This release focuses on improving role-based access control capabilities across the platform to give administrators granular control over user roles, as well as improving CB ThreatHunter to make searching for anomalies in your environment as easy as possible.

Our March 2019 release of the PSC includes:

PSC

- Customizable roles - open beta
- Onboarding widget to help set up the PSC

CB Defense

- Easily identify outdated AV signature packs
- Reduced focus on observed activity
- Fixed in this release
- Known issues

CB ThreatHunter

- Event search on Process Analysis page
- Search enhancements: value search
- Search enhancements: syntax highlighting
- Watchlists on the Process Analysis page
- Reputation on the Process Analysis page
- Also in this release
- Fixed in this release
- Known issues

CB LiveOps

- macOS enablement

CB ThreatSight

- Configure settings for CB ThreatSight report recipients

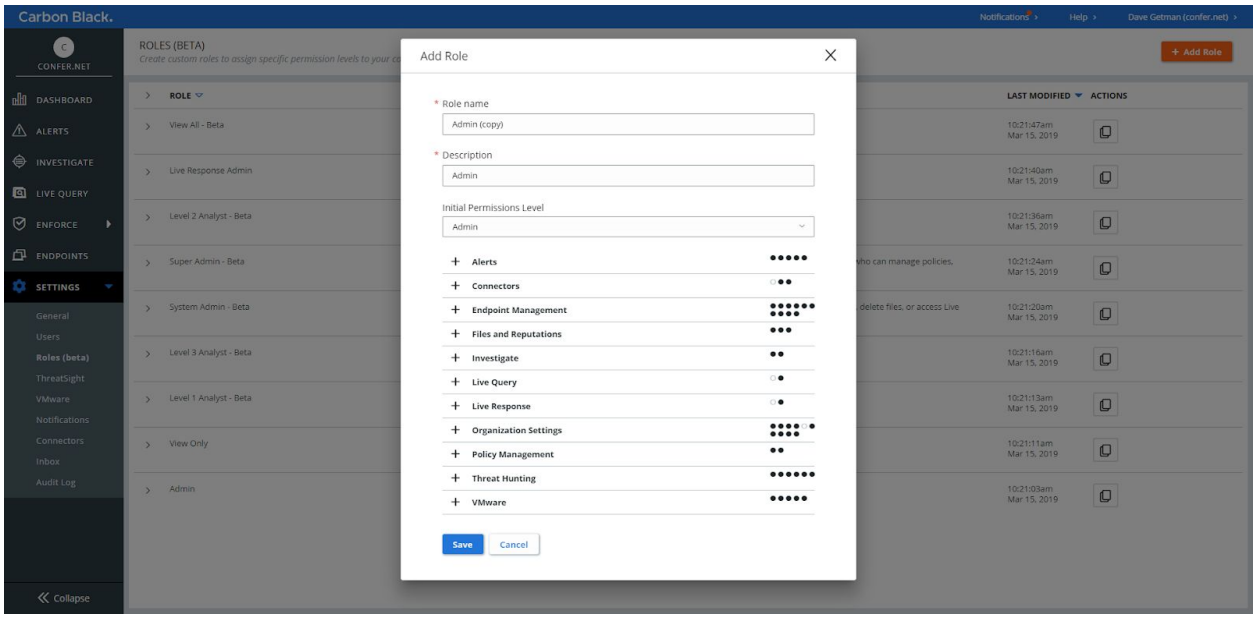
We'll start rolling out these changes the fourth week of March 2019.

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

Carbon Black.

Customizable roles - open beta

You can create your own roles. You can duplicate existing roles to add or remove permissions, resulting in roles that are a better fit for your needs.



New custom roles continue to enforce least privilege. Users who have the **Manage User** permission can only manage users who have the same or lesser permissions than themselves. Users who have the **Manage Roles** permission can only create roles by using the permissions they already have. Learn more here.

Update to Beta Roles: The **View All** beta role has **View Live Query** permission with the 0.45.0 release, keeping it consistent in its ability to view all pages, but take no action.

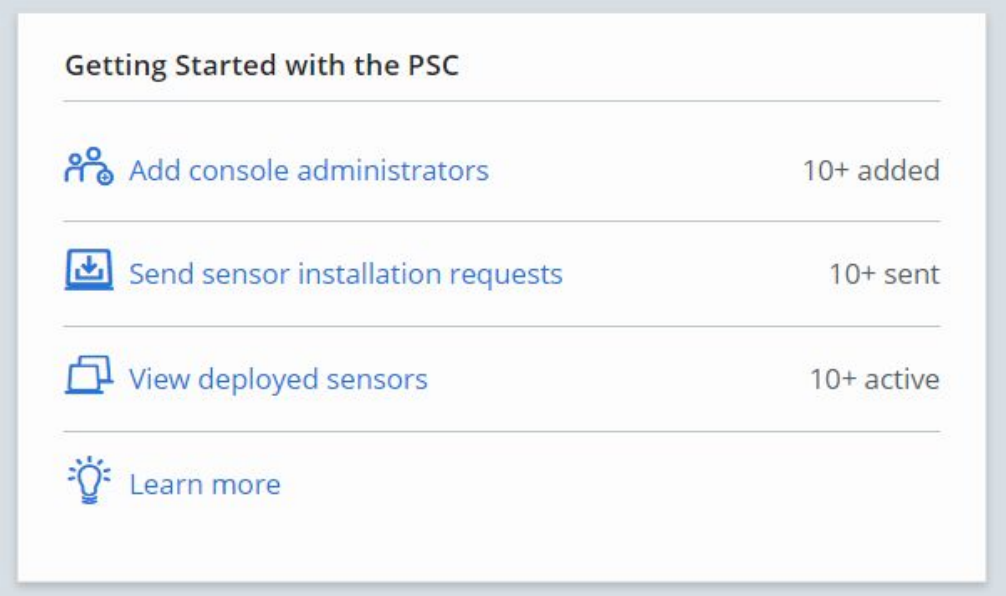
Carbon Black.

Onboarding widget to help set up the PSC

A new Dashboard widget can help you set up the PSC quickly to get data flowing into your console. The widget dynamically updates as you:

- Add administrative users
- Send installation requests via email
- Install sensors

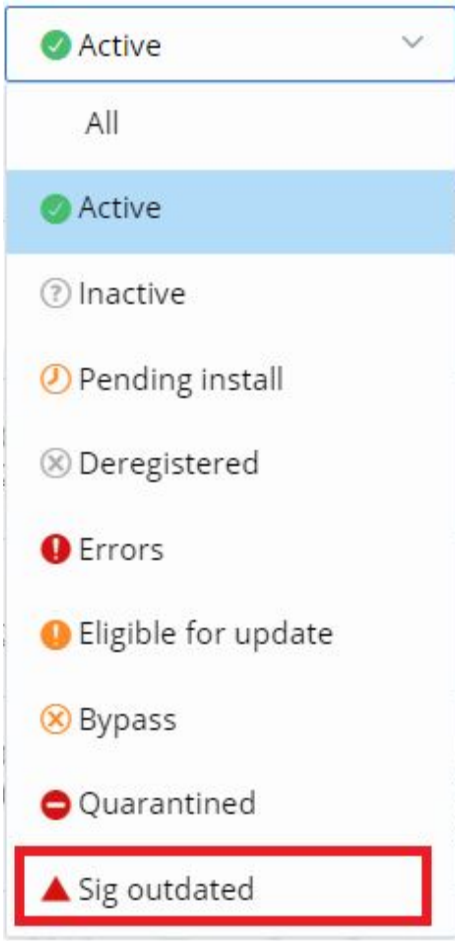
It also includes a link to learn more by navigating to the User Guide.



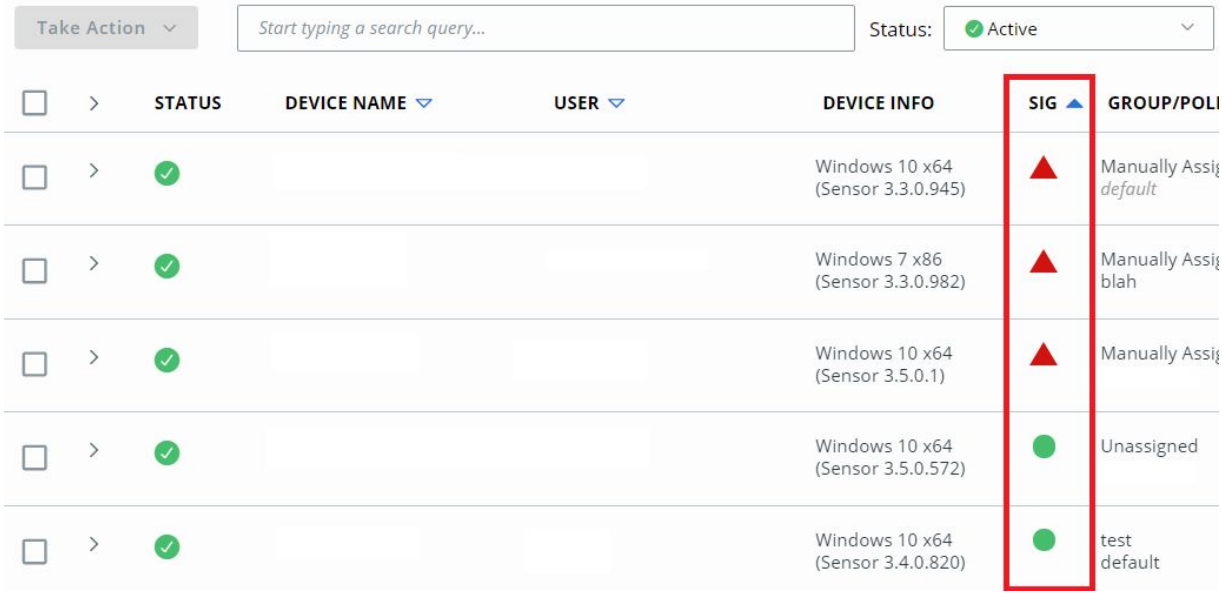
CB Defense

Easily identify outdated AV signature packs

We've added a new status type on the **Endpoints** page that is called **Sig outdated**. Filtering on this status allows you to quickly find sensors (Active, Bypass, Quarantined, Eligible for update) whose AV Signature packs have not updated in the last 7 days. On the **Policies** page, you can make administrative updates to the frequency with which your AV Signature packs update.



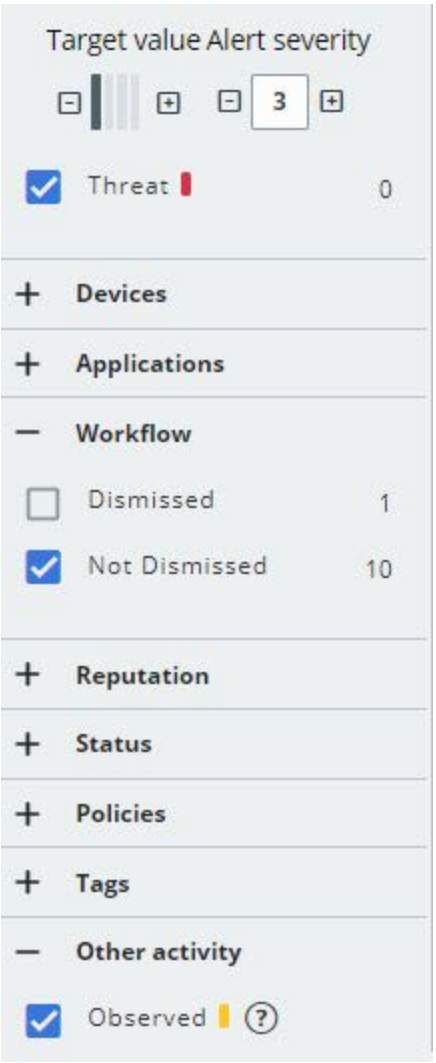
We've added a **SIG** column to the **Endpoints** page, which you can use to sort by updated or out-of-date signature packs. Sorting on this column displays sensors in the order in which their AV signature packs have updated. By using this technique, you can drill down into sensor details by filtering on sensor status, or by searching for other sensor details (for example, operating system or sensor version).



Carbon Black.

Reduced focus on observed activity

To help you focus on the highest priority alerts, we renamed the **Monitored** alert types to **Observed**. On the **Alerts** page, observed activity now exists in its own filter panel labeled **Other Activity**, and is unchecked by default. You can view this data by checking the filter box.



Fixed in this release

Issue ID	Description
DSER-14097	All CB Defense emails, including user invitations and send installation requests, are now sent from “noreply@carbonblack.com” instead of from “cloud@confer.net”.
DSER-7403	Fixed an issue where, when exporting large data sets from the UI, if the export took longer than 60 seconds, no data was returned.
DSER-10275	Fixed an issue where Live Response sessions took up to 30 seconds to initiate.
DETECT-3	Fixed a false positive detection that was causing excessive monitored alerts when Microsoft Office applications invoked Microsoft-approved helper applications to cache documents.
DETECT-154	Fixed a false positive detection that was causing excessive alerts on ransomware-related activity from native Windows applications.
DETECT-432	Improved ability to detect certain types of system, security, and network registry modifications.
DSER-10888	Fixed an issue where GET CURL requests to our Connector APIs were failing.
DSER-11040	Fixed an issue where Live Response `EXECFG` commands were not parsing quotes and whitespace properly.

Known issues

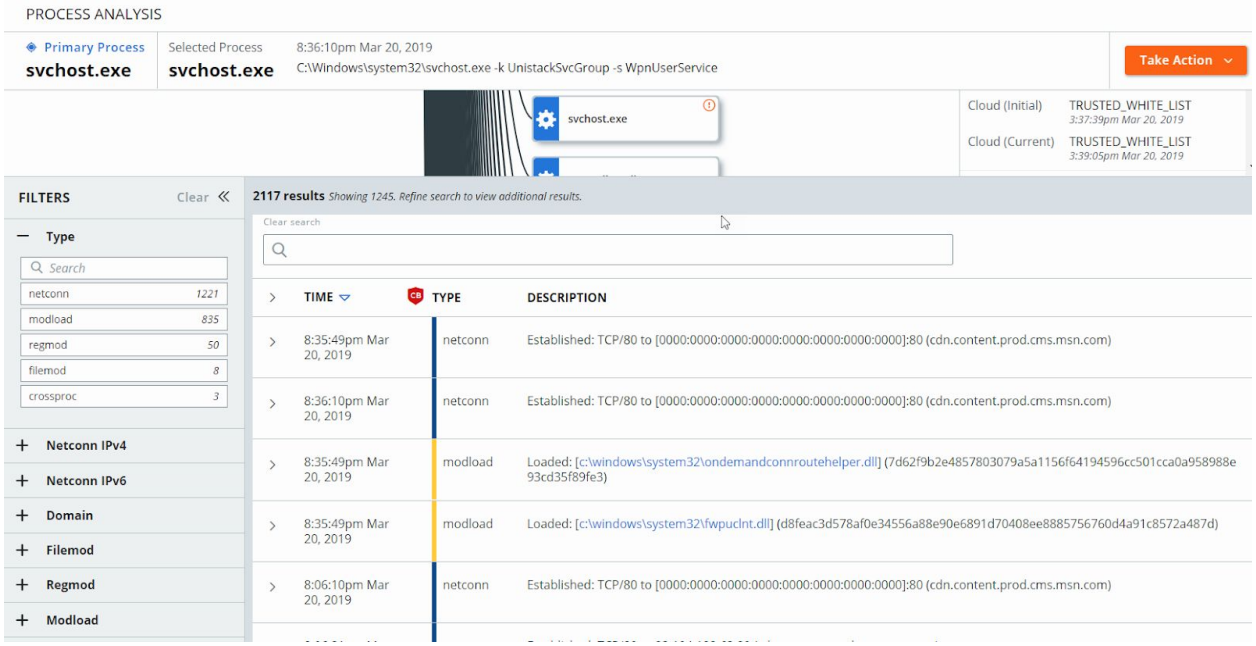
ID	Description
DSER-4390	Some sensors that should be **Eligible for Upgrade** are not marked as such.
DSER-5437	Additional markup is added to events forwarded via the event forwarder.
DSER-8725	Emailed sensor download invite results in **Token invalid** message when clicking the link.

DSER-9664	Occasionally, clicking the link on an emailed alert notification results in the **Alert Triage** page not rendering correctly.
DSER-9670	Searching for “Threat Category: Malware” on the **Alerts** page returns results that are non-malware.
DSER-10342	Selecting **Take Action > Uninstall** from the **Endpoints** page fails to uninstall sensors in some cases. This leaves the sensor installed on an endpoint, but unable to communicate with the cloud.
DSER-10667	When an application's reputation is first determined to be NOT_LISTED and is then whitelisted, events shows WHITE_LISTED on the **Investigate** page. The application still shows as NOT_LISTED in the **Applications** tab.
DSER-10714	An incorrect API URL is listed on **Settings > Connectors > Download**. See this KB for the proper URLs: https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-What-URLs-are-used-to-access-the-API/ta-p/67346.
DSER-10961	Older macOS sensor versions allow deletion of sensor files from the backend. This can occur on macOS sensor versions 3.1 and lower. This only occurs if an org admin manually triggers the deletion.
DSER-11370	If an alert dismissal reason is selected when dismissing an alert, the alert does not dismiss properly.
DSER-12676	A notification for an alert can be sent when dismissing an alert, causing duplicate notifications to appear.
DSER-12728	In rare situations, navigating to some pages in the UI causes the page to render as gray. Refresh the page to render the page as expected.
DSER-13914	Auto-delete of deregistered devices is not functioning properly. Manual deregistration is working as expected.

CB ThreatHunter

Event search on Process Analysis page

The event table on the **Process Analysis** page now features a search bar that lets you search through all events that are relevant to the process tree.

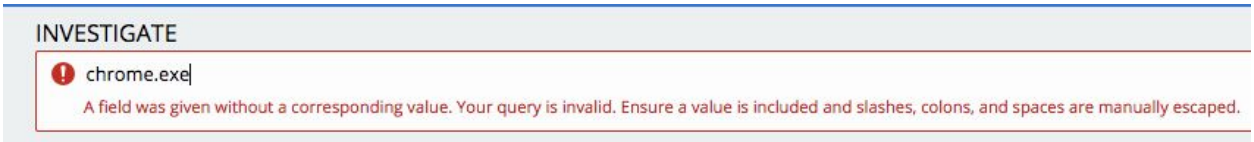


Search enhancements: value search

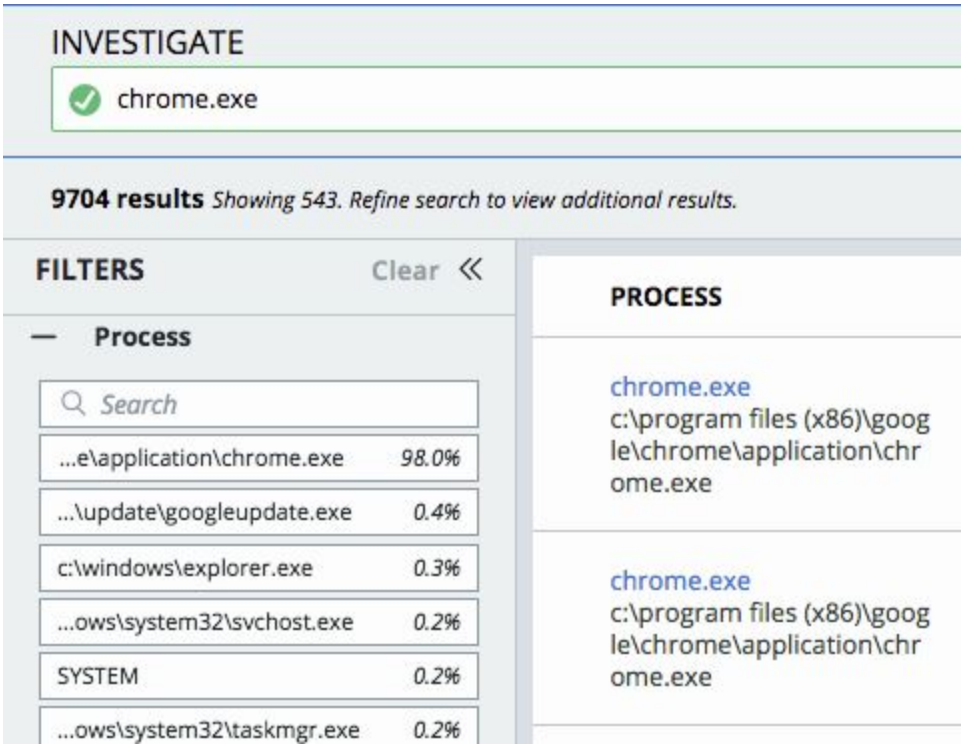
NOTE: This feature will be released in mid-April of 2019.

- For many search fields, the user 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 on both **Investigate** and **Process Analyze** search bars.

Previously:



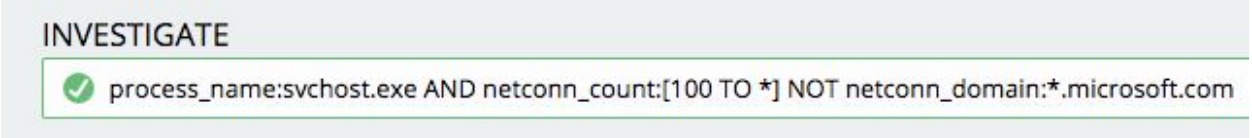
Now:



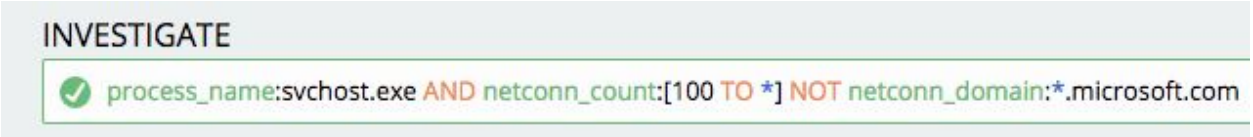
Search enhancements: syntax highlighting

- When you type correct search syntax, CB ThreatHunter highlights the syntax with specific colors to emphasize that the query is formulated correctly. This includes highlighting of all supported field names, operators (AND, OR, NOT, TO), the wildcard ("*" or "?") and fuzzy ("~") search characters.
- This capability is available on both **Investigate** and **Process Analyze** search bars.

Previously:

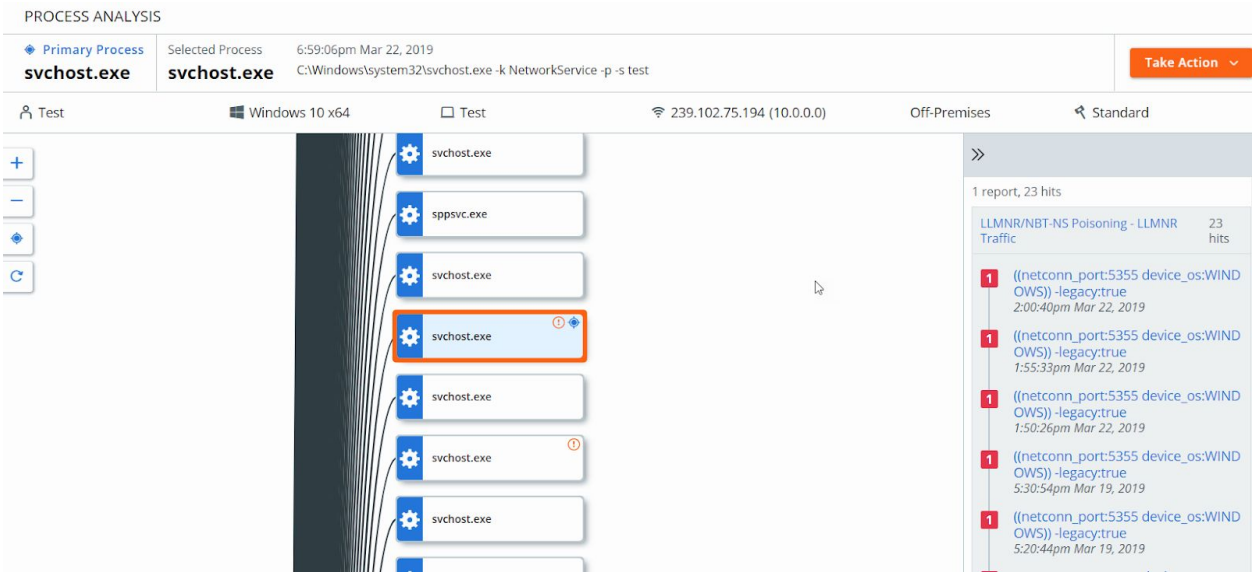


Now:



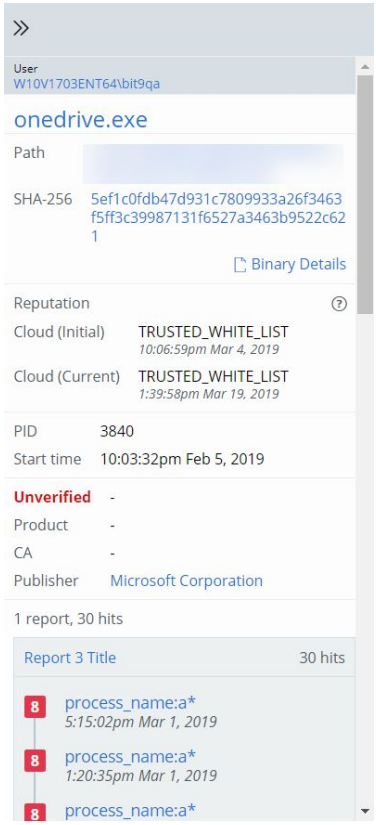
Watchlists on the Process Analysis page

Watchlist functionality is available on the **Process Analysis** page. You can see which processes in the **Process Analysis** tree have Watchlist hits on them.



Reputation on the Process Analysis page

Reputation is now present on the **Process Analysis** page at the process level.



Also in this release

- You can edit IOCs from custom Threat Reports.
- You can edit or delete custom Threat Reports from custom Watchlists.
- You can search for all matching processes for a Watchlist, Threat Report or an IOC to gauge the breadth of coverage by using new **Investigate** buttons for Watchlist, Threat Report or IOC.

- The **Investigate** and **Process Analyze** search include improved suggestions for well-known search field values (for example, reputation fields, TTP, sensor_action).

- Performance improvements make sure that **Process Analyze** trees that have extremely high numbers of process events load completely. Note that it might require up to three page refreshes for all results to become available in the **Events** table.
- CB ThreatHunter now supports an Event Forwarder by using a customer-supplied AWS S3 bucket for customers who want to acquire a copy of the protobuf data from the Carbon Black sensors as it is received by Carbon Black. See this Carbon Black User Exchange article for more details.

Fixed in this release

Issue ID	Description
UAV-713	PSC sensor did not send all process create events in some cases. (Requires PSC sensor version 3.4.0.820 or later.)
UAV-777	PSC did not accept new policy when organization opted out of UBS uploads until reboot. (Requires PSC sensor version 3.4.0.863 or later.)
DSER-11508	**Investigate** page searches that include regex statements are flagged by the UI as invalid, but are accepted if you submit the search.
DSER-11760	User cannot edit IOCs that are created in their organization.
DSER-11839	Some nodes do not expand on first click on the **Process Analysis** page.
DSER-12355	IPv6 addresses are incorrectly displayed in ThreatHunter detail and facet view on the **Process Analysis** page.
DSER-12424	Data access events from the PSC macOS sensor generate alerts, but do not display in **Investigate** page results.
DSER-12540	Exclusion filters aren't excluding processes in search results on the **Investigate** page.
DSER-12710	Sorting clears filters on **Investigate** page.
DSER-12718	Watchlist alerts do not always appear on **Alerts** page.
DSER-12719	Hash fields only returns results for all-lowercase hash values in the **Investigate** page.
DSER-12727	Processes are reported without a name, but are reported with PID = 0.
DSER-12737	Clearing facets on the **Investigate** page ignores search parameters on URL, and changing facet selections overrides the existing query.

DSER-12739	Excluding a facet value or clearing a selected facet overrides the existing query on the **Investigate** page.
DSER-13028	The **Investigate** page sometimes displays the error "Encountered two searcher groups whose assigned times violate internal requirements".
DSER-13060	Selecting Watchlists and Watchlist tabs often temporarily shows the previous results and no loading state.
DSER-13176	When using the "add query to watchlist" feature on the **Investigate** page, not all custom Watchlists or Reports are available to select.
DSER-13206	When you remove Report from Watchlist, no confirmation message displays.
DSER-13207	Child processes are missing in events for processes that started before the sensor initialized.
DSER-13251	Watchlist reports state isn't kept up-to-date on **Enabled Watchlists' Reports** tab.
DSER-13977	Missing cmdline in **Process Analysis** page that should have a cmdline.
DSER-14271	The wrong parent process can appear in crossproc events. This only occurs if the event does not have a target parent in the original event.
DSER-14664	Search for netconns fails on **Investigate** page for some netconn events

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-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	**Help** menu is missing the **User Guide** for organizations that are subscribed 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 has been completed in the background.
DSER-13404	When a user opens/reloads any page in the PSC UI and looks at the API calls, they see broken healthCheck calls that are safe to ignore.
DSER-13506	**Sort by Process Name** doesn't work as expected on the **Investigate** page.
DSER-14090	If CB Defense is enabled on the PSC, and the WSC integration is enabled and the org removes CB Defense, then 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.

CB LiveOps

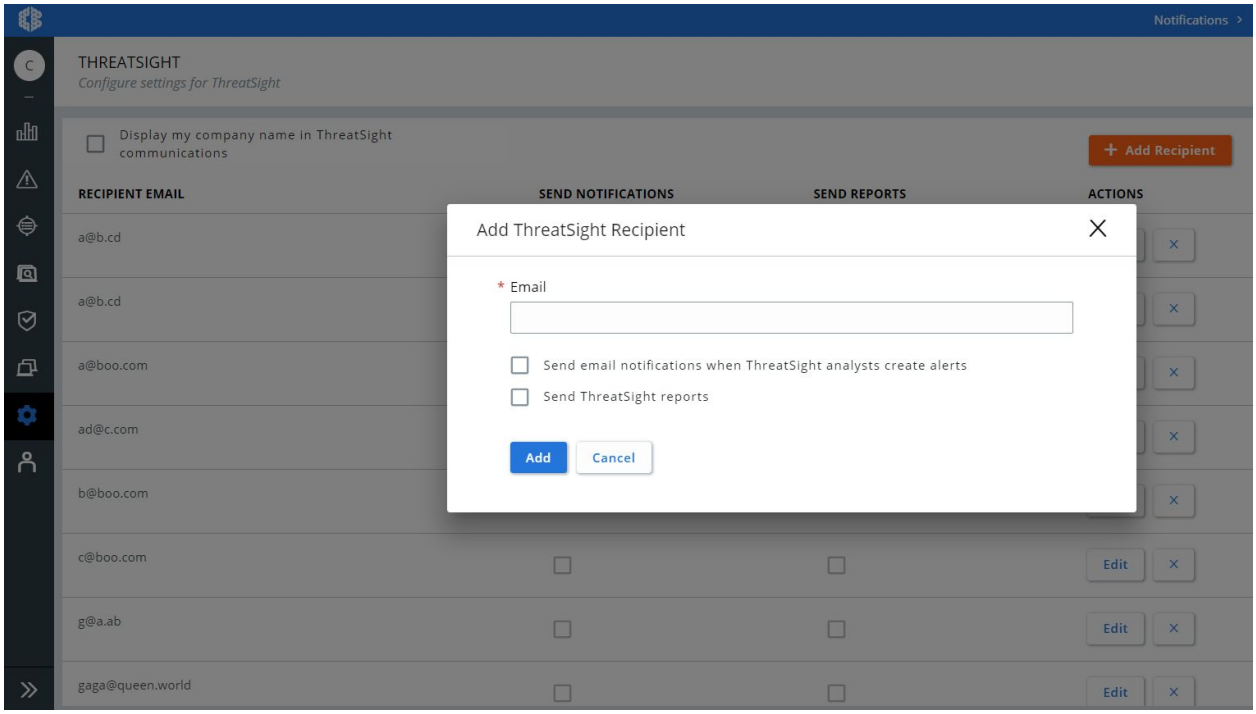
macOS enablement

CB LiveOps is now available for use with your macOS devices. Osquery supports over 160 tables for macOS, and we now offer access to these via our query builder so that you can get answers from those devices. *Devices must be running the 3.3 macOS sensor or higher to receive a query response.*

CB ThreatSight

Configure settings for CB ThreatSight report recipients

We've added a CB ThreatSight configuration page, which lets you configure your own settings for CB ThreatSight report recipients. You can add or edit the email addresses of recipients to view alert notifications or CB ThreatSight trend reports.


Notifications
THREATSIGHT
Configure settings for ThreatSight
Display my company name in ThreatSight communications
+ Add Recipient
RECIPIENT EMAIL
SEND NOTIFICATIONS
SEND REPORTS
ACTIONS
a@b.cd
a@b.cd
a@boo.com
ad@c.com
b@boo.com
c@boo.com
g@a.ab
gaga@queen.world
Edit
Add ThreatSight Recipient
* Email
Send email notifications when ThreatSight analysts create alerts
Send ThreatSight reports
Add
Cancel