Abstract

This guide will help you use the capabilities of MITRE ATT&CK™ Matrix – Enterprise aligned with EventTracker v9.3 (all the EventTracker v9.3 editions except ETLM) 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.

Audience

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

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

The EventTracker MITRE ATT&CK™ framework matches Windows data

**Note:** This is not a User Guide for MITRE ATT&CK™ but it is a guide for using EventTracker with MITRE ATT&CK™
The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

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

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

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

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

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

1. What’s new in EventTracker v9.3 ............................................................................................................. 4
2. The MITRE ATT&CK™ Framework ........................................................................................................... 4
3. ATT&CK™ matrix with EventTracker ........................................................................................................ 4
4. Accessing MITRE ATT&CK™ in EventTracker ....................................................................................... 4
5. Options for viewing the techniques/incidents ........................................................................................... 7
   5.1 Dashboard view ................................................................................................................................. 7
   5.2 Tabular format view ............................................................................................................................. 8
6. Filtering in the Dashboard view ................................................................................................................ 9
7. Getting detailed information on a specific technique/incident ................................................................. 12
   7.1 ATT&CK™ techniques detected by system pane ................................................................................. 12
   7.2 Timeline of ATT&CK™ techniques detected by system pane ......................................................... 16
   7.3 ATT&CK™ Navigator Pane ............................................................................................................... 18
8. Acknowledging and Unacknowledging Techniques .................................................................................... 21
1. What’s new in EventTracker v9.3

EventTracker v9.3 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.

2. The MITRE ATT&CK™ Framework

The ATT&CK matrix by MITRE Corp., contains 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, EventTracker SIEM integrates the “Enterprise” domain knowledge base.

3. ATT&CK™ matrix with EventTracker

EventTracker 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™. EventTracker 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 EventTracker MITRE ATT&CK™ framework is enabled for EventTracker Admin, MSP, and Master MSP to monitor the IT infrastructure of multiple clients at the same time.


Using the MITRE ATT&CK™ framework within EventTracker, you can identify adversarial tactics, techniques and malicious threats within your network.

To access the MITRE ATT&CK™ integration in EventTracker,

1. Log into EventTracker, and the Home page opens.
2. Point to Dashboard, then click MITRE ATT&CK™.
MITRE ATT&CK™ Home page opens.

The default view which is the Dashboard view of the page displays color-coded icons and heat map representing the systems and the technique incidents.

The Dashboard view has three panes:

- **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 visualize defensive coverage. Layers can be created within the Navigator for comparison of techniques.
5. Options for viewing the techniques/incidents

You can view the incidents data in **Dashboard format** and in **Tabular format**.

### 5.1 Dashboard view

The Dashboard view is the default view.

- Click **Last 1 Day** tab, you can perform day-to-day analysis and visualization of attacks and techniques.

You have the options of viewing incidents based on time range - Quick, Relative, and Absolute.

- Click **Quick** to see the incidents occurred in minutes, hours or a week.

- Click **Relative** to view incidents time interval by entering values in the boxes.
Click Absolute to view incidents using the calendar dialogue by entering From and To data ranges and times.

Figure 6

5.2 Tabular format view

Click view Tabular on the upper right corner to view the data in Tabular form.

You will see column titles with technique attack details listed across the top First Occurrence, Last Occurrence, Technique ID, Title, computer, Score, Ack in the Tabular form.

Figure 8
6. Filtering in the Dashboard view

Filters in the MITRE ATT&CK™ dashboard are an effective way to detect common and relevant techniques and logs.

You can filter the incident data by two categories – Titles and Technique ID.

The Filter drop-down list allows you to filter on Title or Technique ID.

![Figure 9](image)

When you select Title by clicking +, the Title is added as a filter, and all the incidents associated with this category are displayed.

![Figure 10](image)
You can also filter the incident data by Title category by clicking **View field value**.

- **Values for Title** window opens.
- Select the titles in the list by checking on the boxes.
- Click **Include**, if you want to look at details of the incidents.
- Click **Exclude**, if you want to move on to next incidents.
- Click **Close**, to close the **Values for Title** window.

When you select **Technique ID** by clicking +, the **Technique ID** is added as filter, and all the incidents associated with this category are displayed.
You can also filter the incident data by Technique ID category by clicking **View field value**.

- **Values for Technique ID** window opens.
- Select the IDs in the list by checking on the boxes.
- Click **Include**, if you wish to look at details of the incidents.
- Click **Exclude**, if you wish to move on to the next incidents.
- Click **Close**, to close the **Values for Technique ID** window.
7. Getting detailed information on a specific technique/incident

7.1 ATT&CK™ techniques detected by system pane

The upper pane of the Dashboard provides a graphical representation of the systems/computers in the form of bubble icons.

Click View By drop-down list to classify/view/sort the computers based on Technique Variety or Threat Score.

Similarly, in the Top option to choose the number of computers to be displayed.

By default, values Technique Variety and 10 are selected.

Figure 17
When you hover the mouse on the bubble, you will see the **system name** and the **number of threat attacks** on that system.

![Diagram](image)

**Figure 18**

When **Score** is selected in the **View By** drop-down list to classify/view/sort the computers and hovering the mouse on the bubble, you will see the **system name** and the **threat score** for that system.

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

![Diagram](image)

**Figure 19**
To view the count of a specific technique occurrences on a system:

- Click on the bubble icon, all the **technique hit occurrences** for that system/computer appears.
- A sub list option **Include** or **Exclude appears**.
- Click **Include** if you want to know more about the technique attack/hits on the computer. **Note:** Clicking **Include** will add the computer name in the Filter. All the incidents associated with this system are displayed.
- Click **Exclude** to exit out of that computer and move on to the next computer.

![Figure 20](image)

Example of a technique occurrence count.

To understand the technique occurrences counts.

1. Select the system bubble **ettvmlbr2w10-2**.
2. The system name along with a score 128 is displayed.  
   **Note:** The score calculation is based on the hits of the detected techniques
3. You will see the bubble expands into nested bubbles. Each nested bubble has a Technique ID.  
   There are 7 nested bubbles, which mean there are 7 different adversary techniques attacking the system **ettvmlbr2w10-2**.
4. The nested bubble will further expand to show the number of hits for every Technique ID.
5. You will notice that 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:

- **Include**.
- **Exclude**.
- **Log search**.
- **View Technique**.

- **Include**: Click **Include** to know more about the technique attack/hits on the computer
  
  **Note**: Clicking **Include** will add the computer name/technique to the Filter. All the incidents associated with this system are then displayed.

- **Exclude**: Click **Exclude** to exit out of that technique and move on to the next computer.

- **Log search**: Click **Log search**, EventTracker log search page opens.

- **View Technique**: Click **View Technique**, MITRE technique page opens. This page contains all the information associated with the selected Technique ID.
https://attack.mitre.org/techniques/T1057/
Follow the link to know more about the MITRE ATT&CK’s predefined technique.
https://attack.mitre.org/techniques/enterprise/

7.2 Timeline of ATT&CK™ techniques detected by system pane

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.

The technique hits and time are represented in the form of color-coded heat map.

Each pin represents the time of the attack and the interval line following the pin is the duration/interval of the attack.

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

By default, you see all the attacks plotted on the computers 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 for more detailed viewing.

You can choose to see technique/incident details based on system.
By clicking Include you choose these actions in the ATT&CK™ techniques detected by system pane.

![Timeline of ATT&CK™ techniques detected by system](image)

**Figure 25**

You can choose to see technique/incident details based on Technique ID.

By clicking Include you choose these actions.

Click include on the technique bubble you want to view in the ATT&CK™ techniques detected by system pane, to see the selected technique.

![Timeline of ATT&CK™ techniques detected by system](image)

**Figure 26**

Basic details about the technique are displayed when you hover the mouse on the interval line.
To know more about the technique, click on the pin or the interval line. The log search page then opens.

Figure 28

7.3 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 has displays 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. (100 is most threatening)
When you hover the mouse on each technique, you will see the Technique ID, e.g. T1057 and the threat score.

When you click on a technique you get an options list: view technique, log search and Acknowledge.

Click Log search, EventTracker log search page opens.
**Note:** Clicking the computer name will add it to the Filter. All the incidents associated with this computer are displayed.

- **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/T1057/

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

- To sort by alphabetical order or by score, click icon [A]

- Click the [icon] icon to Hide/Show criteria/techniques.
8. Acknowledging and Unacknowledging Techniques

You can acknowledge and unacknowledge Techniques from the Tabular view or from the navigator.

From ATT&CK™ navigator page, when you click on a highlighted technique you get an option to Acknowledge.

Click Acknowledge, The EventTracker Acknowledge page opens.

To Acknowledge the techniques:

- Select the Ack check box \(\square\) to acknowledge the Techniques. The Acknowledge wizard appears when the Ack check box is clicked. Based on the user selection Techniques are acknowledged.

- In the Notes box you can write comments and choose an option from the list. Click OK to acknowledge.

  **Current selection only**: Acknowledges the selected item.

  **All detections from [Name of the System/computer]**: Acknowledges all detections from the identified system/computer.

  **All [MITRE T1059: Command Line Interface] detections**: Acknowledges all detections of the identified technique (in this example T1059) irrespective of the machines.
All [MITRE T1059: Command Line Interface] detections from [Machine Selected]: Acknowledges all detections of the identified technique (in this example T1059) on the machine selected.

To unacknowledge the Technique.

In the Show dropdown list choose unacknowledged. All the unacknowledged technique attack details appear. Based on the user selection Techniques are unacknowledged.

Figure 35

○ Select the Ack check box to unacknowledge the Techniques. The Acknowledge wizard appears when the Ack check box is clicked.

Figure 36

○ In the Notes box you can write comments and choose an option from the list. Click OK to unacknowledge. Based on the user selection Techniques are unacknowledged

**Current selection only**: Unacknowledges the selected item.

**All detections from [Name of the System/computer]**: Unacknowledges all detections from the identified system/computer.

**All [MITRE T1059: Command Line Interface] detections**: Unacknowledges all detections of the identified technique (in this example T1059) irrespective of the machines.
All [MITRE T1059: Command Line Interface] detections from [Machine Selected]:
Unacknowledges all detections of the identified technique (in this example T1059) on the machine selected.