Lifecycle for February - **EOL:** 3.3 Linux, 3.4 macOS, 3.5 Windows. EOS: 4.3 Windows and Linux.
Lifecycle for March - EOL: 3.6 macOS

SentinelOne Guide

W

Articles in this section

Search

Storyline in Deep Visibility

Shira Rosenfeld
Updated 16 days ago

Follow

Storyline from version Kauai, or TrueContext ID in Jamaica and earlier versions, is an ID given by SentinelOne to a group of related events, based on the intelligent event query engine. Query by Storyline to see only the detections related to the specific threat or IOC. When you find an abnormal event that seems relevant, use the Storyline to find all related events.

Storyline lets security analysts understand the full story of what happened on an endpoint. Use it to hunt easily, see the full chain of events, and save time for your security teams.

To use a Storyline in a query if you have the ID:

1. In **Visibility**, enter a query with this syntax:

```
SrcProcStorylineId = "<Storyline ID>"
```

For Example: `SrcProcStorylineId = "0D94A18F8B06C5DE"`

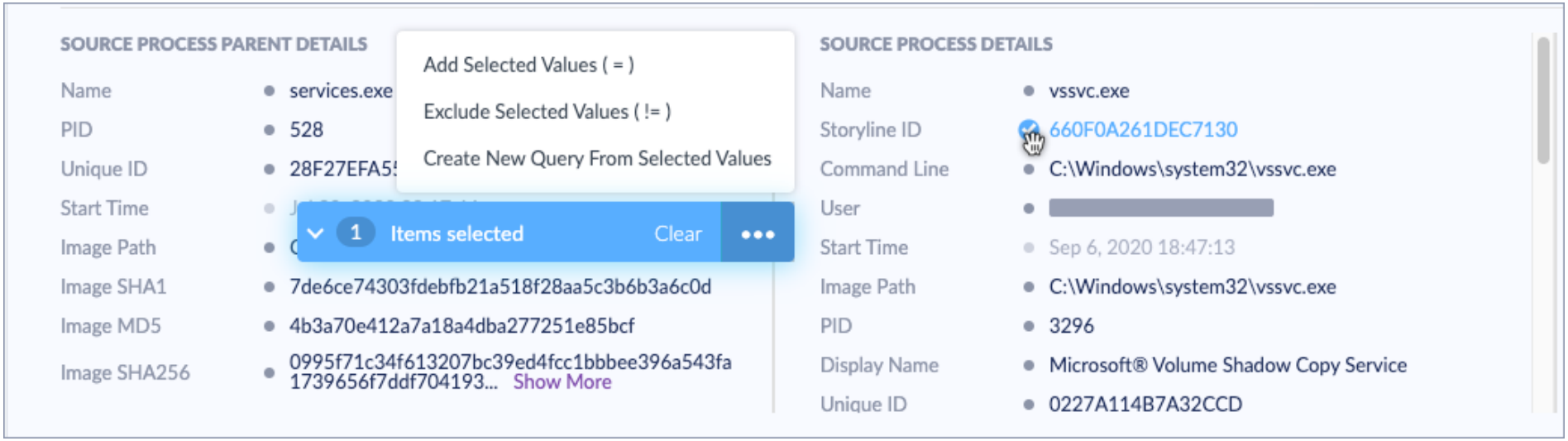
2. Select a time period and press Shift + Enter to run the query.

To use a Storyline ID from a query result:

1. In **Visibility**, run a query. In the query results, click a line to expand it.

   You can run a preset query from the Deep Visibility view to get started.

2. Move the mouse over an attribute to open a floating menu bar.



Tip: Drag the floating menu bar to move it to a convenient place on your screen.

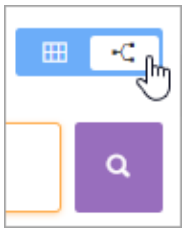
3. Click the three dots (ellipses) to open the menu. Select the option to use the Storyline in a new query.

   The storyline is added to the new query. For example:

   ```
   SrcProcStorylineId = "0D94A18F8B06C5DE"
   ```

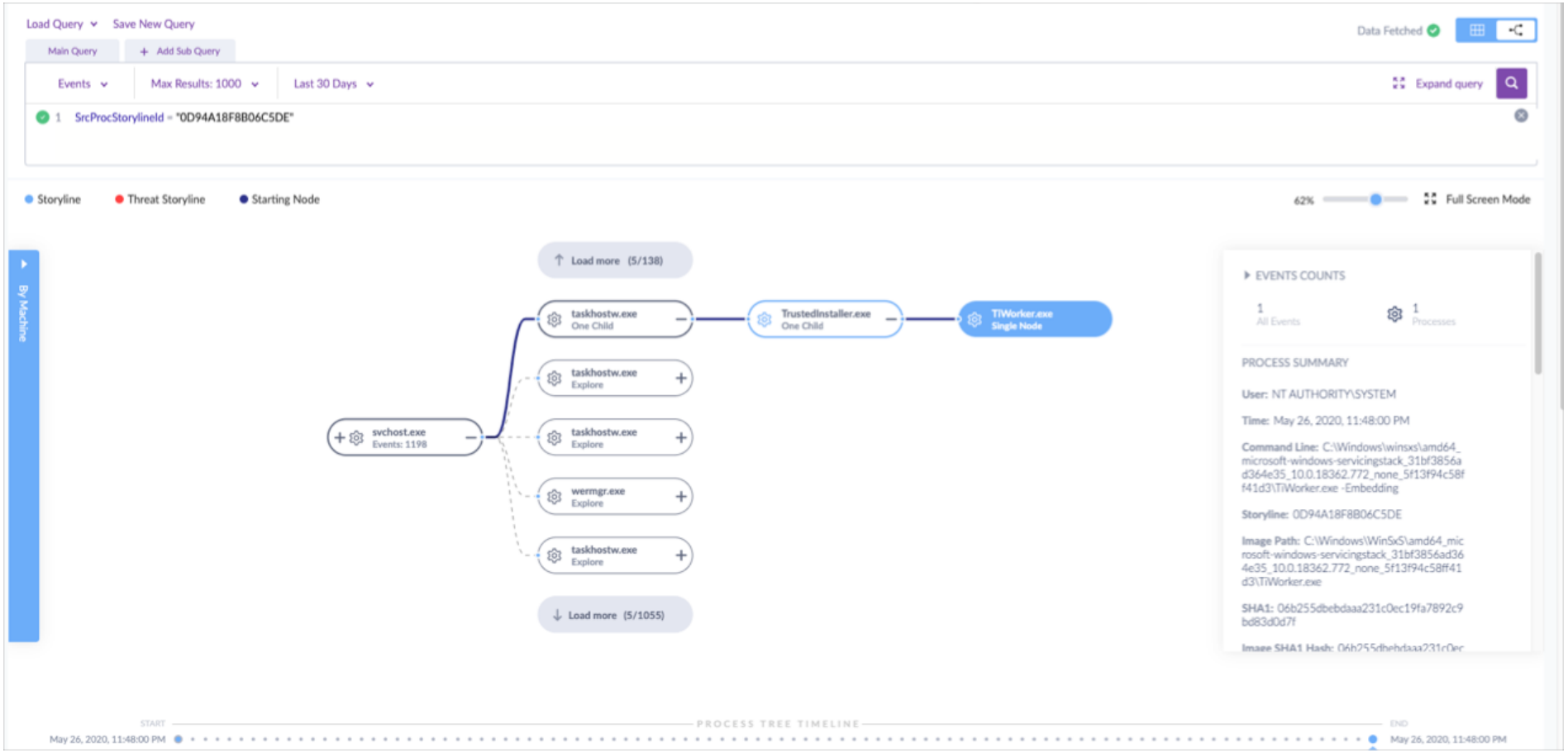
4. Select a time period and press Shift + Enter to run the query.

5. The results show in a table, automatically filtered by time. Click the process tree toggle to change to a graphic view.



6. Select the endpoint and process to see in the tree.

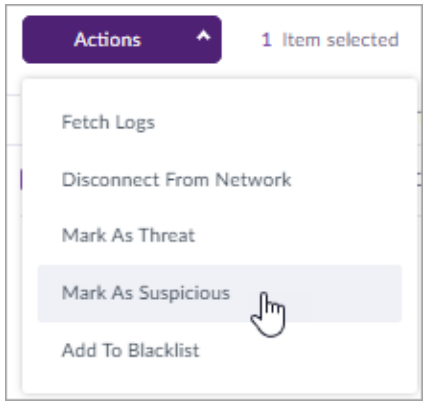
   The events of the selected node also show in the table below the tree.



In this example, we expanded the process tree to show the originating process of the node that we started from. The starting node and the line of the Storyline show in dark blue.

We see the chain of events: svchost.exe ran taskhostw.exe, which ran TrustedInstaller.exe, which ran TiWorker.exe.

In the table below the process tree, we can select events and mark them as malicious or suspicious. We can then mitigate the whole Storyline from **Incidents** > **Threats**.



To run a Deep Visibility query from the Storyline of a threat:

Pivot from the Storyline of a threat in the Forensic details directly to a query for that Storyline in Deep Visibility.

1. In **Incidents** > **Threats** > Forensic details, in the Threat Information, click the Storyline ID and select **Open in Deep Visibility**.

2. The Deep Visibility view opens in a new tab.

3. Select a time period and press Shift + Enter to run the query.

These KB articles might be helpful:

- Storyline for Threats

Related articles

- Configuring Deep Visibility Data Collection
- Storyline for Threats
- Query Types - Deep Visibility 3.0
- Deep Visibility Query Syntax
- Operators

Recently viewed articles

- Storyline for Threats
- Active EDR with Storyline
- Architecture
- Ranger Overview
- Ranger

Was this article helpful?

Yes No

0 out of 0 found this helpful

Comments

0 comments

Sort by

W

Be the first to write a comment.