Threat Hunting with CylanceOPTICS™ InstaQuery (IQ)

Feature Focus

CYLANCE™

Threat Hunting with CylanceOPTICS InstaQuery (IQ)

In security, threat hunting has long been considered a task that could only be completed by elite security analysts with years of in-the-field experience. These analysts – using tools designed specifically for them – craft complex hunts to bring hidden threats into the light where they can then be mitigated.

These skilled and experienced hunters have no doubt saved many a business from major breaches and countless data compromises. Unfortunately, elite security analysts are an increasingly rare commodity, and the reality of the current security talent shortage has left most organizations without effective in-house threat hunting capabilities. Until now.

CylanceOPTICS now provides any security team with the ability to perform smart threat hunting with InstaQuery (IQ).

Unlike the complex and specialized threat hunting tools that dominate the market, the CylanceOPTICS smart threat hunting with IQ feature brings threat hunting to the masses, providing instant access to the forensically relevant data collected from endpoints. With IQ, security analysts can create enterprise-wide searches for indicators of compromise, suspicious activity, or any specific business need where information is needed from the vast array of endpoints.

In CylanceOPTICS v2.0, users can create simple searches via the IQ search page for:

- Files
- Registry Keys
- Processes
- Network Connections

Upon initiating the search, CylanceOPTICS will query the selected endpoints for the information requested, interrogating the data stored on the endpoints and collecting all responsive items. The results of the IQ search are stored in the cloud so they can be easily referenced in the future.

Once a query has reached completion, the user can review the results in a table format or, for targeted searches, use the facet breakdown view to drill into the results of the query. This simple interrogation of endpoint data means that anyone, regardless of skill level, can gain insights into their endpoint activity in a matter of minutes.

The following tables outline the IQ results that will be displayed based on different artifacts:

Technical Details Summary	
InstaQuery Result	**Description**
Name	The name of the InstaQuery
Description	The description of the InstaQuery
Date Created	The date the InstaQuery was created
Search Term	The specific value of the search
Artifact	The type of item for which the search is being conducted
Facet	The attribute for the artifact being searched
Zones	The zones included in the query (only devices in these zones are included in this query)
Devices Queried	The total number of devices associated with the query
Devices Responded	The number of devices that responded to the query request
Devices with Results	The total number of devices that matched the query
Total Results	The total number of artifacts returned from the query

Artifact Type: File	
Facet	**Description**
Path	The path to the file
Created	The date the file was created
MD5	The MD5 hash for the file
SHA256	The SHA256 hash for the file
Device	The name of the device on which the file was found
Owner	The name of the user that owns the file

Artifact Type: Process	
Facet	**Description**
Name	The name of the process
Start Date	Date/time the process started
Image Path	The path to the process executable file
Command Line	The command used to initiate the process
Image MD5	The MD5 hash for the file
Owner	Owner of the process
Device	The name of the device on which the process was found

Artifact Type: Network Connection	
Facet	**Description**
Destination Address	The IP address to which the source is connecting Note: All queries are run on destination IP addresses only
Destination Port	The port number the source IP address is trying to use to connect to the destination
Process Name	The name of the process related to the network connection
Image Path	The path to the process executable file
Device	The name of the device

Results displayed for network connections are filtered if the connection is entirely localized to certain IP ranges, such as private, linklocal, non-routable, multi-cast, and loopback.

Artifact Type: Registry	
Facet	**Description**
Path	The path to the registry key
Value Name	The registry value
File Path	The file path for the extracted from the registry key, value, or value contents
File MD5	The MD5 hash for the file
Is Persistence Point	If the registry key being modified is a persistence point monitored by CylanceOPTICS
Device	The name of the device

From the InstaQuery results page, a user can take further response actions under the Action row expand, as well as discard a query, which will remove it from the Previous Queries list.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

20170428-0999