Carbon Black.

Cb Defense Sensor 1.2.4 for Mac

Release Notes

August 2nd, 2017

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

General Notes

Cb Defense Sensor version 1.2.4 is a GA (General Availability) release for Mac operating systems only. These notes are *cumulative*, and provide information on all 1.2.4 releases to date.

New Features

This section lists features introduced in the 1.2.4 version of Cb Defense Sensor. (For a more thorough description of the new features in this release, see the User's Guide.)

Reverse Shell Detection 2.0

This release contains new reverse shell behavioral detection engine with improved detection rate compared to previous releases. Detection now covers more techniques and types of payloads (binaries, scripts), effectively improving detection of several types of payloads generated by metasploit and other frameworks alike. Monitored and Threat Alerts are raised, depending on confidence level and are tagged with REVERSE_SHELL TTP. In case of unobfuscated attacker's input, the input is logged as part of Alert, otherwise "[bin]" string is logged. False positives can be managed with Threat "Dismiss" functionality.

Issues Resolved in 1.2.4

ID	Description
DSEN-860	Performance optimizations for Policies groups that contain only Blocking and Isolation rules for Blacklisted applications and for applications by path. Such configurations are sometimes used for "detect only" use-case. Now, even with these Blocking and Isolation rules enabled, users will experience the same highest performance, as with no Blocking and Isolation rules.
DSEN-800	Interoperability improvements when editing files on network file systems.
DSEN-789	Improved origin detection and prevention of Windows malware spreading through Macs.
DSEN-746	Improved policy enforcement with behavioral rules for not listed application targets.

CIT-11064	Quarantine status displayed in backend console was incorrect for quarantined devices.
CIT-9596	Sensor UI icon was sometimes not loaded after sensor install or upgrade, until next user login.
CIT-11079	Sensor installer crashed during https proxy auto-detection in some proxy environments, especially on macOS 10.12.
DSEN-875	macOS 10.12.5 and 10.12.6 whitelist updates for optimal performance.
DSEN-999	Fixed potential repmgr crash due to race condition.
DSEN-975	Fix interop issue with Cb Response.