DC\=edu	System
07/20/2020 05:34:45 PM	R1S5-VM30\172.27.100.40-	Process	lsass.exe	3028	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=r	System

Figure 5

- **StealthINTERCEPT: AD Replication Monitoring Events -** This report provides information related to AD replication monitoring events in StealthINTERCEPT.

LogTime	Computer	Attribute Name	Policy Name	Domain	Source Address	Event Type	Success	Source User Info	Source User	New Value	Object Class
07/20/2020 05:34:39 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.12	AD Replication MonitoringdomainDNSDcSync	True	cn\=ads02,ou\=wsus prod 1 tues 1am,ou\=domain controllers,dc\=rowanads,dc\=rowan,dc\=edu	ads02	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-GET-CHANGES-IN-FILTERED-SET	domainDNS
07/20/2020 05:34:39 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.16	AD Replication MonitoringdomainDNSDcSync	True	CN\=ADS06,OU\=WSUS Prod 3 Sat 1am,OU\=Domain Controllers,DC\=rowanads,DC\=rowan,DC\=edu	ADS06	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-GET-CHANGES-IN-FILTERED-SET	domainDNS
07/20/2020 05:34:39 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.17	AD Replication MonitoringdomainDNSDcSync	True	CN\=ADS07,OU\=WSUS Prod 1 Tues 1am,OU\=Domain Controllers,DC\=rowanads,DC\=rowan,DC\=edu	ADS07	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-GET-CHANGES-IN-FILTERED-SET	domainDNS
07/20/2020 05:34:39 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.14	AD Replication MonitoringdomainDNSDcSync	True	cn\=ads04,ou\=wsus prod 3 sat 1am,ou\=domain controllers,dc\=rowanads,dc\=rowan,dc\=edu	ads04	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-GET-CHANGES-IN-FILTERED-SET	domainDNS
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.12	AD Replication MonitoringdomainDNSDcSync	True	cn\=ads02,ou\=wsus prod 1 tues 1am,ou\=domain controllers,dc\=rowanads,dc\=rowan,dc\=edu	ads02	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-GET-CHANGES-IN-FILTERED-SET	domainDNS
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.16	AD Replication MonitoringdomainDNSDcSync	True	CN\=ADS06,OU\=WSUS Prod 3 Sat 1am,OU\=Domain Controllers,DC\=rowanads,DC\=rowan,DC\=edu	ADS06	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-GET-CHANGES-IN-FILTERED-SET	domainDNS
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.17	AD Replication MonitoringdomainDNSDcSync	True	CN\=ADS07,OU\=WSUS Prod 1 Tues 1am,OU\=Domain Controllers,DC\=rowanads,DC\=rowan,DC\=edu	ADS07	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-GET-CHANGES-IN-FILTERED-SET	domainDNS
07/20/2020 05:34:40 PM	R1S5-VM30\172.27.100.40-SYSLOG	permissions	StealthDEFEND for AD	ROWANADS	10.240.4.14	AD Replication MonitoringdomainDNSDcSync	True	cn\=ads04,ou\=wsus prod 3 sat 1am,ou\=domain controllers,dc\=rowanads,dc\=row	ads04	DS-REPLICATION-GET-CHANGES;DS-REPLICATION-GET-CHANGES-ALL;DS-REPLICATION-	domainDNS

Figure 6

4.4 Dashboards

- **StealthINTERCEPT: Authentication Failed by Username**

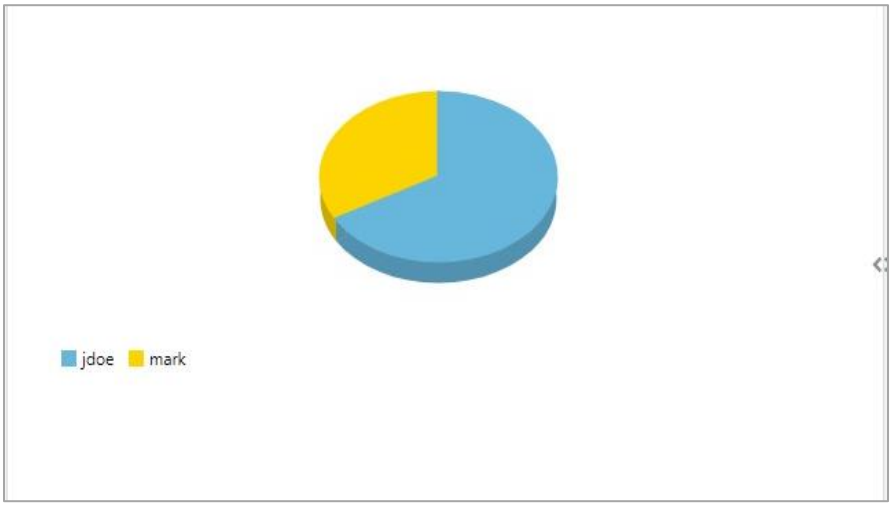

Figure 7

- **StealthINTERCEPT: Authentication Success by Username**

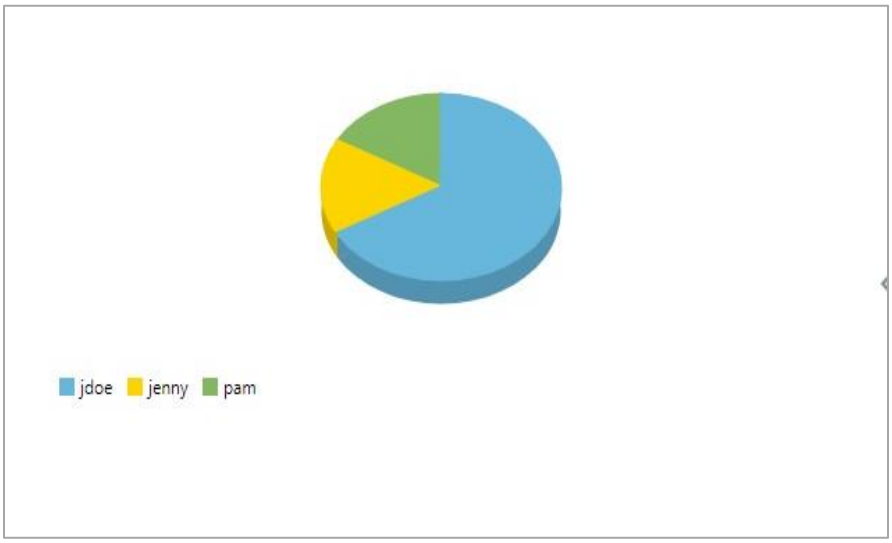

Figure 8

- **StealthINTERCEPT: Active Directory Activities**

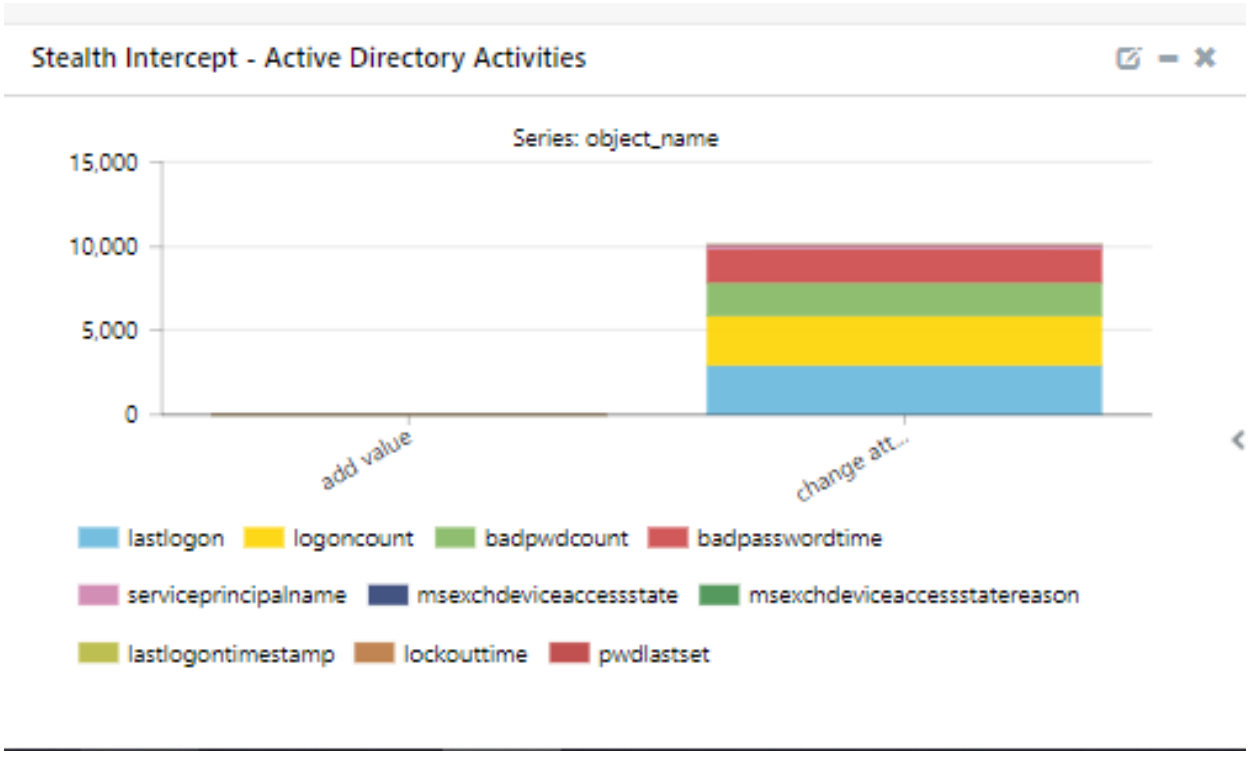

Figure 9

- **StealthINTERCEPT: Password Changes by Username**

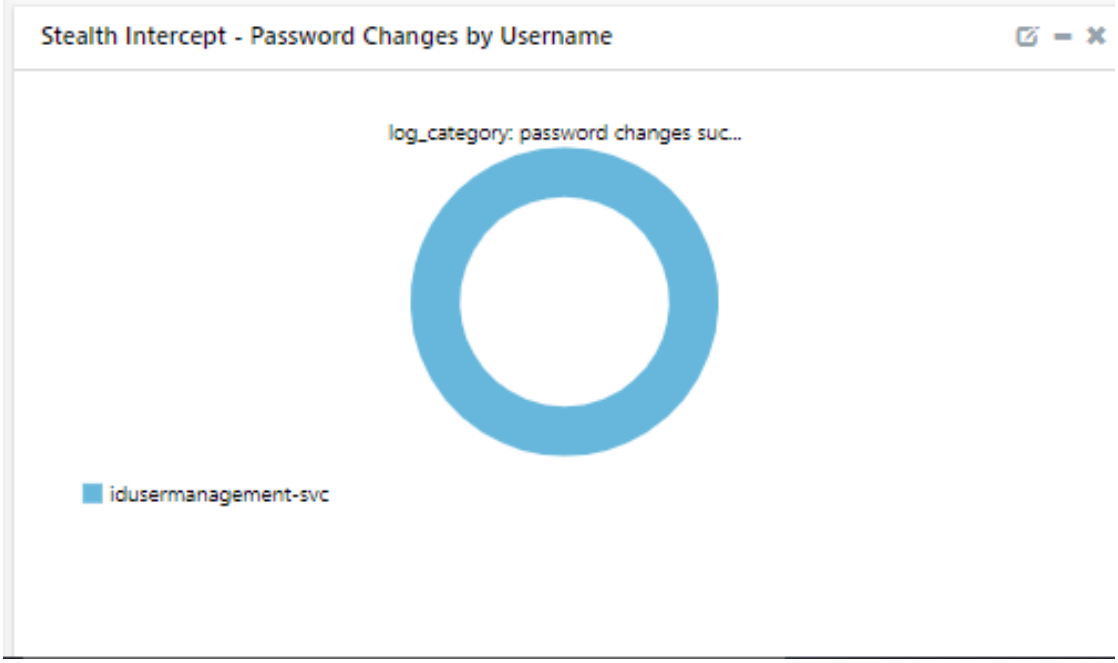

Figure 10

- **StealthINTERCEPT: LSASS Activites**

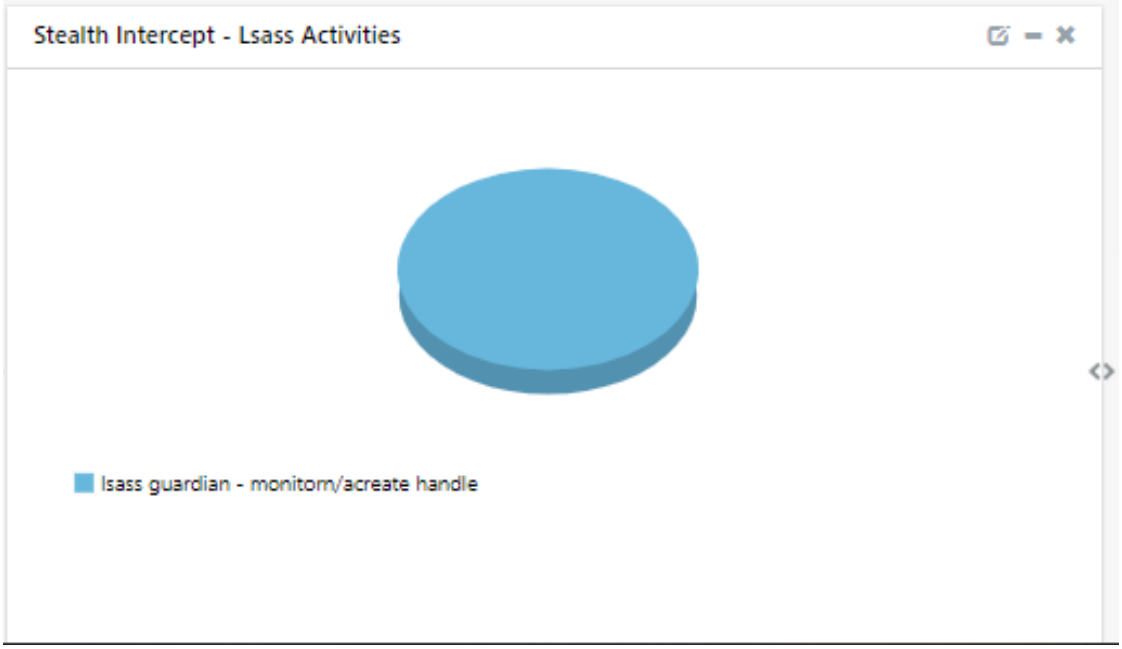

Figure 11

5. Importing StealthINTERCEPT knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Report
- Dashboard

16. Launch **EventTracker Control Panel**.
17. Double click **Export Import Utility**.

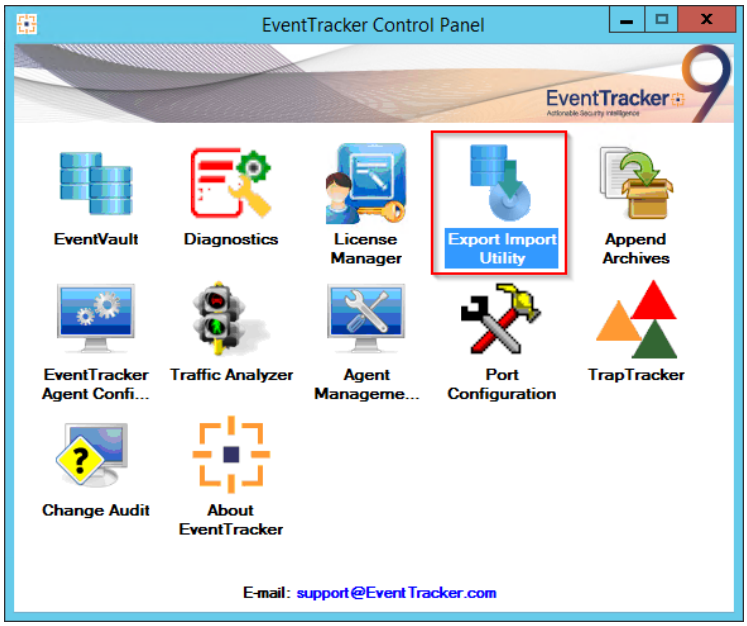

Figure 12

18. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then click Browse ... .

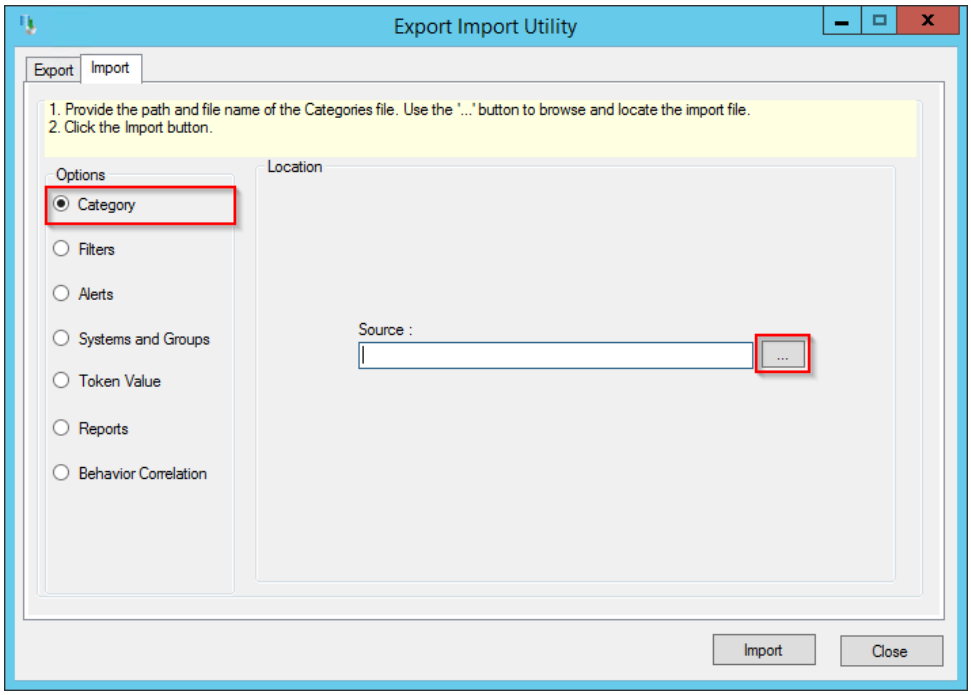

Figure 13

2. Locate **Category_StealthINTERCEPT.iscat** file, and then click **Open**.
3. To import categories, click **Import**.

EventTracker displays success message.

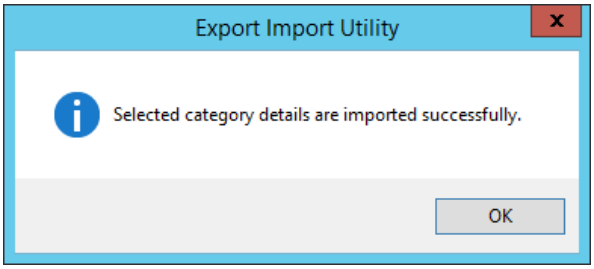

Figure 14

4. Click **OK,** and then click **Close**.

5.2 Alert

1. Click **Alert** option, and then click **browse** ... .

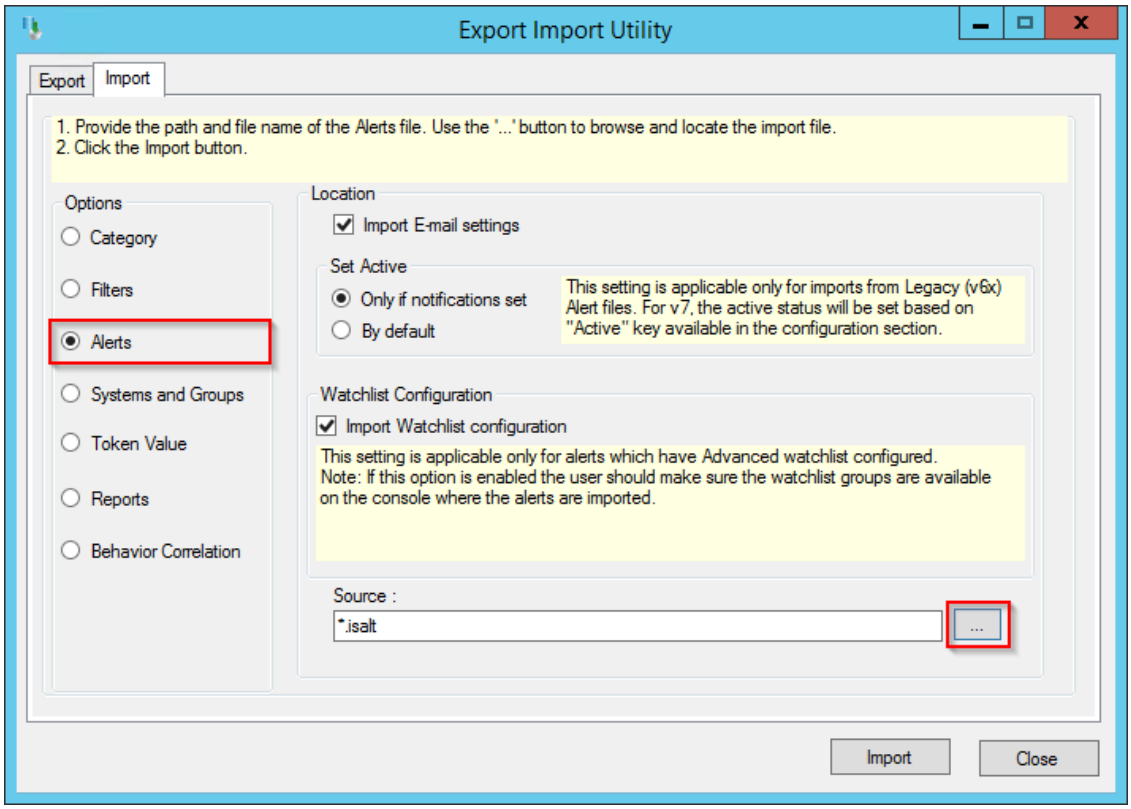

Figure 15

2. Locate **Alert_StealthINTERCEPT.isalt** file, and then click **Open**.
3. To import alerts, click **Import**.
   EventTracker displays success message.

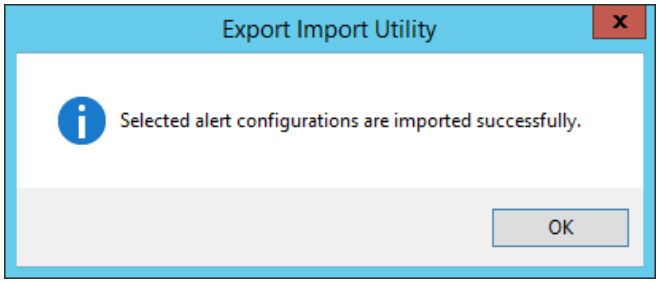

Figure 16

4. Click **OK**, and then click **Close**.

5.3 Knowledge Object

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.

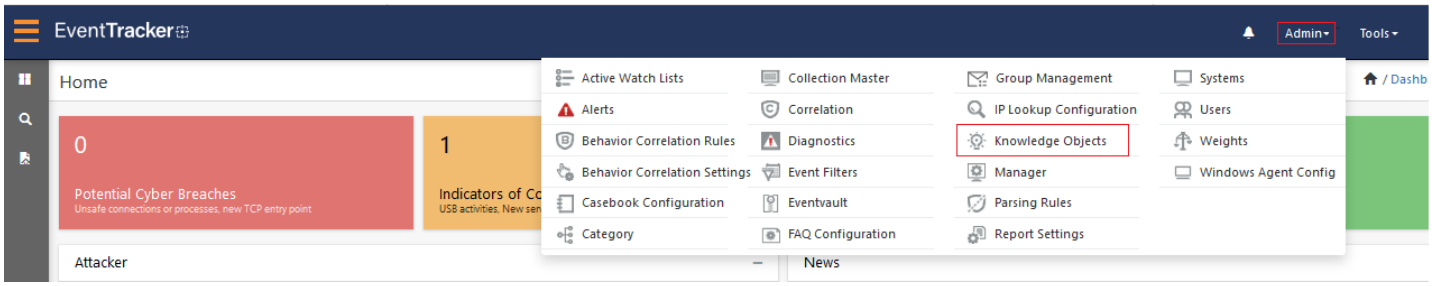

Figure 17

2. Click on **Import** button as highlighted in the following image.

Figure 18

3. Click **Browse**.

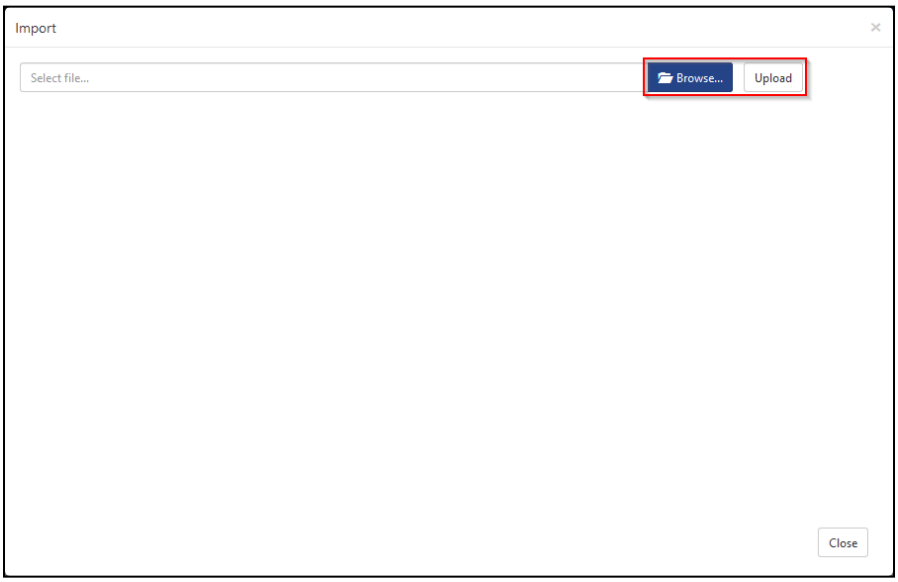

Figure 19

4. Locate the file named **KO_StealthINTERCEPT.etko**.
5. Now select the check box and then click **Import**.

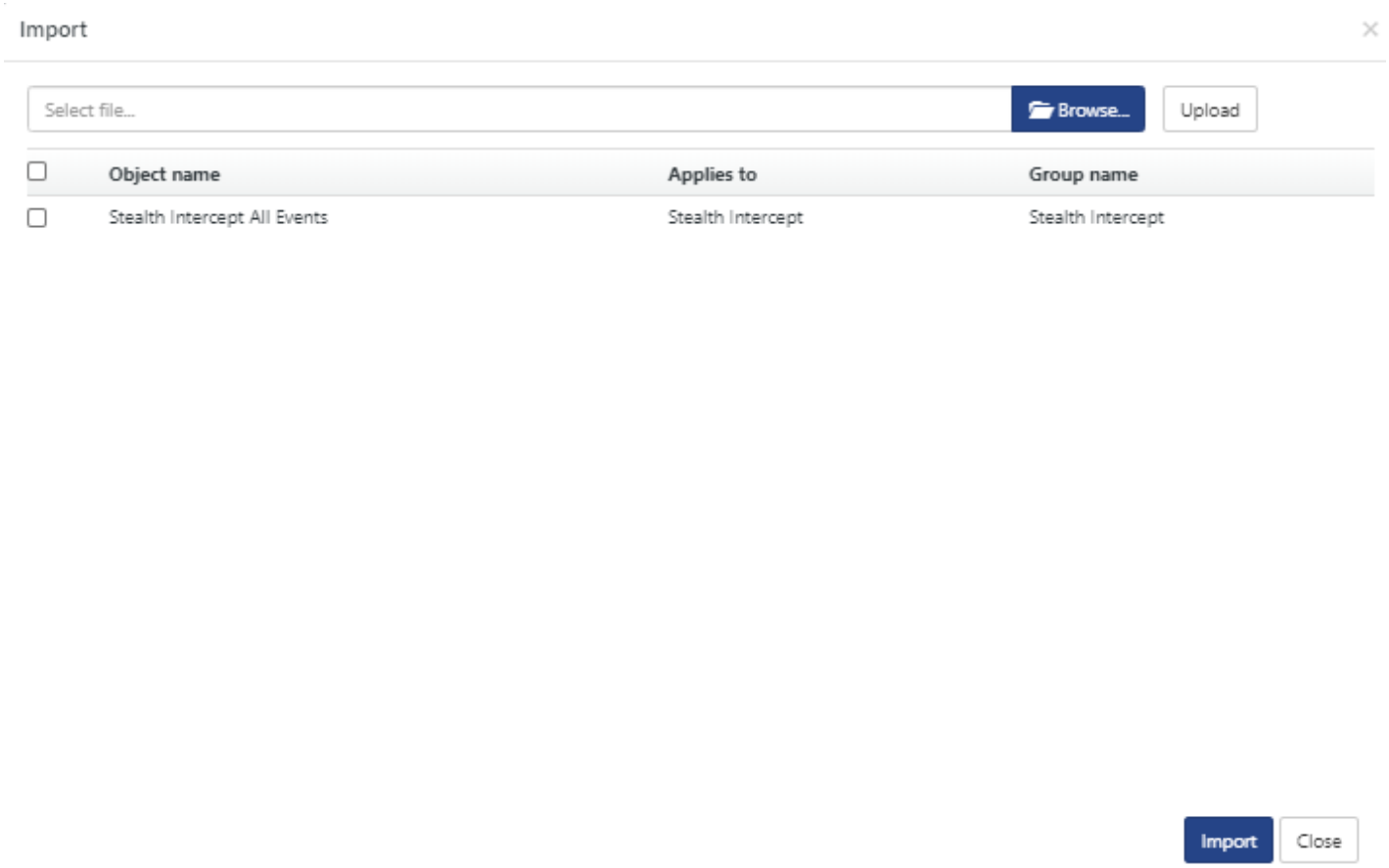

Figure 20

6. Knowledge objects are now imported successfully.

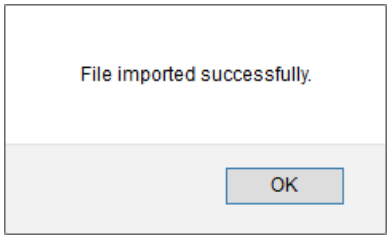

Figure 21

5.4 Report

1. Click **Reports** option, and select **New (*.etcrx)** option.

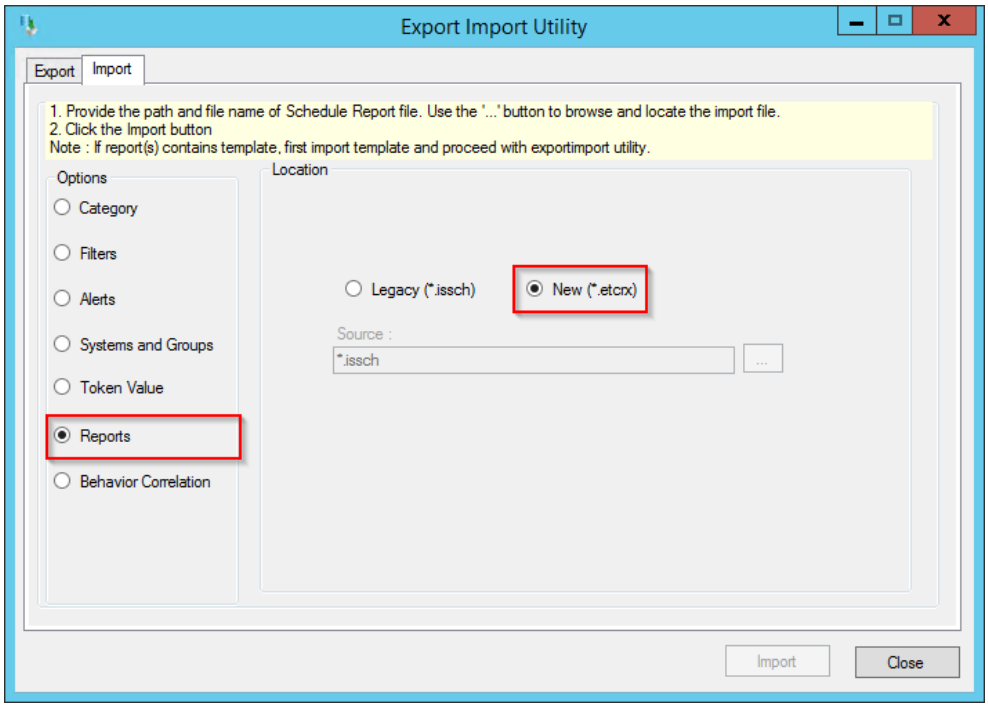

Figure 22

2. Locate the file named **Reports_ StealthINTERCEPT.etcrx** and select the check box.

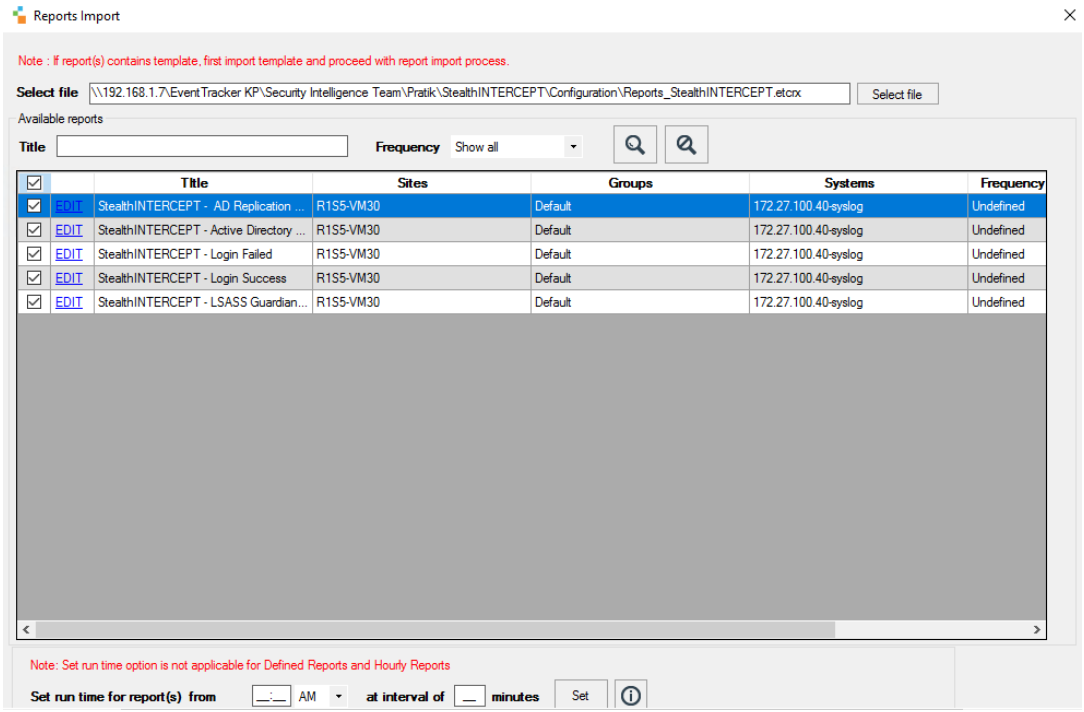

Figure 23

3. Click the **Import** button to import the report. EventTracker displays success message.

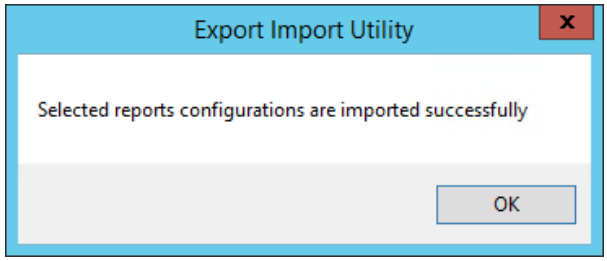

Figure 24

5.5 Dashboards

NOTE: The following steps are specific to EventTracker 9 and later.

1. Open **EventTracker** in browser and logon.

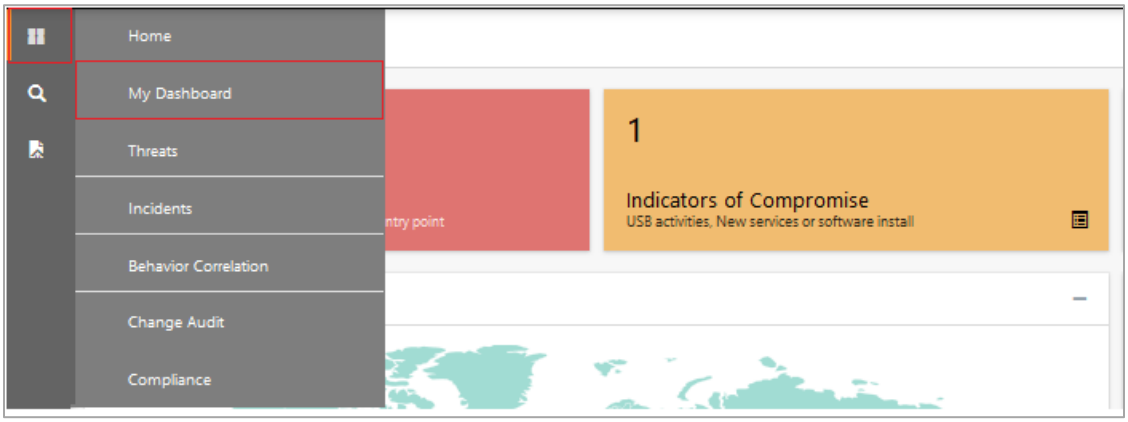

Figure 25

2. Navigate to **My Dashboard** option as shown above.
3. Click on the **Import** button as show below.

Figure 26

4. Import dashboard file **Dashboard_StealthINTERCEPT.etwd** and select **Select All** checkbox**.**
5. Click **Import** as shown below.

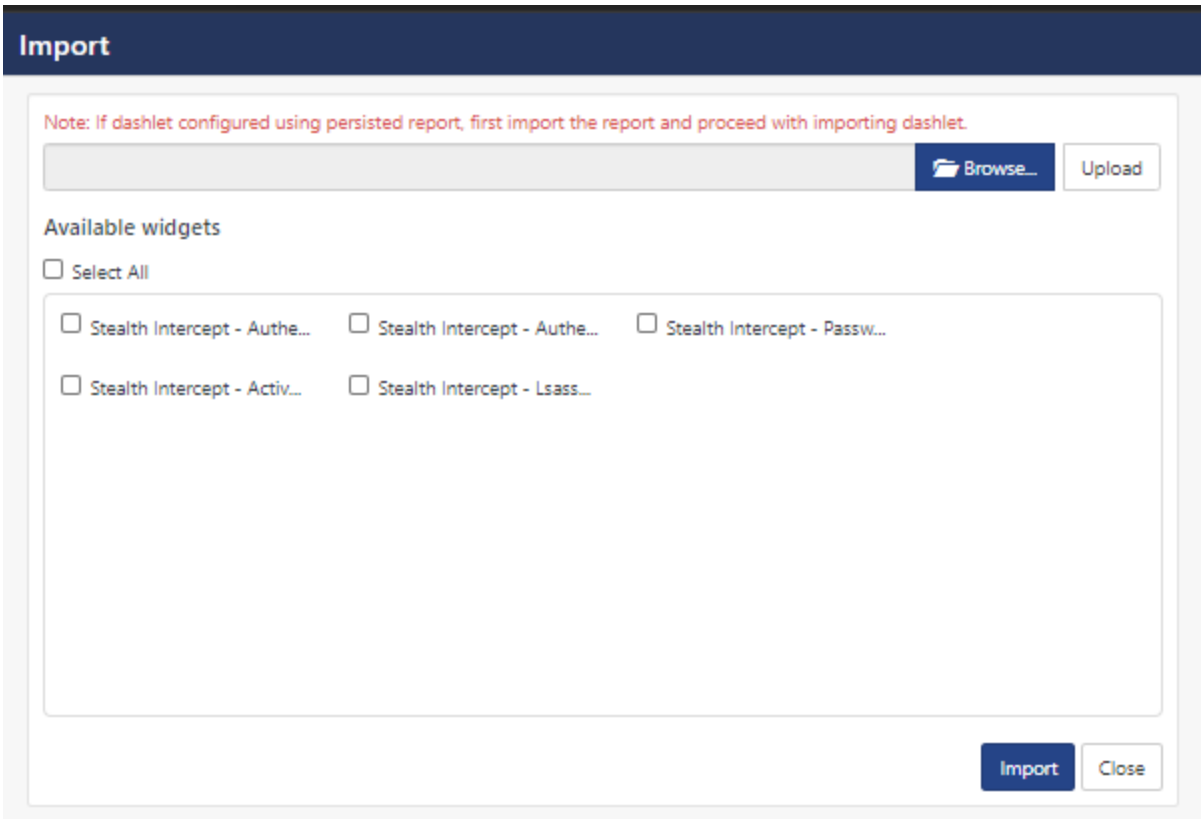

Figure 27

6. Import is now completed successfully.

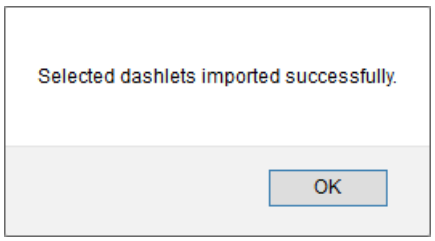

Figure 28

6. Verifying StealthINTERCEPT knowledge pack in EventTracker

6.1 Category

1. Log into **EventTracker**.
2. Click **Admin** dropdown, and then click **Category**.

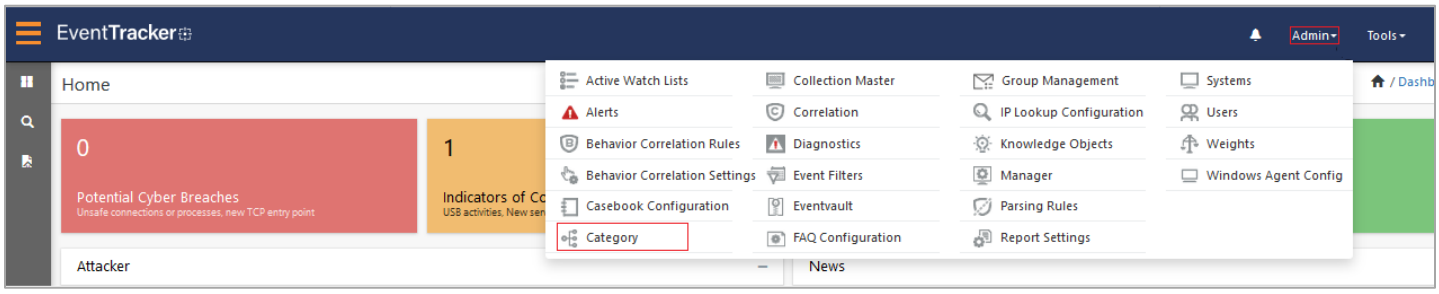

Figure 29

3. In **Category Tree** to view imported category, scroll down and expand **StealthINTERCEPT** group folder to view the imported category.

6.2 Alert

1. Log into **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.

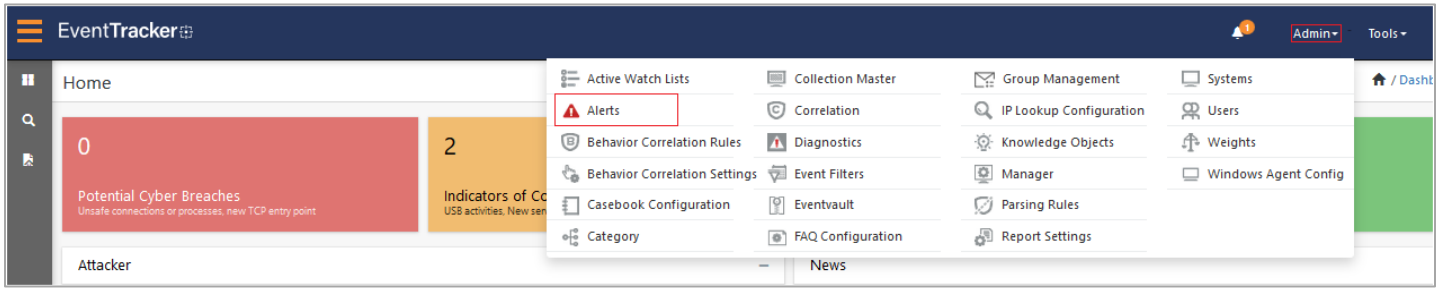

Figure 30

3. In the **Search** box, type '**StealthINTERCEPT**, and then click **Go**.
   Alert Management page will display the imported alert.

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.

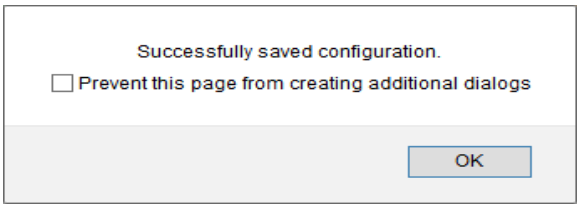

Figure 31

5. Click **OK**, and then click the **Activate Now** button.

NOTE: Please specify appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects.**

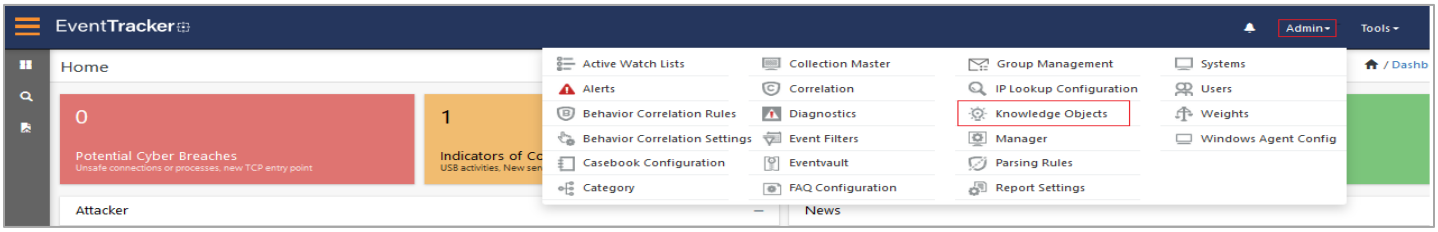

Figure 32

2. In the Knowledge Object tree, expand **StealthINTERCEPT** group folder to view the imported knowledge object.

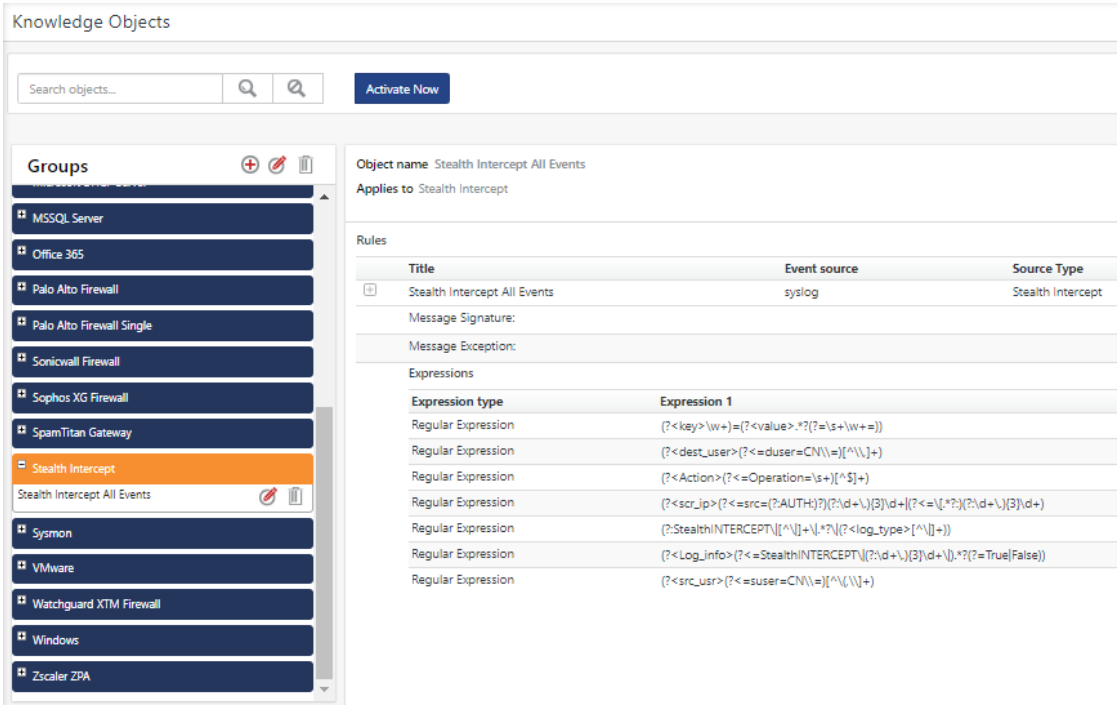

Figure 33

3. Click **Activate Now** to apply imported knowledge objects.

6.4 Report

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.

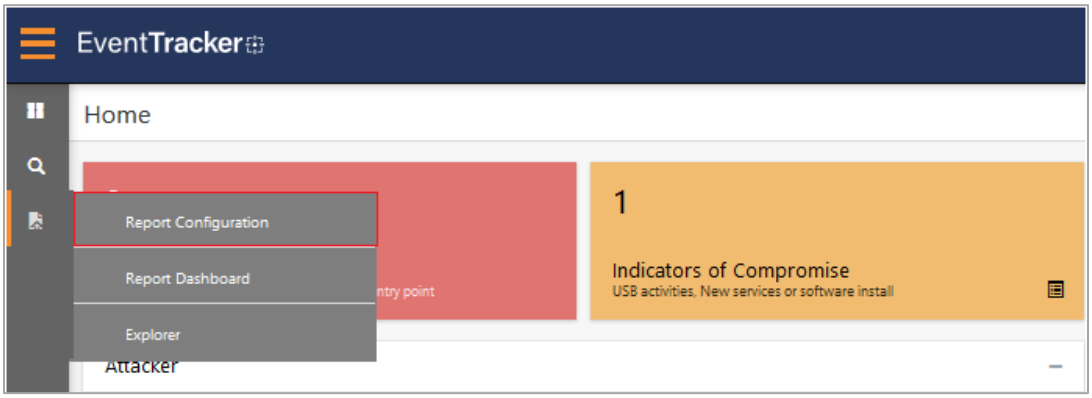

Figure 34

2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **StealthINTERCEPT** group folder to view the imported reports.

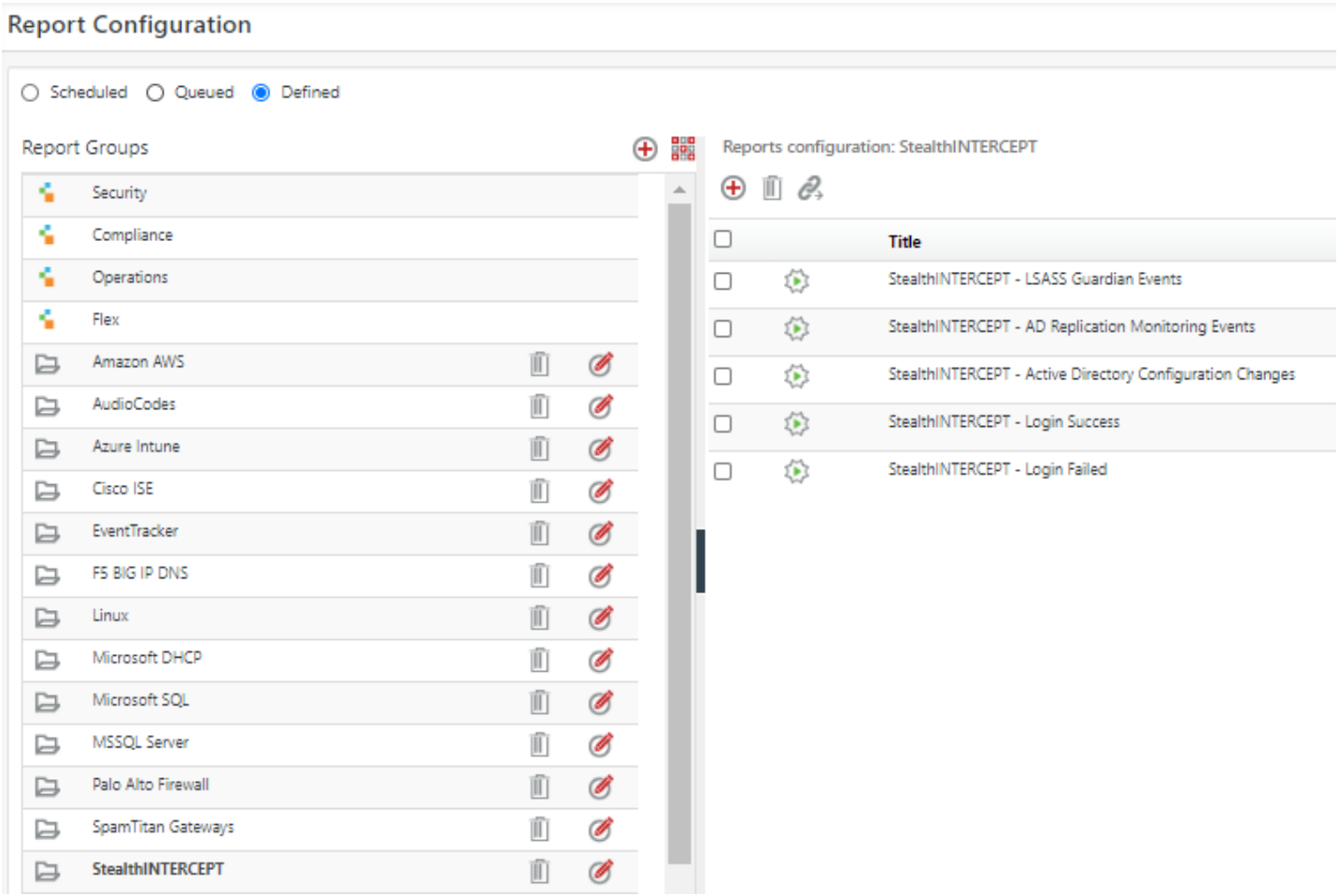

Figure 35

6.5 Dashboards

1. In the EventTracker web interface, Click **Home** and select "**My Dashboard**".

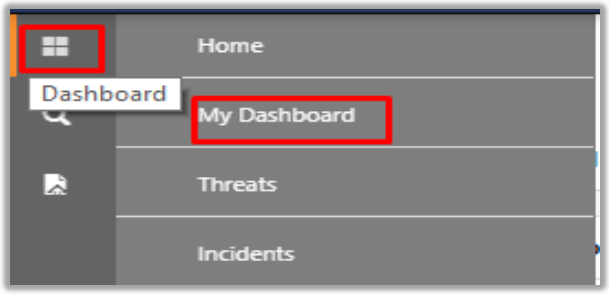

Figure 36

2. In the "**StealthINTERCEPT**" dashboard the following screen appears.

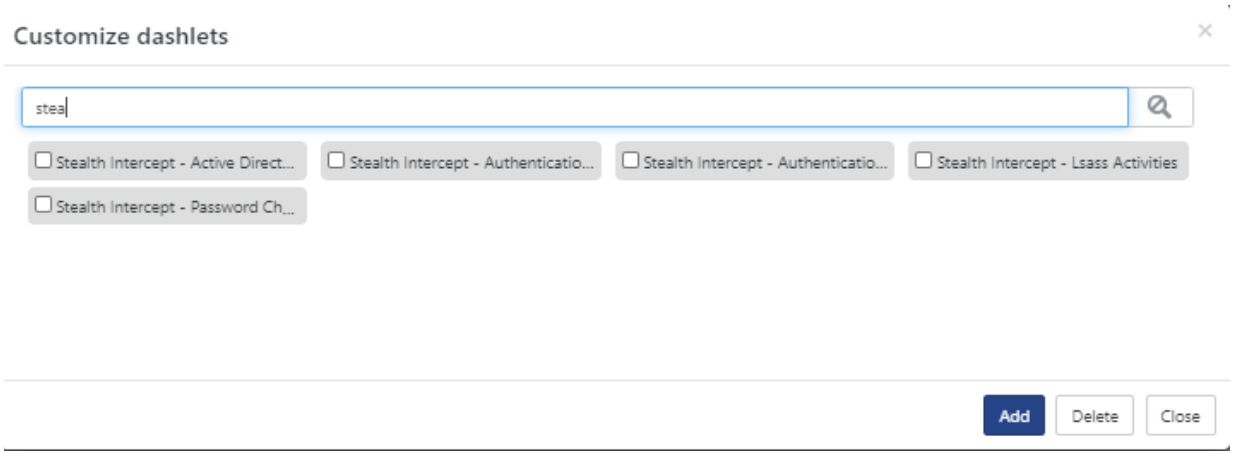
Customize dashlets
stea
Stealth Intercept - Active Direct...
Stealth Intercept - Authenticatio...
Stealth Intercept - Authenticatio...
Stealth Intercept - Lsass Activities
Stealth Intercept - Password Ch...
Add
Delete
Close

Figure 37