EDR/XDRとは

EPP/EDR/XDR 概要紹介

EPPとは

- “Endpoint Protection Platform”の略
  侵入を試みる脅威に対して直接ブロックや駆除などの対応を行うことで、
  PCやサーバーなどの端末（エンドポイント）をマルウェア感染から守る
  セキュリティ対策の1つ

当社ソリューションだと

<クライアント対策>

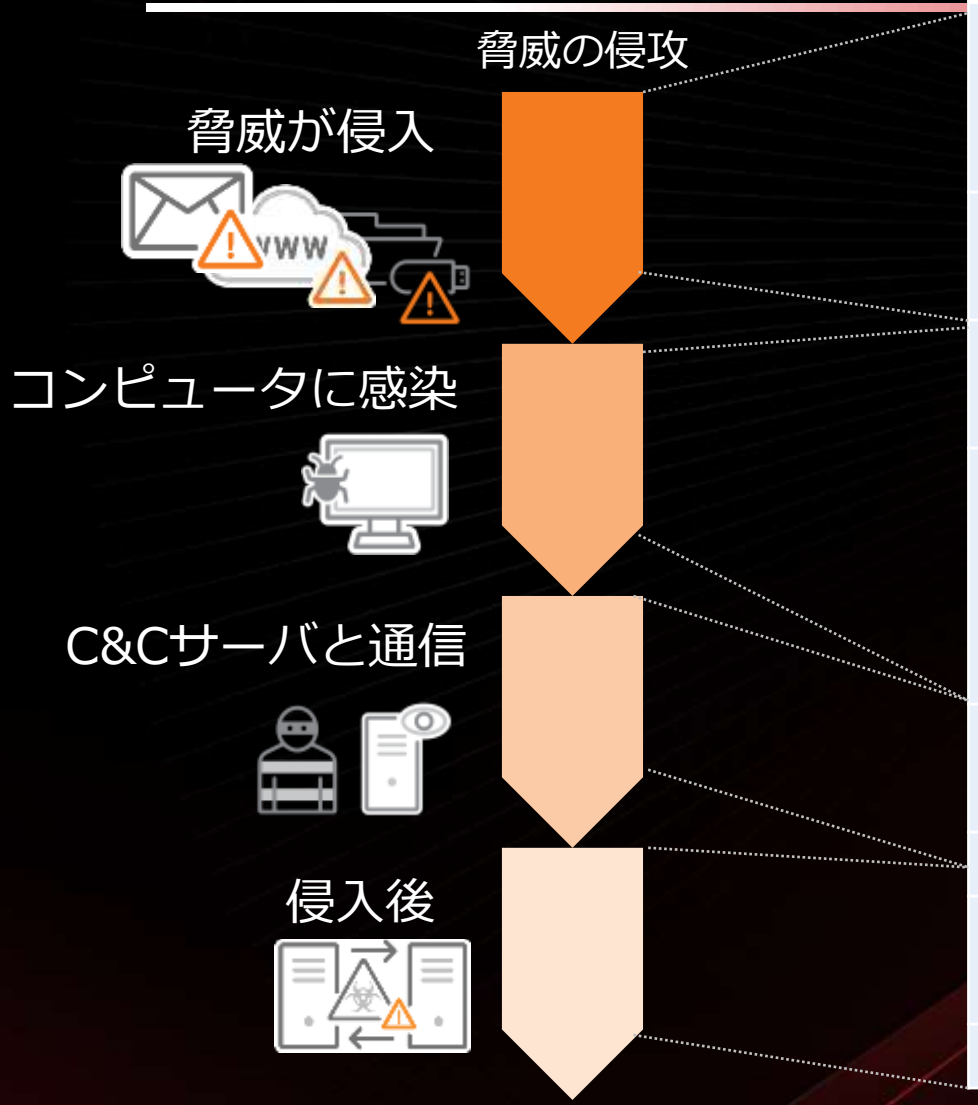
- **Apex One**
- **Apex One SaaS**

<サーバ対策>

- **Deep Security**
- **Cloud One Workload Security**

などが該当します。

シングルエージェントで複数技術を組み合わせ、多層防御を提供



Apex One が提供する機能	
通信制御	ファイアウォール
	Webレピュテーション
	仮想パッチ(IPS)
未然防止	デバイスコントロール
	アプリケーションコントロール
既知の脅威対策	パターンマッチング・スマートスキャン
	スパイウェア対策
未知の脅威対策 ・ファイル特性 ・ふるまい検知	機械学習型検索(ファイル)
	挙動監視・イベント監視・ランサムウェア対策
	機械学習型検索(プロセス)
	サンドボックス連携
通信検知	Webレピュテーション
	不審接続監視
横感染防止	仮想パッチ(IPS)
XDR	Endpoint Sensor: アクティビティを元にした痕跡の検出(EDR※)
	Endpoint Sensor: データレコーディングによる侵害調査(EDR※)
復旧	ダメージクリーンナップエンジン

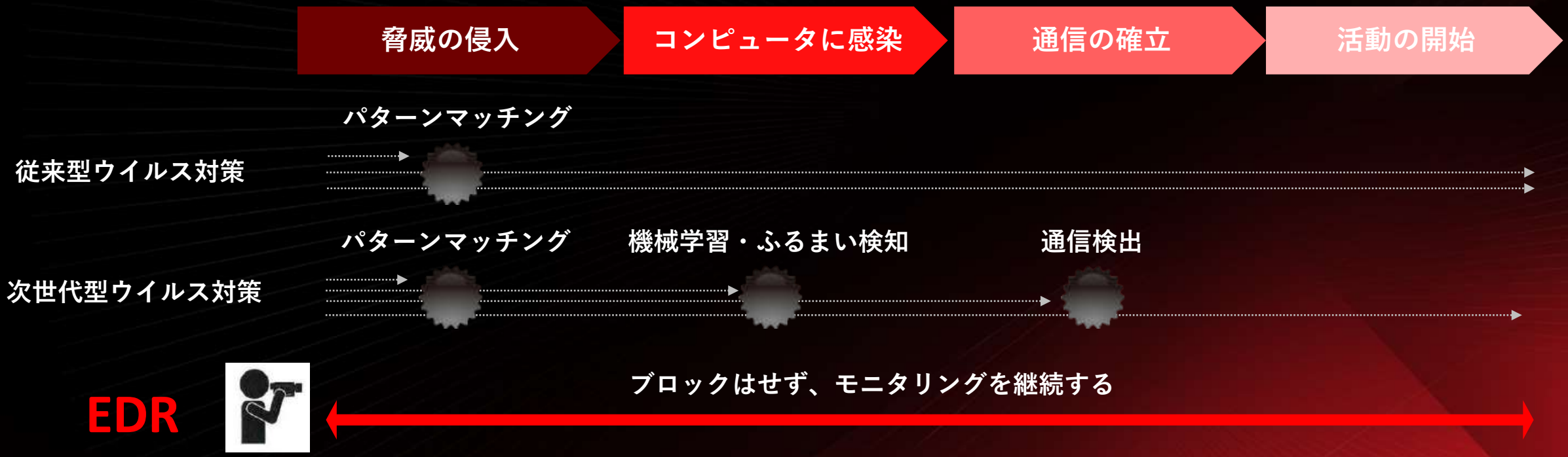
※EDR = Endpoint Detection and Response

EDR はエンドポイントにおける検知と対応を行うソリューション

Endpoint Detection & Response

検知　　インシデント対応

インシデントの早期検知と対処に役立つのが ”EDR”



- ウイルス対策技術(EPP)は不正な侵入を止めるアプローチ
- EDRは侵入から活動まで正/不正に関わらず記録し続けることで後から脅威を可視化するアプローチ
  - ① シグネチャに依存しないのでファイルレス攻撃にも対応し、検知することが可能
  - ② 正/不正に関わらず記録し続けているので検知後の侵入経路特定も可能

EDR による可視化と対処

エンドポイントにおける
日々のイベントや
プロセスを記録

↓

脅威情報※を元に調査、
被害状況や影響範囲を
特定

※ドメイン名, IPアドレス, ファイル名, ハッシュ値など

↓

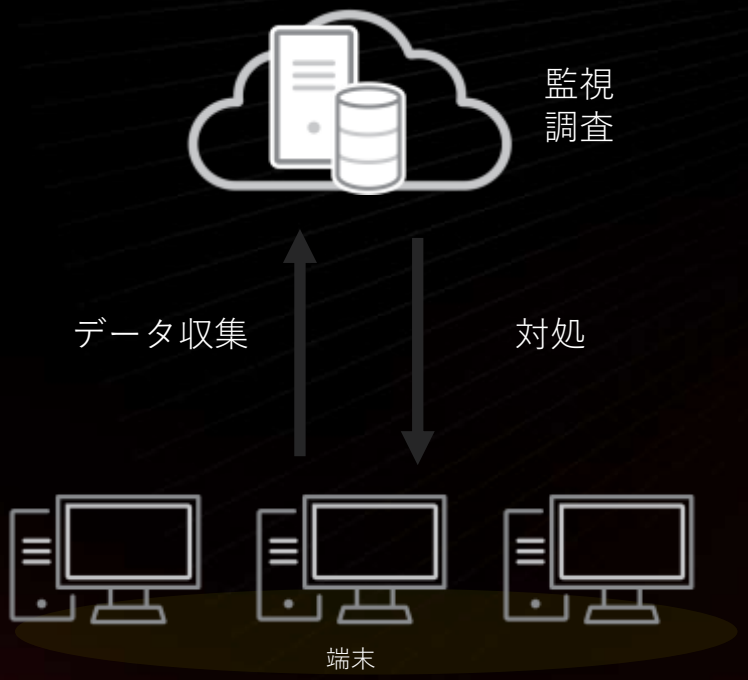
侵入経路や感染拡大
の流れを可視化、
結果を元に対処

よく使われる例え： ドライブレコーダー

EDRをさらに拡張し、レイヤーを跨いだ検出/解析を可能にしたのが “XDR”

TrendMicro XDRは、端末に加え**拡張された領域**の
センサーから収集した情報を使い**高度な脅威解析を行う技術**です。

一般的なEDR
（Endpoint Detection & Response）



TrendMicro XDR
（Extended Detection & Response）

XDRの検出ロジック: クロスプロダクト

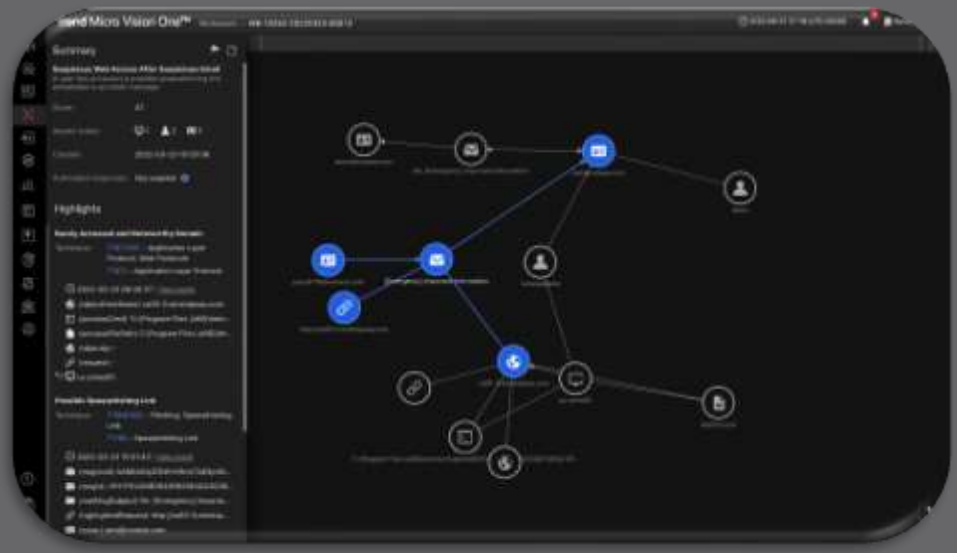
XDRでは、**複数レイヤーの製品を横断して**検出情報を収集し、**それらを相関させる**ことによって、より確度の高い脅威を検出することが可能となります。

XDRの検出ロジック: クロスプロダクト

EPPのみ

EPP + XDR (エンドポイント/ネットワーク/E-mail)

Workbench



セキュリティレイヤーを超えて
疑わしいふるまい、マルウェアなど
攻撃の検知、調査、対応を可能に

複数レイヤーにセンサーを導入することで
EPPだけでは気がつけない攻撃を捉える可能性向上

EMOTET侵入時にEPPが出力するアラート例

検知フェーズ	検知機能	検知対象(例)	検知名(例)	処理結果
マクロ開封時	リアルタイム検索	20220308.xls	Trojan.X97M.EMOTET.YXCB2	隔離
	機械学習型検索	20220308.xls	TROJ.Win32.TRX.XXXM09AHM	隔離
	挙動監視	Powershell.exe (マクロが実行したコード)	不正な挙動のブロック	停止
DLLダウンロード	リアルタイム検索	wtfkxwc.dll	Trojan.Win32.EMOTET.UWAOIBEMZ	隔離
	機械学習型検索	wtfkxwc.dll	TROJ.Win32.TRX.XXPE50F13015	隔離
情報収集	Webレピュテーション 不審接続監視	http://wrs71.winshipway.com/abc/index.html	C&Cサーバ	ブロック

⇒ 各フェーズごとに単発の検出ログ記録となるため、攻撃の全体像の把握が難しい

EDR/XDRを導入した場合

ランサムウェアなどの感染により個人情報の漏えいが確認された場合、関係各所への報告、情報公開が必要となります。
その際、**「実際の被害範囲/発生原因/再発防止策 」を適切かつ迅速にまとめる必要があります。**
しかし実際には様々な検出ログを確認して解析する必要があり、**全体像の把握には高度なスキルと時間を要します**。
EDRは情報を可視化し脅威の全体像をとらえるため、発生の経緯と対処すべき項目を迅速に把握することができます。

攻撃の見え方(イメージ)

検出ログからは個別に対処結果を把握できますが、攻撃の全体像の可視化までは行えません。
EDRでは「攻撃の一連の流れ」を常時記録することで、全体像の把握を実現します。

EDR/XDRによる可視化～対処の流れ

影響範囲の可視化

- 組織内で脅威の影響がどこまで拡がっているかを確認します

根本原因調査 (Root Cause Analysis)

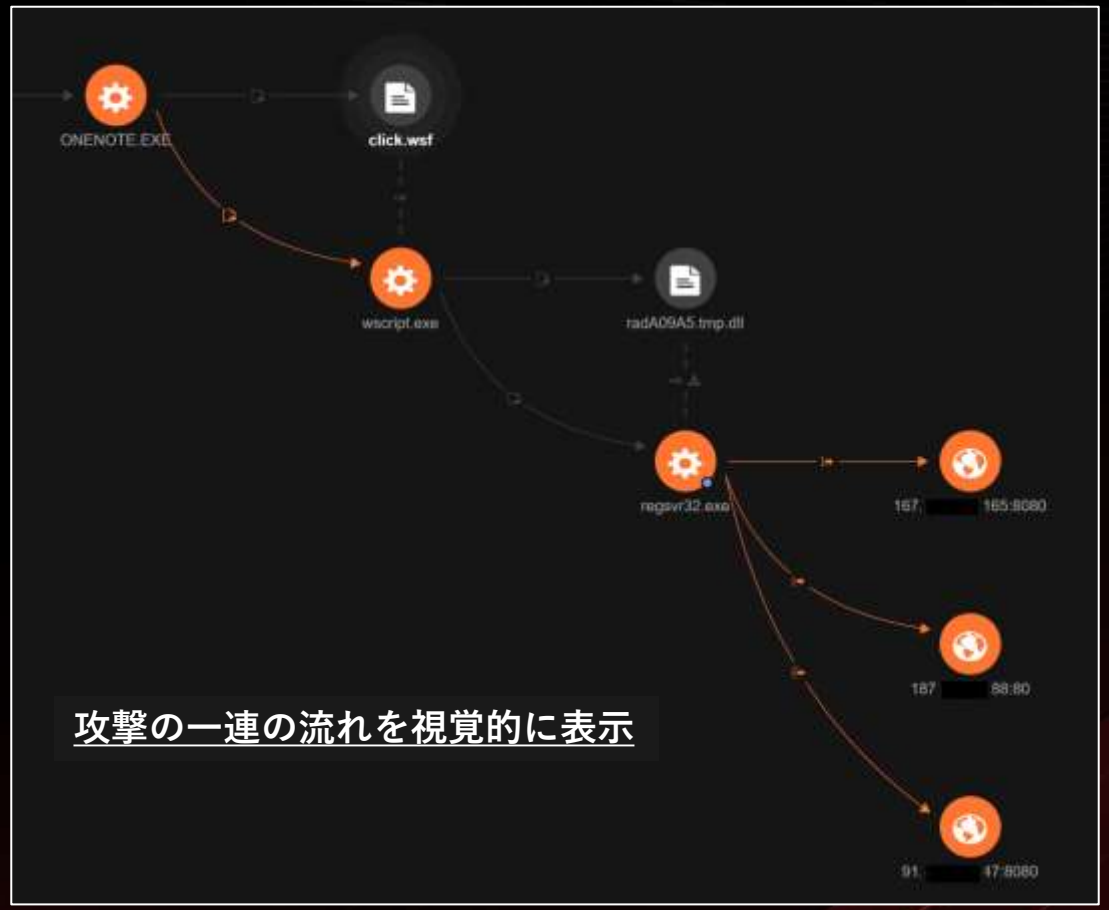
- 特定の端末における脅威の活動から侵入プロセスの詳細を可視化/調査します

対処

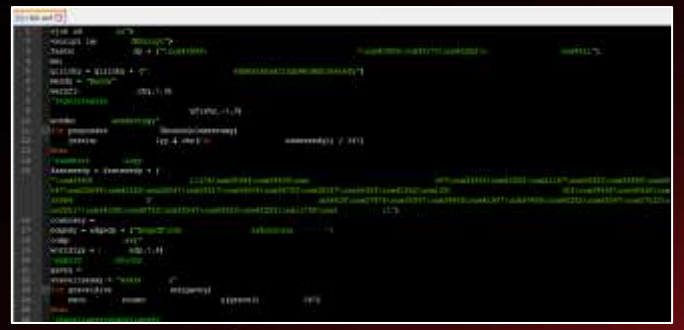
- エンドポイントの隔離/復旧
- 不正プロセスの終了
- ブロックリストへの追加/解除　　など

EDR/XDRによる検知アラート例 (OneNote型EMOTET検出)

検出名: **Possible Execution of Malicious Command via OneNote**



1. **OneNoteを起動し、Viewボタンを押すと、Windowsスクリプトファイル(click.wsf)がwscriptによって実行される。**



*難読化されたclick.wsf (一部マスク済)

2. **その結果、EMOTET本体であるdllファイル(radA09A5.tmp.dll)が生成され、regsvr32.exeで実行される。**
3. **その結果、外部のC&Cサーバへ通信を行っていたことを確認**

