

Endpoint Detection and Response 技術サポート

当資料は Endpoint Detection and Response (EDR)利用時の技術サポート提供範囲についての解説となります。

- EDR とは？

従来のエンドポイントセキュリティ製品 (EPP)が「侵入を防ぐことに特化」していたのに対し EDR は「侵入を許してしまった後の対応」に焦点を当てています。EDR はコンピュータ端末内プロセスアクティビティを一連の動作(コンテキスト)/近接時間帯他プロセスを含めて統合的にモニターし「深刻スコア」が一定に達した際 Broad Context Detection (BCD)を生成します。導入企業は BCD を監視し適切な対処を行う必要があります。Withsecure EDR 製品購入は製品使用ライセンスのみを含み、BCD イベント脅威分析サービスは提供されません。その為 EDR 製品をご利用いただく場合 BCD インシデント(※)に対する日常的な脅威分析オペレーションが必要となります。EDR 製品のインストールや Elements Security Center 操作についての技術サポートは Withsecure から提供させていただきます。

- BCD オペレーションとは？

日常的に BCD を監視し適切な対処を行うオペレーションが必要となります。社内管理者のアクティビティ(リモートコマンド/プロセス制御/etc)も BCD イベント生成トリガーとなります。その為下記のようなオペレーションが必要となります。

- A. BCD 誤検知判断後、「閉じる」→「誤検出」登録処理
- B. 誤検知判断後、「閉じる」→「受け入れられる動作」登録処理
- C. 誤検知判断後、端末調査(フルスキャン/ユーザ聞き取り調査等)
- D. 「エスカレーション」での Withsecure 脅威分析(有償の誤検知/脅威分析)
- E. 多数の類似検知が発生した際のホワイトリスト登録(Withsecure サポートへの依頼)
※プロセスや実行条件等がハッキング等の脅威に非常に類似している場合、ホワイトリスト登録では検知抑制ができない場合があります。その場合該当プロセスや実行環境の見直し等が必要となります。

- Managed Detection and Response (MDR)/Security Operation Centre SOC) とは？

EDR で検知されたインシデント (BCD)を日常的に脅威分析する為の有償オペレーションサービスとなります。EDR を導入したがインシデント監視や脅威分析を日常的に行えない企業が利用するサービスとなります。Withsecure では英語ベースでの提供となります。

- ホワイトリスト登録とは？

多数の類似検知が発生しその原因となるプロセスが安全と判断できる場合、Withsecure に該当プロセスを報告する事で BCD 検知から除外する作業。脅威分析はプロセス実行環境を含めたスコア制で行われ、実行環境(ユーザ/オプション)等が異なる場合除外は適用されません。その為完全に検知抑制する事はできません。

- 受け入れられる動作とは？

ユーザ企業管理者のメンテナンス作業等が BCD 検知された際、該当作業を「閉じる」→「受け入れられる動作」に登録する事で自動的に「誤検知」として閉じる事。

<https://www.withsecure.com/content/dam/with-secure/ja/support-news/support-news/2024/20240628-EDRAcceptedBehaviourRev02.pdf>

[Elements EDR - New Feature - Accepted Behavior - WithSecure Community](#)

Tips

Q1. EPP/EDR において、ネットワーク隔離が機能しない

A1. GPO にて、ローカルシステム上でシステム権限で Windows Firewall のルールの書き換えができないような設定の場合、ネットワーク隔離が動作しません。GPO で Windows Firewall のルールの変更ができるように GPO での管理を無効にしてください。

Q2. EPP/EDR において、隔離はできるが、隔離後の解放ができない

A2. 端末上に URL フィルタリングやネットワーク隔離機能を有するエージェントが起動し、クラウドプロキシを参照している場合、隔離中の接続がそのプロキシを経由するため、WithSecure のセキュリティクラウドにつながらず、解放できません。該当エージェントを Firewall の設定でプロセス除外し、クラウドプロキシにてセキュリティクラウドで必要なドメインへの接続許可が必要になります。