Our April 15, 2019 release of the PSC includes:

CB ThreatHunter

These changes are live in all production environments as of April 15, 2019.

Carbon Black, Inc. | 1100 Winter Street, Waltham, MA 02451 USA | Tel: 617.393.7400

CB ThreatHunter

Simplified search results on the Investigate page

The **Investigate** page search operates on data that is submitted by PSC sensors that is combined and delivered in five minute increments. The search results operate on this combined data and sometimes return redundant segments that describe similar behavior for the same process.

CB ThreatHunter has optimized the search results to return a smaller, more relevant set of results for each process. Generally, the only results you should see are:

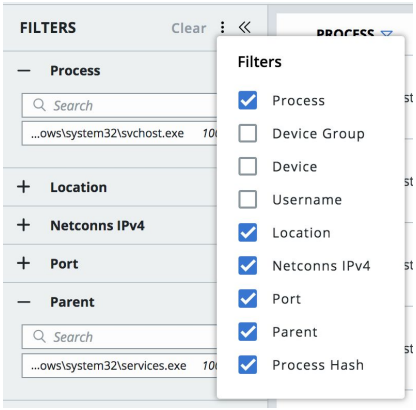
- One result for the latest observed event.
- One or more results for the latest analytics results.
- One result for each time a sensor observes a sensor_action (TERMINATE or BLOCK).
- One result for each time that CB ThreatHunter matched a sensor event against an organization's subscribed Watchlists.

The expected reduction in the number of returned search results depends on the lifetime and behavior of the process.

Configure filters

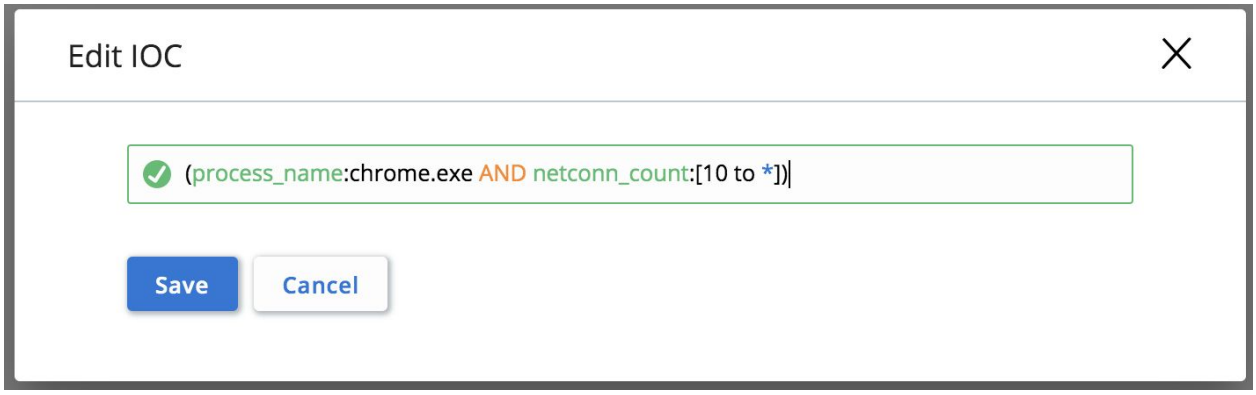
The **Investigate** page includes a set of filters that are set by default to be appropriate for expected customer usage. However, some customers use the search in other ways; they need to show or hide certain filters to make their workflow more efficient.

The **Investigate** page now includes a convenient way to select filter categories. After they are set, these selections persist across sessions in the same browser.

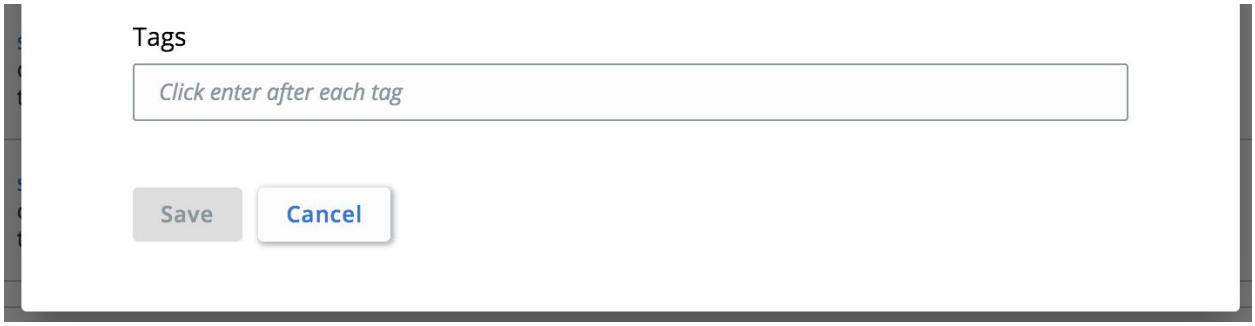


Also in this release

- Added ability to sort by process name on the **Investigate** page.
- Updated **Search Basics** content in the **Search Guide** on the **Investigate** page.
- Added a progress bar to the **Process Analysis** page events table. This provides a visible progress indicator when you are loading a process that has a large number of events.
- Added syntax validation and syntax highlighting when editing an IOC on the **Watchlist** pages:



- Added confirmation requirement to the **Watchlist** pages when a user tries to delete a threat report.
- Removed invalid actions from the **Watchlist Threat Reports** details page **Actions** menu.
- Added placeholder text in the **Tags** textbox of **Add Query** to clarify how to create Threat Report tags.



Fixed in this release

Issue ID	Description
DSER-13239	Error message from **Investigate** search was confusing when no data exists.
DSER-13405	On **Investigate** page, selecting a custom time for a single day caused a search for 12pm-12pm.
DSER-14295	**Process Analysis** page filtered out certain filemod events from the Events table.
DSER-14667	Search Guide content on **Investigate** page for process_original_filename had a misspelling.

Known issues

ID	Description
TPLAT-6201	**First seen as** field on the **Binary Details** page (and from the API) does not return paths in prevalence order; therefore, it is not possible to guarantee the actual first seen instance.
DSER-10685	Text remains in **Investigate** search bar if user navigates away and uses navigation **Investigate** option return to the **Investigate** page
DSER-11445	Hovering the mouse on a **Investigate** search filter hides the percentage values.
DSER-11662	After a user deselects a selected filter on the **Investigate** page, an otherwise-empty search still displays search results.
DSER-12453	ThreatHunter Watchlist tags do not show up on the **Notes/Tags** tab of the **Alerts** page — these are a different type of tag data.
DSER-13177	The **User Guide** is missing from the **Help** menu for organizations that subscribe to CB ThreatHunter.

DSER-13295	For processes that have a very large number of events, the **Process Analysis** page for that process can be manually reloaded to load additional events until the query is completed in the background.
DSER-13404	When you open/reload any page in the PSC UI and looks at the API calls, you see broken healthCheck calls that are safe to ignore.
DSER-14090	If CB Defense is enabled on the PSC with WSC integration enabled, and you remove CB Defense, the WSC integration is not disabled.
DSER-14295	Specific filemod events are filtered out from the **Process Analysis** page. This is *only* filemods where a process that opened a file with write access did not perform any changes and then closed the file.