

Our April 29, 2019 release of the PSC includes:

#### *CB Defense*

- [Fixed in this release](#)

#### *CB ThreatHunter*

- [Value Search](#)
- [Fixed in this release](#)
- [Known issues](#)

#### *CB LiveOps*

- [Fixed in this release](#)

# Carbon Black.

## CB Defense

### Fixed in this release

Issue ID	Description
DSER-15073	Fixed an issue where, after resetting 2FA, the QR scan screen was not appearing.

## CB ThreatHunter

### Value search

*Note: this feature was documented as "coming soon" in the March 2019 Release Notes.*

- For many search fields, you can now search without having to specify the field name; for example, searching for "chrome.exe" previously returned an error, but now searches across all fields where a filename is relevant.
- Fields include all fields with "process", "proc", "reputation" and "hash" in their name, netconn\_ipv4, netconn\_ipv6, TTP, sensor\_action and crossproc\_action.
- This capability is available in both **Investigate** and **Process Analyze** search.

*Previously:*

INVESTIGATE

❗ chrome.exe|

A field was given without a corresponding value. Your query is invalid. Ensure a value is included and slashes, colons, and spaces are manually escaped.

# Carbon Black.

Now:

**INVESTIGATE**

✔ chrome.exe

**9704 results** Showing 543. Refine search to view additional results.

**FILTERS** Clear <<

— Process

...e\application\chrome.exe	98.0%
...\update\googleupdate.exe	0.4%
c:\windows\explorer.exe	0.3%
...ows\system32\svchost.exe	0.2%
SYSTEM	0.2%
...ows\system32\taskmgr.exe	0.2%

**PROCESS**

---

chrome.exe

c:\program files (x86)\google\chrome\application\chrome.exe

---

chrome.exe

c:\program files (x86)\google\chrome\application\chrome.exe

## Fixed in this release

Issue ID	Description
DSER-12783	(Unknown) in <b>Investigate</b> results is ambiguous and has been replaced with "---" to designate that no event counts are available.
DSER-13205	<b>Watchlists</b> and <b>Investigate</b> pages never stop requesting search results.
DSER-13337	Threat Report was deleted but still appeared in the Watchlist Details API response.
DSER-14091	Syntax highlighted mis-highlights; for example, "OR" in REP_IGNORE in <b>Investigate</b> search bar.
DSER-14586	Red error toast message in <b>Investigate</b> page after API returns partial results and stops retrying.
DSER-14731	Watchlist <b>Description</b> field is required by API but not in the <b>Watchlist</b> pages UI.

# Carbon Black.

DSER-14831	Adding IOC to existing Report via <b>Investigate</b> page replaces existing IOC, rather than appending a second IOC to the Report
------------	---

## Known issues

---

ID	Description
TPLAT-6201	<b>First seen as</b> field on the <b>Binary Details</b> 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 <b>Investigate</b> search bar if user navigates away and uses navigation <b>Investigate</b> option return to the <b>Investigate</b> page.
DSER-11445	Hovering the mouse on a <b>Investigate</b> search filter hides the percentage values.
DSER-11662	After you deselect a selected filter on the <b>Investigate</b> page, an otherwise-empty search still displays search results.
DSER-11904	Count of devices with hash on the <b>Process Analysis</b> page, is different than count of devices on the <b>Investigate</b> page.
DSER-11959	When user types "-" or "+" then accepts a suggested search field name, the + or - character is removed from search bar on the <b>Investigate</b> page.
DSER-12453	ThreatHunter Watchlist tags do not show up on the <b>Notes/Tags</b> tab of the <b>Alerts</b> page — these are a different type of tag data.
DSER-12538	<b>Binary Details</b> page crashes when UBS APIs return unexpected output.
DSER-13061	Feed API "replace reports" API call responds with 500 when it should send 400.
DSER-13177	The <b>User Guide</b> is missing from the <b>Help</b> menu for organizations that subscribe to CB ThreatHunter.
DSER-13271	No field descriptions/examples in many suggestions for search fields on <b>Process Analysis</b> page.

# Carbon Black.

DSER-13283	When you search for Reports for a new Watchlist, you cannot access/add a Report that was returned by the search.
DSER-13295	For processes that have a very large number of events, the <b>Process Analysis</b> page for that process can be manually reloaded to load additional events until the query is completed in the background.
DSER-13636	Facets do not update when you navigate away from the <b>Investigate</b> page and then navigate back.
DSER-13773	Watchlist link still showing on <b>Process Analysis</b> page side panel after Watchlist is deleted.
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-14148	When <b>Investigate</b> search bar overflows to multiple lines, user cannot use keyboard navigation or selection.
DSER-14276	When user deletes a custom Watchlist from enabled <b>Watchlists</b> page, results section of page reports "no watchlists enabled".
DSER-14758	Searching by device_internal_ip returns no results for CBTH-native events on the <b>Investigate</b> page.
DSER-14764	For an organization that only uses ThreatHunter, the CB Defense icon still appears in the Explorer tray and the Programs List.
DSER-14832	When there is only one device_group available, the /results API does not return device_group and the Device Group filter group disappears from the <b>Investigate</b> page.
DSER-15013	Rule Preview links show inconsistent result counts when you use wildcards on the <b>Policies</b> page.
DSER-15052	More Watchlist Notification emails sent than number of Watchlist Hits or Alerts.
DSER-15187	"process_publisher" searches on the <b>Investigate</b> page lead to signed and unsigned binaries.
DSER-15385	Result count drops and rises when changing filters or terms on <b>Investigate</b> search.

# Carbon Black.

DSER-15386	When user deletes the last Report in an enabled Watchlist, the <b>Reports</b> tab on <b>Watchlists</b> page shows all available reports rather than "No Reports for this Watchlist".
------------	--



## Fixed in this release

---

Issue ID	Description
DSER-15344	<b>Learn more</b> links in Recommended Queries displayed as "null" when there was no related link.
DSER-15160	The OS icons in the <b>Query Builder</b> table did not always match the osquery schema, thereby causing confusion.