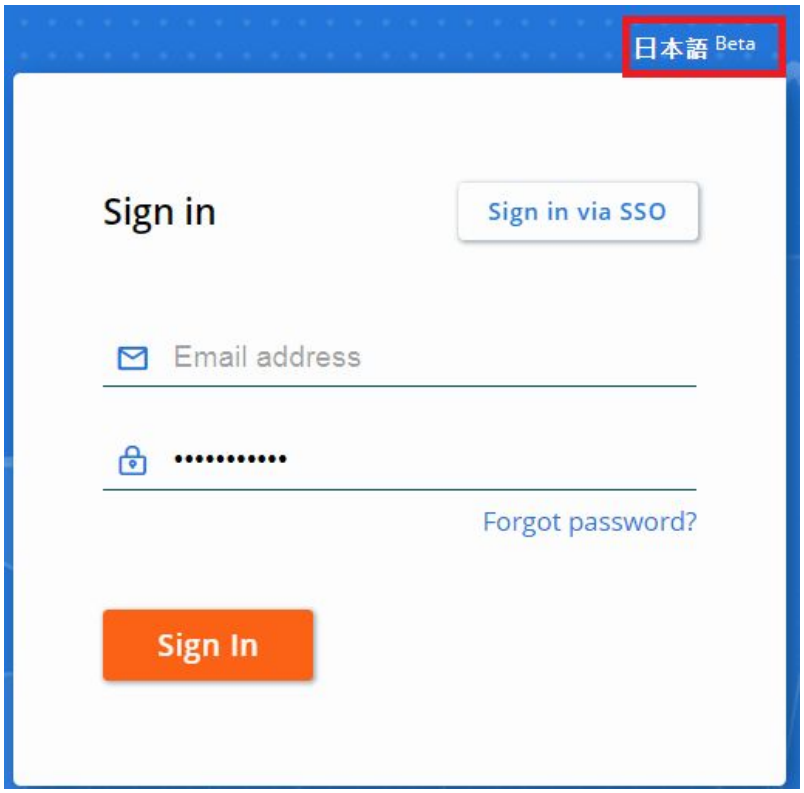
Our January 2019 release of the PSC includes the following:

- Japanese localization open beta
- CB Defense: Fixed in this release and Known issues
- CB ThreatHunter: Fixed in this release and Known issues
- CB LiveOps: Clone a query

We'll start rolling out these changes the third week in January 2019.

Japanese localization open beta

You can now switch between English and Japanese languages in the PSC console. Static content is translated to Japanese; in future releases, dynamic content will be translated. You can switch languages from the login page, or from the top navigation menu that opens when you click your username.



CB Defense

Fixed in this release

Issue ID	Description
DSER-10679	The date/time format in the device API output changed in the September release to a new format.
DETECT-235	Eliminated alerts related to code injection activity that is known to not be suspicious.
DSER-13257	Fixed an issue where sensor group auto-assignment on the **Endpoints** page incorrectly assigned devices with syntax of “Active Directory Domain \ Device ID”.
DSER-11040	Fixed an issue where Live Response commands failed if quotes were used to escape whitespace in arguments.

Known issues

ID	Description
DSER-5437	Additional markup was added to events that are forwarded via the event forwarder.
DSER-9144	When copying out of the **Investigate** page, additional line breaks were included. Pasting this directly into the search bar did not return any results.
DSER-9664	Occasionally, clicking the link an an emailed alert notification resulted in the **Alert Triage** page not rendering correctly.
DSER-9670	Searching for **Threat Category: Malware** on the **Alerts** page returned Non-Malware results.

DSER-10667	After whitelisting a file, the reputation on the **Application** tab of the **Investigate** page erroneously displayed as NOT_LISTED.
DSER-10714	The API URLs presented under **Settings -> Connectors -> Download** were incorrect.
DSER-10790	IT Tool whitelist upload removed backslash and the next character.
DSER-10961	On non-current sensor versions, the request to delete PSC sensor files from the backend succeeded, which caused the sensor to stop functioning.
DSER-11370	When dismissing alerts, selecting a dismissal reason caused the alert to not dismiss properly.
DSER-12676	Notifications were sent when dismissing alerts, causing two notifications to be sent per alert.
DSER-12728	A gray screen appeared on the **Endpoints** page after performing some actions. A refresh of the page cleared this issue.
DSER-12809	The **Malware Removal** page occasionally did not show the filename for malware.
DSER-12858	In cases where an organization is deprovisioned, the uninstall command was not properly sent to the sensors.

CB ThreatHunter

Features

Investigate Search enhancements

- ThreatHunter Investigate search results now include icons to indicate the process segment including Blocked and/or Terminated events.
- ThreatHunter **Investigate** and **Process Analysis** page filters behave more consistently.
- Advanced, fast substring search is available for regmod and filemod events.
- Multi-term queries are faster.
- You can search on the process_start field.

Test a Policy (CB Defense required)

In the **Policy** page, on the **Preventions** tab, you can test a policy before rolling it out to endpoints.

Fixed in this release

Issue ID	Description
DSER-11841	Fixed an issue where navigating from **Alerts** page to **Investigate** page via hyperlink sometimes threw "The query is invalid" due to undefined device_id.
DSER-12162	**Binary type** field was reported as "Unknown" on the **Binary Details** page.
DSER-12465	Search results for certain kinds of events did not include/exclude results that correspond to Watchlist hits on the **Investigate** page.
DSER-12493	Search exclusion for device_os did not eliminate "Hit" search results.
DSER-12068	All characters including `/ : ( ) { } [ ] " + - & | ! ^ ~ * ?` and spaces must always be escaped or enclosed in double quotes in ThreatHunter searches.
DSER-12880	Fixed an issue where fuzzy search wasn't supported for the netconn_domain field.

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-13177	**Help** menu is missing the User Guide for organizations that are subscribed to CB ThreatHunter.
DSER-11508	**Investigate** page searches that have 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-12355	IPv6 addresses are not properly formatted on the **Process Analysis** page.
DSER-12424	Data access events from from the PSC sensor feature do not show up in **Investigate** page results.
DSER-12540	Exclusion filters aren't excluding processes in search results on the **Investigate** page.
DSER-12355	IPv6 addresses are displayed in incorrect order in the **Process Analysis** page events table.
DSER-13295	For processes that have a very large number of events, the **Process Analysis** page for that process can be reloaded manually 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 and ask for Support/help in troubleshooting
DSER-12453	ThreatHunter Watchlist tags do not show up on the Notes/Tags tab of Alerts page - these are a different type of "tag" data.

CB LiveOps

Please contact your account representative to get CB LiveOps for your team.

LiveOps: Clone a query

You can clone a query, edit it, and run it. This lets you quickly adjust a query and rerun it.