



User Guide

The Netsurion Open XDR platform MITRE ATT&CK

Publication Date:

March 30, 2023

Abstract

This guide facilitates to utilize the capabilities of MITRE ATT&CK® Matrix – Enterprise aligned with the Netsurion Open XDR platform v9.4 for better security management. MITRE ATT&CK® is a security intelligence framework with comprehensive tactics and techniques leveraged to detect and assess cyber threats at different levels of enterprise IT network.

Note:

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

Audience

This guide is intended for use by all the Netsurion Open XDR platform users responsible for investigating and managing network security. This guide assumes that you have the Open XDR platform access and understanding of networking technologies.

Note:

This guide describes using the Netsurion Open XDR platform with MITRE ATT&CK® and not a user guide for MITRE ATT&CK®.

Note:

This guide is updated for Open XDR version v9.4 and some functionality may not exist in Open XDR version 9.3.

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	Overview.....	4
1.1	What’s new in the MITRE ATT&CK® Framework in Open XDR v9.4.....	4
1.2	MITRE ATT&CK® Framework.....	4
1.3	ATT&CK® matrix with the Netsurion Open XDR platform.....	4
2	Accessing MITRE ATT&CK®.....	5
2.1	MITRE ATT&CK® Dashboard Details.....	5
2.2	UI Conventions.....	7
3	MITRE ATT&CK® Framework - Comprehensive View.....	14
3.1	ATT&CK® techniques detected by system.....	14
3.2	Timeline of ATT&CK® techniques detected by system pane.....	18
3.3	ATT&CK® Navigator Pane.....	20
4	Acknowledging and UnAcknowledging Techniques.....	24

1 Overview

The Netsurion Open XDR platform v9.4 comes with an additional layer of security assuredness by integrating/aligning with MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK®) Framework (ATT&CK® matrix). We believe this combination of cybersecurity intelligence, aligning SIEM, and a broadly accepted knowledge base can help your enterprise to stay on top of the ever-evolving threat landscape.

1.1 What's new in the MITRE ATT&CK® Framework in Open XDR v9.4

From Release 9.4 onwards, the MITRE ATT&CK® Navigator is upgraded to the latest version of 11 and comes with Sub-Technique concept in MITRE ATT&CK dashboard/rules.

1.2 MITRE ATT&CK® Framework

The ATT&CK® matrix by MITRE Corp., comprises the most comprehensive list of tactics, techniques, and procedures (TTPs) available in the industry today. The MITRE ATT&CK® provides a well-defined standard for attack identification and protection. It contains over 220 methodologies of attack techniques mapped to various stages of the attack, or the 'kill-chain'. It provides a deep understanding into real-world attack vectors from end to end attack stages--from primary system access, to data theft, to sabotage. While MITRE has several technology domains, the Open XDR platform SIEM integrates the "Enterprise" domain knowledge base.

1.3 ATT&CK® matrix with the Netsurion Open XDR platform

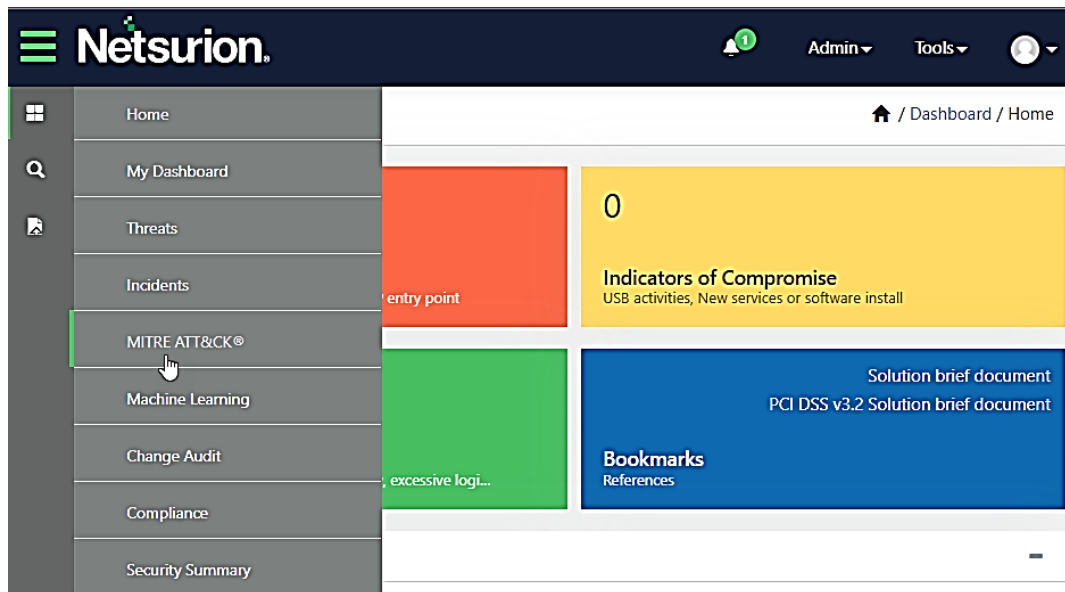
The Netsurion Open XDR platform is well aligned with the MITRE framework through threat chains and behavioral analytics to detect and assess the highest risk threats. Our platform is almost perfectly coordinated with MITRE ATT&CK®. The Open XDR platform has added features to help analysts combine the information they see in the ATT&CK® matrices - to help identify threat risk levels, plan mitigation, and execute effective defense methods and procedures.

The enhanced functionality of the multi-tenancy architecture of the Open XDR platform MITRE ATT&CK® framework is enabled for the Open XDR platform Admin, MSP, and Master MSP to monitor the IT infrastructure of multiple clients at the same time.

2 Accessing MITRE ATT&CK®

Using the MITRE ATT&CK® framework within the Open XDR platform, you can identify adversarial tactics, techniques, sub-techniques, and malicious threats within your network.

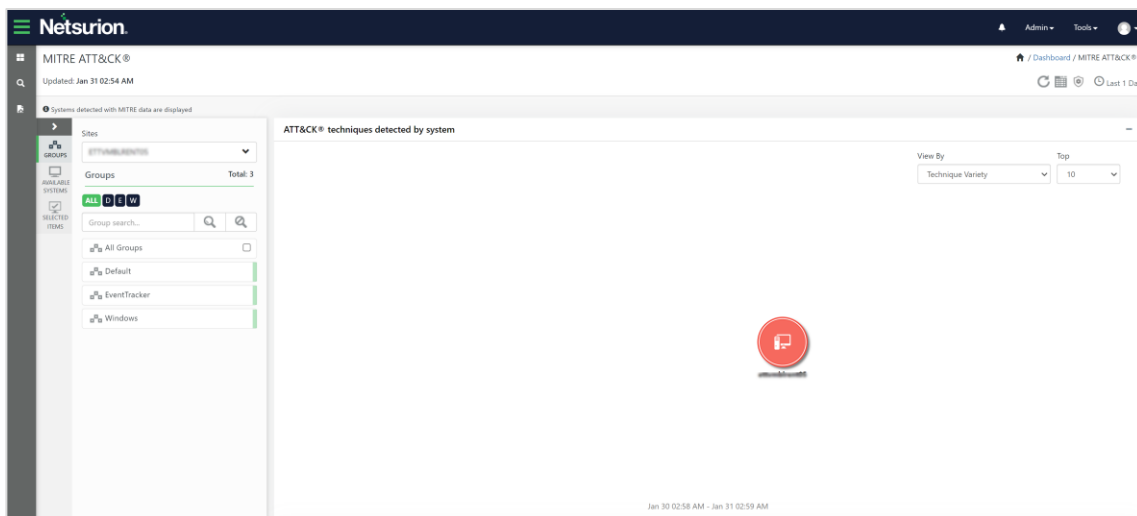
In the **Open XDR platform**, go to **Dashboard** and click **MITRE ATT&CK®** to access the MITRE ATT&CK® integration in the Open XDR platform.



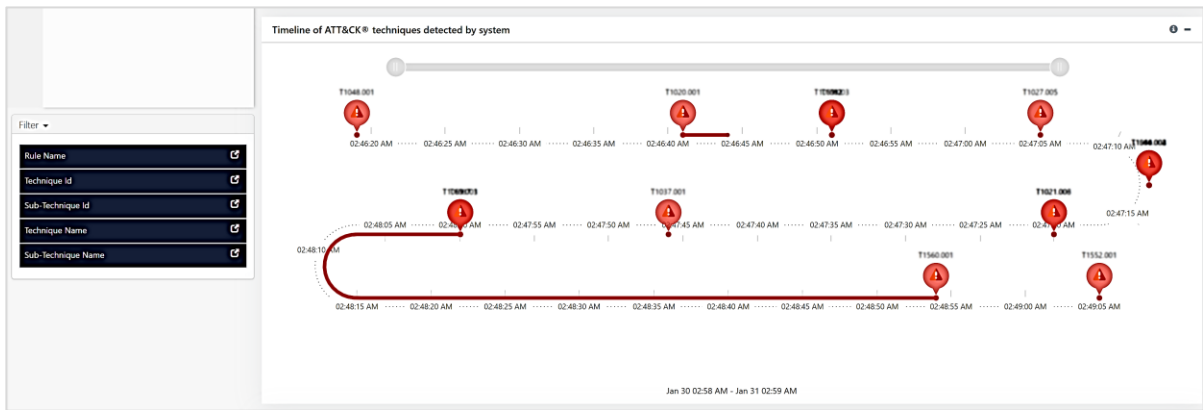
2.1 MITRE ATT&CK® Dashboard Details

The **MITRE ATT&CK®** interface provides a centralized view of system activities and greater threat and techniques visibility in a single dashboard. The dashboard includes three panes.

1. **ATT&CK® techniques detected by system:** This pane enables you to see the adversarial techniques/incidents attacking the systems and the threat score.



- Timeline of ATT&CK® techniques detected by system:** This pane recreates the timeline of the detected techniques by the system. It helps analyze techniques plotted on the system with reference to the time of attack.



- ATT&CK® Navigator:** The ATT&CK® Navigator enables you to view defensive coverage. Layers can be created within the Navigator for comparison of techniques.

ATT&CK® Navigator

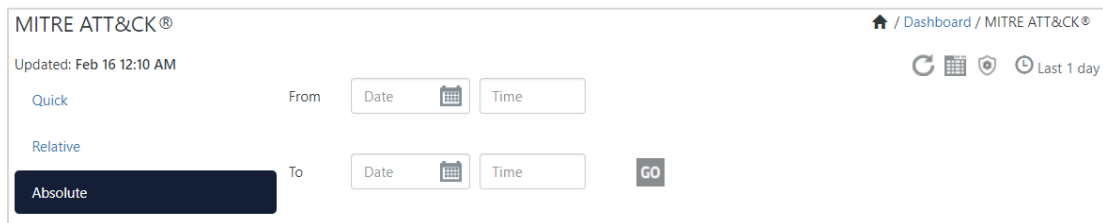
Score Range: 1 (green) to 100 (red)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques
Drive-by Compromise	Command and Scripting Interpreter (1/6)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)
Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (1/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)
External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (2/6)	Browser Session Hijacking
Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (1/3)	Escape to Host	Direct Volume Access	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object
Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (1/15)	Execution Guardrails (0/1)	Modify Authentication Process (0/5)	Container and Resource Discovery	User Execution (0/3)	Data from Configuration Repository (0/2)
Valid Accounts (0/4)	System Services (0/2)	Event Triggered Execution (1/15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion	Windows Management Instrumentation	Data from Information Repositories (0/3)
	User Execution (0/3)	External Remote Services	Hijack Execution Flow (0/12)	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System
		Hijack Execution Flow (0/12)	Process Injection (0/12)	Hide Artifacts (1/12)	Multi-Factor Authentication Request Generation	Group Policy Discovery		Data from Network Shared Drive
		Implant Internal Image	Scheduled Task/Job (0/5)	Hijack Execution Flow (0/12)	Network Sniffing	Network Service Discovery		Data from Removable Media
		Modify Authentication Process (0/5)	Valid Accounts (0/4)	Impair Defenses (0/9)	OS Credential Dumping (0/6)	Network Share Discovery		Data Staged (0/2)
		Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Steal Application Access Token	Network Sniffing		Email Collection (0/3)
		Pre-OS Boot (0/5)		Indirect Command Execution	Steal or Forge Kerberos Tickets (0/4)	Password Policy Discovery		Input Capture (0/4)
		Scheduled Task/Job (0/5)		Masquerading (1/7)	Steal Web Session Cookie	Peripheral Device Discovery		Screen Capture
		Server Software		Modify Authentication Process (0/5)		Permission Groups Discovery (1/3)		Video Capture
				Modify Cloud Compute		Process Discovery		

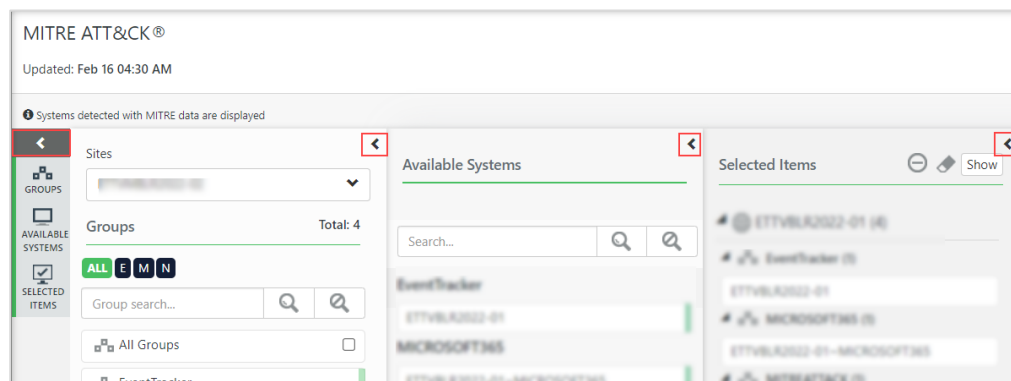
From	Specify the time range starting with which the incident details must be visible. This field accepts only integers
	To calculate and provide the incident details accordingly, choose either hours, weeks, months, or days from the calendar
To	By default the To field is set to the current time and cannot be modified

▪ **Absolute**

Click **Absolute** to set an absolute time range by specifying the values in the **From** and **To** fields along with the required **Time** (including hours, minutes and seconds), and then click **Go** to view the incident details.



Click the **Right anchor** button to expand and view the **Groups**, **Available Systems**, **Selected Items** panels, and the **Left anchor** button to collapse the panels.



and

Note:

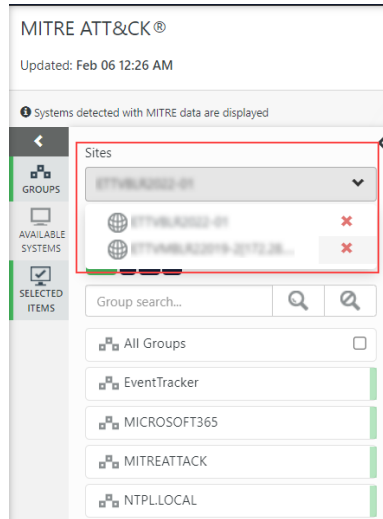
You can also click **Collapse** button on each pane to hide.

- **Groups**

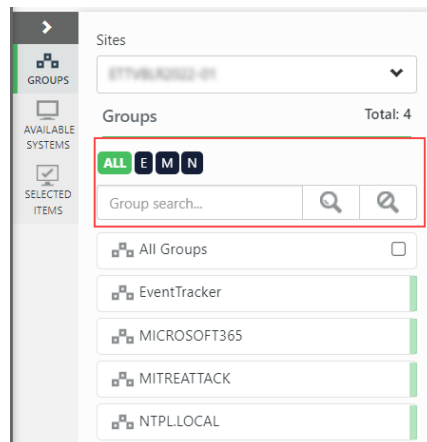
The **Groups** pane displays each Site's associated groups of systems.

Note:

The First Site in the drop-down list will always be either the **Console Manager (CM)** or **Collection Point (CP)** depending on the user login. Multiple Collection Point data (also known as Sites) on a Collection Master (also known as Centralized Console) is available in MITRE ATT&CK® dashboard on latest version of the Open XDR platform v9.4 and later.



- In the **Groups** pane, choose the required Site name from the **Sites** drop-down list to view the respective groups of system in that Site.
- To search for a particular Group, specify the group name in the **Group** search field or click the hotkeys to search the **Groups** in alphabetical order.



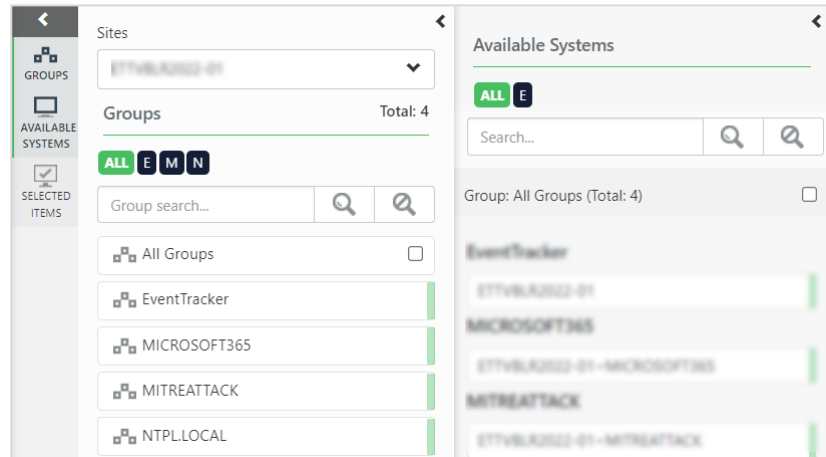
Note:

The interface displays only those Groups with systems having MITRE ATT&CK® data.

- **Available Systems**

The Available Systems displays all the available systems in the selected group of a specific site.

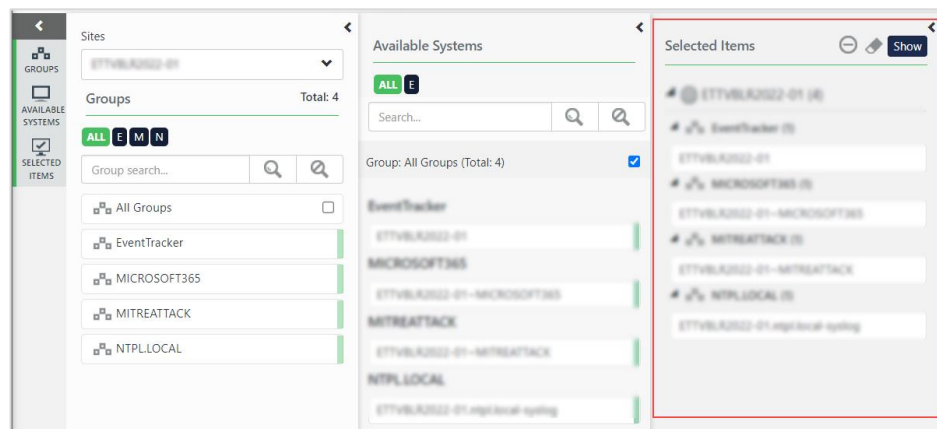
- a. Click **Available Systems** to view all the available systems of all the groups or select the required group to view all the available systems of the selected group.
- b. To search for a particular system, specify the system name in the Search field or click the hotkeys to search for the required System in alphabetical order.



▪ **Selected Items**

The Selected Items displays the selected site details.

- a. Click **Show** to view the information of that site, which displays the groups and its system details.
- b. Click the **Erase** button to clear the selections.
- c. Click the **Collapse** button to collapse the detailed view of the selected sites.



Note:

If Collection Points (Sites) are in different time zone from the Collection Master (Centralized console), then the log search time duration might vary.

Filters in the MITRE ATT&CK® framework facilitates an effective way to detect the common and relevant techniques and logs by including or excluding the required Filter values.

Filter Categories

Filter the incident data by five categories - **Rule Name**, **Technique ID**, **Sub-Technique Id**, **Technique Name** and **Sub-Technique Name**.

Filter Functions

The **Include** function adds the filter and the **Exclude** function rules out the filters based on the selection.

Filters

MITRE ATT&CK®
Updated: Feb 06 12:33 AM

Systems detected with MITRE data are displayed

Sites
Groups: ETTVBLR2022-01 (Total: 4)

AVAILABLE SYSTEMS
SELECTED ITEMS

Group search...

- All Groups
- EventTracker
- MICROSOFT365
- MITREATTACK
- NTPLOCAL

Filter

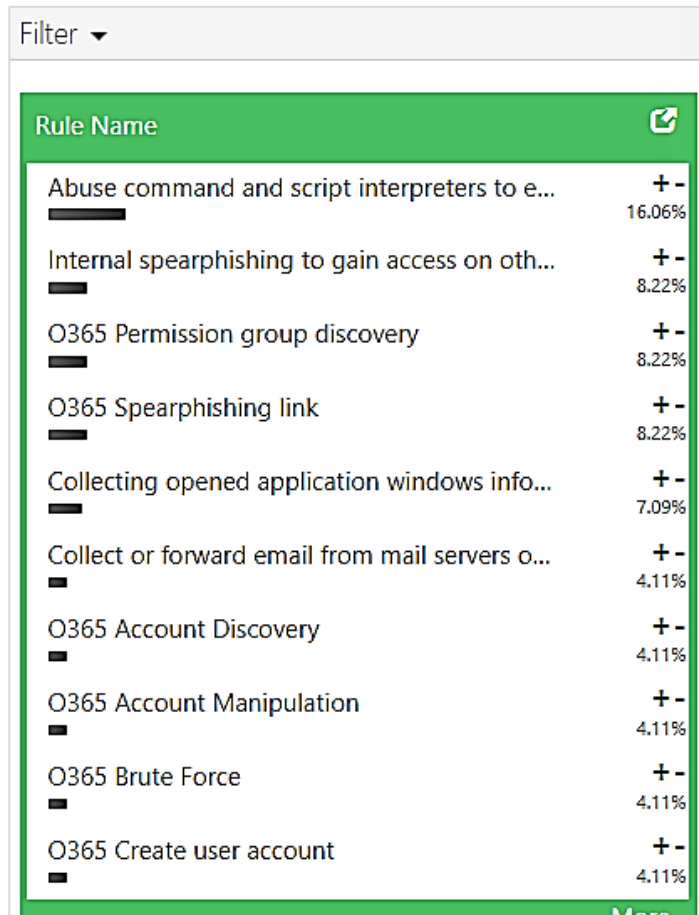
- Rule Name
- Technique Id
- Sub-Technique Id
- Technique Name
- Sub-Technique Name

Filter

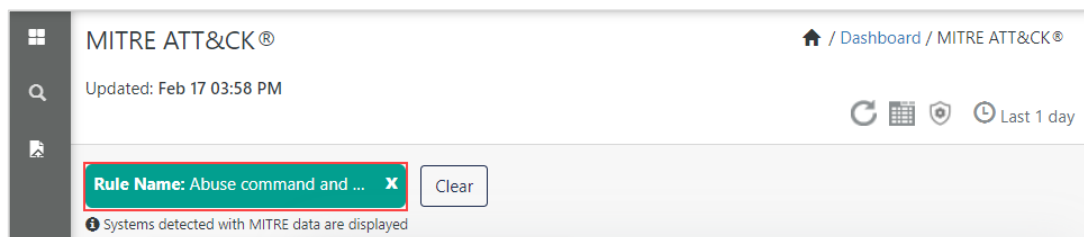
- Rule Name
- Technique Id
- Sub-Technique Id
- Technique Name
- Sub-Technique Name


Procedure to ADD/ INCLUDE a Filter

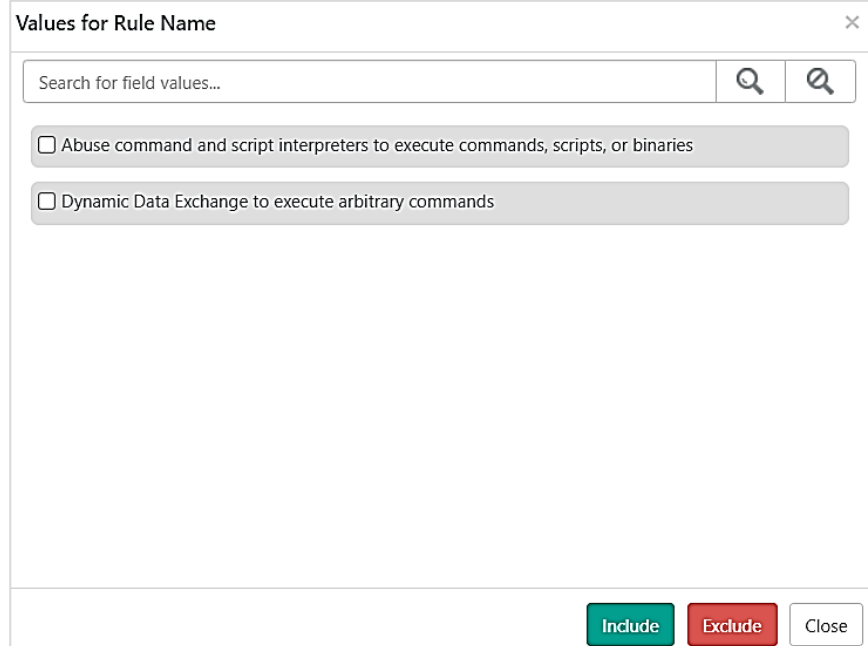
- a. In the **Filter** panel, go to the required filter category (for example, **Rule Name** filter) to view the available filter details and click **+** to include the filter.



When the selected filter (that is, the selected Rule Name) is added to the filter list, the items that meet the filter criteria will be displayed.



- b. To include or exclude multiple filters, go to the required filter category (for example, Rule Name) and click the **View field value**  button to view all the filter details.



Values for Rule Name

Search for field values...

Abuse command and script interpreters to execute commands, scripts, or binaries

Dynamic Data Exchange to execute arbitrary commands

Include Exclude Close

- c. In the **Values for Rule Name** window, select the required filter category details from the list and click **Include** or **Exclude** accordingly.
- d. Click **Close** to close the window.

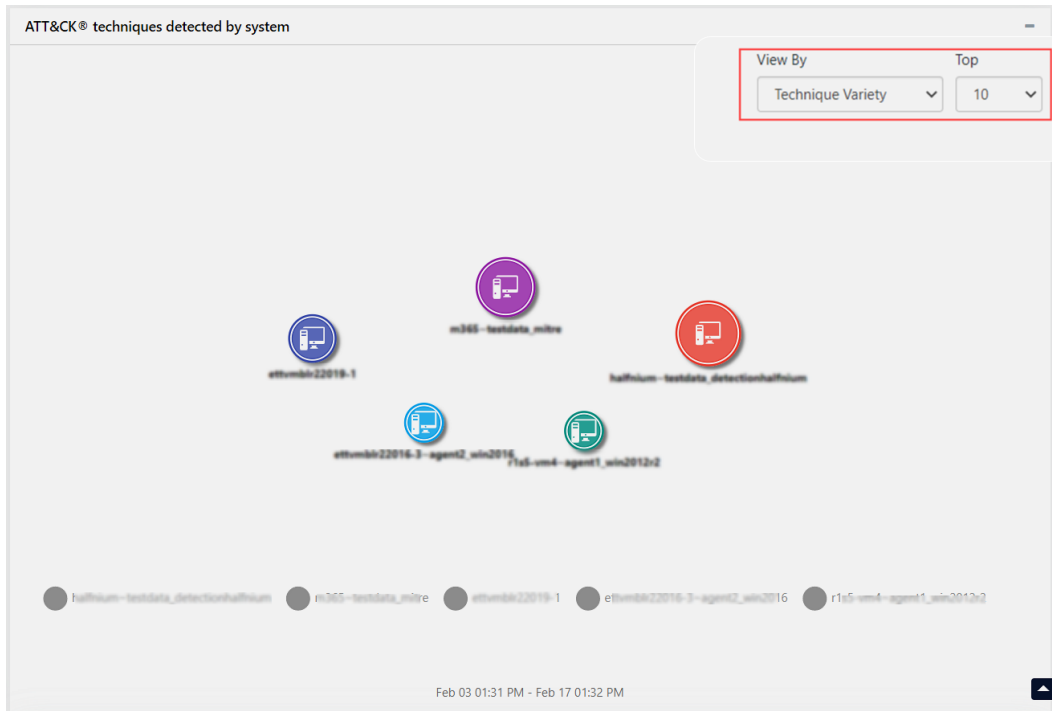
Note:

By applying the same process, you can filter the techniques for the following Filter categories; **Rule Name, Technique ID, Sub-Technique Id, Technique Name** and **Sub-Technique Name**.

3 MITRE ATT&CK® Framework - Comprehensive View

3.1 ATT&CK® techniques detected by system

In this panel, the Systems are represented graphically by bubble icons.



- In the **View By** drop-down list, choose either **Technique Variety** or **Score** to classify/view/sort the systems accordingly.

Note:

The score calculation is based on the hits of the detected techniques.

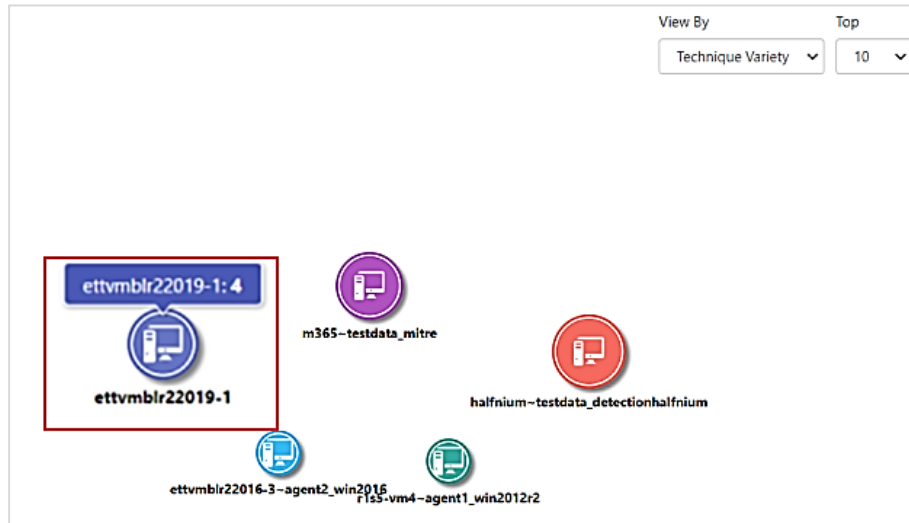
- In the **Top** drop-down list, choose the number of systems you require to be displayed.

Note:

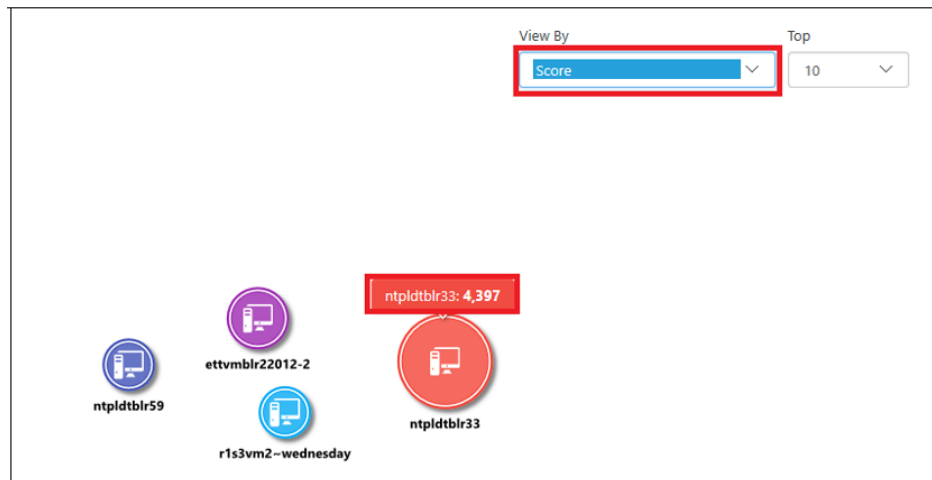
By default, the **View** is selected as **Technique Variety** and **Top** is selected as **10**.

- Hover over the bubble icon to view the details of the **system name** and **number of threat attacks** on that system.

Sample Image for Technique Variety



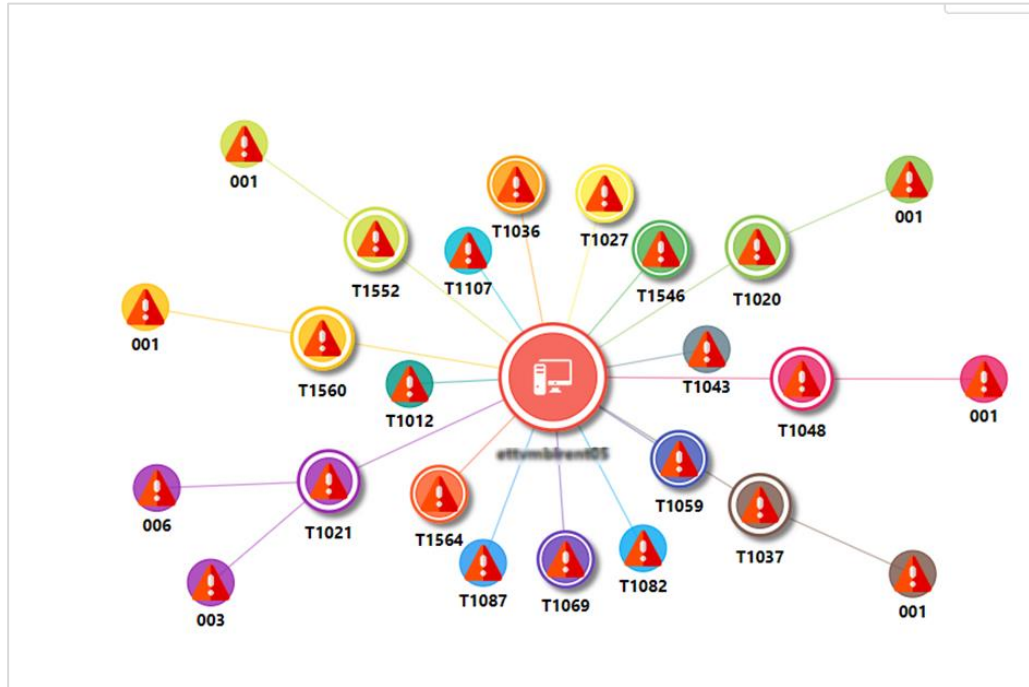
Sample Image for Score



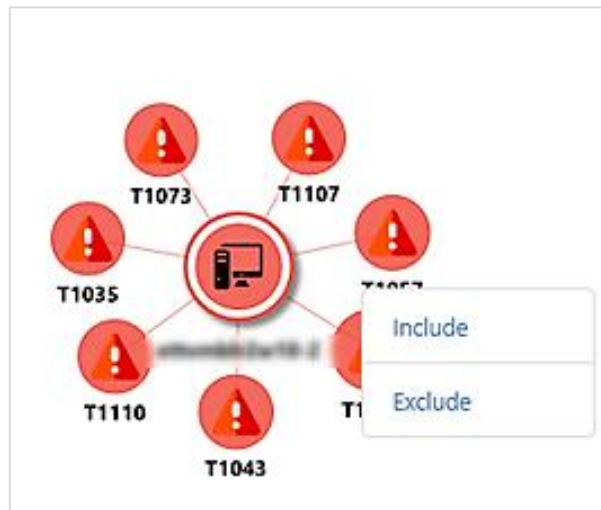
To view the count of a specific technique occurrences on a system,

1. Click the required system's bubble icon to view all the **technique hit occurrences** of that system.
 - The bubble expands into nested bubbles and each nested bubble has a Technique ID.

- The nested bubble will further expand and displays the Sub-Technique Id as shown in the below image.



When clicked on the bubble icon, a drop-down menu with **Include** and **Exclude** function is displayed.



2. Click **Include** to see more about the system's technique attack or hits.

Note:

Include function will add the system name to the Filter so that all the incidents associated with this system will be displayed.

3. Click **Exclude** to rule out the system details from the filter.

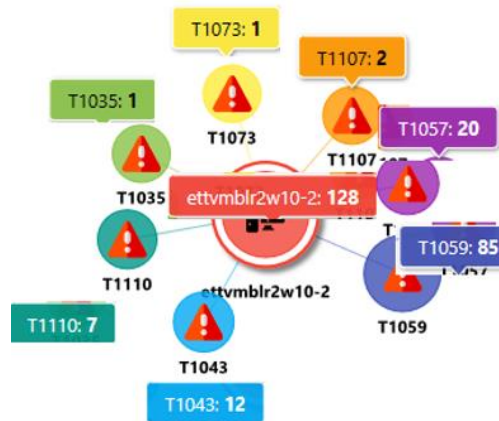
Example for a technique occurrence count.

- Select the system bubble **ettvmb1r2w10-2**.
- The system name along with a score 128 will be displayed.

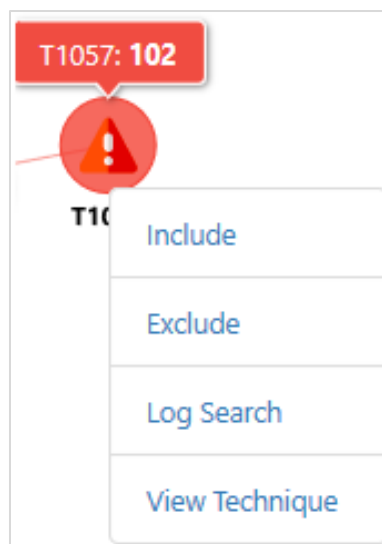
Note:

The score calculation is based on the hits of the detected techniques.

- The bubble expands into nested bubbles and each nested bubble includes a Technique ID or a Sub-Technique Id.



- There are 7 nested bubbles, which mean there are 7 different adversary techniques attacking the system **ettvmb1r2w10-2**.
- The nested bubble will further expand to show the number of hits for every Technique ID.
- The number of hits of all the 7 occurrences will add to make a score 128.
- The severity of this score is determined in the ATT&CK® **Navigator pane**.
- To know about the trigger incident of the **technique**, click on the technique bubble icon, and choose an action from the sub-list options:



<p>Include</p>	<p>Click Include to know more about the technique attack or hits on the system.</p> <p>Note:</p> <p>Include function will add the system name or technique to the Filter which displays all the incidents associated with this system.</p>
<p>Exclude</p>	<p>Click Exclude to exit out of that technique and move on to the next system.</p>
<p>Log search</p>	<p>Click Log search and the application navigates to the Open XDR platform log search page.</p>
<p>View Technique</p>	<p>Click View Technique and the application navigates to the MITRE technique web page. This page contains all the information associated with the selected Technique ID.</p> <p>Note:</p> <p>Follow the link to know more about the MITRE ATT&CK®'s predefined technique. https://attack.mitre.org/techniques/enterprise/.</p>

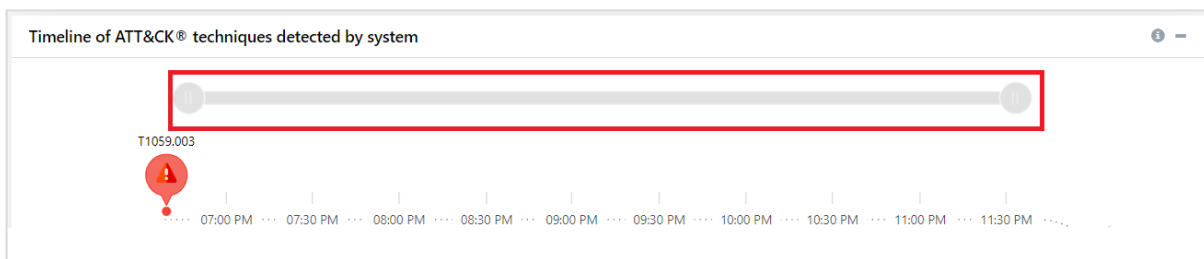
3.2 Timeline of ATT&CK® techniques detected by system pane

This pane recreates timeline of the detected techniques by the system. It helps analyze techniques plotted on the system with reference to the time of attack. The technique hits and time are represented in the form of color-coded heat map.

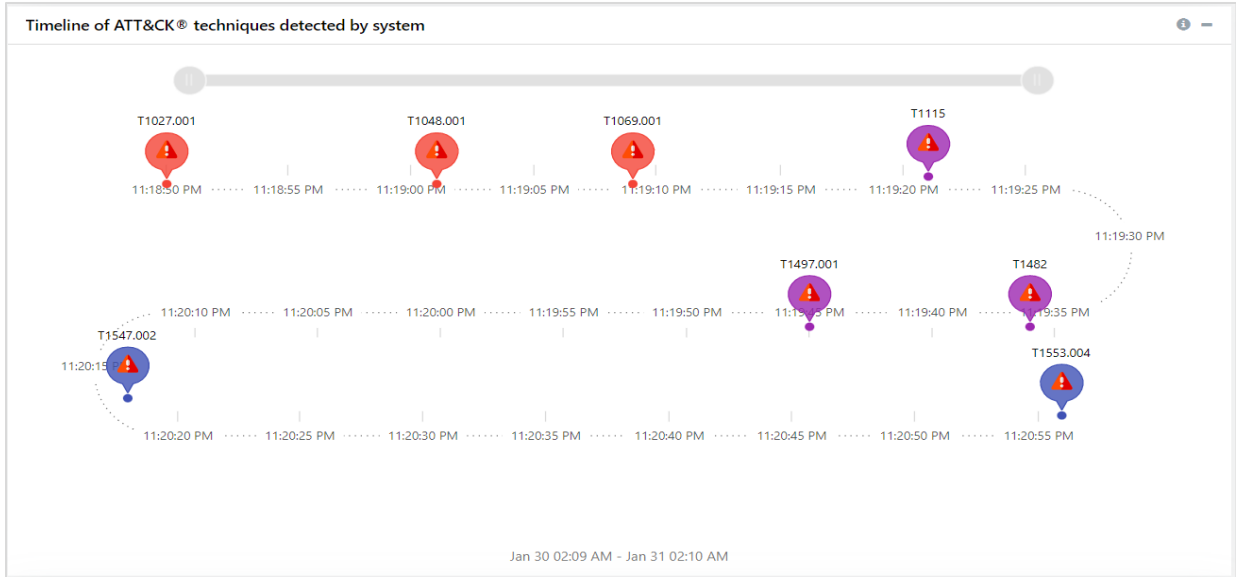
Each pin represents time of the attack and the interval line, following the pin is the duration or interval of the attack. By default, all the attacks plotted on the systems are available at that time. To view the attacks for a specific time in the timeline, a slider is provided for zooming in and zooming out to provide a more detailed viewing.

Note:

While each system’s bubble icon has a specified color, all techniques, icons, pins, and graphs associated to that system are represented in the same color.



- Click **include** on the system or the technique bubble icon to view the details in the **ATT&CK® techniques detected by system** pane.



- Basic details about the technique are displayed when you hover the mouse on the interval line.

- Click the pin or the interval line to go to the log search interface to know more about the specific technique.

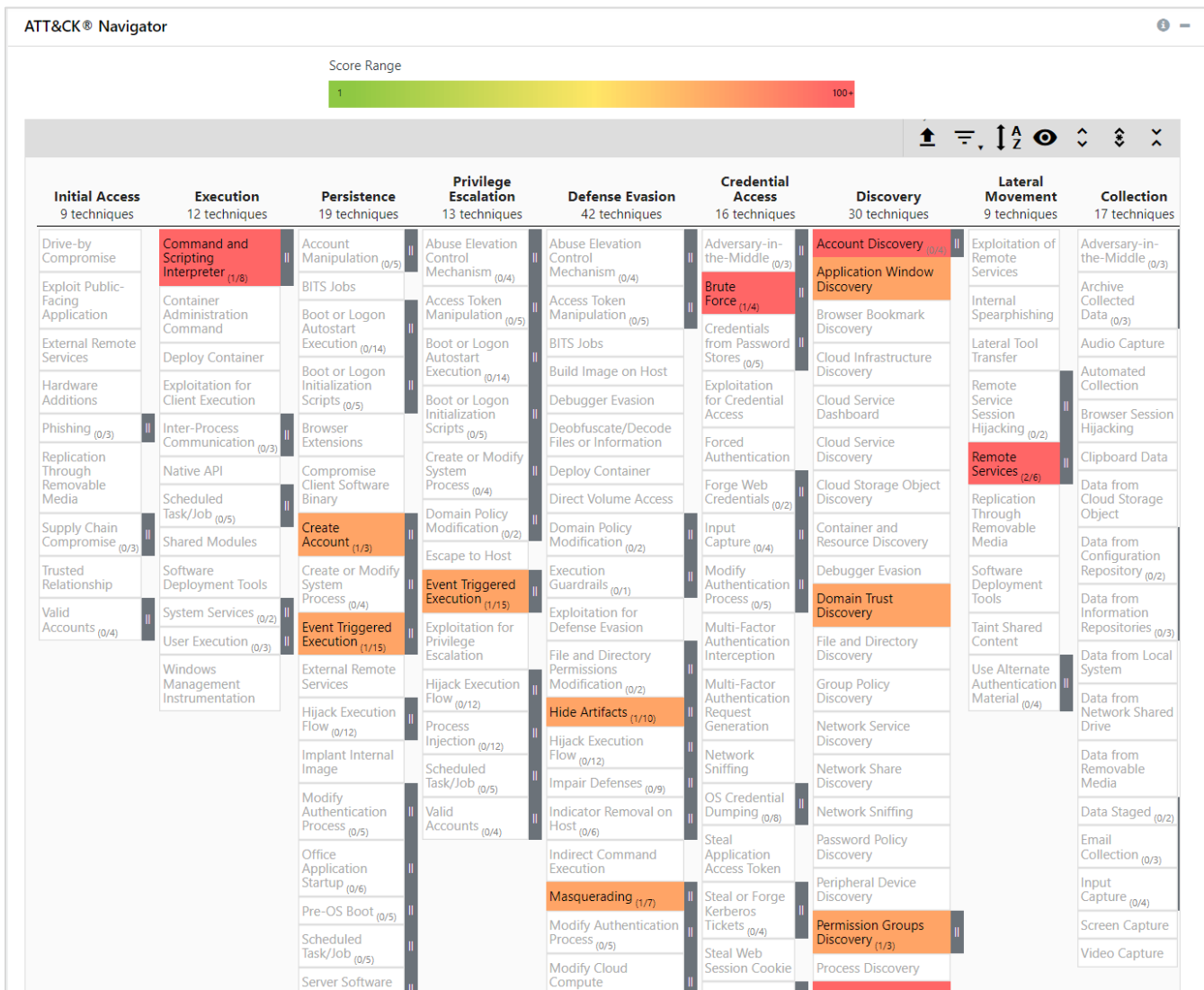


3.3 ATT&CK® Navigator Pane

The main feature of the ATT&CK® Navigator is the ability to visualize data. You can define layers, for example, viewing just the techniques for a system, creating heat maps for frequently seen techniques, or visualizing defensive coverage. Layers can be created and viewed within the Navigator for techniques comparison.

The **ATT&CK® Navigator Pane** displays Techniques in columns and Tactics as column headings. A gradient color scale, displaying Score Range, makes it easy to determine the number of attacks and the severity of attacks.

Green represents a lower number of attacks (1 is least threatening), and Red represents a higher number of attacks (and 100 is most threatening).



- Click the Technique to view the Sub-Technique details.

Note:

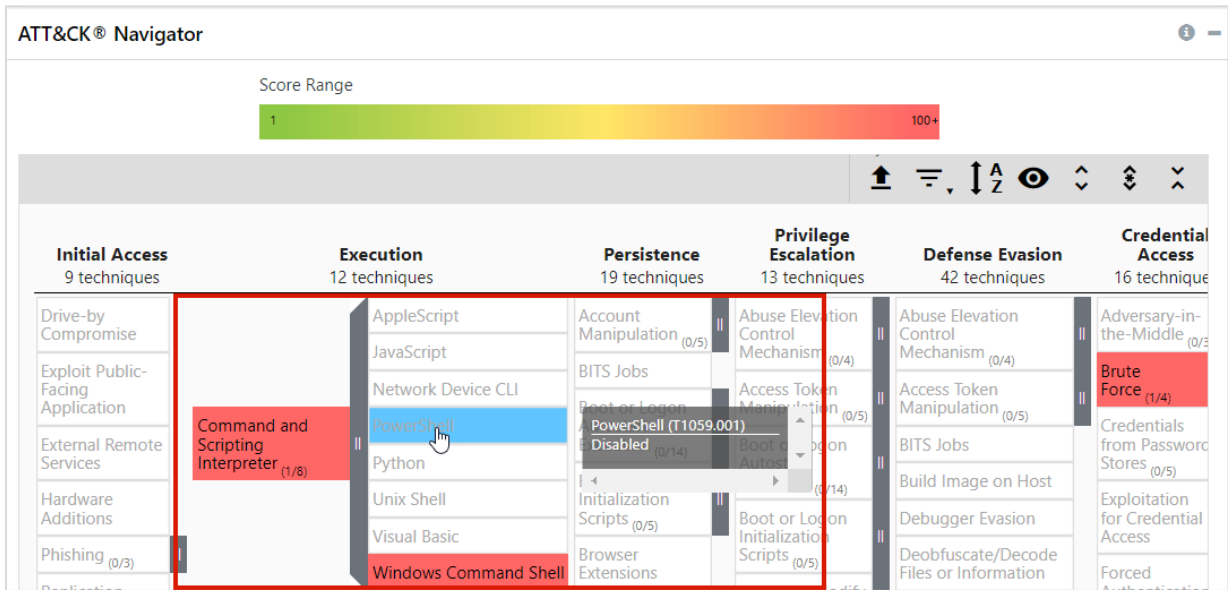
Not all the Technique will contain the Sub-Technique details.

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lat Move 9 tech
Drive-by Compromise	AppleScript	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploita Remote Services
Exploit Public-Facing Application	JavaScript	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (1/4)	Application Window Discovery	Internal Spearph
External Remote Services	Network Device CLI	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral T Transfer
Hardware Additions	PowerShell	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijackin
Phishing (0/3)	Python	Browser Extensions	Browser Extensions	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services
Replication Through Removable Media	Unix Shell	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replicat Through Remova Media
Supply Chain Compromise (0/2)	Visual Basic	Deploy Container	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Container and Resource Discovery	Software Deploy Tools
Trusted Relationship	Windows Command Shell	Exploitation for Client Execution	Escape to Host	Direct Volume Access	Modify Authentication Process (0/5)	Debugger Evasion	Taint Sh Content
Valid Accounts (0/4)	Container Administration Command	Inter-Process Communication (0/3)	Event Triggered Execution (1/15)	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Domain Trust Discovery	Use Alte Authent Material
	Native API	Scheduled Task/Job (0/5)	Event Triggered Execution (1/15)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	File and Directory Discovery	
	Scheduled Task/Job (0/5)	Shared Modules	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Network Service Discovery	Group Policy Discovery	
	Software Deployment Tools	Software Deployment Tools	Hijack Execution Flow (0/12)	Hide Artifacts (1/10)	Network Sniffing	Network Service Discovery	
	System Services (0/2)	System Services (0/2)	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Network Share Discovery	Network Share Discovery	
			Implant Internal Image	Impair Defenses (0/18)			

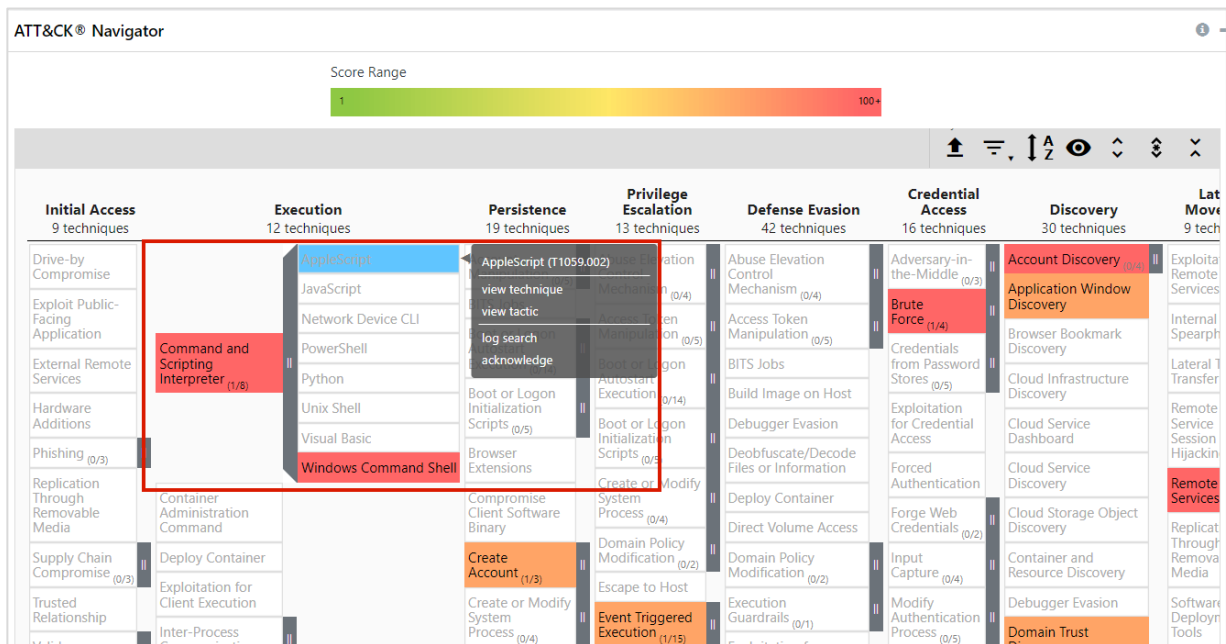
- Hover the mouse on each technique to see the Technique ID and its threat score.

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques
Drive-by Compromise	Command and Scripting Interpreter (1/8)	Command and Scripting Interpreter (T1059) Score: 2100	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)
Exploit Public-Facing Application	Container Administration	Autostart Execution (0/14)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (1/4)	Application Window Discovery
External Remote Services	Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Phishing	Exploitation for Client Execution	Browser Extensions	Browser Extensions	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
	Inter-Process Communication (0/3)	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery
	Native API	Deploy Container	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Container and Resource Discovery
	Scheduled Task/Job (0/5)	Exploitation for Client Execution	Escape to Host	Direct Volume Access	Modify Authentication Process (0/5)	Debugger Evasion
	Shared Modules	Inter-Process Communication (0/3)	Event Triggered Execution (1/15)	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Domain Trust Discovery
	Software Deployment Tools	Scheduled Task/Job (0/5)	Event Triggered Execution (1/15)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	File and Directory Discovery
	System Services (0/2)	System Services (0/2)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Network Service Discovery	Group Policy Discovery
			Hijack Execution Flow (0/12)	Hide Artifacts (1/10)	Network Sniffing	Network Service Discovery
			Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Network Share Discovery	Network Share Discovery
			Implant Internal Image	Impair Defenses (0/18)		

- Hover the mouse on each sub-technique to see the Sub-Technique ID and its threat score.



- When you click on a technique or a sub-technique you get the following option lists **tooltip**, **view technique**, **view tactic**, **log search**, and **acknowledge**.



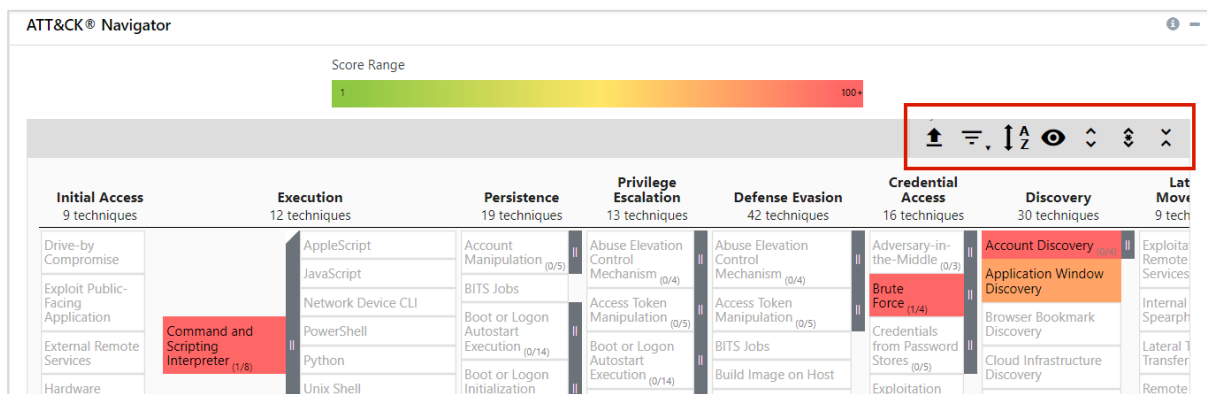
View technique	Click View Technique to visit the MITRE technique page. This page contains all the information associated with the selected technique ID https://attack.mitre.org/techniques/T1059/
View tactic	Click View Tactic to visit the MITRE tactics page. This page contains all the information associated with the selected tactic https://attack.mitre.org/tactics/TA0002/

Log Search	Click Log search , and the application navigates to the Open XDR platform log search interface. Clicking the system name will add it to the Filter. All the incidents associated with this system are displayed
Acknowledge	Click Acknowledge to acknowledge the incidents.

Note:

Follow the link to know more about the MITRE ATT&CK®'s predefined technique <https://attack.mitre.org/techniques/enterprise/>

- You can export, filter, sort, and hide the criteria/techniques from the **ATT&CK® Navigator Pane**.



	Click Export to export the criteria/techniques to excel.
	Click Filters to filter the criteria/techniques according to the platforms.
	Click Sort to sort by alphabetical order or by score.
	Click Hide/Show to either hide or show the criteria or detected techniques.
	Click expand sub-techniques to view the sub-techniques of all techniques.
	Click expand annotated sub-techniques to view the sub-techniques of detected techniques
	Click collapse sub-techniques to shrink the expanded sub-techniques

4 Acknowledging and UnAcknowledging Techniques

You can acknowledge and un-Acknowledge Techniques from the Tabular view.

To Acknowledge the Technique,

- In the **Show** drop-down and select **Unacknowledged** to list all the unacknowledged technique attack details. Based on the user selection Techniques are acknowledged.
- From the list, select a Technique you want to acknowledge, and click the **Ack** checkbox.

First Occurrence	Last Occurrence	Technique Id	Technique Name	Rule Name	Site Name	Computer	Score	Ack
Feb 17 13:10:46 PM	Feb 17 13:10:46 PM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22019-1	3	<input type="checkbox"/>
Feb 17 13:07:37 PM	Feb 17 13:07:37 PM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22016-3-agent2_win2016	2	<input type="checkbox"/>
Feb 17 13:07:36 PM	Feb 17 13:07:36 PM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22016-3-agent2_win2016	1	<input type="checkbox"/>
Feb 17 13:06:39 PM	Feb 17 13:06:39 PM	T1569.002	System Services:Service Execution	Dynamic Data Exchange to execute arbitrary commands	ETTVMBLR22019-1	r1s5-vm4-agent1_win2012r2	1	<input type="checkbox"/>
Feb 17 01:47:53 AM	Feb 17 01:47:54 AM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22019-1	3	<input type="checkbox"/>

- In the **Acknowledge** window, enter the comments for the **Notes** and choose an option from the list, and then click **OK** to acknowledge.

Acknowledge

Notes

Current selection only
 All detections from [ettvmlr2w10-2]
 All [Abuse command and script interpreters to execute commands, scripts, or binaries] detections
 All detections from [ETTVMBLR2W10-2] site
 All [Abuse command and script interpreters to execute commands, scripts, or binaries] detections from [ettvmlr2w10-2]

OK Close

Current selection only	Acknowledges the selected item
All detections from [Name of the System/computer]	Acknowledges all detections from the identified system.

All [Rule Name] detections	Acknowledges all detections of every single rule name of the same type irrespective of the systems.
All detections from [selected] site	Acknowledges all detections from the selected site irrespective of the systems.
All [Rule Name] detections from [Machine Selected]	Acknowledges all detections of the Rule Name on the machine selected

To UnAcknowledge the Technique,

- In the **Show** drop-down and select acknowledged to list all the acknowledged Technique attack details. Based on the user selection Techniques are unacknowledged.
- From the list, select a Technique you want to UnAcknowledge and click the **Ack** checkbox.

First Occurrence	Last Occurrence	ID	Name	Rule Name	Site Name	Computer	Score	Ack
Feb 17 13:10:46 PM	Feb 17 13:10:46 PM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22019-1	3	<input checked="" type="checkbox"/>
Feb 17 13:07:37 PM	Feb 17 13:07:37 PM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22016-3-agent2_win2016	2	<input type="checkbox"/>
Feb 17 13:07:36 PM	Feb 17 13:07:36 PM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22016-3-agent2_win2016	1	<input type="checkbox"/>
Feb 17 13:06:39 PM	Feb 17 13:06:39 PM	T1569.002	System Services:Service Execution	Dynamic Data Exchange to execute arbitrary commands	ETTVMBLR22019-1	r1s5-vm4-agent1_win2012r2	1	<input type="checkbox"/>
Feb 17 01:47:53 AM	Feb 17 01:47:54 AM	T1059.003	Command and Scripting Interpreter:Windows Command Shell	Abuse command and script interpreters to execute commands, scripts, or binaries	ETTVMBLR22019-1	ettvmlr22019-1	3	<input type="checkbox"/>

- In the **Unacknowledge** window, enter the comments for the **Notes** and choose an option from the list, and then click **OK** to UnAcknowledge.

Unacknowledge

Notes

Current selection only

All detections from [ettvmlr2w10-2]

All [Commonly used port to bypass firewalls or network detection systems] detections

All detections from [ETTVMBLR2W10-2] site

All [Commonly used port to bypass firewalls or network detection systems] detections from [ettvmlr2w10-2]

OK **Close**

Current selection only	UnAcknowledges the selected item
All detections from [Name of the System/computer]	UnAcknowledges all detections from the identified system.
All [Rule Name] detections	UnAcknowledges all detections of every single rule name of the same type irrespective of the systems.
All detections from [selected] site	UnAcknowledges all detections from the selected site irrespective of the systems.
All [Rule Name] detections from [Machine Selected]	UnAcknowledges all detections of the Rule Name on the machine selected

IMPORTANT

After upgrading the Open XDR platform from version 9.3 to 9.4, deprecated techniques are still displayed in the MITRE dashboard. Any UI operations using those techniques, such as log search, Ack/Unack, and more, will not produce the desired results. However, depending on how often the index is purged, these outdated techniques will not be visible eventually.

About Netsurion

Netsurion® 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 offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection 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 www.netsurion.com.

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>