CARBON BLACK

Product Name: Carbon Black Enterprise Protection and Carbon Black Enterprise Response

Main Website: https://www.carbonblack.com/

Product Website: https://www.carbonblack.com/products/carbon-black-enterprise-protection/

Product Integration Type

Endpoint

Integration Objective

- Cyphort integrates with CB Enterprise Response in two ways:
  - File Upload. CB Enterprise Response server uploads suspicious binary and OS X files to Cyphort for analysis
  - Execution. When Cyphort sees a network download, it polls CB to check if the binary was executed on the endpoint
- Cyphort integrates with CB Enterprise Protect:
  - File Upload. CB Enterprise Protect server can upload locally unapproved binaries to Cyphort for further analysis

Customer Value Proposition

- File Upload
  - CB servers send the objects to Cyphort for further analysis. CB has built-in detection capabilities and accepts threat intelligence from other feeds. Cyphort is one of the threat intelligence feeds and can provide deeper analysis on the files
- Execution
  - Generally, the IR team does not have sufficient information to determine if the endpoint has been infected. With Cyphort, when it sees a network download, it can poll the CB server to check if the binary ran on the endpoint. If it did, the chances of infection are high and the endpoint may need to be reimaged.

Tested Vendor Versions

- CB Enterprise Response: 5.1.1
- CB Enterprise Protect: 7.2.1

Integration Classification

Other: Incident Response

Integration Details

Basic. Typically works with a single server in small environments.

Integration Method

- Cyphort Pull: CB Enterprise Response File Execution. Cyphort polls CB server if file has been executed on an endpoint.
- There are two different connectors—one for CBER and another for CBEP
  - File Upload. CBER (Carbon Black Enterprise Response): A CBER connector (a python script) must be installed on the CBER server. The CBER server sends suspicious executables and OS X files to the connector. The connector uses Cyphort's upload API to submit the file, receive the analysis and send the result back to CBER. The CBER connector is available here:
    - https://github.com/carbonblack/cb-cyphort-connector
  - File Upload. CBEP (Carbon Black Enterprise Protect): A CBEP connector must be installed on the CBEP server. The CB server sends suspicious executables and OS X files to the connector. The connector uses Cyphort's upload API to submit the file, receive the analysis and send the results back to CBEP. The CBEP connector is available here:
    - http://go.cyphort.com/rs/181-NTN-682/images/Cyphort-CarbonBlack-JSB.pdf

Integration Detail Summary (API, CLI)

- File Upload from Connectors: Uses regular file upload API
- Execution: Cyphort calls CB APIs to poll for information

Cyphort Manager GUI Component

- Yes
- File Upload
  - As of version 3.4, Cyphort does not have any GUI changes for File upload from CB. Objects uploaded from CBER and CBEP show up as “File Upload” incidents. They can be identified using the File name field

GUI Operational Use Case

- Objects uploaded from CBER have filenames such as:
  - CarbonBlack-Upload-8E5ED7B7D6F2AB7DB77D690 DE0741863
    - 8E5ED7B7D6F2AB7DB77D690DE0741863 is the MD5 Hash of the object that was uploaded
- Objects uploaded from CBEP have detailed filenames such as:
  - Server_URL: https://192.168.1.114, Server_IP: 192.168.1.114
    - Server_URL and Server_IP are the Carbon Black server URL and IP
  - Agent_version: 7.2.1.2002
    - Agent version is the Carbon Black version of the endpoint agent
  - Client_Name: WORKGROUP\SE-CB-CLIENT, Client_IP: 52.9.36.127, Client_OS: Windows Server 2012
    - Client_name, client_IP, and client_OS are the endpoint agent’s hostname, IP address and OS
  - Time: Tue_Apr_12_17:49:08_2016
    - Time is the time the connector agent submitted the object to Cyphort
  - Md5sum: abf64234f3462571e66527828040219b”
    - Is the MD5 Hash of the object that was uploaded
- On both CBER and CBEP, there are links pointing to the incident on Cyphort. Please refer to the Cyphort Integration with Carbon Black Solution Brief for more details
  - http://go.cyphort.com/rs/181-NTN-682/images/Cyphort-CarbonBlack-JSB.pdf
- File Execution
  - On Cyphort’s UI, the kill chain has the label EX when the object is executed on the endpoint agent

Threat Score Impact

- Yes
- For File Upload, there is no threat score impact
- For File Execution, since the file has been executed on the endpoint, the relevance increases thus increasing the threat score

Integration Documentation

http://go.cyphort.com/rs/181-NTN-682/images/Cyphort-CarbonBlack-JSB.pdf

Integration Demo

No

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com

Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com