Feature Focus: Context Analysis Engine

Powering CylanceOPTICS™ Dynamic Threat Detection and Automated Response

CYLANCE

The ability to quickly detect threats and initiate a response can make the difference between a small compromise and a massive, headline-stealing breach. Unfortunately, many of the security products in the market today that promise speedy threat detection and response are built on an infrastructure that is prone to latency issues, false positives, and limited enterprise-wide visibility.

To address these issues, Cylance® has developed a new approach to threat detection and response, known as the **Context Analysis Engine**, that pushes down both the threat detection and response to the endpoint. Now, every endpoint in your organization acts as its own virtual security operations center with the ability to dynamically detect threats and take response actions without human intervention, around the clock. Your security team can now focus on investigating advanced threats, improving your overall security infrastructure, or any other business critical project, with the confidence that the CylanceOPTICS Context Analysis Engine is working to keep the endpoint, and the business, secure.

A Closer Look at the Context Analysis Engine

The CylanceOPTICS Context Analysis Engine (CAE) is a high-performance analysis and correlation engine that monitors events as they occur on an endpoint in near real time to identify malicious or suspicious activities. With the engine deployed on the endpoint, this monitoring occurs with zero reliance on, or need for, a cloud connection. Without requiring an active network connection to make intelligent decisions, the CAE's architecture allows you to monitor multiple suspicious behavior paths continuously without posing potential performance impacts.

When the CAE identifies potentially malicious activity, automated response actions against the associated artifacts of interest can begin without any human intervention. These response actions are initiated from the endpoint with no cloud connection required, eliminating the latency that can occur with other products when threat detection and response are initiated from the cloud.

The CAE's functionality and configuration can be found in the **Detections** tab in the Cylance cloud-based management console. The **Detections** dashboard allows users to quickly understand and view trends of events that are occurring across their environment. From this dashboard, users can investigate and respond to these events in a meaningful manner without needing to leave the management console. The CAE can be easily configured to fit many environments by creating Detection Rule Sets that can be applied to one or more Device Policies.

To create a unified experience, the new **Detections** section of the console was designed with integration into other CylanceOPTICS features in mind. As such, events and artifacts identified by the CAE can be extended upon by creating additional Focus Views, retrieving files of interest with the File Retrieval features, or quarantining an endpoint on the network by issuing a Device Lockdown.

Note: *The CylanceOPTICS Context Analysis Engine and Response Actions require CylanceOPTICS 2.1.1000 or greater installed.*

Configuring the Context Analysis Engine

By default, the CylanceOPTICS Context Analysis Engine does not have any Rules or Response Actions configured. As such, when a user first navigates to the CylanceOPTICS section of the Cylance Management Console, they will be presented with a **Detection Environment** onboarding page.

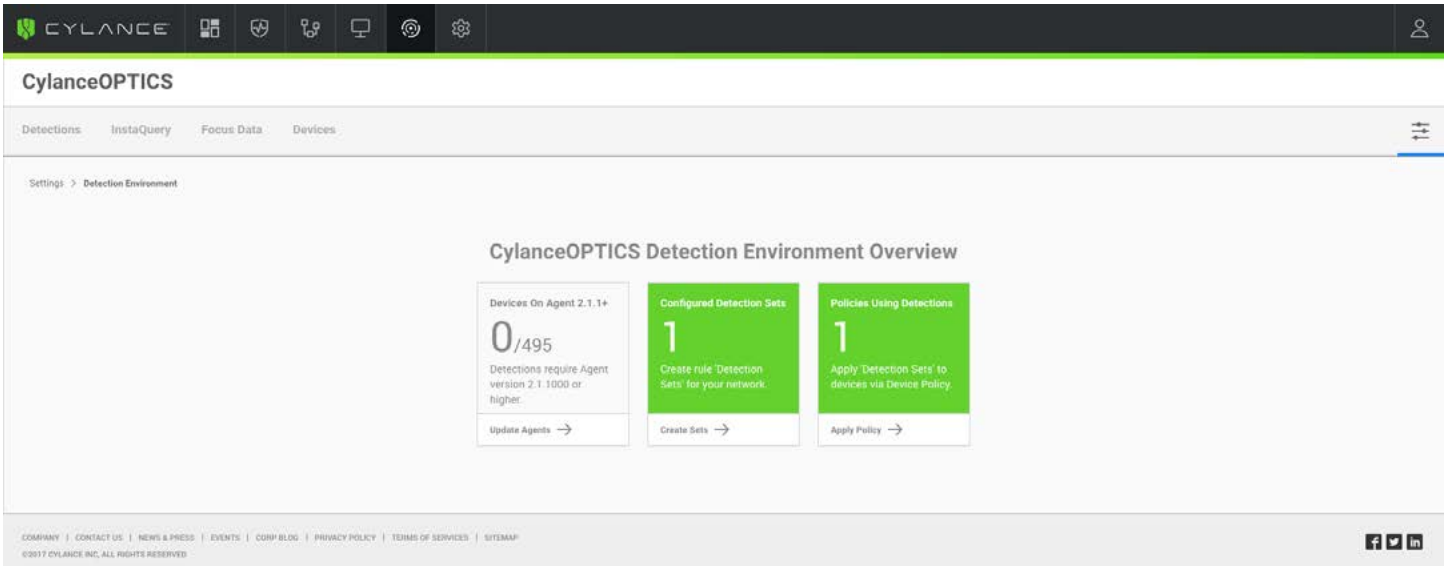

Figure 1: CylanceOPTICS Detection Environment Onboarding

The onboarding page gives an overview of the currently configured CAE settings, including:

- The number of devices with CylanceOPTICS version 2.1.1000 or greater installed
- The number of Detection Rule Sets configured
- The number of Device Policies with a Detection Rule Set selected

Note: *After the minimum requirements to enable* ***Detections*** *from the Context Analysis Engine have been met, the onboarding page will not be displayed by default. It can be accessed at any time by clicking the* ***Settings*** *slider and selecting the* ***Detection Environment*** *option.*

Configuring Detection Rule Sets

The center box of the onboarding page displays the number of Detection Rule Sets that exist in the tenant. Detection Rule Sets are the central configuration point for the Context Analysis Engine that determine the Detection Rules, Automated Responses, and Endpoint Notifications that are applied to endpoints. Detection Rule Sets are ultimately applied to endpoints on a Device Policy basis; that is, a user will select a Detection Rule Set to apply to a Device Policy. Endpoints will automatically receive the desired Detection Rule Set when the policy is applied.

CylanceOPTICS includes a default Detection Rule Set that has the following attributes:

- All rules are enabled
- All automated response actions are disabled
- All endpoint notifications are disabled

This configuration is designed to act as a 'tuning' or 'monitor-only' mode for testing and initial deployment purposes. Users will gain an understanding of areas of their environment that may trigger false positives so that automated response actions can be tuned accordingly.

Custom Detection Rule Sets can be created by navigating to the **Settings** slider and selecting the **Detection Rule Sets** option. This menu will list all the current Detection Rule Sets as well as provide the option to copy, delete, or edit current Detection Rule Sets; it also contains a link to create a new Detection Rule Set.

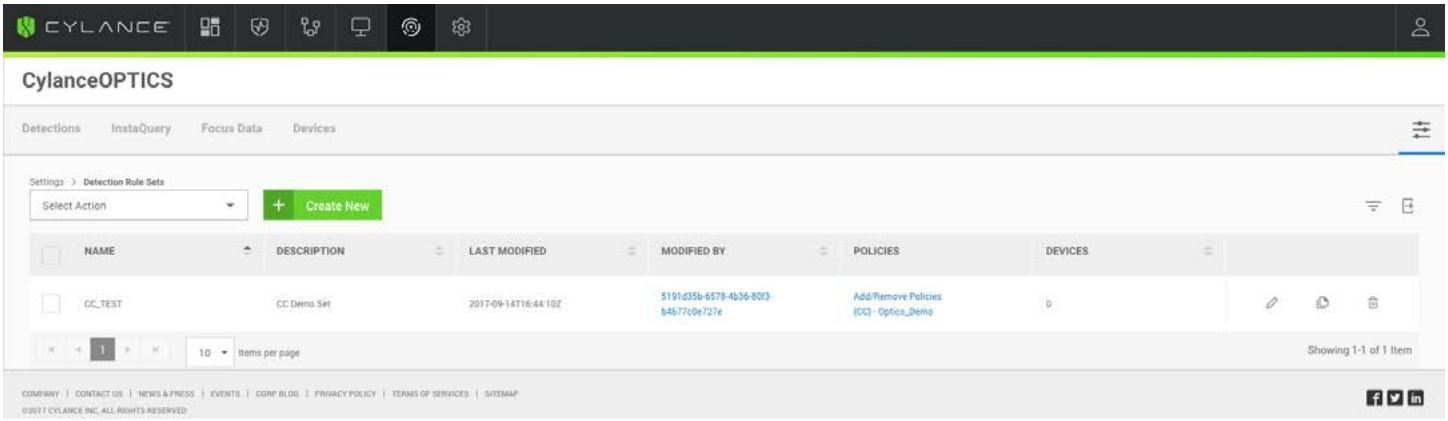

Figure 2: Detection Rule Set Listing

The **Create New** button displays a configuration wizard where users can select which rules they would like enabled, as well as which automated responses to take on a per-rule basis. The user also must provide a unique Set Name and Description. After completing the wizard, the new Detection Rule Set will be visible in the list where it can be applied to a Device Policy.

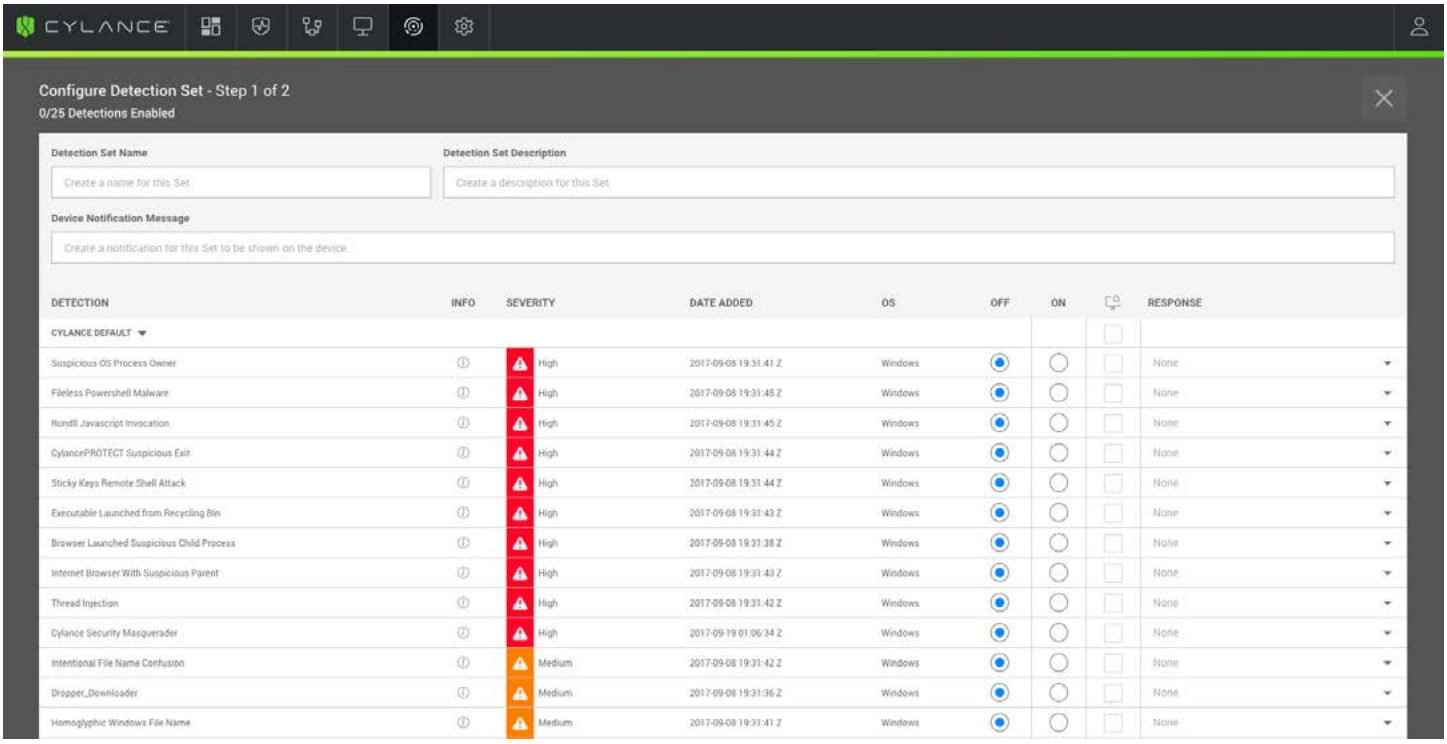

Figure 3: Create a Detection Rule Set

Applying a Detection Rule Set To a Device Policy

Once a user has sufficiently configured a Detection Rule Set, they can associate it with a Device Policy to complete the final step needed to receive detection alerts from endpoints with CylanceOPTICS installed. When the Device Policy is saved, it will prompt all endpoints with the policy applied to retrieve the Detection Rule Set, consisting of rule, automated response, and endpoint notification configurations, from Cylance's cloud services. Any devices that are added to the policy will also have these configurations applied upon connection to Cylance's cloud services.

Viewing and Interacting with Detection Alerts

The default **Detections** tab in CylanceOPTICS provides users with a clean, yet detailed, view into alerts triggered by endpoints configured with the Context Analysis Engine. From this dashboard, users can see trends in events over varying time frames, the severity of different detections, and a summary view of each of the detections that has occurred. Filtering and sorting features present in the dashboard allows users to further drill into the data presented to further identify trends throughout the environment

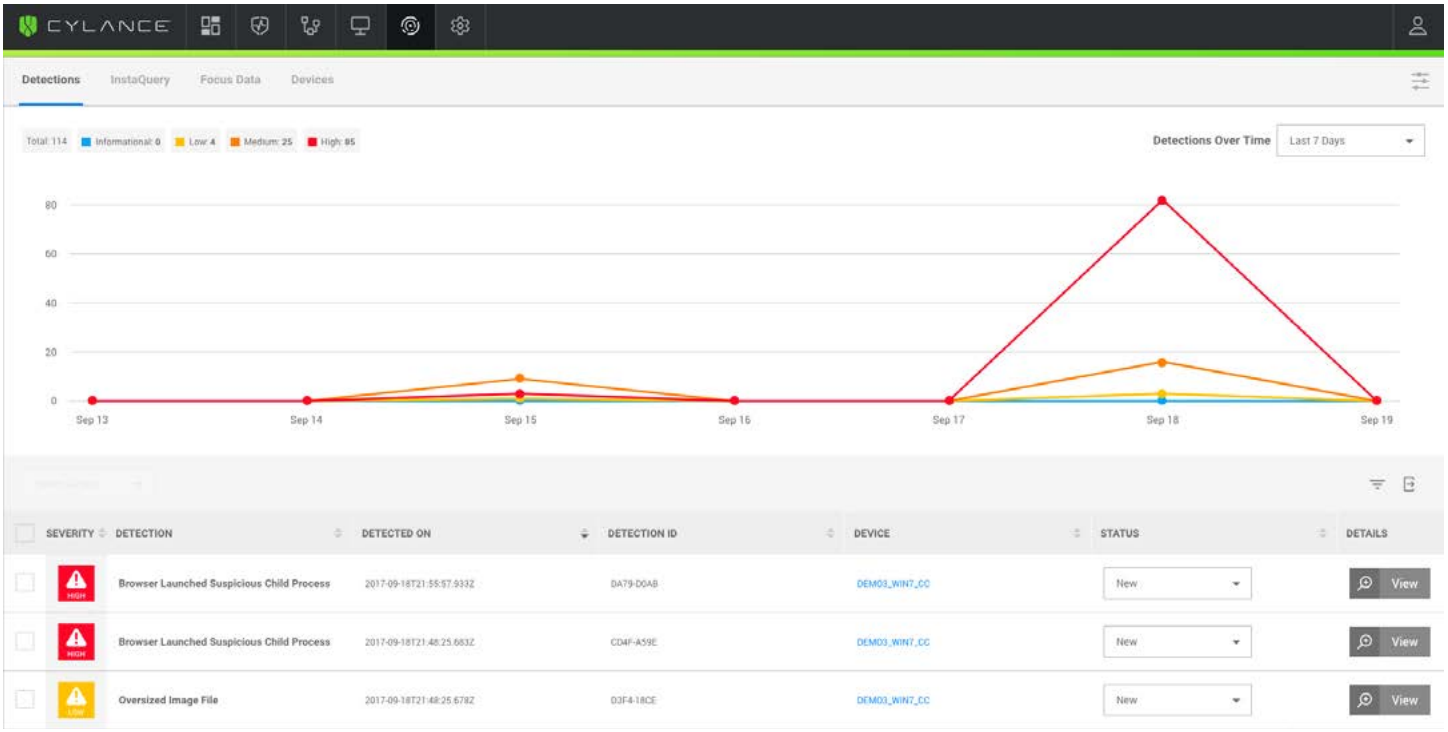

Figure 4: Detections Dashboard

Each detection event contains an entire series of data that can be viewed by clicking the **View** button in the rightmost column of the dashboard's table. The resulting Detection Details page displays a wealth of information about the detection, including the detection's name, severity, and description, as well as the number of events, artifacts of interest, and automated responses associated with that detection.

The Detection Details page also allows for further interaction and investigation by acting as a platform to launch Device Lockdowns, File Retrievals, and Focus Views where applicable. Supporting events and artifacts associated with the detection can be further analyzed to provide users with additional context around why the detection was triggered so that further investigations or responses can be taken if needed.

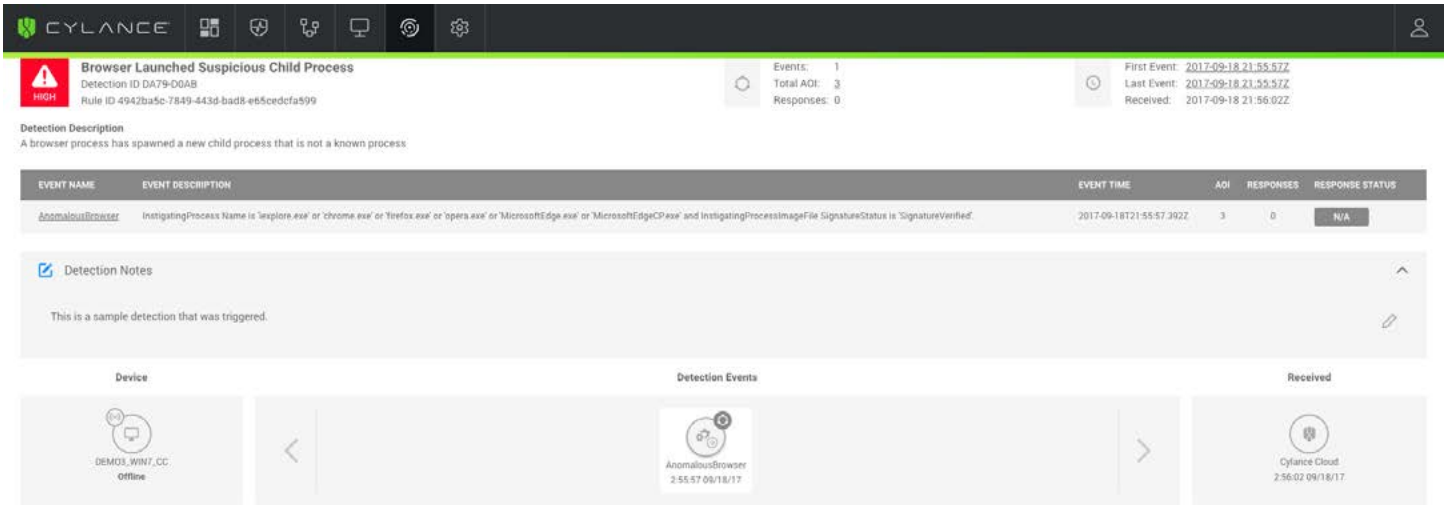

Figure 5: Detection Details

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618