

User Guide

The Netsurion Open XDR platform MITRE ATT&CK

Publication Date:

March 30, 2023

© Copyright Netsurion. All Rights Reserved.



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	Ove	erview	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	Acc	cessing MITRE ATT&CK [®]	5
	2.1	MITRE ATT&CK [®] Dashboard Details	5
	2.2	UI Conventions	7
3	MI	TRE 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	Ack	knowledging 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.

≡	Netsurion.		A D	Admin -	Tools -	•
=	Home			A	/ Dashboard	d / Home
۹	My Dashboard					
R	Threats		0			
	Incidents	entry point	Indicators of Compr USB activities, New services	omise or software insta	all	
	MITRE ATT&CK®			Sol	ution brief d	ocument
	Machine Learning		P	CI DSS v3.2 Sol	ution brief d	ocument
	Change Audit	-; excessive logi	Bookmarks References			
	Compliance					
	Security Summary					-

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.

≡	Net	surion.				•	Admin v	Tools 🗸 🕠	-
	MITRE	ATT&CK®					🕈 / Dashboar	d / MITRE ATT&CK	0
٩	Updated	Jan 31 02:54 AM					C 🖿		lay
ß	0 Systems	a detected with MITRE data are d	isplayed						
	>	Sites			ATT&CK® techniques detected by system			-	
	gROUPS	ETTVMBLADN715		~		View By	Toj		
		Groups		Total: 3		Technique Variety	~	10 🗸	
		ALL DEW							
	SILICTED	Group search	Q	Q,					
		a [∎] a All Groups							
		∎ [®] ∎ Default							
		∎ ^B ∎ EventTracker							
		a ^p a Windows							
					Jan 30 02:58 AM - Jan 31 02:59 AM				



2. 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.

	Timeline of ATT&CK* techniques detected by system	0
ar • Jie Name Cf	Those and Those and	02:47:10 ANTINA 004
chnique Id C Ib-Technique Id C chnique Name C	TRADES AN	02:47:15 AM
ıb-Technique Name 🕑		• 02:49:05 AM
	Jan 30 0258 AM - Jan 31 0259 AM	

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

T&CK [®] Navigat	or							0
		Score Range				100+		
							₹, ĴŽ O	\$ \$ X
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	Lateral Movement 9 techniques	Collection 17 technique
Drive-by Compromise	Command and Scripting	Account Manipulation (0/5)	Abuse Elevation Control	Abuse Elevation Control	Adversary-in- the-Middle (0/3)	Account Discovery	I Exploitation of Remote	Adversary-in- the-Middle (0/3)
Exploit Public-	Interpreter (1/8)	BITS Jobs	Mechanism (0/4)	Mechanism (0/4)	Brute	Application Window Discovery	Services	Archive
Facing Application	Container Administration Command	Boot or Logon Autostart	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Force (1/4) Credentials	Browser Bookmark Discovery	Internal Spearphishing	Collected Data (0/3)
External Remote Services	Deploy Container	Execution (0/14)	Boot or Logon Autostart	BITS Jobs	from Password II	Cloud Infrastructure	Lateral Tool Transfer	Audio Capture
Hardware	Exploitation for	Boot or Logon Initialization	Execution (0/14)	Build Image on Host	Stores (0/5) Exploitation	Discovery	Remote	Automated Collection
Additions	Client Execution	Scripts (0/5)	Boot or Logon Initialization	Debugger Evasion	for Credential Access	Cloud Service Dashboard	Service Session	Browser Sessio
Phishing _(0/3) II	Inter-Process Communication (0/3)	Browser Extensions	Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced	Cloud Service	Hijacking (0/2)	Hijacking
Replication Through	Native API	Compromise	Create or Modify System	Deploy Container	Authentication	Discovery	Remote Services (2/6)	Clipboard Data
Removable Media	Scheduled	Client Software Binary	Process (0/4)	Direct Volume Access	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication	Data from Cloud Storage
Supply Chain	Task/Job (0/5)	Create	Domain Policy Modification (0/2)	Domain Policy	Input	Container and	- Through Removable	Object
Compromise (0/3)	Shared Modules	Account (1/3)	Escape to Host	Modification (0/2)	Capture (0/4)	Resource Discovery	Media	Data from Configuration
Trusted Relationship	Software Deployment Tools	Create or Modify System	Event Triggered	Execution Guardrails (0/1)	II Modify Authentication II	Debugger Evasion	Software Deployment	Repository (0/2)
Valid "	System Services (0/2)	Process (0/4)	Execution (1/15)	Exploitation for	Process (0/5)	Domain Trust Discovery	Tools	Data from Information
Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (1/15)	Exploitation for Privilege	Defense Evasion	Multi-Factor Authentication	File and Directory	Taint Shared Content	Repositories (0/
	Windows	External Remote	Escalation	File and Directory Permissions	Interception	Discovery	Use Alternate	Data from Loca System
	Management Instrumentation	Services	Hijack Execution Flow (0/12)	Modification (0/2)	Multi-Factor Authentication	Group Policy Discovery	Authentication I Material (0/4)	Data from
		Hijack Execution Flow (0/12)	Process	Hide Artifacts (1/10)	II Request Generation	Network Service	(0) 1)	Network Share Drive
		Implant Internal	Injection (0/12)	Hijack Execution Flow (0/12)	II Network	Discovery		Data from
		Image	Scheduled Task/Job (0/5)	Impair Defenses (0/9)	Sniffing	Network Share Discovery		Removable Media
		Modify Authentication	Valid	Indicator Removal on	OS Credential Dumping (0/8)	Network Sniffing		Data Staged
		Process (0/5)	Accounts (0/4)	Host (0/6)	Steal	Password Policy		Email
		Office Application		Indirect Command Execution	Application Access Token	Discovery		Collection (0/3)
		Startup (0/6)		Masquerading (1/7)	II Steal or Forge	Peripheral Device Discovery		Input Capture _(0/4)
		Pre-OS Boot (0/5)		Modify Authentication	Kerberos II Tickets (0/4)	Permission Groups	1	Screen Capture
		Scheduled Task/Job (0/5)		Process (0/5)	Steal Web	Discovery (1/3)		Video Capture
		Server Software		Modify Cloud Compute	Session Cookie	Process Discovery		



2.2 UI Conventions

C	Click the Refresh $^{m C}$ button to view the la	atest details.		
	By default, the interface displays the incid Click the Tabular view button to view The Tabular view displays the colur First Occurrence, Last Occurrence,	the incident details in T nn titles with technique	abular layout. attack details listed	
	Name, Computer, Score, and Ack h		★ / Dashboard / MTRE ATTACC	
	PM PM If Feb 05 23.41.47 Feb 05 23.42.08 T1069.003 Permitsion Groups Discovery:Cloud Groups PM If Feb 05 23.41.09 PM T1059.003 Command and Scripting Interpreter:Windo PM If Feb 05 23.41.09 Fb 05 23.41.09 T1059.003 Command and Scripting Interpreter:Windo Command Shell		2 - Strapping	100
	Click the Clock ^(L) button to view the incident of the click Quick Click Quick to select the required for to see the incident details.		-	r a week)
G	Updated: Feb 16 12:10 AM Quick Last 1 Hour Relative Last 1 Day Absolute Last 1 Week	Last 2 Hours Last 4 Ho Last 2 Days Last 3 Day		day
	 Relative Click Relative to select the relative fields, and then click Go to see the 			lowing
	Updated: Feb 16 12:10 AM Quick From 4 Relative To Now Absolute	GO Hour(s) ago V Hour(s) ago V Day(s) ago V Week(s) ago Month(s) ago		🔟 💿 🛈 Last 1 day



Updated: Feb 16 12:10 AM Quick From Date Time Relative Absolute To Date Time Time Click the Right anchor button to expand and view the Groups, Available Systems, Sel Items panels, and the Left anchor button to collapse the panels. MITRE ATT84CK® Updated: Feb 16 04:30 AM Systems directed with MITRE data are displayed Systems Systems Syste		From		Specify the time range starting with which the incident details must be visible. This field accepts only integers			
I d and cannot be modified • Absolute Click Absolute to set an absolute time range by specifying the values in the From an fields along with the required Time (including hours, minutes and seconds), and the Go to view the incident details. MITRE ATT&CK® Click the Right anchor > button to expand and view the Groups, Available Systems, Sel Items panels, and the Left anchor < button to collapse the panels. MITRE ATT&CK® () and the Left anchor Items panels, and the Left anchor		Hour(s) ago Day(s) ago Week(s) ago		accordingly, c	accordingly, choose either hours, weeks, months,		
Click Absolute to set an absolute time range by specifying the values in the From an fields along with the required Time (including hours, minutes and seconds), and the Go to view the incident details.		То				et to the curren	t time
Click the Right anchor button to expand and view the Groups, Available Systems, Sell Items panels, and the Left anchor button to collapse the panels.		MITRE ATT&CK®				^ /	′ Dashboard / MITRE ATT C Ⅲ ⑥ ① La
Click the Right anchor be button to expand and view the Groups, Available Systems, Sel Items panels, and the Left anchor be button to collapse the panels.	l		From	ate 💼 Time			C 🖩 🖲 🕒 La
Items panels, and the Left anchor dution to collapse the panels.		Relative	-				
ANALABLE SYSTEMS SILCETO ITEMS			To	ate 🛅 Time	GO		
		Absolute	button to t anchor	o expand and vie button to col	ew the Grou lapse the pa	nels.	۲
0 EuropTractar		Absolute	button te t anchor	 expand and vie button to col Available Systems Search 	ew the Grou lapse the pa	Selected Items	Show



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.

MITRE ATT&CK® Updated: Feb 06 12:26 AM						
• Systems detected with MITRE data are displayed						
<	Sites					
GROUPS	ETTVBLA2022-01	*				
AVAILABLE SYSTEMS	•	×××				
SELECTED ITEMS	Group search Q	Q				
	All Groups					
	EventTracker					
	MICROSOFT365					
	MITREATTACK					
	NTPL.LOCAL					

- **a.** 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.
- **b.** 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.

>	Sites		
GROUPS	£771v8LA2522-01		~
AVAILABLE	Groups		Total: 4
SYSTEMS			
SELECTED	Group search	Q	Q,
	All Groups		
	EventTracker		
	MICROSOFT365		
	MITREATTACK		
	NTPL.LOCAL		

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.

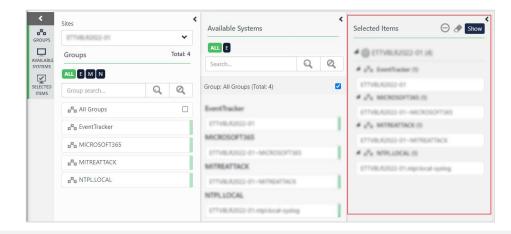
- **a.** Click **Available Systems** to view all the available systems of all the groups or select the required group to view all the available systems of the selected group.
- **b.** To search for a particular system, specify the system name in the Search field or click the hotkeys to search for the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

<	Sites	< ~	Available Systems	<
AVAILABLE SYSTEMS		Total: 4	ALL E Search Q	Q
SELECTED ITEMS	Group search	ର୍ ଷ୍	Group: All Groups (Total: 4)	
	All Groups		EventTracker	
	EventTracker		£77VBLA2522-01	
	■ MICROSOFT365	i	MICROSOFT365	
	MITREATTACK		(TTVB.A3522-01-MICROSOFT365 MITREATTACK	
	NTPL.LOCAL		ETTVBL/2022-01-MITREATTACK	

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** I button to clear the selections.
- c. Click the Collapse $^{\bigcirc}$ 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.

		ATT&CK® Fed 06 12:33 AM			
	-	detected with MITRE data are displayed			
	<		۲.		
	GROUPS	Sites ETTVBLR2022-01	~		
		Groups	Total: 4		
	AVAILABLE SYSTEMS				
	SELECTED ITEMS	Group search	Q		
	inclus	B ^B All Groups			
		EventTracker			
ilters		□□ MICROSOFT365	- i I		
			— i I		
		B NTPL.LOCAL	— i I		
				Filter 👻	
				Rule Name	C
				Technique Id	
	Filter •	,		rechnique to	୯
	Rule I	lame	C	Sub-Technique Id	ย ช
	Rule M		с С		



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.

ilter 🗸	
Rule Name	C
Abuse command and script interpreters to e	+ - 16.06%
Internal spearphishing to gain access on oth	+ - 8.22%
O365 Permission group discovery	+ - 8.22%
O365 Spearphishing link	+ - 8.22%
Collecting opened application windows info	+ - 7.09%
Collect or forward email from mail servers o	+ - 4.11%
O365 Account Discovery	+ - 4.11%
O365 Account Manipulation	+ - 4.11%
O365 Brute Force	+ - 4.11%
O365 Create user account	+ - 4.11%
	Moro

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.

=	MITRE ATT&CK®	↑ / Dashboard / MITRE ATT&CK®
٩	Updated: Feb 17 03:58 PM	C 🏢 💿 🕑 Last 1 day
R	Rule Name: Abuse command and X	
	Systems detected with MITRE data are displayed	



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

	Values for Rule Name		×	
	Search for field values	Q	Q	
	Abuse command and script interpreters to execute commands, scripts, or binaries			
	Dynamic Data Exchange to execute arbitrary commands			
	Include	xclude	Close]
c.	In the Values for Rule Name window, select the required filter cat the list and click Include or Exclude accordingly.	egory	detail	s from
d.	Click Close to close the window.			
Note:				
	ing the same process, you can filter the techniques for the followin, me, Technique ID, Sub-Technique Id, Technique Name and Sub-Tec	-	-	



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.

ATT&CK® techniques detected by system		-
	View By	Тор
	Technique Variety 🗸 🗸	10 🗸
) Suurbathium	
ettveskir22016-3- agent2, min2018 11s5-vm4- agent1, min2012+2		
🕒 hullhium-lestävis, detectionhullhium 🌑 m355-testävis, mitte 🜑 ethentik 22019-1 🜑 ethentik 22016-3-agent2	unin 2016 r1n5 mm4-agent1 mi	-2012-2
Feb 03 01:31 PM - Feb 17 01:32 PM		

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.

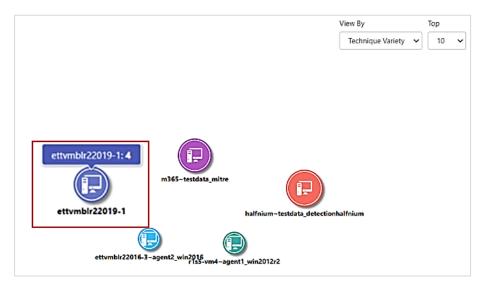
In the **Top** drop-down list, choose the number of systems you require to be displayed.

Note:

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

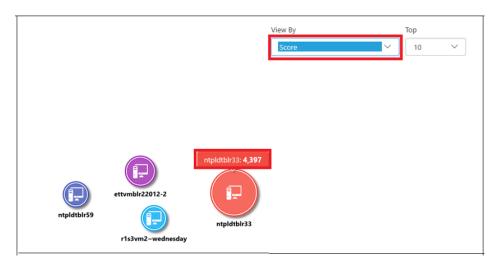


Hover over the bubble icon to view the details of the system name and number of threat attacks on that system.



Sample Image for Technique Variety

Sample Image for Score

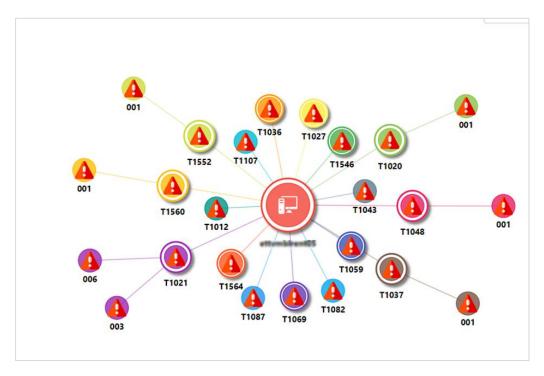


To view the count of a specific technique occurrences on a system,

- 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.



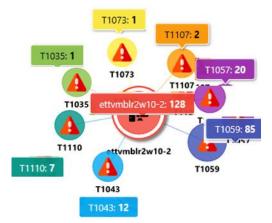
Example for a technique occurrence count.

- Select the system bubble **ettvmblr2w10-2**.
- The system name along with a score 128 will be displayed.

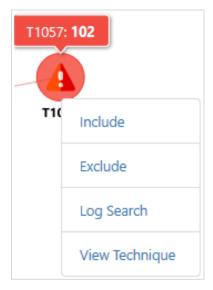
Note:

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 **ettvmblr2w10-2**.
- 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**, **c**lick on the technique bubble icon, and choose an action from the sub-list options:





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

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.

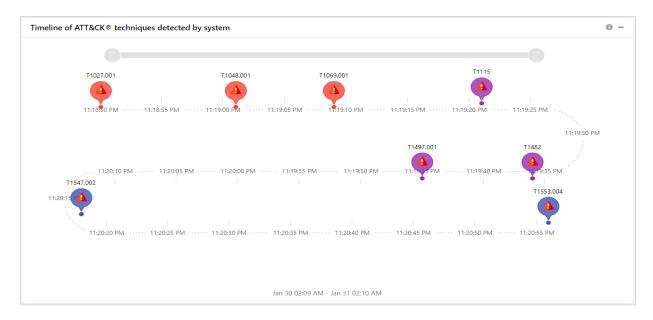
Note:

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.

			-0	
T1059.003				
	I I			

• 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.

ELASTIC				Netsurion
Duration: Feb 17 01:47:53 AM - Feb 17 01:47:54 AM Search criteria: 11059:003: Command and Scripting Interpreter/Windov Show Lucene query Lar filters event_computer: ettymb/22019-1 X	vs Command Shell		Add search to Q	1 O Gose
Top 10 (event_computer)	Top 10 (event_id)	Top 10 (src_user_name)	T	C op 10 (log_source)
ettymbir22019-1	3221	E system	eventtracker	

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).

T&CK [®] Navigat	or							0
		Score Range				_		
		1				100+		
						±	₹, ‡^ Ø	≎
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	Lateral Movement 9 techniques	Collection 17 technique
Drive-by Compromise	Command and Scripting	Account Manipulation (0/5)	Abuse Elevation Control	Abuse Elevation Control Mochanism	Adversary-in- the-Middle (0/3)	Account Discovery (0/4) Application Window	II Exploitation of Remote Services	Adversary-in- the-Middle (0/3)
xploit Public-	Interpreter (1/8)	BITS Jobs	Mechanism (0/4)	Mechanism _(0/4)	Brute Force (1/4)	Discovery	Internal	Archive Collected
Application	Administration Command	Boot or Logon Autostart	Manipulation (0/5)	Manipulation (0/5)	Credentials	Browser Bookmark Discovery	Spearphishing	Data (0/3)
external Remote Services	Deploy Container	Execution (0/14)	Boot or Logon Autostart	BITS Jobs	from Password I Stores (0/5)	Cloud Infrastructure	Lateral Tool Transfer	Audio Capture
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Execution (0/14) Boot or Logon	Build Image on Host	Exploitation for Credential	Discovery Cloud Service	Remote Service	Automated Collection
hishing (0/3)	Inter-Process	Browser	Initialization I Scripts (0/5)	II Deobfuscate/Decode	Access	Dashboard	Session Hijacking (0/2)	Browser Session Hijacking
Replication	Communication (0/3)		Create or Modify	Files or Information	Forced Authentication	Cloud Service Discovery	Remote	Clipboard Data
Through Removable Media	Native API Scheduled	Compromise Client Software Binary	System Process (0/4)	Deploy Container	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Services (2/6) Replication	Data from Cloud Storage
Supply Chain	Task/Job (0/5)	Create	Domain Policy Modification (0/2)	Domain Policy	Input	Container and	- Through Removable	Object
Compromise (0/3)	Shared Modules	Account (1/3)	Escape to Host	Modification (0/2)	Capture (0/4) Resource Discov		Media	Data from Configuration
rusted Relationship	Software Deployment Tools	Create or Modify System Process (0/4)	Event Triggered Execution (1/15)	Execution Guardrails (0/1)	Modify Authentication II Process (0/5)	Debugger Evasion Domain Trust	Software Deployment Tools	Repository (0/2)
/alid Accounts _(0/4)	System Services (0/2)	Event Triggered	Exploitation for	Exploitation for Defense Evasion	Multi-Factor	Discovery	Taint Shared	Information Repositories (0/3
(0/4)	User Execution (0/3)	Execution (1/15) External Remote Services	rnal Remote	e File and Directory Permissions	Interception I Multi-Factor	File and Directory Discovery	Content	Data from Loca System
	Windows Management Instrumentation					Group Policy Discovery	Use Alternate Authentication II Material (0/4)	
		Hijack Execution Flow (0/12)	Process	Hide Artifacts (1/10)	II Request Generation	Network Service	(0/4)	Network Shared Drive
		Implant Internal Image	Injection _(0/12) Scheduled	Hijack Execution Flow (0/12)	II Network Sniffing	Discovery Network Share		Data from Removable
		Modify	Task/Job (0/5)	Impair Defenses (0/9)	OS Credential	Discovery Network Sniffing		Media
		Authentication I Process (0/5)	Valid Accounts _(0/4)	Host (0/6)	st (0/6)			Data Staged _{(0/2} Email
		Office Application		Indirect Command Execution	Application Access Token	Password Policy Discovery		Collection (0/3)
		Startup (0/6)		Masquerading (1/7)	I Steal or Forge	Peripheral Device Discovery		Input Capture (0/4)
		Pre-OS Boot (0/5)		Modify Authentication Process (0/5)	Kerberos Tickets (0/4)	Permission Groups Discovery (1/3)	Ш	Screen Capture
		Task/Job (0/5)		Modify Cloud	Steal Web Session Cookie	Process Discovery		Video Capture
		Server Software		Compute		On the Desident		



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

Note:

ATT&CK® Navigator 0 -Score Range 100-± ╤, 12 ⊙ ≎ 💲 × Credential Access 16 techniques Privilege Escalation Lat Mov∉ Initial Access Execution Persistence Defense Evasion Discovery 13 techniques 9 techniques 12 techniques 19 techniques 42 techniques 30 techniques 9 tech II Drive-by Compromise opleScript II Adversary-in-he-Middle (n Account Discovery ₍₀ xploita lechanism (0/4) Mechanism (0/4) Application Window Exploit Public Facing Application rute Discovery Access Token Manipulation _{(0/5} Network Device CLI ccess Token Vanipulation (0/5) ot or Logon Itostart Spearph PowerShell ommand and Boot or Logon from Password Stores (0/5) Lateral 1 Transfer External Remo Services cripting terpreter , ecution (0/14) Execution (0/14) Boot or Logon Initialization ot or Logon Build Image on Host ripts _(0/5) Debugger Evasion for Credential Access Cloud Service Dashboard /isual Basic Phishing (0/3) Deobfuscate/Decode Files or Information Scripts (0/5) Cloud Service Windows Command She Create or Modify Remote Services Replication Through Discovery Deploy Container Compromise Client Software System Process _(0/4) Forge Web Credentials _{(0/2} Cloud Storage Object Administration Command Removable Media Replicat Through Remova Media Direct Volume Access Domain Policy Modification (0/2) Discovery Deploy Container Domain Policy Modification _(0/2) Input Capture _(0/4) Supply Chain Compromise _{(0/2} Create Account (1/3) Container and Resource Discovery Exploitation for Client Execution scape to Host II Software Deployn Tools Modify Create or Modify Trusted Relationship II Event Triggered Execution (1/15) System Process (0/4) Authentication Process (0/5) Guardrails (0/1) Domain Trust Discovery Inter-Process Inter-Process Communication (0/3) II Valid Accounts (0/4) Event Triggered Execution (1/15) Multi-Factor Authentication Interception Exploitation for Taint Sh Content II Native API File and Directory Discovery Privilege scalation File and Directory Scheduled Task/Job (0/5) II Use Alte External Remote ermissions odification (0/2 . Group Policy Discovery Hijack Execution Multi-Factor II low (0/12) Hijack Execution Flow _(0/12) Shared Modules Hide Artifacts Request Generation Network Service Discovery rocess njection (0/12) Software Deployment Tools Implant Internal Image Network Sniffing OW (0/12) Network Share Scheduled Ш П Impair Defenses , , , , a Task/Job (0/5 Discovery

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

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

T&CK [®] Navigat	or					6
	Score Range					
	1				100+	
					± =, 1₄ (D
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	Command and Scriptin II Interpreter (T1059) Score: 2100	Con	Abuse Elevation Control Mechanism _(0/4)	Adversary-in- II the-Middle (0/3)	Account Discovery Application Windo
Exploit Public- Facing	Interpreter (1/8) Container	BITS Jobs	▼ (0/4) To ten	Access Token	Brute Force (1/4)	Discovery
Application	Administration Command	Autostart	Manipulation (0/5)		Credentials	Browser Bookmark Discovery
External Remote Services	Deploy Container	Execution _(0/14) Boot or Logon	Boot or Logon Autostart	BITS Jobs Build Image on Host	from Password II Stores (0/5)	Cloud Infrastructure Discovery
Hardware Additions	Exploitation for Client Execution	Initialization II Scripts (0/5)	Execution (0/14) Boot or Logon	Debugger Evasion	Exploitation for Credential	Cloud Service
Dhishing	Inter-Process	Browcor	Initialization Scripts	Deobfuscate/Decode	Access	Dashboard



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

ATT&CK® Naviga	tor					9 -
	Score Ra	nge				
	1				100+	
				1	t , ↓ A ⊙	\$ \$ X
Initial Access 9 techniques		Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 technique
Drive-by Compromise		AppleScript	Account Manipulation (0/5)	Abuse Elevation Control	Abuse Elevation Control	Adversary-in- the-Middle (0/3
Exploit Public- Facing Application		JavaScript Network Device CLI	BITS Jobs	Mechanism (0/4) Access Token Manipruntion (0/5)	Mechanism (0/4) Access Token Manipulation (0/5)	Brute Force (1/4)
External Remote Services	Command and Scripting Interpreter (1/8)	PowerShell Python	A PowerShell (T1059.0 E Disabled (0/14)	Boot o Autost	BITS Jobs	Credentials from Password Stores (0/5)
Hardware Additions		Unix Shell	Initialization I Scripts (0/5)	Boot or Logon	Build Image on Host Debugger Evasion	Exploitation for Credential
Phishing _(0/3)		Visual Basic Windows Command She	Browser Extensions	Initialization Scripts _(0/5)	Deobfuscate/Decode Files or Information	Access Forced

• 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**.

T&CK [®] Navigator								0
	S	core Range						
		1			100	•		
						1 =	₹, ‡ <u>^</u> • • ≎	\$ X
Initial Access 9 techniques	Execution 12 technique		Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	La Mor 9 teo
Drive-by Compromise	Apples		AppleScript (T1059	002) ation	Abuse Elevation Control	Adversary-in- the-Middle (0/3)	Account Discovery (0/4)	I Exploi Remot
Exploit Public- Facing Application	Netwo	rk Device CLI	view technique view tactic log search	Access To ten Manipulation (0/5)	Mechanism _(0/4) Access Token Manipulation _(0/5)	Brute Force (1/4)	Discovery Browser Bookmark	Intern
External Remote	nmand and pting erpreter (1/8)		acknowledge Boot or Logon	Boot or Legon Autostart Execution 0/14)	BITS Jobs Build Image on Host	Credentials from Password I Stores (0/5)	Discovery Cloud Infrastructure Discovery	Latera Transf
Hardware Additions	Unix S Visual		Initialization I Scripts (0/5)	Boot or Logon	Debugger Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Remo Servic Sessio
Phishing _(0/3) Replication Through	Windo	ws Command Shell	Browser Extensions Compromise	Scripts (0/5 Create or Modify System	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Discovery	Hijack Remo Servic
Removable Adr	ninistration nmand		Client Software Binary	Process (0/4)	Deploy Container Direct Volume Access	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replic
Compromise (0/2)	oloy Container		Create Account (1/3)	Modification (0/2)	Domain Policy Modification (0/2)	II Input Capture (0/4)	Container and Resource Discovery	Remo Media
Trusted Clie Relationship	ent Execution		Create or Modify System Process (0/4)	Escape to Host Event Triggered Execution (1/15)	Execution Guardrails _(0/1)	Modify Authentication Process (0/5)	Debugger Evasion Domain Trust	Softw Deplo Tools

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



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 <u>https://attack.mitre.org/techniques/enterprise/</u>

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

T&CK® Navigat	or							6
		Score Range						
		1			100	D+		
						1 =	, ‡2 ⊙ ≎	\$×
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	L Mo 9 te
Drive-by Compromise		AppleScript	Account Manipulation (0/5)	Abuse Elevation Control	Abuse Elevation Control	Adversary-in- the-Middle (0/3)	Account Discovery (0,4)	I Exploi
Exploit Public-		JavaScript	BITS Jobs	Mechanism (0/4)	Mechanism (0/4)	Brute	Application Window Discovery	Servic
Facing		Network Device CLI		Access Token	Access Token	Force (1/4)	-	Intern
Application	Command and	PowerShell	Boot or Logon Autostart	Manipulation (0/5)		Credentials	Browser Bookmark Discovery	Spear
	Scripting	II Python	Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	from Password II Stores (0/5)	Cloud Infrastructure	Latera Transf
External Remote Services	Interpreter (1/8)				Build Image on Host		Discovery	

Ħ	Click Export to export the criteria/techniques to excel.
₹,	Click Filters . to filter the criteria/techniques according to the platforms.
<u>‡ </u> 2	Click Sort 12 to sort by alphabetical order or by score.
Θ	Click Hide/Show 💿 to either hide or show the criteria or detected techniques.
\$	Click expand sub-techniques $\stackrel{\clubsuit}{\circ}$ to view the sub-techniques of all techniques.
\$	Click expand annotated sub-techniques <a>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.

	RE ATT&CK®	MITRE ATT&CK® A / Dashboard / MITRE ATT&CK® / Act						/ Ackno	wled
							C 🎞	C Last	: 1 D
<	1 v of 1	Show Una	cknowledged	~				Tota	al: 5
	First Occurrence	Last Occurrence	Technique Id	Technique Name	Rule Name	Site Name	Computer	Score	A
+	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	ettvmblr22019-1	3	
+	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	ettvmblr22016- 3~agent2_win2016	2	
	Feb 17 13:07:36	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	ettvmblr22016- 3~agent2_win2016	1	
+	PM					ETTVMBLR22019-	r1s5-vm4~agent1 win2012r2	1	
+	PM 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	1	TISS-VIN4~agent1_WIN201212	1	

• 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 [ettvmblr2w10-2]	
 All [Abuse command and script interpreters to execute commands, scripts, or binaries] detections 	
○ All detections from [ETTVMBLR2W10-2] site	
O All [Abuse command and script interpreters to execute commands, scripts, or binaries] detections from [ettvmblr2w10-2]	
	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.

Net	surion						🔎 Admin v To	ools v	0
MITR	RE ATT&CK®					†	/ Dashboard / MITRE ATT&CK	/ Acknow	wledg
							C 🎞	🕒 Last	t 1 Day
		Show							
<	1 v of 1		knowledged	~				Tota	tal: 5
	First Occurrence		owledged	Name	Rule Name	Site Name	Computer	Score	Acl
+	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	ettvmblr22019-1	3	•
+	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	ettvmblr22016- 3~agent2_win2016	2	
+	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	ettvmblr22016- 3~agent2_win2016	1	
+	Feb 17 13:06:39 PM	Feb 17 13:06:39 PM	T1569.002	System Service:Service Execution	Dynamic Data Exchange to execute arbitrary commands	ETTVMBLR22019- 1	r1s5-vm4~agent1_win2012r2	2 1	
+	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	ettvmblr22019-1	3	

• 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 [ettymblr2w10-2]	
 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 [ettvmblr2w10-2] 	
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 <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