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**.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	0	verview
2.	Pr	erequisites
3.	In	tegrating StealthINTERCEPT with EventTracker3
4.	Ev	ventTracker Knowledge Pack
	4.1	
	4.2	Alert
	4.3	Report5
	4.4	Dashboards
5.	In	nporting StealthINTERCEPT knowledge pack into EventTracker
	5.1	Category11
	5.2	Alert
	5.3	Knowledge Object
	5.4	Report15
	5.5	Dashboards17
6.	Ve	erifying StealthINTERCEPT knowledge pack in EventTracker19
	6.1	Category
	6.2	Alert19
	6.3	Knowledge Object
	6.4	Report
	6.5	Dashboards

Netsurion. EventTracker

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** \rightarrow **Alerts**.
- 4. Click the SIEM tab.
- 5. Click the button in front of **Disabled** to toggle the setting to **Enabled**.

SI System Alerting				
Email Event Log SIEM				
		Events	Configure	Disabled
Security	Bad User ID (by source host) Bad User ID (by user)	<select please="" profile,=""> <select please="" profile,=""></select></select>		Ongoing Attack Alerts Ongoing Attack Alerts
Operations	Breached Password Brute Force Attack	<select please="" profile,=""> <empty></empty></select>		Origoing Attack Alerts Origoing Attack Alerts
Configuration	Concurrent Logins File System Attacks (by user)	SIEM Profile 1 SIEM Profile 2	"	Ongoing Attack Alerts Ongoing Attack Alerts
Analytica	Forged PAC Golden Tickets			Ongoing Attack Alerts Ongoing Attack Alerts
Policies	Horizontal Movement Attacks Imperionation Logins			Ongoing Attack Alerts Ongoing Attack Alerts Ongoing Attack Alerts
	Kerberos Weak Encryption	<select please="" profile,=""> <select please="" profile,=""></select></select>		Cingoing Attack Alerts
	3			
	Select All Desslect All			
				OK Cancel

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.

Netsurion. EventTracker

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\=healthmailbox38f36bfa0bd345 c6aa4158999f8f7bd0,cn\=monitori ng mailboxes,cn\=microsoft exchange system objects,dc\=rowanads,dc\=rowan, dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=healthmailbox38f36bfa0bd345 c6aa4158999f8f7bd0,cn\=monitori ng mailboxes,cn\=microsoft exchange system objects,dc\=rowanads,dc\=rowan, dc\=edu	healthmailbox38f36bfa0 bd345c6aa4158999f8f7 bd0	[::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\=r owanads,dc\=rowan,dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=irons al,ou\=affiliates,ou\=accounts,dc\=r owanads,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\=ed u	user	StealthDEFEND for AD	ROWANADS	cn\=miller kevin,ou\=employees,ou\=accounts ,dc\=rowanads,dc\=rowan,dc\=ed u	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\=rowa n,dc\=edu	user	StealthDEFEND for AD	ROWANADS	cn\=fusco catherine m,ou\=wellness,ou\=som,ou\=som, ou\=med,dc\=rowanads,dc\=rowa n,dc\=edu	fusco\	[::ffff:10.84.128.211]
07/24/2020 12:33:29 PM	R1S5-VM30\172.27.100.40- SYSLOG	CN\=HealthMailboxce823841dd344 a99b67d594541483411,CN\=Monit oring Mailboxes,CN\=Microsoft Exchange System Objects,DC\=rowanads,DC\=rowa n,DC\=edu	user	StealthDEFEND for AD	ROWANADS	CN\=HealthMailboxce823841dd344 a99b67d594541483411,CN\=Monit oring Mailboxes,CN\=Microsoft Exchange System Objects,DC\=rowanads,DC\=rowa n,DC\=edu	HealthMailboxce823841 dd344a99b67d5945414 83411	[::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,d c\=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\=rowa n,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,d c\=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\=r owanads,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\=so m,ou\=med,dc\=rowanads,dc\=row an,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\=rowa n,dc\=edu	fusco\
07/24/2020 12:33:28 PM	R1S5-VM30172.27.100.40- SYSLOG	user	StealthDEFEND for AD	ROWANADS	[::ffff:150.250.75.9]	cn\=healthmailbox7a6696c1448b46 cea7a0c4a71b5dfecd,cn\=monitori ng mailboxes,cn\=microsoft exchange system objects,dc\=rowands,dc\=rowan, dc\=edu	healthmailbox7a6696c1448b46cea 7a0c4a71b5dfecd
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\=healthmailbox7a6696c1448b46 cea7a0c4a71b5dfecd,cn\=monitori ng mailboxes,cn\=microsoft exchange system	healthmailbox7a6696c1448b46cea 7a0c4a71b5dfecd

Figure 3

Netsurion. EventTracker

• 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		Attribute Name	Blocked	Destination User	 Object Class 	8 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	1 R1S5- VM30\172. 27.100.40- SYSLOG	lastLogon	False	CN\=Studdeli0020, OU\=GBORO,OU\= Managed,OU\=Wor kstations,DC\=row	computer	StealthDEFEND for AD	ROWANADS	AUTH:Studdell0020	CNI=Anonymous Logon, CNI=WellKnown Security Principals, CNI=Configuration, DCI=r owanads, DCI=rowan, DCI=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	1 R1S5- VM30\172. 27.100.40- SYSLOG	logonCount	False	CN\=Millennium Proxy,OU\=Proxies ,DC\=rowanads,D C\=rowan,DC\=ed	user	StealthDEFEND for AD	ROWANADS	AUTH:MILLENNIUM7	CNI=Anonymous Logon, CNI=WellKnown Security Principals, CNI=Configuration, DCI=r owanads, DCI=rowan, DCI=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	65535		True
07/20/2020 05:34:40 PM	1 R1S5- VM30\172. 27.100.40- SYSLOG	lastLogon	False	CN\=Millennium Proxy,OU\=Proxies ,DC\=rowanads,D C\=rowan,DC\=ed	user	StealthDEFEND for AD	ROWANADS	AUTH:MILLENNIUM7	CNI=Anonymous Logon, CNI=WellKnown Security Principals, CNI=Configuration, DCI=r owanads, DCI=rowan, DCI=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	1 R1S5- VM30\172. 27.100.40- SYSLOG	logonCount	False	CN\=Millennium Proxy,OU\=Proxies ,DC\=rowanads,D C\=rowan,DC\=ed	user	AD: Successful Account Logons	ROWANADS	AUTH:MILLENNIUM7	CNI=Anonymous Logon, CNI=WellKnown Security Principals, CNI=Configuration, DCI=r owanads, DCI=rowan, DCI=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	65535		True
07/20/2020 05:34:40 PM	1 R1S5- VM30\172. 27.100.40- SYSLOG	lastLogon	False	CN\=Millennium Proxy,OU\=Proxies ,DC\=rowanads,D C\=rowan,DC\=ed	user	AD: Successful Account Logons	ROWANADS	AUTH:MILLENNIUM7	CNI=Anonymous Logon, CNI=WellKnown Security Principals, CNI=Configuration, DCI=r owanads, DCI=rowan, DCI=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	1 R1S5- VM30\172. 27.100.40- SYSLOG	logonCount	False	CN\=Martin Mischa Forsberg,OU\=Cfa OU\=SOM,OU\=SO M,OU\=Med,DC\=ro	user	AD: Successful Account Logons	ROWANADS	AUTH:CTXICON001	CNI=Anonymous Logon, CNI=WellKnown Security Principals, CNI=Configuration, DCI=r owanads, DCI=rowan, DCI=edu	Anonymous Logon	Change Attribute	Active DirectoryuserObject Modified	12636		True
07/20/2020 05:34:40 PM	1 R1S5- VM30\172. 27.100.40- SYSLOG	lastLogon	False	CN\=Martin Mischa Forsberg,OU\=Cfa, OU\=SOM,OU\=SO M,OU\=Med,DC\=rc	user	StealthDEFEND for AD	ROWANADS	AUTH:CTXICON001	CNI=Anonymous Logon, CNI=WellKnown Security Principals, CNI=Configuration, DCI=r owanads, DCI=rowan, DCI=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	I 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

- HI	σ		r	Δ	Δ
	5	u		<u> </u>	_

• 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	CNI=System,CNI=WellKnown Security Principals,CNI=Configuration,DCI=r owanads,DCI=rowan,DCI=edu	System
07/20/2020 05:34:45 PM	R1S5- VM30\172.27. 100.40- SYSLOG	Desired	lsass.exe	PROCESS_QUERY_LIMITE D_INFORMATION	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CNI=System,CNI=WellKnown Security Principals,CNI=Configuration,DCI=r owanads,DCI=rowan,DCI=edu	System
07/20/2020 05:34:45 PM	R1S5- VM30\172.27. 100.40- SYSLOG	Desired	lsass.exe	PROCESS_QUERY_INFOR MATION	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CN\=System,CN\=WellKnown Security Principals,CN\=Configuration,DC\=r owanads,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	CNI=System,CNI=WellKnown Security Principals,CNI=Configuration,DCI=r owanads,DCI=rowan,DCI=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	CNI=System,CNI=WellKnown Security Principals,CNI=Configuration,DCI=r owanads,DCI=rowan,DCI=edu	System
07/20/2020 05:34:45 PM	R1S5- VM30\172.27. 100.40- SYSLOG	Desired	lsass.exe	PROCESS_VM_OPERATIO N	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CNI=System,CNI=WellKnown Security Principals,CNI=Configuration,DCI=r owanads,DCI=rowan,DCI=edu	System
07/20/2020 05:34:45 PM	R1S5- VM30\172.27. 100.40- SYSLOG	Desired	lsass.exe	PROCESS_CREATE_THRE AD	n/a	StealthDEFEND for AD	ROWANADS	vmtoolsd.exe	LSASS Guardian - Monitorn/aCreate handle	True	CNI=System,CNI=WellKnown Security Principals,CNI=Configuration,DCI=r owanads,DCI=rowan,DCI=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\=row an,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\=ro wan,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\=ro wan,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\=row an,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\=row an,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\=ro wan,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\=ro wan,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







Integrate StealthINTERCEPT



• StealthINTERCEPT: Authentication Success by Username



• StealthINTERCEPT: Active Directory Activities



Figure 9





• StealthINTERCEPT: Password Changes by Username

• StealthINTERCEPT: LSASS Activites





Netsurion. EventTracker

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

4	Export Import Utility	- 🗆	x
Export Import 1. Provide the path and file nam 2. Click the Import button. Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation 	e of the Categories file. Use the '' button to browse and locate the import file. Location Source :		
	Import	Clos	se

Figure 13

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

EventTracker displays success message.





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

5.2 Alert

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

<u>ц</u>	Export In	nport Utility	– – X
Export Import	Export In the of the Alerts file. Use the '' butto Location Import E-mail settings Set Active Only if notifications set By default Watchlist Configuration Import Watchlist configuration Import Watchlist configuration Surce : [*isalt	nport Utility on to browse and locate the import file. This setting is applicable only for imports from Lega Alert files. For v7, the active status will be set base "Active" key available in the configuration section on or alerts which have Advanced watchlist configured. s are imported.	acy (v6x) ad on vailable
		Import	Close

Figure 15

- 2. Locate Alert_StealthINTERCEPT.isalt file, and then click Open.
- 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.



≡	Event Tracker ⊕					Admin-	To ols +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	© Correlation	🔍 IP Lookup Configuration	🛱 Users	_
	0	1	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	1 Weights	
~			🇞 Behavior Correlation Settings	⊽ Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Seventvault	😥 Parsing Rules		
		_		FAQ Configuration	Report Settings		
	Attacker			- News			



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

	Knowledge Objects								
Q R	Search objects	Q	Q Activate Now	Objects 🕀 📳 🏦 🌣					
	Groups	🕂 🔗 🗓		Ĺ					
	E Cylance								
	EventTracker								

Figure 18

Impot × Select file...



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

Netsurion. EventTracker

3. Click Browse.

Import				×
Select	t file		Browse Upload	
	Object name	Applies to	Group name	
	Stealth Intercept All Events	Stealth Intercept	Stealth Intercept	

Import Close

Figure 20

6. Knowledge objects are now imported successfully.



5.4 Report

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



4	Export Import Utility									
Export Import	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility. Location Legacy (* issch) New (*.etcx) Source : *.issch									
	Import									

Figure 22

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

Note	: If report	t(s) contains template, first import template a	and proceed with report import process.			~
Sele	t file	\\192.168.1.7\EventTracker KP\Security	Intelligence Team\Pratik\StealthINTERCE	EPT\Configuration\Reports_StealthINTER	ICEPT.etcrx Select file	
Avail	able repo	orts				
Title			Frequency Show all	- Q Q		
	-	Title	Sites	Groups	Systems	Frequency
	EDIT	StealthINTERCEPT - AD Replication	R1S5-VM30	Default	172.27.100.40-syslog	Undefined
	<u>EDIT</u>	StealthINTERCEPT - Active Directory	R1S5-VM30	Default	172.27.100.40-syslog	Undefined
	EDIT	StealthINTERCEPT - Login Failed	R1S5-VM30	Default	172.27.100.40-syslog	Undefined
	<u>EDIT</u>	StealthINTERCEPT - Login Success	R1S5-VM30	Default	172.27.100.40-syslog	Undefined
	EDIT	StealthINTERCEPT - LSASS Guardian	R1S5-VM30	Default	172.27.100.40-syslog	Undefined
K						>
No	te: Set n	un time option is not applicable for Defined	Reports and Hourly Reports			
Se	t run tii	me for report(s) from	M • at interval of minut	es Set 🚺		

Figure 23

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





5.5 Dashboards

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

1. Open EventTracker in browser and logon.

	Home		
٩	My Dashboard		
R	Threats	1	
	Incidents	Indicators of Compromise ntry point USB activities, New services or software i	nstall 🔳
	Behavior Correlation		
	Change Audit		-
	Compliance		



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

Event Tracker ⊕	٩	Admin -	Tools -	💽 ETAdmin 🔹
My Dashboard		f	/ Dashboar	d / My Dashboard
		(+)	o 🖉 🎯	1 I () ()

Figure 26

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

Ir	nport				
ſ	Note: If dashlet configured using p	persisted report, first import the re	port and proceed with importing	dashlet.	
				🗁 Browse	Upload
	Available widgets Select All				
	Stealth Intercept - Authe	Stealth Intercept - Authe	Stealth Intercept - Passw		
	Stealth Intercept - Activ	Stealth Intercept - Lsass			
				Import	Close

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.

≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	Q Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	reights	
			🇞 Behavior Correlation Settings	🔁 Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Seventvault	Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			



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.

≡	Event Tracker ⊕					🔎 🗛 Admin•	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
٩			Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	2	Behavior Correlation Rules	Diagnostics	Or Knowledge Objects	1 Weights	
~			🗞 Behavior Correlation Settings	Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			



- 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.

≡	Event Tracker ⊕					🐥 🛛 Admin 🕶	Tools -
	Home		E Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	Q IP Lookup Configuration	QQ Users	_
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	r Weights	
			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
		_	● Category	FAQ Configuration	🔊 Report Settings		
	Attacker			- News			

Figure 32

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

Knowledge Objects						
Search objects	Q, Q,	Activ	vate Now			
Groups ¹² _{MSSQL Server}	+ Ø 1	Object Applie	t name. Stealth Intercept All Events es to: Stealth Intercept			
Office 365		Rules	T241_		Event course	Source Turne
Palo Alto Firewall		+	Stealth Intercept All Events		syslog	Stealth Intercept
Palo Alto Firewall Single			Message Signature:			
			Message Exception:			
Sonicwali Firewali			Expressions			
Sophos XG Firewall			Expression type	Expression 1		
SpamTitan Gateway			Regular Expression	(? <key>\w+)=(?</key>	? <value>.*?(?=\s+\w+=))</value>	
E Carabilitation			Regular Expression	(? <dest_user>(?</dest_user>	<=duser=CN\\=)[^\\\]+)	
- Stealth Intercept	et 5		Regular Expression	(? <action>(?<=</action>	Operation=\s+)[^\$]+)	
Stealth Intercept All Events			Regular Expression	(? <scr_ip>(?<=s</scr_ip>	src=(?:AUTH:)?)(?:\d+){3}\d+ (?<=	\[.*?:)(?:\d+\.){3}\d+)
Sysmon			Regular Expression	(?:StealthINTERC	CEPT\[^\]+\!.*?\ (? <log_type>[^\]</log_type>	+))
# Mayoro			Regular Expression	(? <log_info>(?<</log_info>	<=StealthINTERCEPT\ (?:\d+){3}\d	+\).*?(?=True False))
viviwale			Regular Expression	(? <src_usr>(?<=</src_usr>	=suser=CN\\=)[^\(,\\]+)	
Watchguard XTM Firewall						
Windows						
Zscaler ZPA						



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**.





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



Report Configuration

O Sch	eduled 🔿 Queued 💿 Defined							
Report	t Groups			+		Repo	orts configur	ration: StealthINTERCEPT
S.,	Security					€	Î	
S.,	Compliance							Title
S.,	Operations						$\langle \Sigma \rangle$	StealthINTERCEPT - LSASS Guardian Events
S.,	Flex						\otimes	StealthINTERCEPT - AD Replication Monitoring Events
	Amazon AWS	Ĩ	Ø				۵	StealthINTERCEPT - Active Directory Configuration Changes
	AudioCodes	Ĩ	0				(B)	StealthINTERCEPT - Login Success
	Azure Intune	Û	Ø					StealthINTERCEPT - Login Failed
	Cisco ISE	Û	Ø				967°	
	EventTracker	Ĩ	Ø		Ŀ.			
	F5 BIG IP DNS	Û	1		L.			
	Linux	Û	1					
	Microsoft DHCP	Û	1					
	Microsoft SQL	Û	1					
	MSSQL Server	Û	1					
	Palo Alto Firewall	Û	1					
	SpamTitan Gateways	Û	0					
	StealthINTERCEPT	Ĩ	0					

Figure 35

6.5 Dashboards

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

	Home
Dashb	My Dashboard
2	Threats
	Incidents



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



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

Figure 37

