CylanceOPTICS™

CylancePROTECTに追加されたEDR機能モジュールで、
端末上でのイベントをモニタリングした上で脅威の可視化、分析、調査、そして対処を実現します。

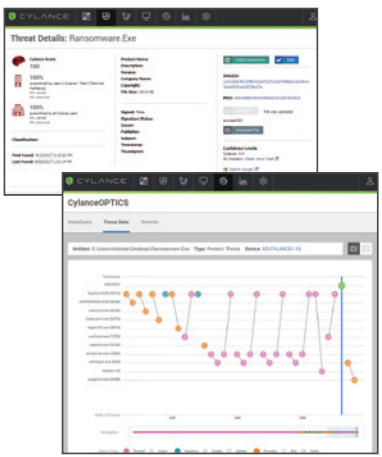
CylanceOPTICS™ の特徴

CylancePROTECT と統合
同一コンソール上で設定・管理が可能

AIを活用
機械学習をイベント分析そして防御に応用

予防にフォーカス
あくまで被害を防ぐことが最優先

- ☑ 分散型モデルによるイベント情報収集
- ☑ 根本原因分析による侵入経路特定
- ☑ 隠れた脅威のハンティング
- ☑ 脅威の封じ込めによる被害の最小化
- ☑ 端末挙動からの動的な脅威検知と対処



利用シーンと目的に応じた製品のカバーエリア

利用ケース	求められる要件	Cylance PROTECT	CylancePROTECT with OPTICS
脅威活動の停止	悪意ある実行ファイルのエンドポイント上での実行を防ぐ	☑	☑
	許可されないスクリプトの実行を防ぐ	☑	☑
	ファイルレスマルウェアによるメモリの不正利用からの防御	☑	☑
	メールに添付された悪性ファイルの実行を防ぐ	☑	☑
	予めインストールされたアプリケーション以外の実行を防ぐ	☑	☑
	感染端末へのインシデントレスポンスと封じ込め		☑
疑わしい活動の確認	悪意ある活動の調査や確認		☑
	侵入経路分析の実施や攻撃/脅威の発生元の特定		☑
脅威ハンティング	疑わしい活動のレビュー		☑
	現状および統計データからの状態のサーチ		☑
	IOC（Indicatorsof Compromise）情報に基づくチェック		☑
疑わしい活動の検知	ルールベースでの脅威イベントの検知		☑