### インジケーター（IoC）

#### 概要

インジケーター（IoC：Indicator of Compromise）は、システムやネットワークが侵害された可能性を示すデジタル証拠です。IoCはセキュリティ脅威の検出および対応において重要な役割を果たします。システムにIoCを登録することで、ユーザーはリアルタイムで脅威を検出し、自動応答によってセキュリティインシデントを軽減できます。IoCの迅速な登録と活用は、組織のセキュリティレベル向上に寄与します。

IoCは、以下のようなシナリオで登録・活用できます。

**外部脅威インテリジェンスの収集時**

* CERT、ISAC、セキュリティベンダーなど、信頼できる外部組織やサービスから新たな脅威インテリジェンスを受信した場合、その情報をIoCとして登録し、積極的に活用します。
* 例：特定のIPアドレスが悪意のある活動に関連しているというレポートがあれば、そのIPアドレスを登録することで、当該IPとのすべての通信を監視・遮断できます。

**内部セキュリティログで不審な活動が検出された場合**

* 内部セキュリティログやイベントの分析を通じて、不審なIPアドレス、ドメイン、ファイルハッシュが特定された場合、それらをIoCとして登録します。
* 例：ログにおいて不審な外部IPへの繰り返し接続試行が確認された場合、そのIPをIoCとして登録することで、自動遮断や強化監視が可能となります。

**フィッシングや悪意のあるメールが検出された場合**

* フィッシングメールや悪意のある添付ファイルを含むメールを受信した場合、送信者のメールアドレス、ドメイン、添付ファイルのハッシュをIoCとして登録し、他のユーザーが同様の攻撃にさらされるのを防ぎます。
* 例：特定のメールアドレスがフィッシングの発信元と判明した場合、そのアドレスをIoCとして登録することで、当該アドレスからのメールをすべて遮断できます。

**マルウェア感染が確認された場合**

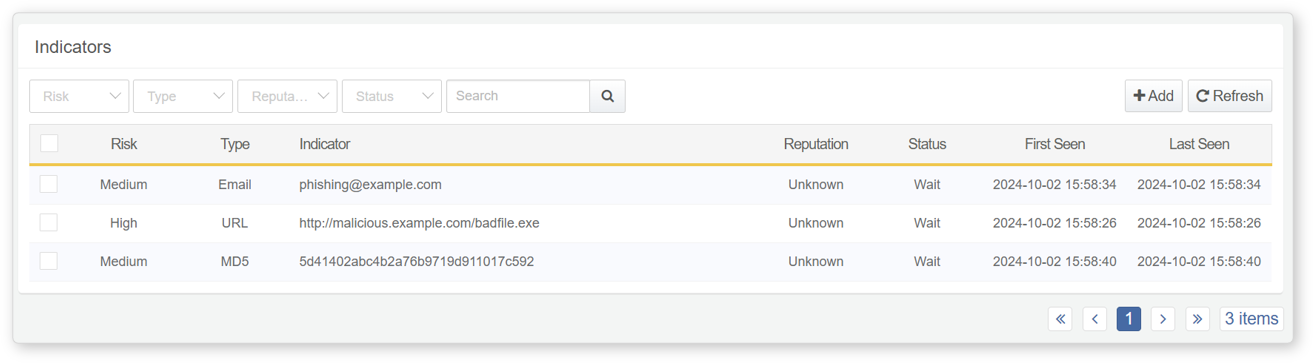
* システムがマルウェアに感染していることが確認された場合、マルウェアファイルのMD5ハッシュをIoCとして登録し、他のシステムへの拡散を防止します。
* 例：システム上でマルウェアファイルが検出された場合、そのハッシュをIoCとして登録することで、同一ファイルが他の場所で検出された際に即時対応が可能です。

**セキュリティ調査中に類似の攻撃パターンが特定された場合**

* 攻撃者によって繰り返し使用される特定のIP、ドメイン、URLパターンが判明した場合、それらをIoCとして登録し、同様のパターンによる将来の攻撃を事前に遮断します。
* 例：悪意のあるウェブサイトのURLパターンが発見された場合、それをIoCとして登録することで、類似URLへのアクセスを防止できます。

#### IoCの検索

IoCは、**ポリシー > インジケーター** で閲覧・検索できます。



* **重大度**: IoCの重大度レベル（良性、低、中、高）
* **タイプ**: IoCのタイプ（IPアドレス、ドメイン、URL、MD5、メールアドレス）
* **インジケーター**: IoCの値
* **レピュテーション**: IoCの信頼性評価
* **疑わしい**: レピュテーション分析により脅威の可能性があると判断されたIoC
* **不明**: まだ検証されていないIoC
* **ステータス**: IoCの現在の状態（保留、完了、エラー、再試行）
* **初回検出日時**: IoCが最初に検出・登録された日時
* **最終検出日時**: IoCが最後に検出された日時

特定のIoCを検索するには、ツールバーの検索ツールを使用します。検索ツールは入力したキーワードに基づいてIoCをフィルタリングします。検索は大文字・小文字を区別しません。

#### IoC一覧の更新

最新情報でIoC一覧を更新するには、ツールバーの **更新** をクリックします。

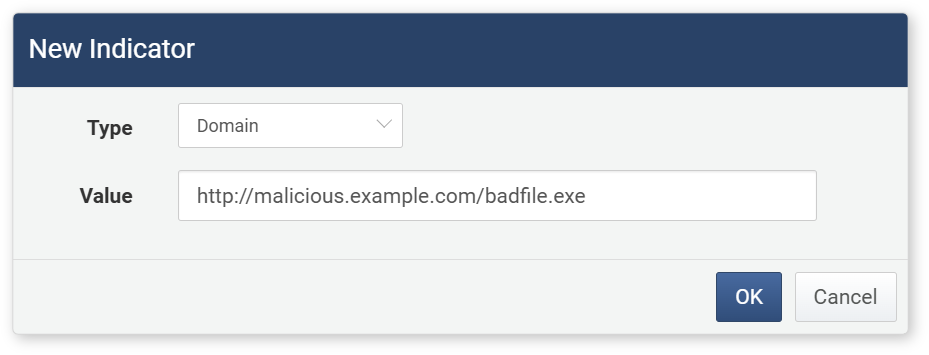
#### IoCの追加

IoCを追加するには：

**ポリシー > インジケーター** に移動し、ツールバーの **追加** をクリックします。

**IoC追加** ダイアログで必要な設定を行います。

* **タイプ**: IoCのタイプ（選択肢：IP、ドメイン、URL、MD5、メールアドレス）
* **値**: 対応するIoCの値



#### IoCの重大度変更

IoCの重大度を変更するには：

変更したいIoCのチェックボックスを選択します。

ツールバーに表示されるアクションメニューから **重大度変更** をクリックします。

希望する重大度レベルを選択します（選択肢：安全、低、中、高）。

#### IoCの削除

IoCを削除するには：

削除したいIoCのチェックボックスを選択します。

アクションメニューが表示されます。

アクションメニューから **削除** をクリックします。

#### 利用方法

* プレイブックのトリガーとして利用
* プレイブックコマンドセット内のIoC関連コマンドの更新用