PSC

Cb Predictive Security Cloud

Release Notes
November 2018

Our November release of the PSC enables you to:

- Bulk-dismiss alerts
- View events on the Alert Triage page
- Easily find and configure policy settings

We'll start rolling out these changes the third week in November 2018.

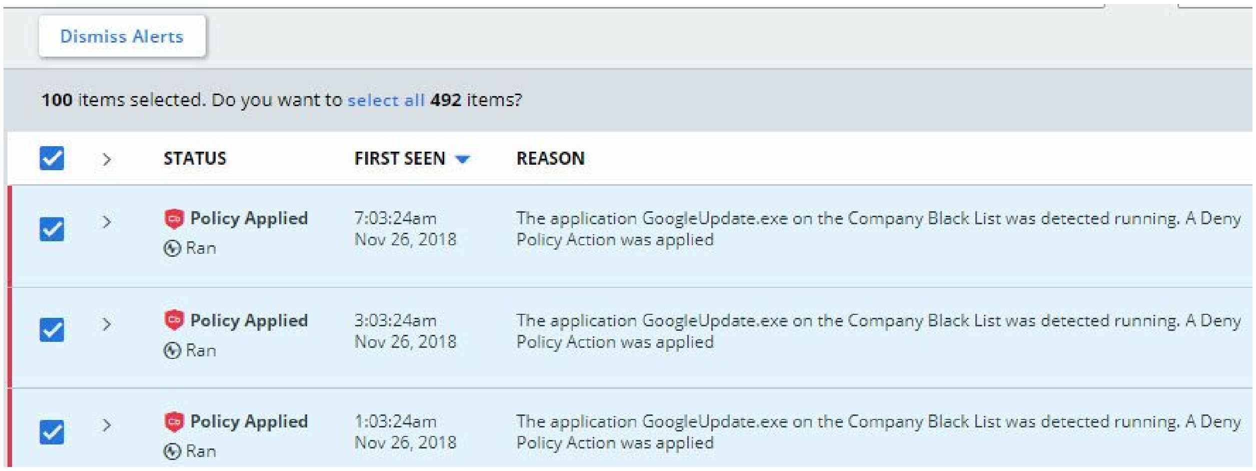
Cb Defense

Features

Bulk-dismiss alerts

You can now select and dismiss more alerts than display on a single page. Instead of dismissing up to 200 alerts at one time, you can simultaneously dismiss many alerts. We recommend that you dismiss no more than 3,000 alerts at a time. To bulk-dismiss alerts:

1. Click **Alerts**.
2. Search for and select alerts that match your criteria.
3. Select the checkbox at the top of the page to select all results that display on the page.
4. Click **select all** to choose all alerts that match your search criteria, even if they do not display on the page.
5. Click the **Dismiss Alerts** button at the top of the alerts page.
6. Click the **Dismiss All Alerts** button to confirm the dismissal.



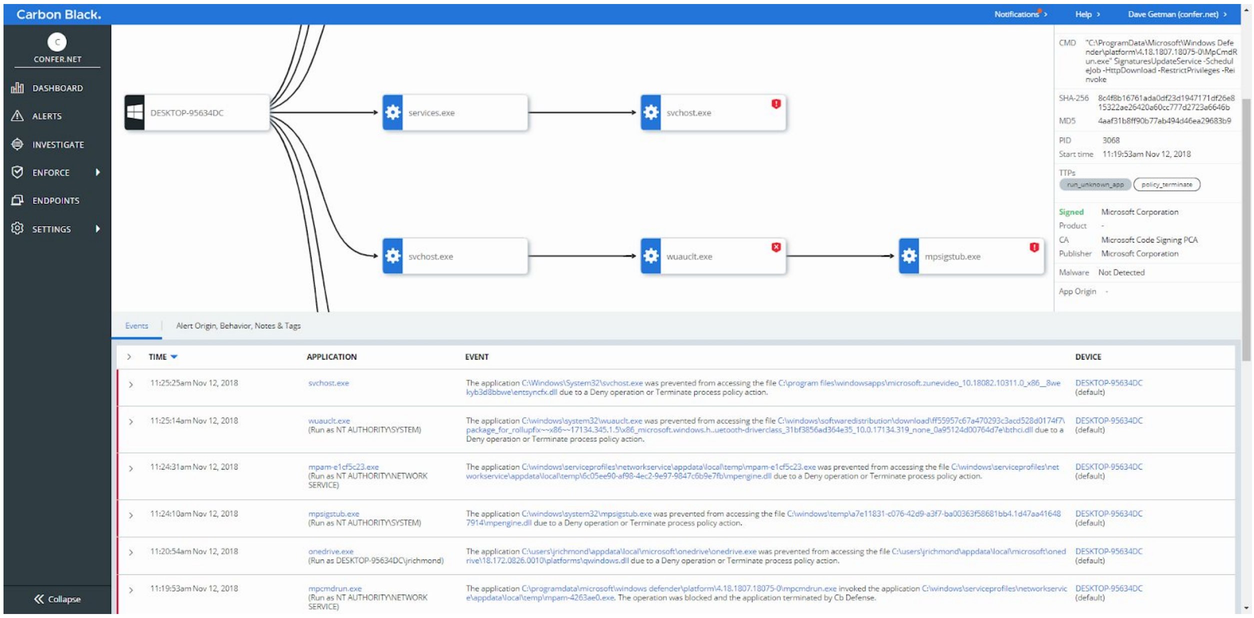
Dismiss Alerts

100 items selected. Do you want to select all 492 items?

☑		STATUS	FIRST SEEN	REASON
☑	>	Policy Applied Ran	7:03:24am Nov 26, 2018	The application GoogleUpdate.exe on the Company Black List was detected running. A Deny Policy Action was applied
☑	>	Policy Applied Ran	3:03:24am Nov 26, 2018	The application GoogleUpdate.exe on the Company Black List was detected running. A Deny Policy Action was applied
☑	>	Policy Applied Ran	1:03:24am Nov 26, 2018	The application GoogleUpdate.exe on the Company Black List was detected running. A Deny Policy Action was applied

View events on the Alert Triage page

A new **Events** view on the **Alert Triage** page lets you view events next to the process tree. You can move between tabs on the **Alert Triage** page to view more information about that alert, without having to change pages.



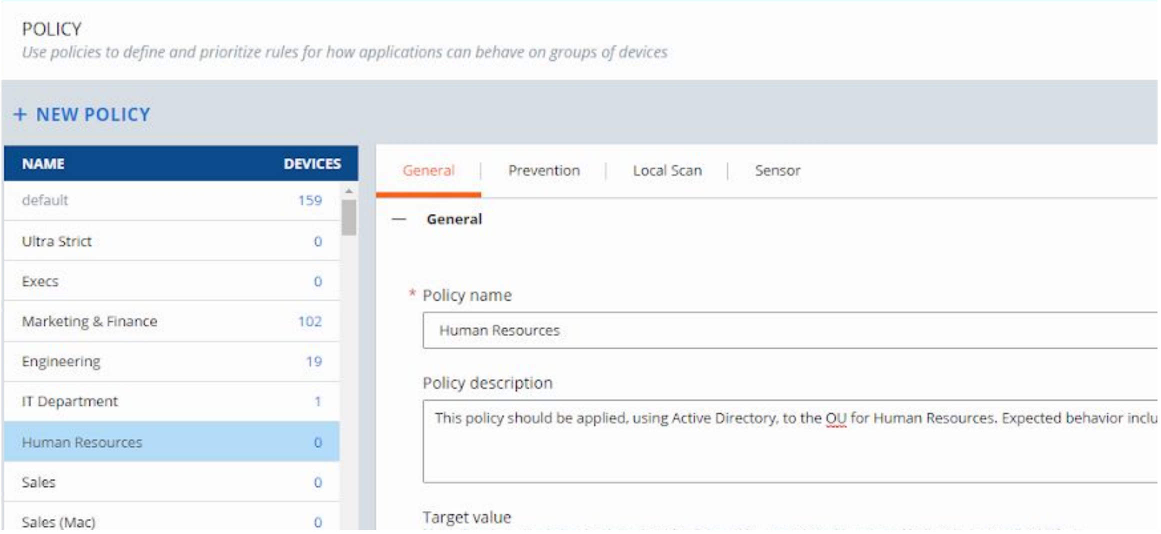
CMD	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.1807.18075-0\MpCmdRun.exe" SignaturesUpdateService -ScheduleJob -HttpDownload -RestrictPrivileges -Reinvoke
SHA-256	8c4f8b16761ada0df23d1947171df26e815322ae26420a60cc777d2723a6646b
MD5	4aaf31b8ff90b77ab494d46ea29683b9
PID	3068
Start time	11:19:53am Nov 12, 2018
TTPs	run_unknown_app policy_terminate
Signed	Microsoft Corporation
Product	-
CA	Microsoft Code Signing PCA
Publisher	Microsoft Corporation
Malware	Not Detected
App Origin	-

>	TIME	APPLICATION	EVENT	DEVICE
>	11:25:25am Nov 12, 2018	svchost.exe	The application C:\Windows\System32\svchost.exe was prevented from accessing the file C:\program files\windowsapps\microsoft.zunevideo_10.18082.10311.0_x86__8wekyb3d8bbwe\entsyncfx.dll due to a Deny operation or Terminate process policy action.	DESKTOP-95634DC (default)
>	11:25:14am Nov 12, 2018	wuauclt.exe (Run as NT AUTHORITY\SYSTEM)	The application C:\windows\system32\wuauclt.exe was prevented from accessing the file C:\windows\softwaredistribution\download\ff55957c67a470293c3acd528d0174f7\package_for_rollupfix~~x86~~17134.345.1.5\x86_microsoft.windows.h..uetooth-driverclass_31bf3856ad364e35_10.0.17134.319_none_0a95124d00764d7e\bthci.dll due to a Deny operation or Terminate process policy action.	DESKTOP-95634DC (default)
>	11:24:31am Nov 12, 2018	mpam-e1cf5c23.exe (Run as NT AUTHORITY\NETWORK SERVICE)	The application C:\windows\serviceprofiles\networkservice\appdata\local\temp\mpam-e1cf5c23.exe was prevented from accessing the file C:\windows\serviceprofiles\networkservice\appdata\local\temp\6c05ee90-af98-4ec2-9e97-9847c6b9e7fb\mpengine.dll due to a Deny operation or Terminate process policy action.	DESKTOP-95634DC (default)
>	11:24:10am Nov 12, 2018	mpsigstub.exe (Run as NT AUTHORITY\SYSTEM)	The application C:\windows\system32\mpsigstub.exe was prevented from accessing the file C:\windows\temp\a7e11831-c076-42d9-a3f7-ba00363f58681bb4.1d47aa416487914\mpengine.dll due to a Deny operation or Terminate process policy action.	DESKTOP-95634DC (default)
>	11:20:54am Nov 12, 2018	onedrive.exe (Run as DESKTOP-95634DC\jrichmond)	The application C:\users\jrichmond\appdata\local\microsoft\onedrive\onedrive.exe was prevented from accessing the file C:\users\jrichmond\appdata\local\microsoft\onedrive\18.172.0826.0010\platforms\qwindows.dll due to a Deny operation or Terminate process policy action.	DESKTOP-95634DC (default)
>	11:19:53am Nov 12, 2018	mpcmdrun.exe (Run as NT AUTHORITY\NETWORK SERVICE)	The application C:\programdata\microsoft\windows defender\platform\4.18.1807.18075-0\mpcmdrun.exe invoked the application C:\windows\serviceprofiles\networkservice\appdata\local\temp\mpam-4263ae0.exe. The operation was blocked and the application terminated by Cb Defense.	DESKTOP-95634DC (default)

Easily find and configure policy settings

The information on the **Policy** page is now categorized into four tabs instead of two, to make it easier to read and navigate.

- **General** includes the policy name and description.
- **Prevention** contains all policy rules.
- **Local Scan** contains local scan settings.
- **Sensor** contains the sensor settings.



POLICY

Use policies to define and prioritize rules for how applications can behave on groups of devices

NAME	DEVICES
default	159
Ultra Strict	0
Execs	0
Marketing & Finance	102
Engineering	19
IT Department	1
Human Resources	0
Sales	0
Sales (Mac)	0

* Policy name: Human Resources

Policy description: This policy should be applied, using Active Directory, to the OU for Human Resources. Expected behavior inclu

Target value

Fixed in this release

Issue ID	Description
DSER-10474	Live Response command line shows the current path, not just the device ID.
DSER-10702	Live Response commands that fail due to 5xx network errors will retry five times. Live Response commands that fail due to 4xx errors show appropriate error messages.
DSER-11200	Running a Live Response command on an inactive session will no longer crash; instead, inactive sessions will clearly show “Inactive” and will not accept commands.
DSER-10343	Fixed an issue where some items with the reputation ‘Known Malware’ were not showing up on the **Malware Removal** page.
DSER-8725	Resolved an issue where the sensor download email invite resulted in **Token invalid** message when clicking the link.

Known issues

ID	Description
DSER-5437	Additional markup is added to events forwarded via the event forwarder.
DSER-9144	When copying out of the **Investigate** page, additional line breaks are included. Pasting this directly into the search bar will not return any results.
DSER-9664	Occasionally, clicking the link an 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 Non-Malware results.
DSER-10667	After whitelisting a file, the reputation on the **Application** tab of the **Investigate** page erroneously displays as NOT_LISTED.
DSER-10679	The date/time format in the device API output changed in the September release to a new format.
DSER-10714	The API URLs presented under **Settings -> Connectors -> Download** are incorrect.
DSER-10790	IT Tool whitelist upload removes backslash and the next character.
DSER-10961	On non-current sensor versions, the request to delete PSC sensor files from the backend succeeds, which causes the sensor to stop functioning.
DSER-11370	When dismissing alerts, selecting a dismissal reason causes the alert to not dismiss properly.