Root Cause Analysis with CylanceOPTICS™

Feature Focus
Root Cause Analysis

CylancePROTECT® prevents known and unknown threats from executing on your endpoints, as well as from attackers attempting to exploit memory, detonate malicious scripts, or use external devices to compromise an endpoint.

With the addition of CylanceOPTICS’ ability to perform on-demand root cause analysis, you can now make use of the blocked attack data to improve your overall security posture.

When CylancePROTECT blocks a malicious executable, memory or script attack, or a corrupt USB device, CylanceOPTICS will gather a set of data associated with the event. That event data will then be sent to the cloud-based web console for a security analyst to perform root cause analysis using the Focus View feature.

The Focus View is a recreation of the events associated with the blocked event that displays the relationship between each event.

Within Focus View, there are three different ways to interact with the data: 1) Graphical view, 2) Event Card view, and 3) Tabular view.

1) Graphical View: As you click on a dot (which represents an activity), the corresponding event card is brought into focus.
2) Event Card View: With this detailed view into a CylancePROTECT blocked event, analysts can adjust their security controls, close vulnerabilities, and improve their overall security framework to ultimately reduce their attack surface.

3) Tabular View: From the tabular view, you can choose to export the event list and complete your root cause analysis using other tools.

Technical Details Summary

Viewing Focus Data:
Focus Data provides an information trail starting with the first event related to an artifact from an InstaQuery result or a CylancePROTECT event.

There are multiple ways to view Focus Data. The Focus Data tab on the CylanceOPTICS page shows a table of previously requested Focus Views from InstaQuery searches, and CylancePROTECT events. If auto-focus is not enabled, Focus Views for CylancePROTECT events must be requested from the Device Details page under Threats and Activates (see next page).

NOTE: Data retention span is 30 days for CylanceOPTICS data, including the Download History.

About Focus Data:
- The time for CylanceOPTICS to return Focus View results is directly proportional to the size of the data being queried. More generic queries will take longer to return results. This is also dependent on the network traffic and bandwidth on the customer’s network.
- If Auto-Focus is enabled in the policy associated with a device, the ‘View Data’ link in the Focus View column will link to the Focus View for the most recent threat. In cases where these detonations take place over multiple minutes, Focus Views from these previous threats are visible in the Focus Data tab in CylanceOPTICS.
<table>
<thead>
<tr>
<th>Focus Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>The name of the device associated with the Focus View</td>
</tr>
<tr>
<td>Description</td>
<td>Facet value of the query, the name of the associated file from an exploit attempt, or the path for a threat</td>
</tr>
<tr>
<td>Artifact Type</td>
<td>The artifact from either the InstaQuery search or the CylancePROTECT event</td>
</tr>
<tr>
<td>Created Date</td>
<td>The date on which the Focus View was requested.</td>
</tr>
<tr>
<td>Focus Data</td>
<td>The link to view the Focus View data</td>
</tr>
</tbody>
</table>

Available Focus Views.