【お知らせ】Elements EDR - Accepted Behaviour(受け入れられる動作)について

2024 年 07 月 01 日 12:00(発行)

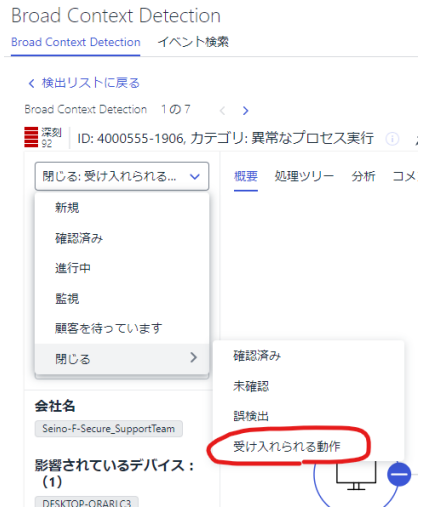
Elements Seurity Center EDR サービスにおいて新機能” Accepted Behaviour(受け入れられる動作)”がご利用いただけるようになりました。当機能はユーザにおいて安全と判断した動作/ファイル等を EDR 検知(BCD イベント)から除外(自動クローズ)するルールを作成する機能となります。当機能を利用する事で「社内作成プログラムの突然の大量検知」等が発生した際の緊急対応が可能となります。BCD イベントのホワイトリスト登録リクエストについては引き続きサポートセンターで受け付け可能です。

コミュニティ記事

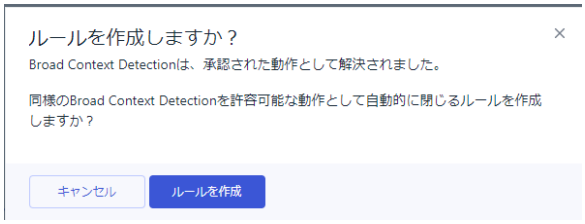
Elements EDR - New Feature - Accepted Behavior - WithSecure Community

当機能は各企業の管理者安全性判断の下、自己責任でのご利用となります。弊社での“最適除外ルール作成提案”等は承れない事をご了承ください。

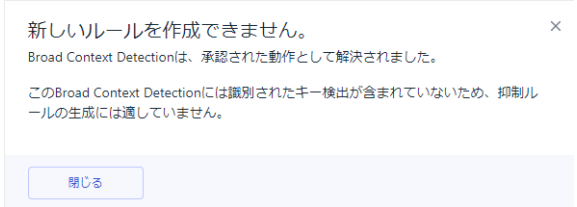
- Accepted Behaviour(受け入れられる動作)の作成方法
  1. BCD イベントの詳細は開き、ステータスを「閉じる」→「受け入れられる動作」で閉じます。



  2. 下記のルール作成確認画面が表示されます。



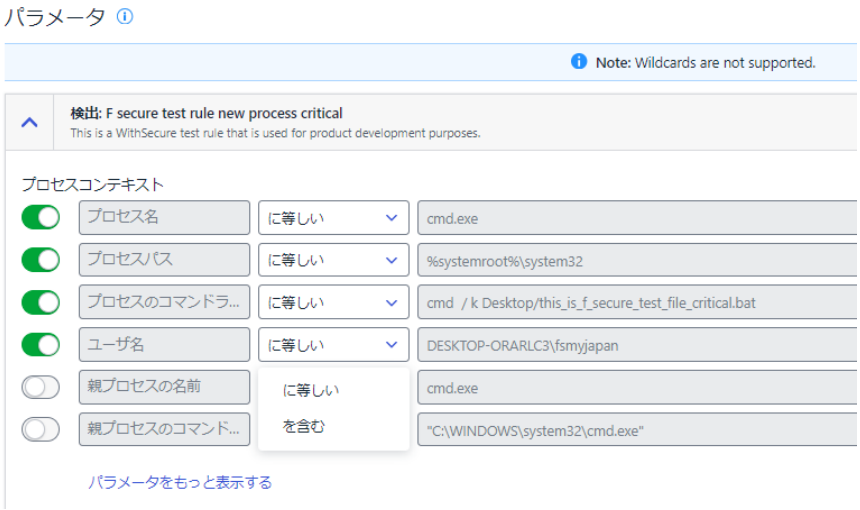
※BCD にルール作成に適した検出が無い場合はルールは作れません。



  3. ルールの適用範囲を選択します。
     対象組織においてすべてのデバイスを対象にする場合は「すべてのデバイス」を選択。BCD が検出さ

れたデバイスのみを対象にする場合は「影響されているデバイス」を選択。

4. ルールのパラメータを選択します。
デフォルトで検出内容完全一致する場合にのみ除外を行うパラメータ(※)が設定されています。パラメータを無効化/変更する事で広範囲に有効なルールに変更できますが意図しないセキュリティ低下を招く可能性があります。特にコマンドプロンプト/powershell 等の広範囲に利用可能なプログラムの操作を除外する場合、「プロセスのコマンドライン」や「ユーザ名」を必須条件にし「管理者による特定コマンドのみ許可する」等のパラメータに設定してください。



※ワイルドカードは致命的なセキュリティ低下につながる為、ご利用いただけません。
※パラメータ解説は当記事末尾参照
※パラメータ指定のサンプル
管理者による特定コマンド(コマンドオプション完全一致)のみ許可
→「プロセス名」＋「プロセスパス」＋「プロセスのコマンドライン」＋「ユーザ名」

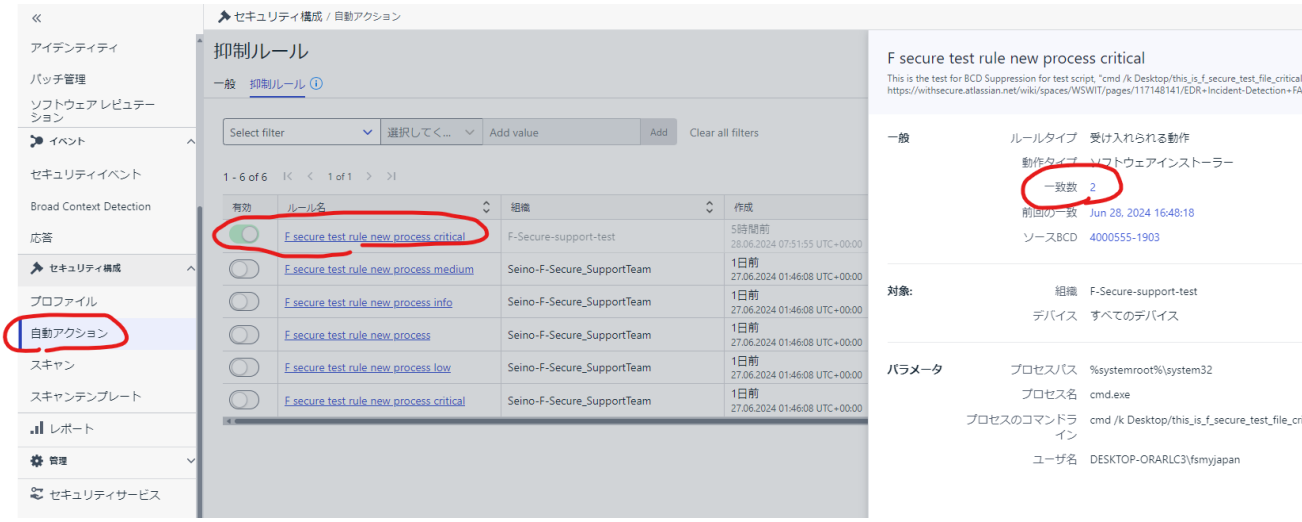
社内作成プログラムの許可
→「プロセス名」＋「プロセスパス」

5. ルールの概要を確認し「作成」を実施します。

6. 完了

- ルールの確認方法

1. 自動アクションタブに作成されたルールが一覧表示されます。



2. ルール名をクリックすると詳細が表示され、ルール該当→自動クローズされた BCD イベント数が表示されます。

3. 一致数をクリックすると自動クローズされた BCD イベント一覧が表示されます。

4. 一致数が「想定される該当動作の数」より多い場合、ルールの再設定もご検討ください。

- ルールの削除方法
  現在削除機能は準備中となり、ルールの左側にあるスイッチでの無効化を行ってください。

- パラメーター一覧

パラメータ	例	説明
プロセス名	support_service.exe	このパラメータはキー検知（※）とプロセス名一致で BCD 抑制します。
プロセスパス	c:\path\admin\support_service.exe	このパラメータはキー検知と実行ファイルパス一致で BCD 抑制します。
プロセスのコマンドライン	"c:\windows\system32\net localgroup group_name /add /domain	このパラメータはキー検知をトリガーするコマンド(オプション完全一致)の BCD を抑制します。
ユーザ名	john_doe	このパラメータはキー検知をトリガーするすべてのプロセスの BCD をユーザ名一致で抑制します。このパラメータを単独使用した場合広範囲のプロセスの BCD を抑制する可能性があります。
親プロセスの名前	support.exe	このパラメータはキー検知と親プロセス名の一致で BCD を抑制します。
親プロセスのコマンドライン	c:\windows\system32\net localgroup group_name /add /domain	このパラメータは指定した親コマンド(オプション完全一致)から生成されたプロセスが生成するすべてのキー検知の BCD を抑制します。このパラメータを単独で利用した場合広範囲のプロセスを除外する可能性があります。
親プロセスパス	c:\path\admin\\support.exe	このパラメータはキー検知と親プロセスの一致で BCD を抑制します。このパラメータを単独で利用した場合広範囲のプロセスの BCD を抑制する可能性があります。

※キー検知とは単独で検知を引き起こす動作。BCD 内で鍵(キー)のアイコンで表示されています。

- テスト用の BCD イベントは下記コマンドをクライアント端末で実行する事で生成できます。
  cmd /k Desktop/this_is_f_secure_test_file_critical.bat

不明な点がある場合は、弊社サポートセンターまでお問い合わせください。
お問合せフォーム
https://www.withsecure.com/jp-ja/support/contact-support/email-support