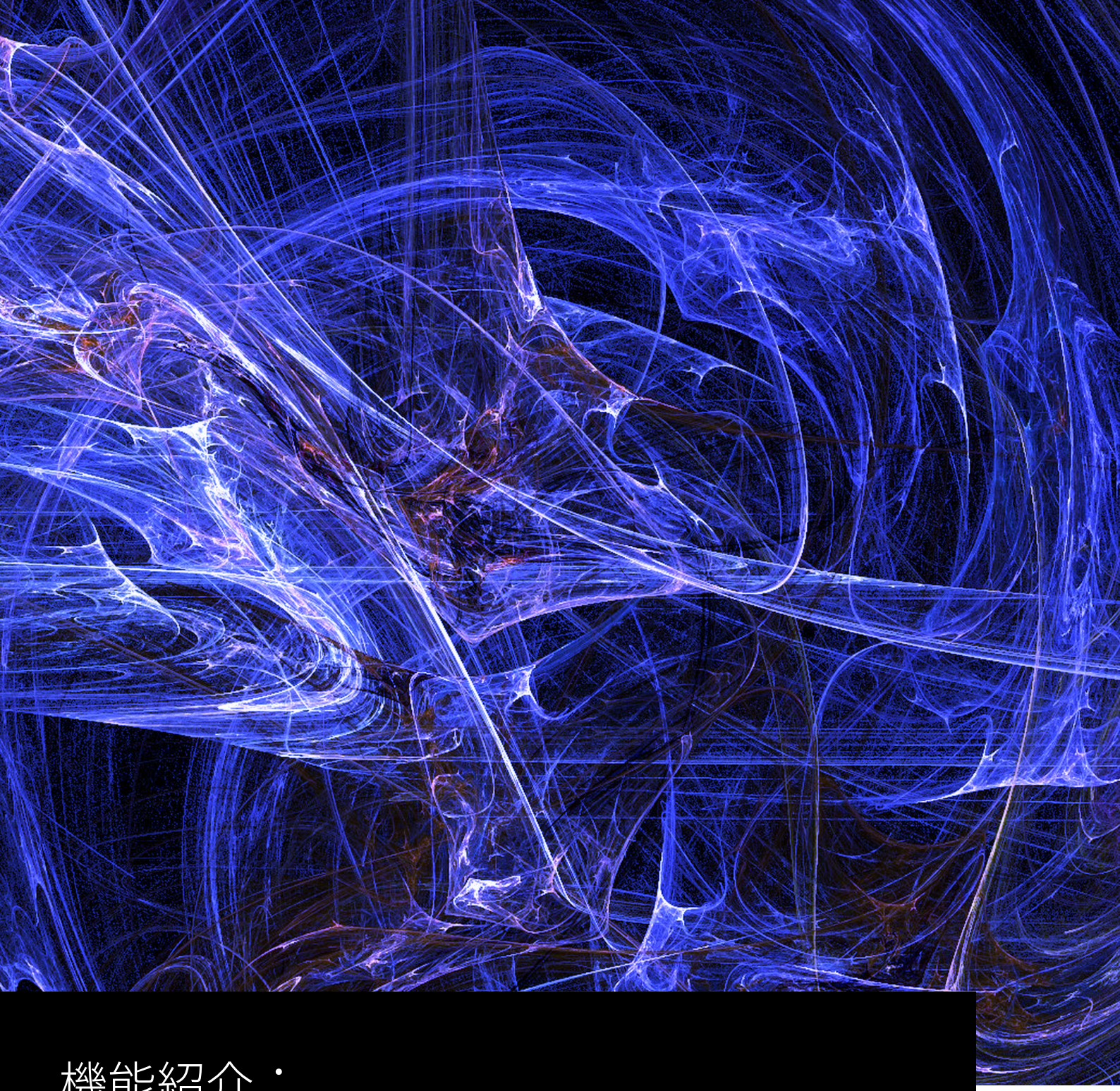

機能紹介：
コンテキスト分析エンジン

CylanceOPTICS™ による動的な脅威検知と
自動的な対応アクション

CYLANCE

すばやく脅威を検知して対応できるかどうか――それにより、些細なセキュリティ侵害で済むのか、トップニュースで報じられる重大な侵害にまで発展するのかが決まります。残念ながら、現在市場に出回っているセキュリティ製品の多くは、迅速に脅威を検出して対応できるとうたってはいるものの、そのインフラストラクチャでは、遅延や誤検知、全社規模の可視化における制限などの問題が発生しがちです。

これらの問題を解決するため、Cylance®（以下、サイランス）は、脅威の検知と対応に役立つ新しいアプローチとして、両方の処理をエンドポイントレベルで行う「**コンテキスト分析エンジン**」を開発しました。このエンジンによって、組織内のエンドポイントが、人の手を煩わせずに 24 時間体制で動的に脅威を検知して対応アクションを実行できる、独自のセキュリティ管理センターの役割を果たすようになります。その結果、セキュリティチームは、CylanceOPTICS のコンテキスト分析エンジンにエンドポイントとビジネスのセキュリティを安心して任せられるので、高度な脅威の調査や、セキュリティインフラストラクチャの全体的な改善といった、ビジネス上重要なプロジェクトに集中できるようになるでしょう。

コンテキスト分析エンジンとは

CylanceOPTICS のコンテキスト分析エンジン（CAE）は、高性能な分析・相関エンジンであり、エンドポイントでのイベントを監視してイベントの発生をほぼリアルタイムで検知し、悪意のあるまたは疑わしいアクティビティを特定します。エンジンをエンドポイントに展開すると、クラウドへの接続に依存する（つまり、クラウドへの接続を必要とする）ことなく、24 時間 365 日監視が行われます。CAE のアーキテクチャは、インテリジェントな意思決定を行ううえで有効なネットワーク接続を必要としないため、パフォーマンスに影響が及ぶリスクを抑えながら複数の疑わしい侵入経路を継続的に監視できます。

CAE が悪意のあるアクティビティのリスクを発見した場合に、関連付けられた対象のアーティファクトに対して自動化されたアクションが人の手を煩わせずに実施されるよう設定できます。それらのアクションはエンドポイント上で実施され、クラウドへの接続が不要なので、他のクラウドから脅威の検知と対応を行う製品に生じがちな遅延を抑えられます。

CAE の機能と構成を確認するには、サイランスが提供するクラウドベースの管理コンソールの「**Detections**」タブにアクセスします。「**Detections**」ダッシュボードでは、ユーザーは環境で発生しているイベントのトレンドをすばやく把握して確認できます。このダッシュボードから、ユーザーは該当のイベントを調査したり、それぞれのイベントに対応したりできます。1 つまたは複数のデバイスポリシーに適用できる検知ルールセットを作成することで、CAE を多くの環境に適合するよう容易に構成できます。

統合された操作環境を提供するため、コンソールの新しい「**Detections**」セクションは、他の CylanceOPTICS 機能を統合して設計されています。追加のフォーカスビューを作成したり、ファイルの取得機能を使用して気になるファイルを取得したり、デバイスのロックダウンを実施して感染が疑われるエンドポイントをネットワークから隔離したりすることで、CAE によって特定されたイベントとアーティファクトから拡張できます。

注：CylanceOPTICS のコンテキスト分析エンジンと対応策を使用するには、CylanceOPTICS 2.1.1000 またはそれ以上がインストールされている必要があります。

コンテキスト分析エンジンの構成

デフォルトでは、CylanceOPTICS のコンテキスト分析エンジンの「Rules」や「Response Actions」は構成されていません。そのため、ユーザーが最初に Cylance 管理コンソールの CylanceOPTICS セクションにアクセスすると、「**Detection Environment**」オンボーディングページが表示されます。

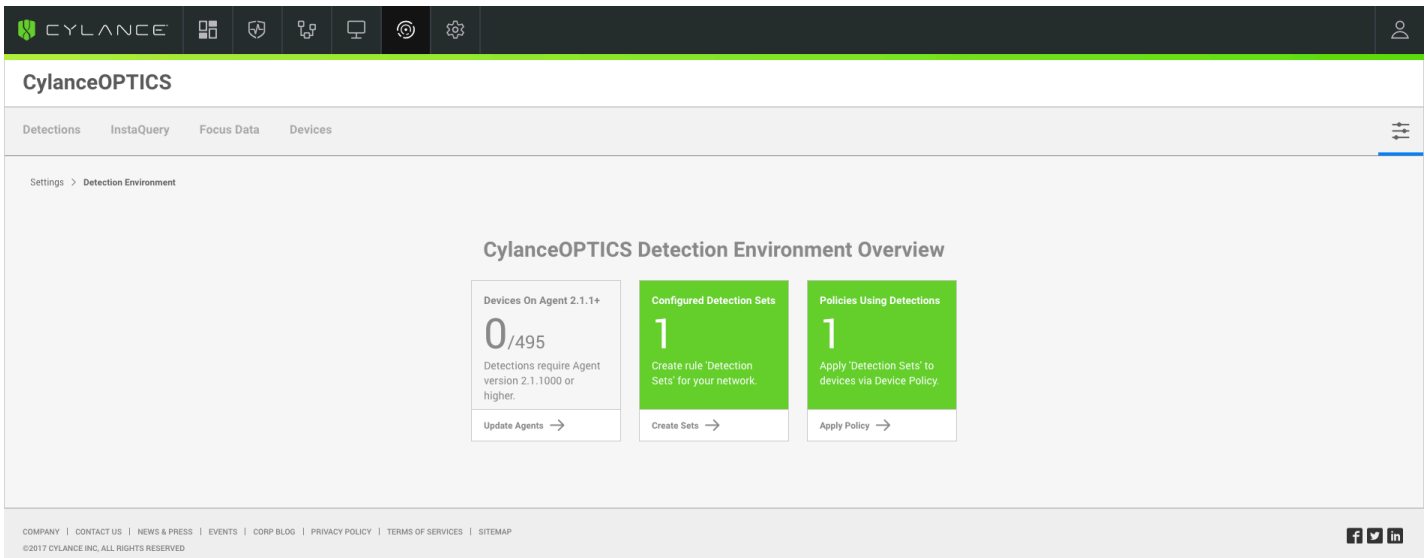

図 1: CylanceOPTICS の「Detection Environment」オンボーディングページ

オンボーディングページには、次のような現在構成されている CAE の設定の概要が表示されます。

- CylanceOPTICS バージョン 2.1.1000 またはそれ以上がインストールされているデバイスの数
- 構成済みの検知ルールセットの数
- 検知ルールセットが選択されているデバイスポリシーの数

注：コンテキスト分析エンジンの「**Detections**」を有効にするための最小要件を満たすと、オンボーディングページがデフォルトで表示されることはなくなります。オンボーディングページには、「**Settings**」スライダをクリックして「**Detection Environment**」オプションを選択すれば、いつでもアクセスできます。

検知ルールセットの構成

オンボーディングページの中央のボックスには、テナントに存在する検知ルールセットの数が表示されます。検知ルールセットの構成はコンテキスト分析エンジンの中心であり、エンドポイントに適用する検知ルール、対応アクション、エンドポイント通知などを決定します。最終的に検知ルールセットはデバイスポリシーベースでエンドポイントに適用されます。つまり、ユーザーが検知ルールセットを選択してデバイスポリシーに適用します。エンドポイントは、ポリシーが適用されたときに目的の検知ルールセットを自動的に受け取ります。

CylanceOPTICS には、次の属性を持つデフォルトの検知ルールセットが含まれます。

- すべてのツールが有効
- すべてのアクションが無効
- すべてのエンドポイント通知が無効

この構成は、テストおよび初期導入を目的として、「チューニング」または「監視のみ」のモードで機能するよう設計されています。ユーザーは誤検知をトリガする可能性のある環境領域を把握できるため、必要に応じて自動アクションを調整できます。

カスタムの検知ルールセットを作成するには、「**Settings**」スライダに移動して「**Detection Rule Sets**」オプションを選択します。このメニューには、現在のすべての検知ルールセットがリストされるとともに、現在の検知ルールセットをコピー、削除、または編集するためのオプションが表示されます。また、新しい検知ルールセットを作成するためのリンクも含まれます。

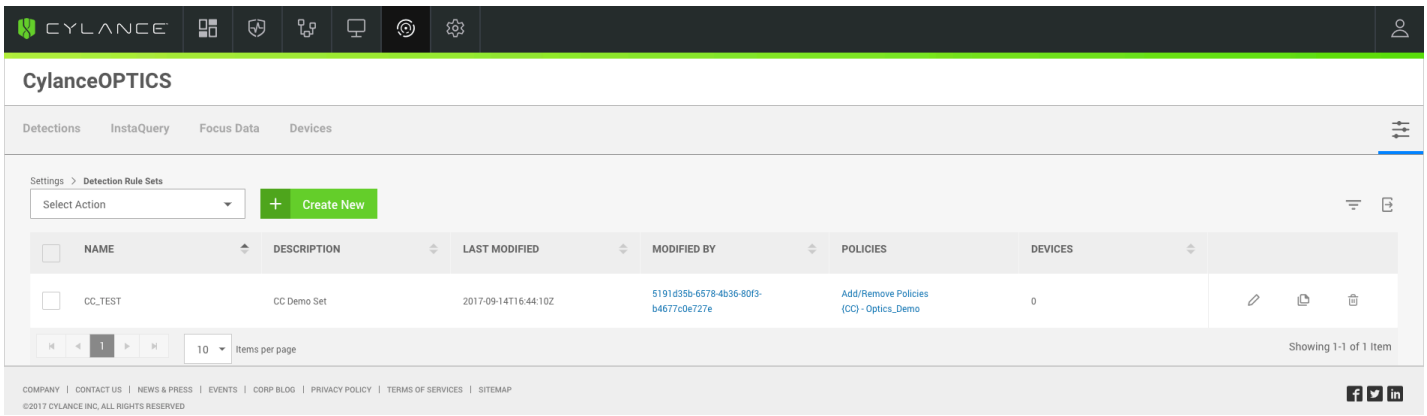

図 2: 検知ルールセットのリスト

「**Create New**」ボタンをクリックすると設定ウィザードが表示され、有効にしたいルールを選択することや、実行したい対応アクションをルールベースで選択することができます。また、ルールセットには一意の名前と説明を指定する必要があります。ウィザードを完了すると、新しい検知ルールセットがリストに表示され、デバイスポリシーに適用できるようになります。

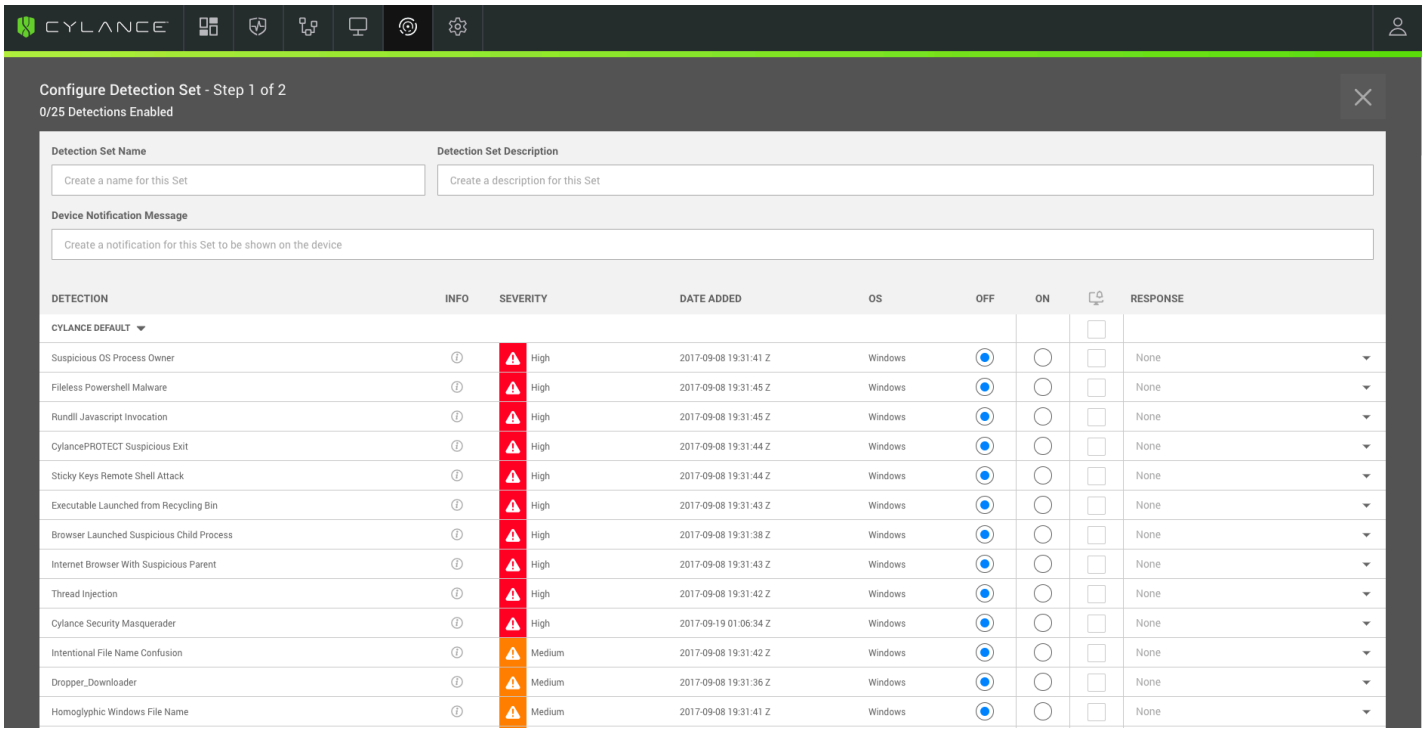

図 3: 検知ルールセットの作成

デバイスポリシーへの検知ルールセットの適用

検知ルールセットを適切に設定すると、そのセットをデバイスポリシーに関連付けて、CylanceOPTICS がインストールされたエンドポイントから検知アラートを受け取るために必要な設定は完了になります。デバイスポリシーを保存すると、そのポリシーが適用されたすべてのエンドポイントが、サイランスのクラウドサービスから検知ルールセット（ルール、対応アクション、エンドポイント通知の設定）を取得します。ポリシーに追加されたすべてのデバイスで、サイランスのクラウドサービスに接続された際にこれらの設定が適用されます。

検知アラートの表示と操作

CylanceOPTICS のデフォルトの「**Detections**」タブでは、コンテキスト分析エンジンで構成されたエンドポイントによってトリガされたアラートについて、見やすい詳細なビューがユーザーに提供されます。このダッシュボードから、ユーザーはさまざまな時間枠におけるイベントのトレンド、各検知の重大度、および発生した各検知の概要ビューを参照できます。ユーザーはダッシュボード内のフィルタリング機能とソート機能を使用し、表示されたデータをさらに掘り下げて、環境全体におけるトレンドをより詳細に把握できます。

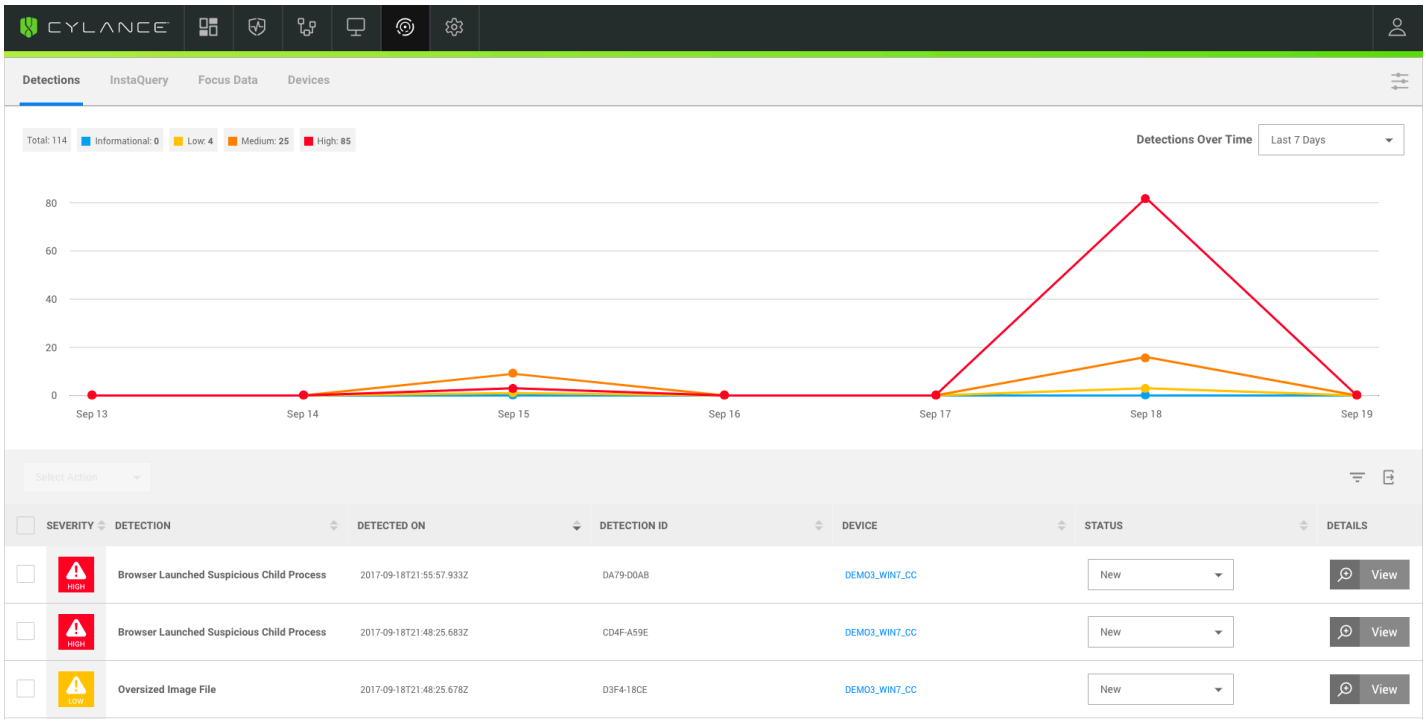

図 4:「Detections」ダッシュボード

各検知イベントには一連のデータがすべて含まれており、そのデータはダッシュボードのテーブルの一番右にある列の「**View**」ボタンをクリックすると表示できます。結果の「Detection Details」ページには、検知に関する豊富な情報が表示されます。たとえば、検知の名前、重大度、説明のほか、イベント数、注目されるアーティファクト、その検知に関連付けられた対応アクションが表示されます。

「Detection Details」ページでは、状況に応じてデバイスのロックダウン、ファイルの取得、フォーカスビューを開始することで、より詳細な操作や調査を行うこともできます。検知に関連付けられた裏付けとなるイベントやアーティファクトをさらに分析して、検知がトリガされた理由に関する追加のコンテキストを提示し、必要に応じてより踏み込んだ調査や対応を行えるようにすることも可能です。

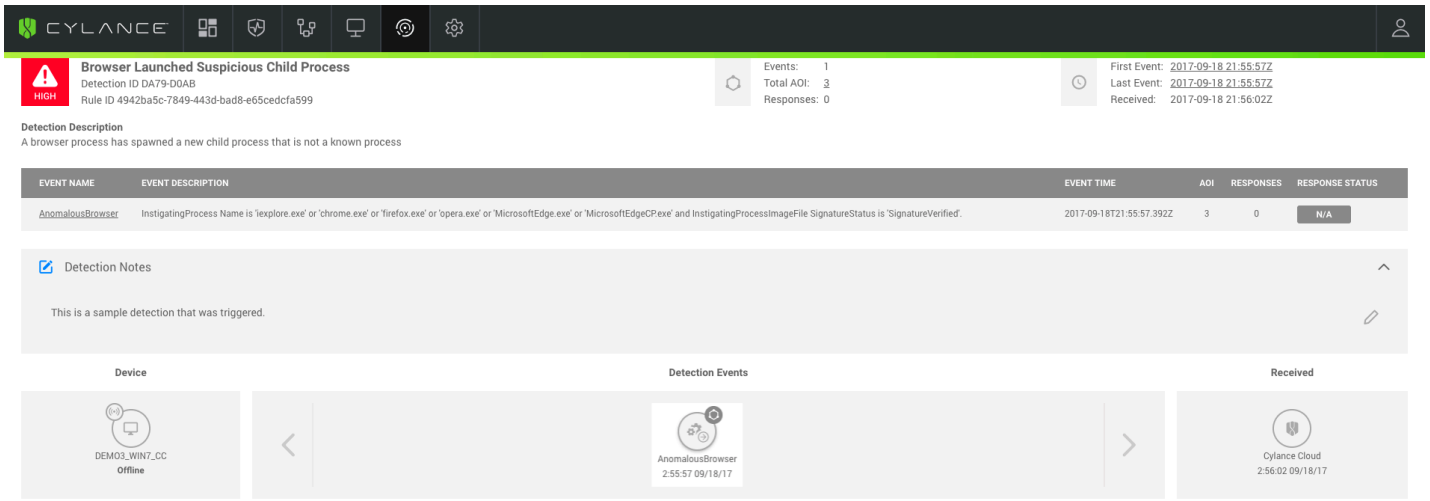

図 5:「Detection Details」ページ

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)