



How-To Guide

# **Configure Detection Rule in the Netsurion Open XDR platform**

**Publication Date:** 

March 30, 2023



# Abstract

The purpose of this document is to aid the Netsurion Open XDR platform administrators to configure and utilize the Detection Rules feature introduced in the version 9.4.

## Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

# Audience

This guide is for all the Netsurion Open XDR platform users who adapts to the Netsurion Open XDR platform version 9.4.

# **Product Terminology**

The following are the terms used throughout this guide:

- The term "Netsurion's Open XDR platform" or "the Netsurion Open XDR platform" or "the Open XDR platform" refers to EventTracker.
- The term "Data Source Integrations" refers to Knowledge Packs.
- The term "Sensor" refers to Agent.



# Table Of Contents

1	Det	ection Rules	4
	1.1	Modifying the Alert for the Built-in Rules	6
	1.2	Configuring a New Rule	7
	1.3	Cloning a Built-in or a User-defined template	13
	1.4	Importing a Rule Configuration	15
	1.5	Exporting a Rule Configuration	17



# 1 Detection Rules

The Detection Rules feature facilitates configuring rules for the attack pattern or technique detected from the MITRE ATT&CK framework, which triggers "tip-off" alerts based on certain criteria when the set threshold is exceeded. This reduces the false positives to a greater extend and eases to notify the users directly to the end point where the attack occurred. This feature also supports detection rules based on EventTracker index.

In the **Open XDR platform**, hover over the **Admin** menu and click **Detection Rules** to view all the configured detection rules.

### **IMPORTANT:**

The Detection Rules feature is accessible only when the MITRE ATT&CK feature license is available on the console.

≡	Netsurion.		🐥 Admin <del>v</del>	Tools 🗸 🌔 🗸
	Hoi 🔚 Active Watch Lists	Eventvault	Manager	🔶 / Dashboard / Home
Q	Alerts	FAQ Tile Configuration	MITRE ATT&CK Rules	
	Casebook Configuration	Group Management	🧭 Parsing Rules	
<u>~</u>	Category	🔍 IP Lookup Configuration	🔊 Report Settings	
	Po Un Collection Master	Knowledge Objects	Systems	
	Detection Rules	M Machine Learning Jobs	💭 Users	
	Diagnos Configuration of Det	ection rules hine Learning Settings	H Weights	Solution brief document
	Event Filters	🄎 Manage API keys		v3.2 Solution brief document
	Potential Insider Threats	Bo	okmarks	

There are certain rules available by default (termed as Built-in rules) and each built-in rule can potentially trigger an alert with the details of the various attacks and techniques. The triggering threshold set varies based on the type of attack detections configured for each rule. The Netsurion Open XDR platform's administrator can also include additional custom rules (termed as user-defined rules) as per the requirement.

Rule Name	Active	Added On	
APT 1		Mar 22 06:40:04 AM	Ø
APT 28		Mar 22 06:40:04 AM	Ø
APT 29		Mar 22 06:40:04 AM	Ø
APT 33		Mar 22 06:40:05 AM	Ø
APT 37		Mar 22 06:40:05 AM	Ø
APT 38		Mar 22 06:40:05 AM	Ø
APT 41		Mar 22 06:40:05 AM	Ø
Microsoft 365 - Brute force		Mar 22 06:40:05 AM	Ø
Microsoft 365 - Password spraying		Mar 22 06:40:05 AM	Ø
Windows - Brute force		Mar 22 06:40:05 AM	Ø
Windows - Password spraying		Mar 22 06:40:05 AM	Ø
Hafnium		Mar 22 06:40:05 AM	Ø
Large number of ATT&CK techniques detected in a system		Mar 22 06:40:05 AM	Ø
Large number of ATT&CK techniques detected in the environment		Mar 22 06:40:05 AM	Ø
Multiple distinct ATT&CK techniques detected in a system		Mar 22 06:40:05 AM	Ø
Multiple distinct ATT&CK techniques detected in the environment		Mar 22 06:40:05 AM	Ø
Wizard Spider		Mar 22 06:40:05 AM	Ø



## Note:

The built-in rules include 13 MITRE ATT&CK index-based detection rules and 4 EventTracker index-based detection rules.

## Note:

The Rule configuration for the built-in rules cannot be modified. The Netsurion Open XDR Administrator can 'Deactivate' a specific rule if needed to avoid any alert for that specific rule.

# **UI** Conventions

÷	Click to add a new Rule configuration
	Select the required Rule name from the list and click to delete the existing Rule configuration from the list.
	Click to import a Rule configuration to the system.
Ŧ	<b>Note:</b> Refer <u>Importing a Rule Configuration</u> section for more details.
	Select the required Rule name from the list and click to export a Rule configuration.
1	<b>Note:</b> Refer <u>Exporting a Rule Configuration</u> section for more details.
< 1 of 1 >	Click < or > to navigate to the Back or the Front page in the Detection Rule interface.
< 1 of 1 > G0	Click <sup>GO</sup> to go to the specified page.
Search	Use the search field to search for a specific Detection Rule name
Activate Now	Click Activate Now to activate all the latest modifications



# 1.1 Modifying the Alert for the Built-in Rules

The Rule configuration for the Built-in rules cannot be modified but, the administrator can decide to trigger or stop the alert for the Built-in rules.

## Note:

By default, the alerts for the Built-in rules will be triggered.

1. In the **Detection Rules** interface, click the **Edit** button of the Built-in rule for which you require to trigger or stop the alert.

lets	surion.		🔎 Admin <del>v</del> Tools <del>v</del> 🕕
etecti	on Rules		🔒 / Admin / Detection Rule
+ i	1 of 1 > CO Activate Now Click 'Activate	Now' after making all changes	Search Q Q Total: 20 Page Size 20 V
	Rule Name	Active Added On	
	APT 1	Mar 22 06:40:04 AM	Ø
	APT 28	Mar 22 06:40:04 AM	Ø
	APT 29	Mar 22 06:40:04 AM	Ø
	APT 33	Mar 22 06:40:05 AM	Ø
	APT 37	Mar 22 06:40:05 AM	Ø
	APT 38	Mar 22 06:40:05 AM	Ø
	APT 41	Mar 22 06:40:05 AM	Ø
	Microsoft 365 - Brute force	Mar 22 06:40:05 AM	Ø
	Microsoft 365 - Password spraying	Mar 22 06:40:05 AM	Ø
	Windows - Brute force	Mar 22 06:40:05 AM	Ø
	Windows - Password spraying	Mar 22 06:40:05 AM	Ø
	Hafnium	Mar 22 06:40:05 AM	Ø
	Large number of ATT&CK techniques detected in a system	Mar 22 06:40:05 AM	Ø
	Large number of ATT&CK techniques detected in the environment	Mar 22 06:40:05 AM	Ø
	Multiple distinct ATT&CK techniques detected in a system	Mar 22 06:40:05 AM	Ø
	Multiple distinct ATT&CK techniques detected in the environment	Mar 22 06:40:05 AM	Ø
	Wizard Spider	Mar 22 06:40:05 AM	Ø

2. The Rule configuration details for the selected Built-in rule will be displayed. Select or clear the selection of the **Generate Alert** check box to trigger or stop the alert for that particular Built-in rule.

### Note:

You cannot edit any of the Rule Configurations for the Built-in Rules.

Rule configuration       Rule name       APT 1       DSL query     Event template	Frequency ① 45 Minutes	Description This rule detects APT 1 activity by monitoring tec	★ / Admin / Detection Rules / Rule Configuration
Source index MITRE ATT&CK	Computer ① \$aggregations.Event_group.buckets[*]C	Computer buckets[*] key	
1 { 2 "query"; { 3 "bool"; { 4 "filter"; [ 5 { 6 "bool"; {			ĺ



**3.** After taking the necessary action, click **Save** to update the alert configuration for the selected Built-in rule.

Note:

The event type will be set to WARNING for the triggered event.

# 1.2 Configuring a New Rule

Perform the following procedure to configure a new Rule.

1. In the Detection Rules interface, click the Add Rule 🕀 button to configure a new rule.

In the **Rule Configuration** interface, provide the following details to configure the new rule.

e configuration			🕈 / Admin / Detection Rules / Rule Configura
Rule name	Frequency ① 15 Minutes	Description	Generate Alert 🛈
DSL query Event template			
Source index	Computer 🛈		
MITRE ATT&CK			
	L		
DSL query 🛈			
1			
2			
3			
5			
6			
7			
8			
10			
11			
12			
13			
14			
16			
47			
		Format JSON Validate	

- 2. In the **Rule name** field, provide a name for the new Rule Configuration.
- **3.** In the **Frequency** drop-down list, select the recurrence time to execute the Rule according to the selected frequency.
- 4. In the **Description** field, specify the details of the new rule configuration.



5. Select the Generate Alert check box to generate an alert for the new Rule configuration.

Note:

If the **Generate Alert** check box is selected, then, the alert will be triggered upon satisfying the configured rule. But, if the **Generate Alert** check box is not selected, then the alert will not be triggered.

Note:

If the Generate Alert check box is selected, then, the alert will be triggered as EventTracker: Detection rule triggered.

- 6. In the Rules Configuration interface, click the DSL query tab to define the search query.
  - Source Index: Select either MITRE ATT&CK or EventTracker (Elasticsearch) source from the drop-down list to validate and obtain the data.

DSL query	Event template			
Source ind EventTra MITRE A EventTra	ex cker K TT&CK cker	Computer ①		
1 2 3 4 5 6				
9 10 11 12 13				
14 15 16			Format JSON	<i>V</i> alidate

- Computer: Specify the node path in JSON response using the JSON path syntax, from which the computer name will be extracted and utilized for event generation.
- DSL query: Provide the Bucket aggregation DSL to query and aggregate data based on the selected index and click Format JSON to rectify the DSL query in JSON FORMAT.

#### Note:

It is necessary to specify the search area in terms of UTC timeticks, aggregation standards, and the aggregated systems.

Click Format JSON to rectify the query in JSON format, and after updating the query click
 Validate to verify the DSL query.



- **7.** In the **Rules Configuration** interface, click the **Event template** tab to define the template format for the alert.
  - Template type: Select either Existing template to use the available template format or New template to create the template format from the drop-down list.

### Image Representation for the Existing template

emplate type	Template name	
Evisting tomplate	ADT Detection	
Existing template		
Select template type		
Existing template		
New template	].Computer.buckets[*].key}} on	
{{\$.aggregations.Event_group.b	vuckets[*].Computer.buckets[*].TopOccurrence.hits.hits[*]source.FirstOccurrence}}	
Details:		
Technique Id: {{\$.aggregations.	Event_group.buckets[*].Computer.buckets[*].Techniqueld.buckets[*].key}}	
Technique: {{\$.aggregations.Eve	ent_group.buckets[*].Computer.buckets[*].Techniqueld.buckets[*].TechniqueName.buckets[*].key}}	
	aations.Event_group.buckets[*].Computer.buckets[*].Techniqueld.buckets[*].Title.buckets[*].kev}	
MITRE Rule detected: {{\$.aggre		
MITRE Rule detected: {{\$.aggre	egations.Event_group.buckets[*].Computer.buckets[*].TopOccurrence.hits.hits[*], source.FirstOccurrence}}	
MITRE Rule detected: {{\$.aggre Detection found from: {{\$.aggre Detection found to: {{\$.aggregation	egations.Event_group.buckets[*].Computer.buckets[*].TopOccurrence.hits.hits[*]_source.FirstOccurrence}} ations.Event_group.buckets[*].Computer.buckets[*].RottomOccurrence.hits.hits[*]_source.LastOccurrence}}	
MITRE Rule detected: {{\$.aggre Detection found from: {{\$.aggre Detection found to: {{\$.aggreg	egations.Event_group.buckets[*].Computer.buckets[*].TopOccurrence.hits.hits[*]source.FirstOccurrence}} ations.Event_group.buckets[*].Computer.buckets[*].BottomOccurrence.hits.hits[*]source.LastOccurrence}}	
MITRE Rule detected: {{\$.aggre Detection found from: {{\$.aggre Detection found to: {{\$.aggregation: System group: {{\$.aggregation:	egations.Event_group.buckets[*].Computer.buckets[*].TopOccurrence.hits.hits[*]source.FirstOccurrence}} ations.Event_group.buckets[*].Computer.buckets[*].BottomOccurrence.hits.hits[*]source.LastOccurrence}} s.Event_group.buckets[*].key}}	

If selecting Existing template, you can select either the built-in templates (APT
Detection, or Brute force, or Password spraying, or Environment Detection, or
Environment system detection) or the User-defined templates from the drop-
down list that formats event description obtained through JSON result of DSL
query.

Existing<br/>templateNote:You cannot edit the built-in templates but, you can clone a built-in template to a<br/>New template. Refer Cloning a Built-in or a User-defined template<br/>section for<br/>more details.Note:Note:You can edit the existing User-defined template. Modifying the existing User-<br/>defined template will impact all the rules using that template. Use the Clone<br/>action if you do not require to reverse the existing User-defined template.



# Image Representation for the New template

DSL query Event tem	plate
Template type New template	▼ Template name
Template	
Note: The template shown JSON result of DSL query.	n above is used to form event description obtained through Preview
	If selecting <b>New template</b> , then provide the template name and create a new template format.
New template	Note:
	If no rules are associated to a template, then that template will be deleted.



Click Preview to view the DSL query result and the Extracted event description based on DSL query result.

## DSL query result:

ew ×	:
query result Extracted event description	
<pre>took':3, toned_out':file. _shard':{ total':8, "siccessful":8, "skipped':0, "failed':0 hits':{</pre>	
"key": "testdata_detectionhalfnium",	•

## **Extracted event description:**

DSL query result	Extracted event description	
Detection rule tria	oered	
Detection rule nan	ne: TEST_RULE-2	
Index: MITRE ATT8 Potential Advanced correspond to Syst	kCK d Persistent Threats (APT) have be tem Network Configuration Disco	n detected on the infrastructure. The technique IDs detected are T1016; T1018; T1059; T1087; T1547; T1548 which ery; Remote System Discovery; Command and Scripting Interpreter; Account Discovery; Boot or Logon Autostart
Execution; Abuse t	evation Control Mechanism on t	e system firmtech-wrksp
Details:		
Technique Id: T101	6; T1018; T1059; T1087; T1547; T	548
Technique: System	Network Configuration Discover	Remote System Discovery; Command and Scripting Interpreter; Account Discovery; Boot or Logon Autostart Execution;
Abuse Elevation C	ontrol Mechanism	
MITRE Rule detect	ed: Network configuration discov	y using default windows tools; Listing of other systems by IP address, hostname, other logical identifiers on a network;
Abuse command a	and script interpreters to execute	immands, scripts, or binaries; Listing of accounts on a system or within an environment; Registry Run Reys / Startup
Polder; bypass use	ami 2/27/2022 5:29:22 AM	
Detection found to	011: 5/27/2023 5:20:22 AM	
Detection loand to	ntech	
System aroun: firm	The best of	



8. After providing all the details, click **Save** to save the newly created Rule configuration.

inducto Obe	Template name
Existing template $\checkmark$	Brute force 🗸
emplate	
Potential brute force attack was dete ([\$-aggregations.Computer.buckets]* [\$-aggregations.Computer.buckets]* Details: Target username: ([\$-aggregations.Coc Source IP address: ([\$-aggregations.Coc Jogin failure count: ([\$-aggregations. Login success count: ([\$-aggregations. Detection found from: ([\$-aggregations.Coc Detection found to: ([\$-aggregations.Coc Starget computer: ([\$-aggregations.Coc	<pre>ted for the user(s) ([5.aggregations.Computer.buckets[*].UserName.buckets[*].FirstLoginAttempt.hits.hits[*]_source.event_datetime]) UserName.buckets[*].UserName.buckets[*].key}) betweent ([\$.aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]_source.event_datetime]) uputer.buckets[*].UserName.buckets[*].LeginFailed Log_Count.value]) Computer.buckets[*].UserName.buckets[*].LoginFailed Log_Count.value]) computer.buckets[*].UserName.buckets[*].LoginFailed Log_Count.value]) computer.buckets[*].UserName.buckets[*].LoginFailed Log_Count.value]) computer.buckets[*].LiserName.buckets[*].LoginFailed Log_Count.value]) computer.buckets[*].LiserName.buckets[*].LoginFailed Log_Count.value]) s.Computer.buckets[*].LiserName.buckets[*].source.event_datetime]) 'omputer.buckets[*].LiserName.buckets[*].source.event_datetime]) puter.buckets[*].LiserName.buckets[*].source.event_datetime]) computer.buckets[*].LiserName.buckets[*].source.event_datetime]) puter.buckets[*].LiserName.buckets[*].source.event_datetime]) </pre>

**9.** Then, go to the **Detection Rules** interface, click **Activate Now** to activate the newly added Detection Rule.

Detection Rules         Image: Class Activate Now after making all changes         Search         Image: Class Activate Now after making all changes           Image: Class Activate Now after making all changes         Total AC         Total AC <t< th=""><th>Netsu</th><th>rion.</th><th></th><th></th><th>🔎 Admin + Tools + 🌔 🖛 +</th></t<>	Netsu	rion.			🔎 Admin + Tools + 🌔 🖛 +
Image: Sector       Sector.       Image: Sector	Detection	Rules			🛧 / Admin / Detection Rules
Rule NameActiveAdded OnAPT 1CMar 22 064004 AMCAPT 28CMar 22 064004 AMCAPT 28CMar 22 064004 AMCAPT 29CMar 22 064004 AMCAPT 29CMar 22 064005 AMCAPT 37CMar 22 064005 AMCAPT 38CMar 22 064005 AMCMicrosoft 365 - Brune forceCMar 22 064005 AMCMicrosoft 365 - Brune fortigrapingCMar 22 064005 AMCMicrosoft 365 - Brune	(+) (1)	of 2     GO   Click 'Activate Now' after making all changes			Search Q Q Total: 22 Page Size 20 V
APT 1       I       Mar 22 064/024 AM       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Rule Name	Active	Added On	
APT 28       Image 20 64004 AM       Image 20 64004 AM         APT 29       Image 20 64005 AM       Image		APT 1	2	Mar 22 06:40:04 AM	Ø
APT 29       Image 20 64004 AM       Image 20 64005 AM         APT 33       Image 20 64005 AM       Image 20 64005 AM         APT 37       Image 20 64005 AM       Image 20 64005 AM         APT 38       Image 20 64005 AM       Image 20 64005 AM         APT 38       Image 20 64005 AM       Image 20 64005 AM         APT 41       Image 20 64005 AM       Image 20 64005 AM         Microsoft 365 - Brute force       Image 20 64005 AM       Image 20 64005 AM         Microsoft 365 - Brute force       Image 20 64005 AM       Image 20 64005 AM         Windows - Brute force       Image 20 64005 AM       Image 20 64005 AM         Windows - Brute force       Image 20 64005 AM       Image 20 64005 AM         Windows - Password spraying       Image 20 64005 AM       Image 20 64005 AM         Windows - Password spraying       Image 20 64005 AM       Image 20 64005 AM         Umare 20 64005 AM       Image 20 64005 AM       Image 20 64005 AM       Image 20 64005 AM         Large number of ATT&CK techniques detected in a system       Image 20 64005 AM		APT 28	2	Mar 22 06:40:04 AM	Ø
APT 33       I       Mar 22 064/005 AM       I         APT 37       I       Mar 22 064/005 AM       I         APT 38       I       Mar 22 064/005 AM       I         APT 41       I       Mar 22 064/005 AM       I         Microsoft 365 - Brute force       I       Mar 22 064/005 AM       I         Microsoft 365 - Brute force       I       Mar 22 064/005 AM       I         Microsoft 365 - Password spraying       I       Mar 22 064/005 AM       I         Windows - Brute force       I       Mar 22 064/005 AM       I         Windows - Brute force       I       Mar 22 064/005 AM       I         Windows - Password spraying       I       Mar 22 064/005 AM       I         Windows - Password spraying       I       Mar 22 064/005 AM       I         Windows - Password spraying       I       Mar 22 064/005 AM       I         Windows - Password spraying       I       Mar 22 064/005 AM       I         Hafnium       I       Mar 22 064/005 AM       I       I         Large number of ATBCK techniques detected in a system       I       Mar 22 064/005 AM       I         Multiple distinct ATTBCK techniques detected in the environment       I       Mar 22 064/005 AM       I		APT 29	2	Mar 22 06:40:04 AM	Ø
APT 37       C       Mar 22 064/005 AM       C         APT 38       C       Mar 22 064/005 AM       C         APT 41       C       Mar 22 064/005 AM       C         Microsoft 365 - Brute force       C       Mar 22 064/005 AM       C         Microsoft 365 - Brute force       C       Mar 22 064/005 AM       C         Windows - Brute force       C       Mar 22 064/005 AM       C         Windows - Brute force       C       Mar 22 064/005 AM       C         Windows - Brute force       C       Mar 22 064/005 AM       C         Windows - Brute force       C       Mar 22 064/005 AM       C         Windows - Password spraying       C       Mar 22 064/005 AM       C         Windows - Password spraying       C       Mar 22 064/005 AM       C         Windows - Password spraying       C       Mar 22 064/005 AM       C         Hafnium       C       Mar 22 064/005 AM       C       C         Large number of ATS&CK techniques detected in a system       C       Mar 22 064/005 AM       C         Large number of ATS&CK techniques detected in a system       C       Mar 22 064/005 AM       C         Multiple distinct ATT&CK techniques detected in a system       C       Mar 22 064/005 AM		APT 33	2	Mar 22 06:40:05 AM	Ø
APT 38       Image 2064/005 AM       Image 2064/005 AM         APT 41       Image 2064/005 AM       Image 2064/005 AM         Microsoft 365 - Brute force       Image 2064/005 AM       Image 2064/005 AM         Microsoft 365 - Brute force       Image 2064/005 AM       Image 2064/005 AM         Windows - Brute force       Image 2064/005 AM       Image 2064/005 AM         Windows - Brute force       Image 2064/005 AM       Image 2064/005 AM         Windows - Password spraying       Image 2064/005 AM       Image 2064/005 AM         Windows - Password spraying       Image 2064/005 AM       Image 2064/005 AM         Hafnium       Image 2064/005 AM       Image 2064/005 AM       Image 2064/005 AM         Large number of ATS&CK techniques detected in a system       Image 2064/005 AM       Image 206		APT 37	2	Mar 22 06:40:05 AM	Ø
APT 41IMar 22 064:005 AMIMicrosoft 365 - Brute forceIMar 22 064:005 AMIMicrosoft 365 - Password sprayingIMar 22 064:005 AMIWindows - Brute forceIMar 22 064:005 AMIWindows - Brute forceIMar 22 064:005 AMIWindows - Password sprayingIMar 22 064:005 AMIHafniumIMar 22 064:005 AMILarge number of ATB&CK techniques detected in a systemIMar 22 064:005 AMIMultiple distinct ATF&CK techniques detected in the environmentIMar 22 064:005 AMIMultiple distinct ATF&CK techniques detected in a systemIMar 22 064:005 AMIMultiple distinct ATF&CK techniques detected in a systemIMar 22 064:005 AMIWitzerd SpiderIMar 22 064:005 AMIIWitzerd SpiderIMar 22 064:005 AMIIWitzerd SpiderIMar 22 064:005 AMIIWitzerd SpiderIMar 22 064:005 AMIIWitzerd SpiderIMar 22 064:005 AMIIMultiple distinct ATF&CK techniques detected in the environmentIMar 22 064:005 AMIWitzerd SpiderIMar 22 064:005 AMIIMultiple distinct ATF&CK techniques detected in the environmentIMar 22 064:005 AMIWitzerd SpiderIMar 22 064:005 AMIIMultiple distinct ATF&CK techniques detected in the environmentIMar		APT 38	2	Mar 22 06:40:05 AM	Ø
Microsoft 365 - Brute forceImage: Constraint of		APT 41	2	Mar 22 06:40:05 AM	Ø
Microsoft 365 - Password spraying       Image: Amar 22 0640.05 AM       Image: Amar 22 0640.05 AM         Windows - Brute force       Image: Amar 22 0640.05 AM       Image: Amar 22 0640.05 AM         Windows - Password spraying       Image: Amar 22 0640.05 AM       Image: Amar 22 0640.05 AM         Hafnium       Image: Amar 22 0640.05 AM       Image: Amar 22 0640.05 AM         Large number of ATT&CK techniques detected in a system       Image: Amar 22 0640.05 AM       Image: Amar 22 0640.05 AM         Large number of ATT&CK techniques detected in a system       Image: Amar 22 0640.05 AM       Image: Amar 22 0640.05 AM       Image: Amar 22 0640.05 AM         Multiple distinct ATT&CK techniques detected in a system       Image: Amar 22 0640.05 AM       Image: Amar 22 064.00 S AM       Image: Amar 22 064.		Microsoft 365 - Brute force	2	Mar 22 06:40:05 AM	Ø
Windows - Brute force       Image: Amar 22 664005 AM       Image: Amar 22 664005 AM         Windows - Password spraying       Image: Amar 22 664005 AM       Image: Amar 22 664005 AM         Hafnium       Image: Amar 22 664005 AM       Image: Amar 22 664005 AM         Large number of ATT&CK techniques detected in a system       Image: Amar 22 664005 AM       Image: Amar 22 664005 AM         Large number of ATT&CK techniques detected in a system       Image: Amar 22 664005 AM       Image: Amar 22 6		Microsoft 365 - Password spraying	2	Mar 22 06:40:05 AM	Ø
Windows - Password spraying       Image: Mar 22 064/035 AM       Image: Mar 22 064/035 AM         Hafnium       Image: Amber of ATT&CK techniques detected in a system       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in a system       Image: Amber of ATT&CK techniques detected in a system       Image: Amber of ATT&CK techniques detected in a system       Image: Amber of ATT&CK techniques detected in a system       Image: Amber of ATT&CK techniques detected in a system       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected in the environment       Image: Amber of ATT&CK techniques detected i		Windows - Brute force	2	Mar 22 06:40:05 AM	Ø
Hafnium       Image: Amage: Amag		Windows - Password spraying	2	Mar 22 06:40:05 AM	Ø
Large number of ATT&CK techniques detected in a system       Image: Amage:		Hafnium	2	Mar 22 06:40:05 AM	Ø
Large number of ATT&CK techniques detected in the environment       Image: Amage:		Large number of ATT&CK techniques detected in a system	2	Mar 22 06:40:05 AM	Ø
Multiple distinct ATT&CK techniques detected in a system       Image: Constraint of the environment       Image: Constraint of the envint of the environment       Image		Large number of ATT&CK techniques detected in the environment	2	Mar 22 06:40:05 AM	Ø
Multiple distinct ATT&CK techniques detected in the environment       Image: Mar 22 064005 AM       Image: Mar 22 064005 AM         Witzard Spider       Image: Mar 22 064005 AM       Image: Mar 22 064005 AM       Image: Mar 23 064005 AM         Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM         Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM         Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM       Image: Mar 23 0625102 AM		Multiple distinct ATT&CK techniques detected in a system	2	Mar 22 06:40:05 AM	Ø
Wizard Spider         Image: Constraint of the spider         Image: Conspider <t< td=""><td></td><td>Multiple distinct ATT&amp;CK techniques detected in the environment</td><td>2</td><td>Mar 22 06:40:05 AM</td><td>Ø</td></t<>		Multiple distinct ATT&CK techniques detected in the environment	2	Mar 22 06:40:05 AM	Ø
Mar 23 02:51:02 AM         Ø           Mar 23 02:55:44 AM         Ø           Mar 23 02:56:44 AM         Ø           Mar 23 04:34:33 AM         Ø		Wizard Spider	2	Mar 22 06:40:05 AM	Ø
Image: Constraint of the second sec		Test, Aule - 1		Mar 23 02:51:02 AM	Ø
□ Mar 23 04:34:33 AM Ø		TEST_MARL-2		Mar 23 02:56:44 AM	Ø
		1037_Auto-3	2	Mar 23 04:34:33 AM	Ø



# **1.3** Cloning a Built-in or a User-defined template

The Open XDR platform facilitates to modify and reutilize the Built-in or the existing User-defined templates. The cloning feature supports creating new templates including the details of the existing Built-in or the User-defined template.

Perform the following procedure to clone a Built-in template.

1. In the new **Rule Configuration** interface, after the providing the necessary details for the Rule name, Frequency, and DSL query, go to the **Event template** tab.

Note:

Refer <u>Configuring a New Rule</u> section to view the detailed process for configuring a new rule.

≡	Netsurion.			🔊 Admin 🗸	Tools <del>-</del>	💽 sadhana 🗸
<b>≡</b> ơ 📧	Rule configuration Rule name	Frequency ① 15 Minutes	Description	<ul><li>↑ Admin / Def</li><li>✓ Generate</li></ul>	ection Rules / R Alert ()	ule Configuration
	DSL query Event template Template type Select template type					Save Close
	Netsurion.	Server Time: Mar 27 02:29 AM	Response: 0.54 secs		© 202	3 Netsurion



2. In the Event template tab, select the Template type as Existing template and select the appropriate existing Built-in Template name from the drop-down list.

DSL query Event template	
Template type Existing template Template	Template name Select Template name APT Detection Brute force Password spraying Environment Detection Environment Detection
Note: The template shown above is used to f DSL query.	orm event description obtained through JSON result of Preview

When the necessary Built-in template is chosen, the **Clone** action button appears in the bottom right-corner of the interface.

3. Click **Clone** to create a user-defined template with the details of the selected Existing template.

	Template name
Existing template 🗸 🗸	Brute force 🗸
emplate	
Potential brute force attack was de ([\$.aggregations.Computer.bucket ([\$.aggregations.Computer.bucket Details: Target username: ([\$.aggregations Source IP address: ([\$.aggregation Login failure count: ([\$.aggregation Login success count: ([\$.aggregations Detection found from: ([\$.aggregations)	ected for the user(s) ((5.aggregations.Computer.buckets[*].UserName.buckets[*].key)) from the IP(s) [*].UserName.buckets[*].IPAddress.buckets[*].key)) between ([\$aggregations.Computer.buckets[*].FirstLoginAttempt.hits.hits[*]_source.event_datetime}] and [*].LastLoginAttempt.hits.hits[*]_source.event_datetime}] computer.buckets[*].UserName.buckets[*].Key)] .Computer.buckets[*].UserName.buckets[*].IPAddress.buckets[*].key]) s.Computer.buckets[*].UserName.buckets[*].JoginFailed.Log_Count.value}] ns.Computer.buckets[*].UserName.buckets[*].LoginFailed.Log_Count.value}] ns.Computer.buckets[*].VserName.buckets[*].SerName.buckets[*].Source.event_datetime]]
Detection found to: ((\$.aggregatio Target computer: ((\$.aggregations.	is.Computer.buckets[*].LastLoginAttempt.hits.hits[*]source.event_datetime]) Computer.buckets[*].keyj}



The DSL query of the Existing template will be replicated to the New template and you can make the necessary modifications.

**4.** Provide a unique Template name and after making the modifications click **Save** to save the new template format.

letsurion.								<b>A</b>	Admin <del>-</del>	Tools 🗸	💽 sadhan
DSL query Event template	•										
Template type New template	~	Template name									
Potential brute force attack w {{\$.aggregations.Computer.b {{\$.aggregations.Computer.b Details: Target username: {{\$.aggregations.computer.b Login failure count: {{\$.aggregations.computer.b Login success count: {{\$.aggregations.computer.b Detection found from: {{\$.aggregations.computer.computer.computer.b} Detection found to: {{\$.aggregations.computer.computer.computer.c}}}}}	vas detected fo uckets[*]. <u>LastLo</u> ations.Compute jations.Comput egations.Compu gregations.Comp gregations.Comp ations.Compute	r the user(s) ([\$.aggregatio lame.buckets[*].UBAddress. ) xinAttempt.hits.hits[*]so r.buckets[*]. <u>UserName.buc</u> er.buckets[*]. <u>UserName.buc</u> ter.buckets[*]. <u>UserName.buc</u> uputer.buckets[*]. <u>UserName.buckets[*].UserName.buckets[*]. puter.buckets[*].<u>UserName.buckets[*].EisstLoginAt</u> r.buckets[*].<u>LastLoginAt</u> r.buckets[*].<u>LastLoginAt</u></u>	ns.Computer.buck buckets[*],key]} be urce.event_datetim kets[*].PAddress uckets[*].LoainSi uckets[*].LoainSi vAttempt.bits.hits[*]	ets[*]. <u>UserNam</u> etween {{\$.aggre ne}} <u>s.buckets</u> [*].key} <u>uccess.Log Counts</u> <u>uccess.Log Counts</u> *]. <u>source.event</u> source.event di	ie.buckets[f*].key)} egations.Compute aues) nt.value) i. datetime)) atetime))	from the IP(s) er.buckets[*]. <u>Firstl.</u>	oginAttempt.h	i <u>ts.hits</u> [*].	_source.event_	<u>datetime</u> )} ar	nd
Note: The template shown abo DSL query.	ive is used to fo	rm event description obta	ined through JSOI	N result of							Preview
											Save Clos

5. Then, go to the **Detection Rules** interface, select the newly cloned rule name check box from the Rule list and click **Activate Now** to activate the Rule.

# **1.4 Importing a Rule Configuration**

1.

Perform the following procedure to import a Rule Configuration.

- In the **Detection Rules** interface, click the **Import u** button to import the Rule configuration.
- 2. In the **Import** window, click **Browse** to select the **.etdr** file and then click **Import** to import the file details.

Import	×
Select file	Browse Import
	Close



## Importing a Rule with Built-in Rule Name

### Note:

You cannot import a Rule with the Built-in Rule name.

The following error message stating '*Rule(s) name is same as Built-in rule. Please change the rule name and retry.*' appears if you try to import a Rule with the Built-in Rule name.

Netsurion.			<b>Å</b> 1	Admin <del>-</del>	Tools 🗸		•
Detection Rules					🛧 / Admir	/ Detectio	on Rules
Rule(s) name is same as Built-In rule. Please change the rule name and retry							
I of 2 GO Activate Now Click 'Activate Now' after making a	all changes			Se Total:	earch 24 Page	Q Q	<b>a</b>
Rule Name	Active	Added On					
APT 1		Mar 22 06:40:04 AM			۷	3	
APT 28		Mar 22 06:40:04 AM			(	8	
APT 29	<b>~</b>	Mar 22 06:40:04 AM			(4	8	

## Importing a Rule with Existing Rule Name

Importing a rule with existing rule name will overwrite the configurations of the existing rule. The following confirmation message stating '*Rule with same name already exists. Do you want to overwrite?*' appears.

• Click **OK** to overwrite or **Cancel** to terminate the process.

≡	Netsu	rion.	Rule with the same r	name already exists. Do you want to ov	verwrite?	🗈 Admin 🕶 Tools 🕶 🌍 👻
	Detection	Rules		ОК	Cancel	Admin / Detection Rules
Q R	(+) (+) (+) (+) (+) (+) (+) (+) (+) (+)	of 2 > G0 Activ	vate Now Click 'Activ	ate Now' after making all changes		Search     Q     Q       Total:     24     Page Size     20
		Rule Name		Active	Added On	
		APT 1			Mar 22 06:40:04 AM	Ø
		APT 28			Mar 22 06:40:04 AM	Ø
		APT 29			Mar 22 06:40:04 AM	Ø
		APT 33			Mar 22 06:40:05 AM	Ø
		APT 37		Working	Mar 22 06:40:05 AM	Ø
		APT 38			Mar 22 06:40:05 AM	Ø
		APT 41			Mar 22 06:40:05 AM	Ø



# 1.5 Exporting a Rule Configuration

Perform the following procedure to export a Rule Configuration.

In the Detection Rules interface, select the required Detection Rules from the list and then click the Export <sup>1</sup> button to export the configured rules.

## Note:

The default Rules (that is, the Built-in rules) cannot be exported.

ш с	Detection F	Rules			Admin / Detection Rules
R	• 1	Export         Form         Click 'Activate Now' after making all changes			Search Q Q Total: 14 Page Size 20 ~
		Rule Name	Active	Added On	
		APT 1		Jan 30 03:58:47 PM	Ø
		APT 28		Jan 30 03:58:47 PM	Ø
		APT 29		Jan 30 03:58:47 PM	Ø
		APT 33		Jan 30 03:58:47 PM	Ø
		APT 37		Jan 30 03:58:47 PM	Ø
		APT 38		Jan 30 03:58:47 PM	Ø
		APT 41		Jan 30 03:58:47 PM	Ø
		Halfnium		Jan 30 03:58:47 PM	Ø
		Large number of ATT&CK techniques detected in a system		Jan 30 03:58:47 PM	Ø
		Large number of ATT&CK techniques detected in the environment		Jan 30 03:58:47 PM	Ø
		Multiple distinct ATT&CK techniques detected in a system	<b>Z</b>	Jan 30 03:58:47 PM	Ø
		Multiple distinct ATT&CK techniques detected in the environment	<b>Z</b>	Jan 30 03:58:47 PM	Ø
		Wizard Spider	<b>Z</b>	Jan 30 03:58:47 PM	Ø
		APT_100	<	Feb 05 10:02:04 PM	Ø
javascrip	t:doPostBack(*ct	100\$ContentPlaceHolder1\$InkExport;")			
0	DetectionRules_1	Letdr A			Show all



# **About Netsurion**

Netsurion<sup>®</sup> delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's Managed Threat Protection includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at <u>www.netsurion.com</u>.

# **Contact Us**

## **Corporate Headquarters**

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

## **Contact Numbers**

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

https://www.netsurion.com/eventtracker-support