Netsurion. EventTracker

Integrate ProtectWise

EventTracker v9.2 and above

Publication Date: August 31, 2020

Abstract

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

Scope

The configuration details in this guide are consistent with EventTracker version v9.2 or above and **ProtectWise.**

Audience

Administrators, who are assigned the task to monitor and manage ProtectWise 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.	٥v	/erview	3
2.	Pr	erequisites	3
3.	Int	tegration of ProtectWise with EventTracker	3
4.	Ev 4.1	entTracker Knowledge Pack Category	4 4
	4.2	Alert	4
	4.3	Report	4
	4.4	Dashboards 1	2
5.	lm 5.1	porting ProtectWise knowledge pack into EventTracker1 Category	.6 17
	5.2	Alert 1	.8
	5.3	Knowledge Object1	.9
	5.4	Report 2	21
	5.5	Dashboards 2	22
6.	Ve 6.1	erifying ProtectWise knowledge pack in EventTracker	25 25
	6.2	Alert	26
	6.3	Knowledge Object	27
	6.4	Report 2	28
	6.5	Dashboards 2	28

1. Overview

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

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

EventTracker, when integrated with ProtectWise, collects logs and creates detailed reports, alerts, dashboards, and categories. These attributes of EventTracker helps user to view/receive the critical and relevant information regarding security, operations and compliance.

Report contains a detailed summary of threat detected by ProtectWise in IP, URL, DNS, certificate, events and many more in column-value pair.

Alerts are triggered as soon as a high scored threat is received by EventTracker for ProtectWise

Dashboards is a graphical representation of all the activities happening in ProtectWise. These include threat category by threat level, threat by source IP, threat score for all log types and others.

These attributes or configurations of EventTracker allows administrators to quickly take appropriate actions against any threat/adversaries trying to jeopardize an organization's normal operation.

2. Prerequisites

- EventTracker v9.2 or above should be installed.
- **ProtectWise** should be configured.
- Port 514 should be open.
- EventTracker Public IP is required.

3. Integration of ProtectWise with EventTracker

Configuring syslog Message Forwarding Update the **protectwise-emitter.json** file

- In the udpAdapters, set the Host as EventTracker Public IP.
- Set Port to 514.

```
"udpAdapters": [
{
```

```
"host": "<dest_ip>",
"name": "udp",
"port": 514
}
```

Run the protectwise-emitter. EventTracker will start receiving ProtectWise logs.

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 ProtectWise.

4.1 Category

1

- ProtectWise: Certificate Reputation- This category provides threat data about certificate.
- ProtectWise: DNS Reputation This category provides threat data about DNS.
- ProtectWise: File Reputation This category provides threat data about file.
- ProtectWise: URL Reputation This category provides threat data about URL.
- ProtectWise: IP Reputation This category provides threat data about IP.
- ProtectWise: Heuristics This category provides information about threat methods and tactics.
- ProtectWise: Payload This category provides information about payload and threat related to it.
- **ProtectWise: Events-** This category provides information about resources that describe a threat and contains a collection of observations.

4.2 Alert

• **ProtectWise: Threat detected** - This alert is generated when any threat is detected having threat score and severity greater than 50.

4.3 Report

ProtectWise: IP Reputation - This report gives the threat information about IP. Report contains connection category, threat score and level, src and dst IP address, port and other fields which will provide a detailed view about user activity.

LogTime	Computer	Destination Ip	Destination Port		Kill Chain Stage	Layer 3 Protocol	Layer 4 Protocol	Observation Direction	Protocol	Severity	Source IP
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	127.0.0.2	53	0000015477ea0f8cb2d9e10f0fa5a b8ac461d97e0005	Recon	IPv4	Тср	None	TCP	15	127.0.0.1
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	127.0.0.2	53	0000015477ea0f8cb2d9e10f0fa5a b8ac461d97e0005	Recon	IPv4	Тср	None	TCP	1 5	127.0.0.1
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	127.0.0.2	53	0000015477ea0f8cb2d9e10f0fa5a b8ac461d97e0005	Recon	IPv4	Тср	None	TCP	15	127.0.0.1



addl_info	+- Realtime
addl_info8	+UNKWNTOK-
attributes	+- Proxy
dest_ip_address	+- 127.0.0.2
dest_port_no	+- 53
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+- 1598244010
event_description	Aug 24 10:10:10 172.27.100.13 Aug 05 14:27:46 192.168.1.86 2020-08-05T14:27:57.480-06:00 160901-onsite-nts-01 protectwise-emitter[17790]: [ipRep] s
	ensorName:DMZ category:Suspicious id:0000015477ea0f8cb2d9e10f0fa5ab8ac461d97e0005 observedAt:2016-05-03T12:38:30.708-06:00 isoObservedAtU
	TC:2016-05-03T18:38:30.708Z occurredAt:1462300708748 occurredAt:2016-05-03T12:38:28.748-06:00 isoOccurredAtUTC:2016-05-03T18:38:28.748Z obse
	rvedStage:Realtime observationDirection:None killChainStage:Recon severity:15 threatLevel:Low threatScore:15 threatSubCategory: < no value> type: < no v
	alue> dstip:127.0.0.2 srclp:127.0.0.1 srcPort:61636 dstPort:53 proto:TCP layer3Proto:IPv4 layer4Proto:Tcp nfkey:-UNKWNTOK- nfStartedAt:1462300708748
	isoNfStartedAt:2016-05-03T12:38:28.748-06:00 isoNfStartedAtUTC:2016-05-03T18:38:28.748Z ipRepCategory:Proxy ip:10.126.23.174
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
group_name	+- Recon
interface in	+- DMZ

Figure 2

• **ProtectWise: URL Reputation** - This report gives the threat information about URL. Report contains category, threat score and level, severity, URL reputation category and other details which can be used for further investigation.

LogTime	Computer	Category	Destination Ip	Destination Port	Hostname	ld	Kill Chain Stage	Layer 3 Protocol	Layer 4 Protocol	Observation Direction	Observed St
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.100.13- SYSLOG	Malware	127.0.0.2	53	evil.example.com	0000015477ea0f8cb2d9e10f0fa5a b8ac461d97e0005	Delivery	IPv4	Тср	None	Realtime
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.100.13- SYSLOG	Malware	127.0.0.2	53	evil.example.com	0000015477ea0f8cb2d9e10f0fa5a b8ac461d97e0005	Delivery	IPv4	Тср	None	Realtime
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.100.13- SYSLOG	Malware	127.0.0.2	53	evil.example.com	0000015477ea0f8cb2d9e10f0fa5a b8ac461d97e0005	Delivery	IPv4	Тср	None	Realtime



addl_info	+- Realtime
addLinfo8	+UNKWNTOK-
attributes	+ - Malwaresites
change_info	+- p1=1193\u0026p2=384
dest_host_name	+- evil.example.com
dest_ip_address	+- 127.0.0.2
dest_port_no	+- 53
event_category	+- 0
event_computer	+ - 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+ - 1598244010
event_description	Aug 24 10:10:10 172.27.100.13 Aug 05 14:27:46 192.168.1.86 2020-08-05T14:27:57.482-06:00 160901-onsite-nts-01 protectwise-emitter[17790]: [urlRep] s
	ensorName:DMZ category:Malware id:0000015477ea0f8cb2d9e10f0fa5ab8ac461d97e0005 observedAt:2016-05-03T12:38:30.708-06:00 isoObservedAtUT
	C:2016-05-03T18:38:30.708Z occurredAt:1462300708748 occurredAt:2016-05-03T12:38:28.748-06:00 isoOccurredAtUTC:2016-05-03T18:38:28.748Z obser
	vedStage:Realtime observationDirection:None killChainStage:Delivery severity:15 threatLevel:Low threatScore:15 threatSubCategory: <no value=""> type:<no< td=""></no<></no>
	value> dstlp:127.0.0.2 srclp:127.0.0.1 srcPort:61636 dstPort:53 proto:TCP layer3Proto:IPv4 layer4Proto:Tcp nfkey:-UNKWNTOK- nfStartedAt:146230070874
	8 isoNfStartedAt:2016-05-03T12:38:28:748-06:00 isoNfStartedAtUTC:2016-05-03T18:38:28:748Z urlRepCategory:Malwaresites url:evil.example.com/Tracke
	r/CoT?p1=1193\u0026p2=384 hostname:evil.example.com path:/Tracker/CoT port:80 queryString:p1=1193\u0026p2=384
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
file_path	+ - /Tracker/CoT

Figure 4

• **ProtectWise: File Reputation** – This report gives threat information about File. Report contains category, file type, threat score and level and other useful details for further investigation.

LogTime	Computer	Category	Destination Ip	Destination Port	Kill Chain Stage	Layer 3 Protocol	Layer 4 Protocol	Observation Direction	Stage	Protocol	Severity
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.100.13- SYSLOG	Malware	127.0.0.2	53	Delivery	IPv4	Тср	Dst_to_src	Realtime	Тср	55
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.100.13- SYSLOG	Malware	127.0.0.2	53	Delivery	IPv4	Тср	Dst_to_src	Realtime	Тср	55
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.100.13- SYSLOG	Malware	127.0.0.2	53	Delivery	IPv4	Тср	Dst_to_src	Realtime	Тср	* 55

Figure 5



addl_info	+- Realtime
addLinfo8	+UNKWNTOK-
dest_ip_address	+- 127.0.0.2
dest_port_no	+- 53
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+- 1598244010
event_description	Aug 24 10:10:10 172.27.100.13 Aug 05 14:27:46 192.168.1.86 2020-08-05T14:27:57.464-06:00 160901-onsite-nts-01 protectwise-emitter[17790]: [fileRep]
	sensorName:DMZ category:Malware id:000001546d3d8c34dfed1536f84fc28966c8c57f0007 observedAt:2016-05-03T12:39:33.053-06:00 isoObservedAtUT
	C:2016-05-03T18:39:33.053Z occurredAt:1462121630930 occurredAt:2016-05-01T10:53:50.930-06:00 isoOccurredAtUTC:2016-05-01T16:53:50.930Z obser
	$vedStage: Real time \ observation Direction: Dst_to_src \ kill Chain Stage: Delivery \ severity: 55 \ threat Level: Medium \ threat Score: 54 \ threat SubCategory: t \ threat SubCategory: t \ value > t \ $
	ype:PE dstlp:127.0.0.2 srclp:127.0.0.1 srcPort:1048 dstPort:53 proto:Tcp layer3Proto:IPv4 layer4Proto:Tcp nfkey:-UNKWNTOK- nfStartedAt:1462121630772 i
	soNfStartedAt:2016-05-01T10:53:50.772-06:00 isoNfStartedAtUTC:2016-05-01T16:53:50.772Z
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
group_name	+- Delivery
interface_in	+- DMZ
log_datetime	+- 2016-05-03T18:39:33.053Z
log_direction	+- Dst_to_src
a	• •

Figure 6

• **ProtectWise: DNS Reputation** – This report gives threat information about DNS. Report contains threat category, score, level, DNS query, src and ds tip, port and other useful information.

LogTime	Computer	Category	Dns Conversation	Dns Rep Category	Destination Ip	Destination Port	id	Dns	Kill Chain Stage
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Suspicious	query:[{query:jpdiyo2tuwsma qoq4azid.com,queryType:IPV	5f4z0 MachineGenerated I_AD	127.0.0.2	53	0000015477eab48c409250cd993e 2774610457c00008	jpdiyo2tuwsma5f4z0qoq4azid.com	Beacon
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Suspicious	query:[{query:jpdiyo2tuwsma qoq4azid.com,queryType:IPV	5f4z0 MachineGenerated I_AD	127.0.0.2	53	0000015477eab48c409250cd993e 2774610457c00008	jpdiyo2tuwsma5f4z0qoq4azid.com	Beacon
08/20/2020 11:36:36 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Suspicious	query:[{query:jpdiyo2tuwsma qoq4azid.com,queryType:IPV	5f4z0 MachineGenerated 4_AD	127.0.0.2	53	0000015477eab48c409250cd993e 2774610457c00008	jpdiyo2tuwsma5f4z0qoq4azid.com	Beacon



addl_info	+- Realtime
addl_info8	+UNKWNTOK-
attributes	+- MachineGenerated
change_info	+ - {query:[{query:jpdiyo2tuwsma5f4z0qoq4azid.com,queryType:IPV4_ADDRESS]],response:[{com:[{response:[hostname:a.gtld-servers.net,ipAddress:nul I],responseType:6,ttl:900]]]],responseCode:No_such_name,transactionId:9731}
dest_host_name	+- a.gtld-servers.net
dest_ip_address	+- 127.0.0.2
dest_port_no	+- 53
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+- 1598244010
event_description	Aug 24 10:10:10 172.27.100.13 Aug 05 14:27:41 192.168.1.86 2020-08-05T14:27:56.449-06:00 160901-onsite-nts-01 protectwise-emitter[17790]: [dnsRe
	p] sensorName:DMZ category:Suspicious id:0000015477eab48c409250cd993e2774610457c00008 observedAt:2016-05-03T12:39:32.927-06:00 isoObserv
	edAtUTC:2016-05-03T18:39:32.927Z occurredAt:1462300767491 occurredAt:2016-05-03T12:39:27.491-06:00 isoOccurredAtUTC:2016-05-03T18:39:27.49
	1Z observedStage:Realtime observationDirection:None killChainStage:Beacon severity:45 threatLevel:Medium threatScore:45 threatSubCategory: < no val
	ue> type: <no value=""> dstlp:127.0.0.2 srclp:127.0.0.1 srcPort:49408 dstPort:53 proto:Udp layer3Proto:IPv4 layer4Proto:Udp nfkey:-UNKWNTOK- nfStartedA</no>
	t:1462300750988 isoNfStartedAt:2016-05-03T12:39:10.988-06:00 isoNfStartedAtUTC:2016-05-03T18:39:10.988Z dns:jpdiyo2tuwsma5f4z0qoq4azid.com d
	nsRepCategory:MachineGenerated dnsConversation:{query:[query:jpdiyo2tuwsma5f4z0qoq4azid.com,queryType:IPV4_ADDRESS]],response:[{com:[{resp
	$onse: \{ host name; a:gtld-servers.net, ip Address: null \}, response Type: 6, ttl: 900 \} \}], response Code: No_such_name, transaction Id: 9731 \} \} (a) = 0.5, a) = 0$
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0

Figure 8

• **ProtectWise: Certificate Reputation** - This report gives threat information about certificate. Report contains threat category, level, score, signing chain, src and dst IP and other useful information for further analysis.

LogTime	Computer	Category	ld	Observed Stage	Observation Direction	Kill Chain Stage	Severity	Organization Name	Protocol	Source IP
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.100.13- SYSLOG	MaliciousHost	0000015477ea0f8cb2d9e10f0fa5a b8ad92dd8670009	Realtime	None	Cnc	45	null	Тср	127.0.0.1
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.100.13- SYSLOG	MaliciousHost	0000015477ea0f8cb2d9e10f0fa5a b8ad92dd8670009	Realtime	None	Cnc	45	null	Тср	127.0.0.1
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.100.13- SYSLOG	MaliciousHost	0000015477ea0f8cb2d9e10f0fa5a b8ad92dd8670009	Realtime	None	Cnc	45	null	Тср	127.0.0.1



dest_ip_address	+- 127.0.0.2
dest_port_no	+- 53
enc_type	+- d56903015ed98278e6a8c83514e90fc1eac70203
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+- 1598244010
event_description	Aug 24 10:10:10 172.27.100.13 Aug 05 14:27:46 192.168.1.86 2020-08-05T14:27:57.476-06:00 160901-onsite-nts-01 protectwise-emitter[17790]; [certRep]
	sensorName:DMZ category:MaliciousHost id:0000015477ea0f8cb2d9e10f0fa5ab8ad92dd8670009 observedAt:2016-05-03T12:38:30.896-06:00 isoObserve
	dAtUTC:2016-05-03T18:38:30.896Z occurredAt:1462300708948 occurredAt:2016-05-03T12:38:28.948-06:00 isoOccurredAtUTC:2016-05-03T18:38:28.948Z
	observedStage:Realtime observationDirection:None killChainStage:Cnc severity:45 threatLevel:Low threatScore:33 threatSubCategory: <no value=""> type:<n< td=""></n<></no>
	o value> dstlp:127.0.0.2 srclp:127.0.0.1 srcPort:9001 dstPort:53 proto:Tcp layer3Proto:IPv4 layer4Proto:Tcp nfkey:-UNKWNTOK- nfStartedAt:146230070874
	8 isoNfStartedAt:2016-05-03T12:38:28.748-06:00 isoNfStartedAtUTC:2016-05-03T18:38:28.748Z signingChain:[{alternateNames:null,commonName:www.rr
	ob74a635taf.net,data:308201c33082012ca003020102020900f31f3d18caae9f4f300d06092a864886f70d010105050030273125302306035504030c1c777777
	2e6167353632766d70716e627a37376c78676d726b2e636f6d301e170d3135313232333030303030305a170d31363130323630303030305a3020311e301
	c06035504030c157777772e72726f623734613633357461662e6e657430819f300d06092a864886f70d010101050003818d0030818902818100936244e022b
	91bfa5cb1295e75e866013abd96014f9829d3e278455f0eff657fc851f3ef2598893cfbd1390ea1e1074c874ccb32f50f3efaed3f460fbc9e6a77b6c0cc369858774
	3686bff1610a5e64886f16e023bc64ba76115e14a3c18779b3e0f8cc075ac04e7c695a4574a9abfe1f0aa6fc85448d3ccc3d796042dfa60710203010001300d060
	92a864886f70d01010505000381810056c6662fb2615d5c8e1d49949b19d0e2c72d558abe42ea57e00ca9e90710897df53dda74479c3595a2c7320f752f2e50
	8e387b7ee6f16c61edd83348ecc0bd48dabab63e7d4f36d7fef94d0c86379077776394ceba13b9f94c46a8ecf421e08d3e81f0922c301b67474a592decfcdd241
	34b609d6ab870dba8c97b16c7321dfe, isComplete: true, issuer: www.ag562vmpqnbz771xgmrk.com, md5:712c1b5f4e857aa07da7605c296d2646, organization
	Name:null,serialNumber:00f31f3d18caae9f4f,sha1:d56903015ed98278e6a8c83514e90fc1eac70203,validNotAfter:1.477440000000e+12,validNotBefore:1.4
	50828800000e+13}]
event_group_name	+- Default
event_id	+- 128
avant las tima	to Application

Figure 10

• **ProtectWise: Payload** - This report gives threat data about Payload. Report contains threat category, level, score, src and dst IP and other useful information for further analysis.

LogTime	Computer	Description	Category	Classification	Destination Ip	Destination Port	Kill Chain Stage	Layer 3 Protocol	Layer 4 Protocol	Observation Direction	Observed Sta
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Delivery Test Observation signatureld:68114152	Malware	trojan-activity	127.0.0.2	53	Delivery	IPv4	Udp	None	Realtime
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Delivery Test Observation signatureld:68114152	Malware	trojan-activity	127.0.0.2	53	Delivery	IPv4	Udp	None	Realtime
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Delivery Test Observation signatureld:68114152	Malware	trojan-activity	127.0.0.2	53	Delivery	IPv4	Udp	None	Realtime



addl_into	+ - Kealtime
addl_info8	+UNKWNTOK-
body_text	+- Delivery Test Observation
category	+- trojan-activity
dest_ip_address	+- 127.0.0.2
dest_port_no	+- 53
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+- 1598244010
event_description	Aug 24 10:10:10 172:27.100.13 Aug 05 14:27:46 192.168.1.86 2020-08-05T14:27:57.478-06:00 160901-onsite-nts-01 protectwise-emitter[17790]: [payload]
	sensorName:DMZ category:Malware id:000001546bf7cbacd11a4a02d688790b9241defb0000 observedAt:2016-05-03T12:33:05.420-06:00 isoObservedAtU
	TC:2016-05-03T18:33:05.420Z occurredAt:1462100282284 occurredAt:2016-05-01T04:58:02.284-06:00 isoOccurredAtUTC:2016-05-01T10:58:02.284Z obse
	rvedStage:Realtime observationDirection:None killChainStage:Delivery severity:50 threatLevel:Medium threatScore:50 threatSubCategory: < no value > typ
	e: <no value=""> dstlp:127.0.0.2 srclp:127.0.0.1 srcPort:41424 dstPort:53 proto:UDP layer3Proto:IPv4 layer4Proto:Udp nfkey:-UNKWNTOK- nfStartedAt:146210</no>
	0282284 isoNfStartedAt:2016-05-01T04:58:02.284-06:00 isoNfStartedAtUTC:2016-05-01T10:58:02.284Z classification:trojan-activity description:Delivery Te
	st Observation signatureld:68114152
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
group_name	+- Delivery

Figure 12

• **ProtectWise: All Events Detected-** This report gives information about resources that describe a threat and contains a collection of observations. Report contains threat category, level, score, src and dst IP and other useful information for further analysis.

LogTime	Computer	Destination Ip	Destination Port	Kill Chain Stage	Observed Stage	Protocol	Source IP
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	127.0.0.2	53	Test	Realtime	UDP	127.0.0.1
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xxxx- SYSLOG	127.0.0.2	53	Test	Realtime	UDP	127.0.0.1
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx-SYS	LOG 127.0.0.2	53	Test	Realtime	UDP	127.0.0.1



addl_info	+- Realtime
addl_info4	+- https://visualizer.protectwise.com/#killbox/events?id=00052a944d03db101a620b73a7ad0fe17bd2192ced7ff364cb489b84
dest_ip_address	+- 127.0.0.2
dest_port_no	+- 53
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+- 1598244010
event_description	Aug 24 10:10:10 172.27.100.13 Aug 05 14:27:46 192.168.1.86 2020-08-05T14:27:57.474-06:00 160901-onsite-nts-01 protectwise-emitter[17790]: [event] se
	nsorName;-UNKWNTOK- message:Test Event threat_level:None start_time:2016-02-03T12:29:01.918-07:00 end_time:2016-02-03T12:29:01.918-07:00 srcl
	p:127.0.0.1 dstlp:127.0.0.2 srcPort:57369 dstPort:53 visualizerLink:https://visualizer.protectwise.com/#killbox/events?id=00052a944d03db101a620b73a7ad
	0fe17bd2192ced7ff364cb489b84 category:Test Category endedAt:1454527741918 isoEndedAt:2016-02-03T12:29:01.918-07:00 isoEndedAtUTC:2016-02-0
	3T19:29:01.918Z message:Test Event id:00052a944d03db101a620b73a7ad0fe17bd2192ced7ff364cb489b84 observedStage:Realtime observedAt:14545277
	53860 isoObservedAt:2016-02-03T12:29:13.860-07:00 isoObservedAtUTC:2016-02-03T19:29:13.860Z killChainStage:Test KillChainStage startedAt:1454527
	741918 isoStartedAt:2016-02-03T12:29:01.918-07:00 isoStartedAtUTC:2016-02-03T19:29:01.918Z threatLevel:None threatScore:50 type:Test Type threatSu
	bCategory: <no value=""> visualizerLink:https://visualizer.protectwise.com/#killbox/events?id=00052a944d03db101a620b73a7ad0fe17bd2192ced7ff364cb48</no>
	9b84 dstlp:127.0.0.2 srclp:127.0.0.1 srcPort:57369 dstPort:53 proto:UDP layer3Proto:IPv4
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
group_name	+- Test KillChainStage
interface_in	+UNKWNTOK-

Figure 14

• **ProtectWise: Heuristics** – This report gives information about threat methods and tactics. Report contains threat category, score, src and dest IP, kill chain stage and other information for further analysis.

LogTime	Computer	Category		Observed Stage	Observation Direction	Kill Chain Stage	Severity	Protocol	Source IP	Source Port	Threat Level	Threat Score
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Suspicious	0000015e2e94f852cf8f14bb13edd 636ffb8a7c0000b	Realtime	None	Cnc	75	TCP	17.207.21.1	57200	Medium	38
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Suspicious	0000015e2e94f852cf8f14bb13edd 636ffb8a7c0000b	Realtime	None	Cnc	75	TCP	17.207.21.1	57200	Medium	58
08/24/2020 10:10:10 AM	R1S5-VM30\172.27.xx.xx- SYSLOG	Suspicious	0000015e2e94f852cf8f14bb13edd 636ffb8a7c0000b	Realtime	None	Cnc	75	ТСР	17.207.21.1	57200	Medium	58



addl_info	+- Realtime
addl_info8	+UNKWNTOK-
body_text	+ UNKWNTOK-
category	+UNKWNTOK-
dest_ip_address	+- 192.168.3.21
dest_port_no	+- 666
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 8/24/2020 10:10:10 AM
event_datetime_utc	+- 1598244010
event_description	Aug 24 10:10:10 172.27.100.13 Aug 05 14:27:46 192.168.1.86 2020-08-05T14:27:57.483-06:00 160901-onsite-nts-01 protectwise-emitter[17790]: [heuristic
	s] sensorName:DMZ category:Suspicious id:0000015e2e94f852cf8f14bb13edd636ffb8a7c0000b observedAt:2017-08-29T09:22:12.160-06:00 isoObserved
	AtUTC:2017-08-29T15:22:12.160Z occurredAt:1504020068434 occurredAt:2017-08-29T09:21:08.434-06:00 isoOccurredAtUTC:2017-08-29T15:21:08.434Z o
	bservedStage:Realtime observationDirection:None killChainStage:Cnc severity:75 threatLevel:Medium threatScore:38 threatSubCategory: < no value > type:
	<no value=""> dstlp:192.168.3.21 srclp:17.207.21.1 srcPort:57200 dstPort:666 proto:TCP layer3Proto:IPv4 layer4Proto:Tcp nfkey:-UNKWNTOK- nfStartedAt:15</no>
	04020068434 isoNfStartedAt:2017-08-29T09:21:08.434-06:00 isoNfStartedAtUTC:2017-08-29T15:21:08.434Z classification:-UNKWNTOK- description:-UNK
	WNTOK- signatureld:-UNKWNTOK-
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
avant fina	the Error



4.4 Dashboards

ProtectWise: Threat Detected by Threat Level







ProtectWise: Threat Score

Figure 18



ProtectWise: Severity Score

Figure 19

ProtectWise: Web Traffic by Protocol



Figure 20

ProtectWise: Top Destination IP



Figure 21



ProtectWise: Threat Detected by Source IP



Figure 22

ProtectWise: Top File Type Detected by Source IP



Figure 23



ProtectWise: Killchain Stage Detected



5. Importing ProtectWise knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Report
- Dashboard
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.



Figure 25

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then click the browse button.

<u>Ф</u>	Export Import Utility	- 🗆	x
Export Import			
1. Provide the path and file nam 2. Click the Import button.	e of the Categories file. Use the '' button to browse and locate the import file.		
Options	Location		
 Category 			
◯ Filters			
⊖ Alerts			
 Systems and Groups 	Source :		
O Token Value			
O Reports			
O Behavior Correlation			
	Import	Close	•

Figure 26



- 2. Locate Category_ProtectWise.iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays success message.



Figure 27

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

5.2 Alert

1. Click **Alert** option, and then click the **browse** — button.

9	Export In	nport Utility		_		x
Export Import						
Export Import 1. Provide the path and file name 2. Click the Import button. Options Category Filters Image: Alerts Systems and Groups Token Value Reports Behavior Correlation	e of the Alerts file. Use the '' butto Location	This setting is applicable only for im Alert files. For v7, the active status to "Active" key available in the config on or alerts which have Advanced watch is are imported.	oorts from Legac; will be set based uration section. list configured. t groups are avai	γ (v6x) on ilable		
			L		-	
			Import		Clos	e

Figure 28



- 2. Locate Alert_ProtectWise.isalt file, and then click the Open button.
- To import alerts, click the Import button.
 EventTracker displays success message.





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

5.3 Knowledge Object

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

Event Tracker ⊕					🐥 🛛 Admin-	Tools -
Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
	_	Alerts	C Correlation	🔍 IP Lookup Configuration	Q Users	_
0	1	Behavior Correlation Rules	A Diagnostics	·@ Knowledge Objects	reights 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 			
	EventTracker Home O Potential Cyber Breaches Unsafe connections or processes, new TCP entry point Attacker	EventTracker Home O O Potential Cyber Breaches Unsale connections or processes, new TCP entry point USB activities, New sen Attacker	EventTracker#	EventTracker⊕ Home Image: Active Watch Lists Image: Collection Master 0 A lerts Image: Collection Master 0 Image: Debavior Correlation Rules Diagnostics Potential Cyber Breaches Indicators of CC Image: Debavior Correlation Settings Event Filters Indicators of CC Image: Debavior Correlation Settings Event Filters Attacker Image: Collection Master Image: Collection Master	EventTracker: Home Image: Active Watch Lists Collection Master Image: Group Management Image: Active Watch Lists Image: Collection Master Image: Group Management Image: Active Watch Lists Image: Collection Master Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch Lists Image: Group Management Image: Group Management Image: Active Watch	EventTracker: Mome Collection Master Group Management Systems Alerts Correlation Potential Cyber Breaches Unsafe connections or processes, new TCP entry point Potential Cyber Breaches Indicators of Course and the sector of correlation Settings Event Filters Manager Windows Agent Config Windows Agent Configuration Attacker Face goay FAce Configuration Report Settings Attacker News



2. Click on **Import** I button as highlighted in the below image:

-	Knowledge Ob	jects		👚 / Admin / Knowledge	Objects
Q R	Search objects	Q	Activate Now	Objects 🕀 📳	1¢
	Groups	+ 🖉 iii			±
	Cylance				
	EventTracker				

Figure 31

3. Click on Browse.



Import		×
Select file	🚰 Browse Upload	
		Close



- 4. Locate the file named **KO_ProtectWise.etko**.
- 5. Now select the check box and then click on \blacksquare Import option.

Import			×
Select	file		🖀 Browse Upload
	Object name	Applies to	Group name
	ProtectWise	ProtectWise	ProtectWise
			Import Close

Figure 33





6. Knowledge objects are now imported successfully.



5.4 Report

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

4	Export Import Utility	- 🗆 X
Export Import 1. Provide the path and file nam 2. Click the Import button Note : If report(s) contains templ Options Category Filters Alerts Systems and Groups Token Value Image: Reports Behavior Correlation	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 C Legacy (*.issch) New (*.etcx) Source : *.issch	
	Import	Close



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





ilat	le repo	ints				
le			Frequency Show all	- Q Q		
2		Title	Sites	Groups	Systems	Frequency
2	EDIT	ProtectWise - Certificate Reputation	R1S5-VM30			Undefined
2	EDIT	ProtectWise - Dns Reputation	R1S5-VM30			Undefined
2	EDIT	ProtectWise - Events	R1S5-VM30			Undefined
2	EDIT	ProtectWise - File Reputation	R1S5-VM30			Undefined
2	EDIT	ProtectWise - IP Reputation	R1S5-VM30			Undefined
\square	EDIT	ProtectWise - Payload	R1S5-VM30			Undefined
\sim	EDIT	ProtectWise - Url Reputation	R1S5-VM30			Undefined
2	EDIT	ProtectWise- Heuristics	R1S5-VM30			Undefined
ļ						3
Note	: Set ru	un time option is not applicable for Define	d Reports and Hourly Reports			>
Note	: Set nu	In time option is not applicable for Define	d Reports and Hourly Reports			
Note Set Rep	: Set ru run tir lace	In time option is not applicable for Define ne for report (s) from to	d Reports and Hourly Reports AM • at interval of minute	s Set ①		Activate

Figure 36

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

Export Import Utility	x
Selected reports configurations are imported successfully	
ОК	



5.5 Dashboards

NOTE- Below steps given 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 USB activities, New services or software install	
	Behavior Correlation		
	Change Audit		_
	Compliance	The second s	



- 2. Navigate to My Dashboard option as shown above.
- 3. Click on the **Import** $\overline{\bullet}$ button as show below.

Event Tracker ⊕	Ņ	Admin -	Tools -	💽 ETAdmin 🔹
My Dashboard		A	/ Dashboar	d / My Dashboard
		(+)	o 🖉 🎯 🗳	1 3 0



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

		🗁 Browse	Uploa
Available widgets			
Select All			
ProtectWise: Threat Score	ProtectWise: Threat Detec		
ProtectWise: Severity Sco	ProtectWise: Top Protocol		
ProtectWise: Top Destinat	ProtectWise: Threat Detec		



6. Import is now completed successfully.





Figure 41

7. In **My Dashboard** page select ⊕ to add dashboard.



Figure 42

8. Choose appropriate name for **Title** and **Description**. Click **Save**.

ProtectWise			
Protectivise			
escription			
ProtectWise			
	Samo	Delete	Cancel



9. In **My Dashboard** page select (a) to add dashlets.

My Dashboa	ard		👚 / Dashboard / My Dashboar					
			+ 0 0 × 1 I 0					
CheckPoint	Trend Micr	Microsoft	_					
Figure 44								

10. Select imported dashlets and click Add.





ProtectWi			(a,
ProtectWise: Severity Score	ProtectWise: Threat Detected b	ProtectWise: Threat Detected b	ProtectWise: Threat Score	
ProtectWise: Top Destination IP	ProtectWise: Top Protocols			
			Add Delete	Clos

Figure 45

Verifying ProtectWise knowledge pack in EventTracker

6.1 Category

- 1. Logon to 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	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	The Weights	
2			🇞 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	P Eventvault	🧭 Parsing Rules		
		_	Gategory Category Category	FAQ Configuration	Report Settings		
	Attacker			- News			

Figure 46

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

	linux
	Microsoft DHCP Server
	MSSQL Audit
	NIST 800-171
	PCI DSS
	ProtectWise
	ProtectWise: Certificate Reputation
-	ProtectWise: Dns Reputation
-	ProtectWise: Events
	ProtectWise: File Reputation
	ProtectWise: Heuristics
	ProtectWise: Ip Reputation
-	ProtectWise: Payload
	ProtectWise: Url Reputation



6.2 Alert

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.

≡	Event Tracker ⊕					🔎 🗚 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	🖳 Group Management	Systems	🕈 / Dasht
Q		_	Alerts	Correlation	Q IP Lookup Configuration	였 Users	
	0	2	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	T 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 48

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

Alert Name 🔨	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Ren
ිරි ProtectWise: Threat Detected						



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

EventTracker displays message box.

Successfully saved	configuration. eating additional dialogs
	ОК



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 ⊕						Tools -
	Home	Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb	
a		Alerts	Correlation	Q IP Lookup Configuration	였 Users		
R	0 1 Potential Cyber Breaches Unsafe connections or processes, new TCP entry point UsS activities. New see	1	Behavior Correlation Rules	Diagnostics	· 💮 Knowledge Objects	🕀 Weights	
			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
		Casebook Configuration	Eventvault	🧭 Parsing Rules			
			o- Category	FAQ Configuration	Report Settings		
	Attacker			- News			



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





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 **ProtectWise** group folder to view the imported reports.

Rep	orts confi	guration: ProtectWise					
Ð							
		Title					
	2.23	ProtectWise- Heuristics					
	2003	ProtectWise - Certificate Reputation					
	223	ProtectWise - Events					
	£33	ProtectWise - File Reputation					
	13	ProtectWise - Payload					
	13	ProtectWise - Url Reputation					
	1	ProtectWise - Dns Reputation					
	1	ProtectWise - IP Reputation					

Figure 54

6.5 Dashboards

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





Figure 55

2. In the "ProtectWise" dashboard you should be now able to see something like this.





