Our inaugural release of CB ThreatHunter on the PSC lets you:

- Search through rich, unfiltered endpoint data by using a powerful query language.
- Create custom detections through our enhanced Watchlist functionality.
- Subscribe to threat intelligence that is provided by Carbon Black and third-party sources.
- Capture and store copies of every unique binary that executes in your environment.
- Analyze binary metadata and download a copy of a binary for reverse engineering or detonation.

CB ThreatHunter is generally available as of December 6th, 2018, and includes the preceding features.

# CB ThreatHunter

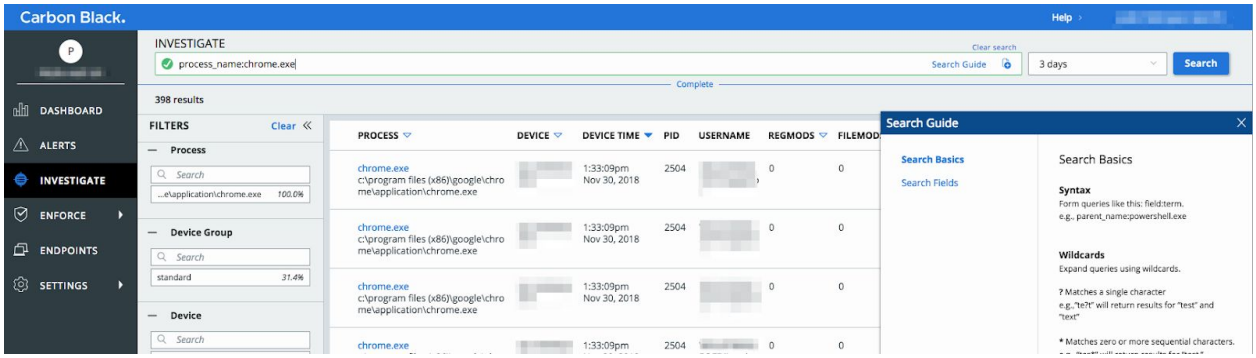
## Features

### Enhanced investigations

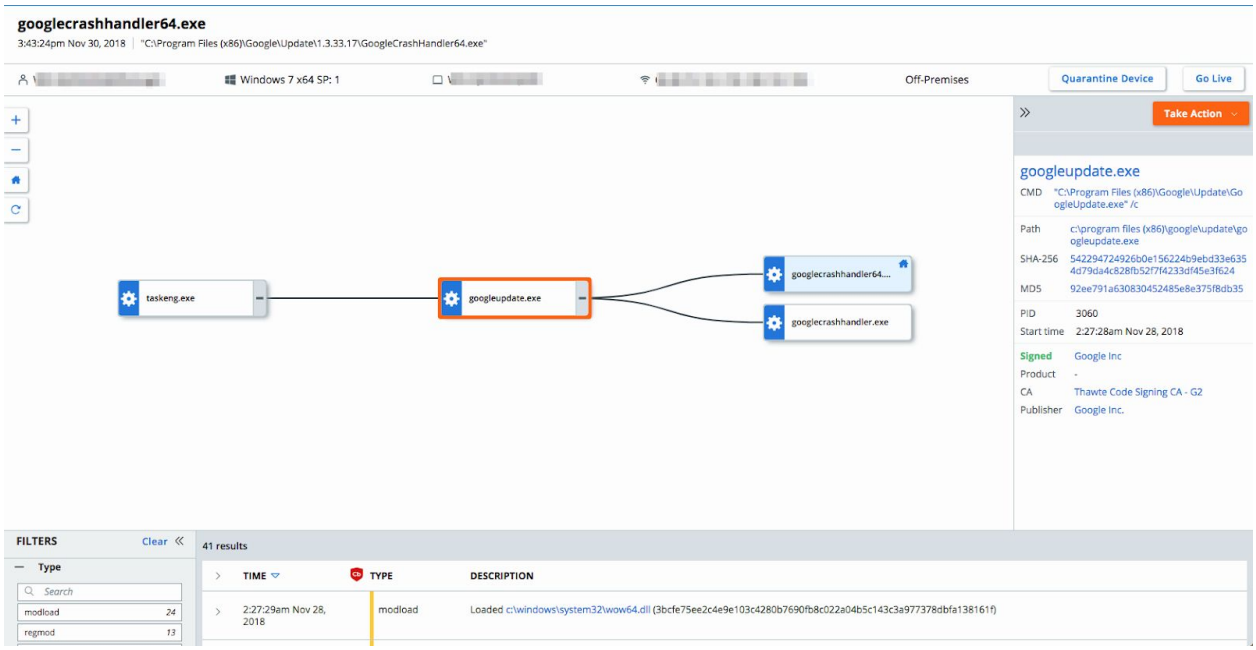
CB ThreatHunter brings unfiltered endpoint data and enhanced search to the PSC. These capabilities accelerate investigations, ensure that essential information is always at your fingertips, and let you rapidly zero-in on the threat that you're hunting for.

**To begin using enhanced investigations**

1. Click **Investigate**.
2. Use the built-in **Search Guide**, **Filters**, and **Contextual Help** to craft complex queries that target a specific activity.
3. Select a **time range** from the dropdown menu (or accept the default value) and click **Search**.
4. Identify a process of interest from the result set and click the **Process Name** for a deeper analysis.




5. On the **Process Analysis** page, explore parent/child process relationships by using the **Process Tree** visualization, The raw event telemetry for the selected process is displayed at the bottom of the page. You can use a variety of filters to parse the event data.



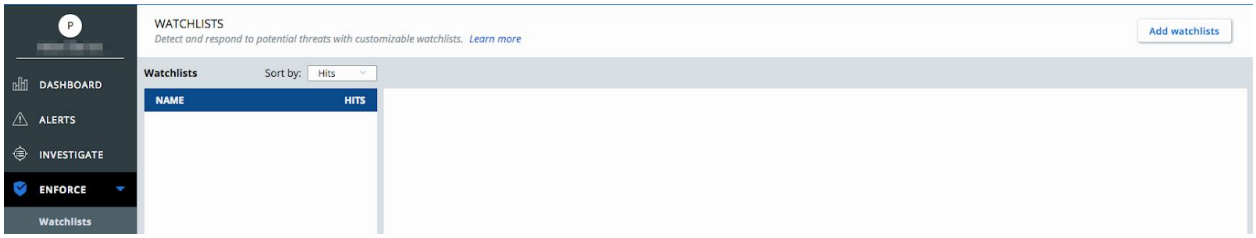

6. To perform actions including **Go Live** and **Quarantine Device**, click the respective buttons.

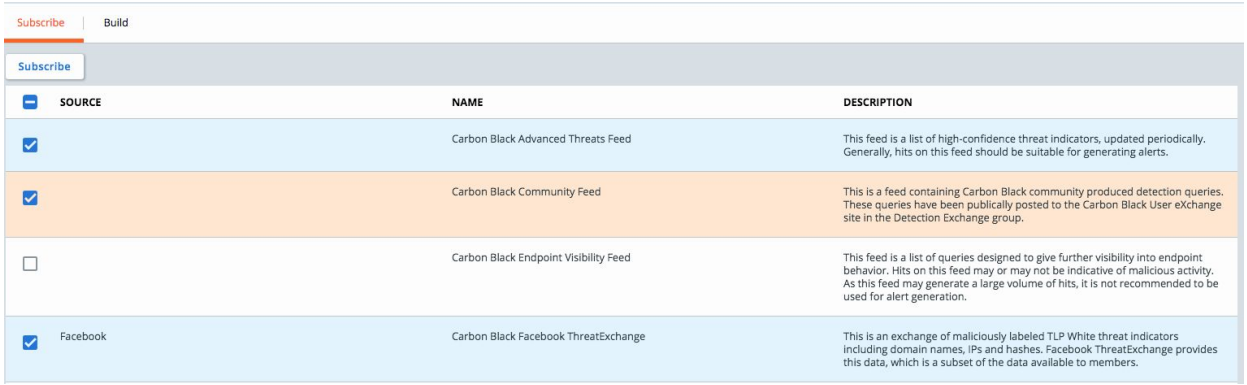
## Custom watchlists

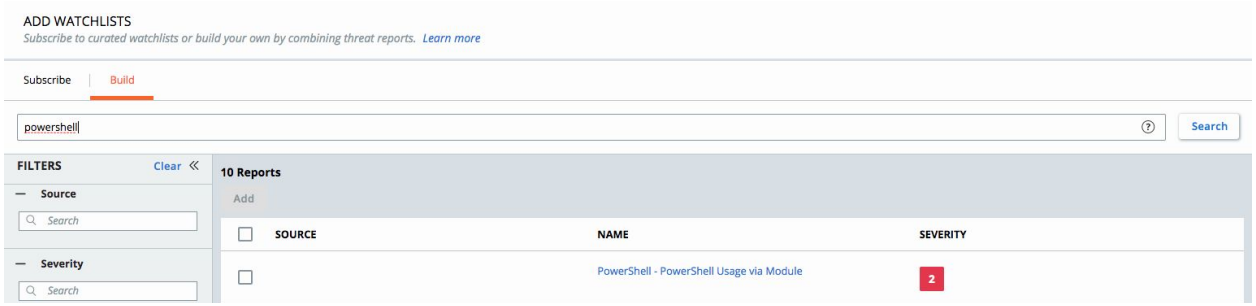
You can create custom detections by using the Watchlist capability. This feature allows you to tailor detection that is specific to your environment. Use your expertise and knowledge to disrupt ongoing and future attacks and close any identified gaps. You can easily integrate your threat intelligence with threat intelligence that is provided by Carbon Black or third-party sources.

## To get started with Watchlists

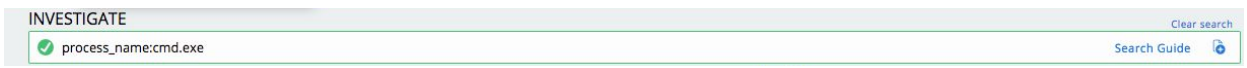
1. Click **Enforce** and click **Watchlists**.
2. Initially, the list of Watchlists is blank. Click **Add watchlists** to subscribe to Carbon Black and third-party intelligence, or use the **Build** functionality to build your own Watchlists from pre-populated reports.

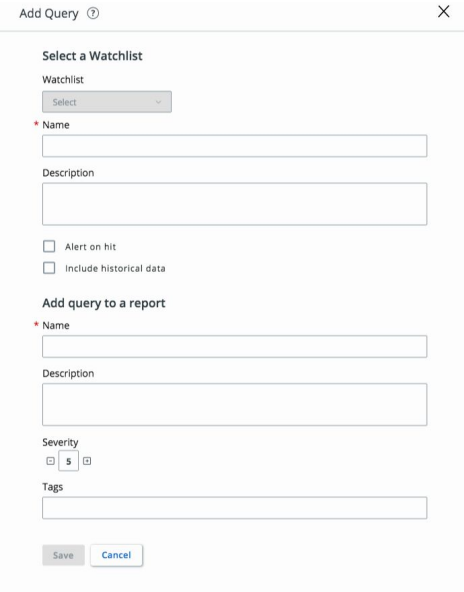



3. On the **Investigate** page, you can transform any query into a Watchlist.
    a. Click **Investigate**.
    **b.** **Type** your query into the search box.
    **c.** **Click** the plus icon inside the search box.
    d. Complete the information in the **Add Query** modal and click **Save**.





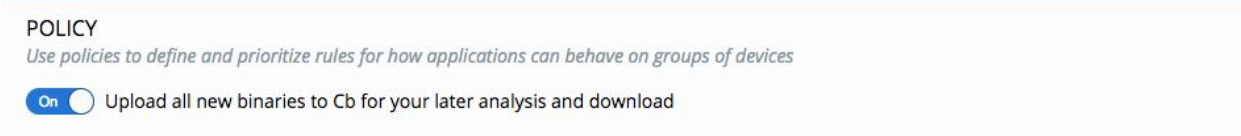

## Unified Binary Store

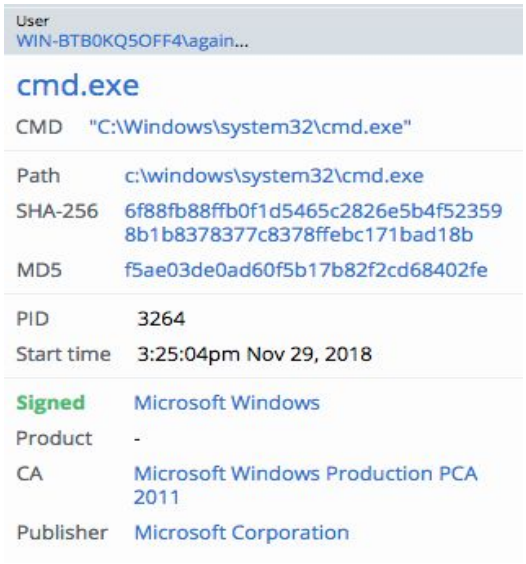
CB ThreatHunter can collect, store, and analyze every unique binary that executes in your environment. This feature is turned OFF by default, but you can turn it ON via the **Policies** page. Thereafter, every time a binary executes, a check determines whether the PSC has seen the binary before. If the PSC has not seen the file before, a copy is collected, tagged with your customer ID for access control purposes, and sent to the PSC Unified Binary Store.

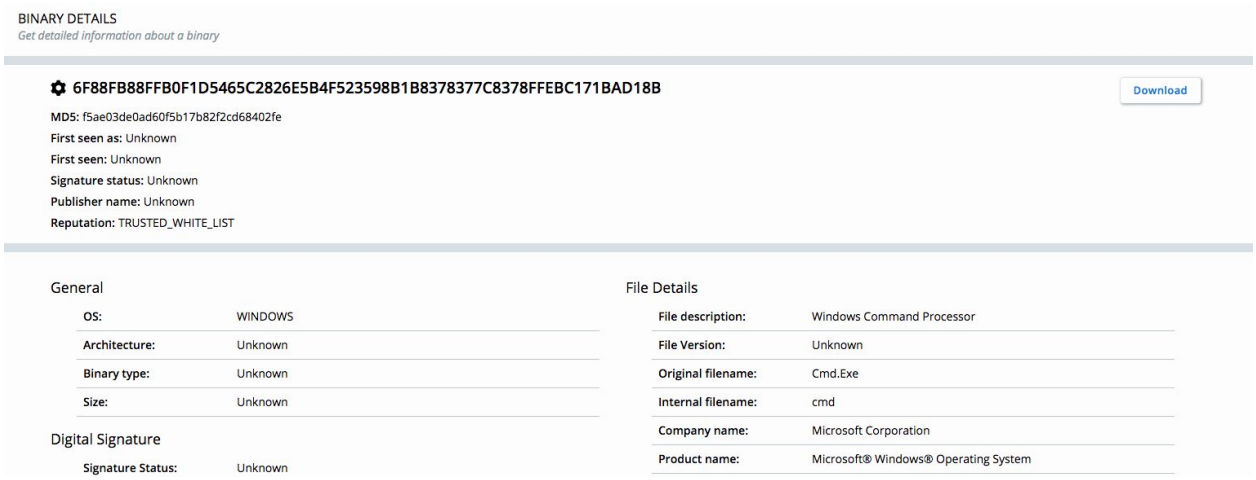
You can review binary metadata and download a copy of any binary for manual analysis, reverse engineering, or detonation purposes.

### To access the Unified Binary Store

1. Click **Enforce** and click **Policies**.
2. At the top of the page, slide the switch for **Upload all new binaries to Cb for later analysis and download** to ON. This selection is global for your environment.
3. To view binary metadata, go to a process of interest via an alert or the **Investigate** page. Metadata that is associated with the process displays to the right of the **Process Tree**.
4. Click the link next to **Publisher** to go to the associated **Binary Details** page.






# Fixed in this release

| Issue ID | Description |
|---|---|
| | Added a new search capability: to find an IP:port combination in a single netconn, you can search in the following manner: `netconn_ipv4:1.1.1.1 AND netconn_port:80` |
| DSER-10132 | Terminology changes in the PSC UI:<br>● **Alert Priority/Priority Score** was changed to **Alert Severity** (or in some instances, just **Severity**). |

| | |
|---|---|
| | • Product names were removed from alert types: CB Analytics, Watchlists. |

## Known issues

| ID | Description |
|---|---|
| | Existing hyperlinks to the **Investigate** page might not work after CB ThreatHunter is enabled. Any saved bookmarks and saved links (for example, in UeX discussions, support case logs) to the **Investigate** page results are redirected to the PSC **Dashboard**. |
| | Two links from Notification emails (**Link to application** and **Link to TTP**) are removed. The **View in PSC** link goes directly to the alert on the **Alert Triage** page. |
| | Because some process segments aren't always linked together, process segments can display as duplicate processes on the **Investigate** page. |
| | The CB Unified Binary Store (UBS) service does not track hash, metadata, or upload binaries for Microsoft-signed binaries. This is primarily to mitigate the network traffic and low-value upload of metadata and binaries from Patch Tuesday events. |
| | The **Investigate** page has specific requirements for escaping special characters in search queries:<br>• `process_name: system32*` does work<br>• `process_name: system32\\*` does work<br>• `process_name: system32\*` does NOT work |
| DSER-12017 | When creating Watchlists and Reports from the **Investigate** page, there is no acknowledgement displayed upon successful submission and the **Add Query** modal persists. However, the Watchlist or Report are generated. |
| DSER-12017 | You cannot delete created reports from the CB ThreatHunter UI. |
| UAV-503<br>DSER-11789 | Process icons are not visible on **Investigate**, **Process Analysis**, or **Binary Details** pages. |

| | |
|---|---|
| UAV-554 | CB ThreatHunter only hashes the first 512MB of every file, and only uploads the first 25MB of uploaded files. |
| DSER-12161 | Reputation is always displayed as *Unknown* on the **Binary Details** page. |