ホワイトリスト登録方法

ホワイトリスト登録について

■ホワイトリストが適用されるシナリオ

CrowdStrikeでは「機械学習エンジンによる検知（ML検知）」と「振る舞いによる検知（IOA検知）」の2種類の検知が存在します。
それぞれの検知ではホワイトリストの方法が下記の通り異なります。

・ML検知の場合

- アラートの「Tactic & Technique」に「Machine Learning via xxxxx」と記載されているものが対象
- 「ハッシュ値」もしくは「ファイルパス/ファイル名/ファイル拡張子」を利用してホワイトリスト登録が可能です。

・IOA検知の場合

- アラートの「Tactic & Technique」が「Machine Learning via xxxxx」と記載されていないものが対象
- 検知右上のCreate IOA exclusionより「ファイル名及びコマンドライン」を利用してホワイトリスト登録が可能です。
- Falcon UI上から設定することができない場合は、弊社まで “検知情報” を添えてご連絡ください。
  （CrowdStrike社へホワイトリスト登録依頼が必要となります）

詳細は次ページ以降でご説明いたします。

ホワイトリスト登録フロー

過検知と判断

※ML検知：Tactic&Techniqueの項目に「Machine Learning via xxxxx」と記載されている検知

ML検知

No

Yes

ファイル名は同じだが、アップデート等によりハッシュ値が変更される場合等

ハッシュ値による除外設定が可能か

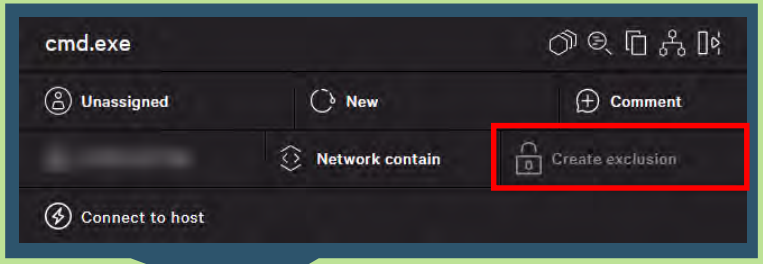
No

Yes

①IOC Management
→P.4~6を参照

②ML Exclusion
→P.7~9を参照

ML検知



Create IOA exclusion がグレーアウトされていないか

No

Yes

③IOA Exclusion
→P.10~12を参照

④マクニカへ登録依頼
→P.14を参照

IOA検知

①IOC Management（ハッシュ値による登録）

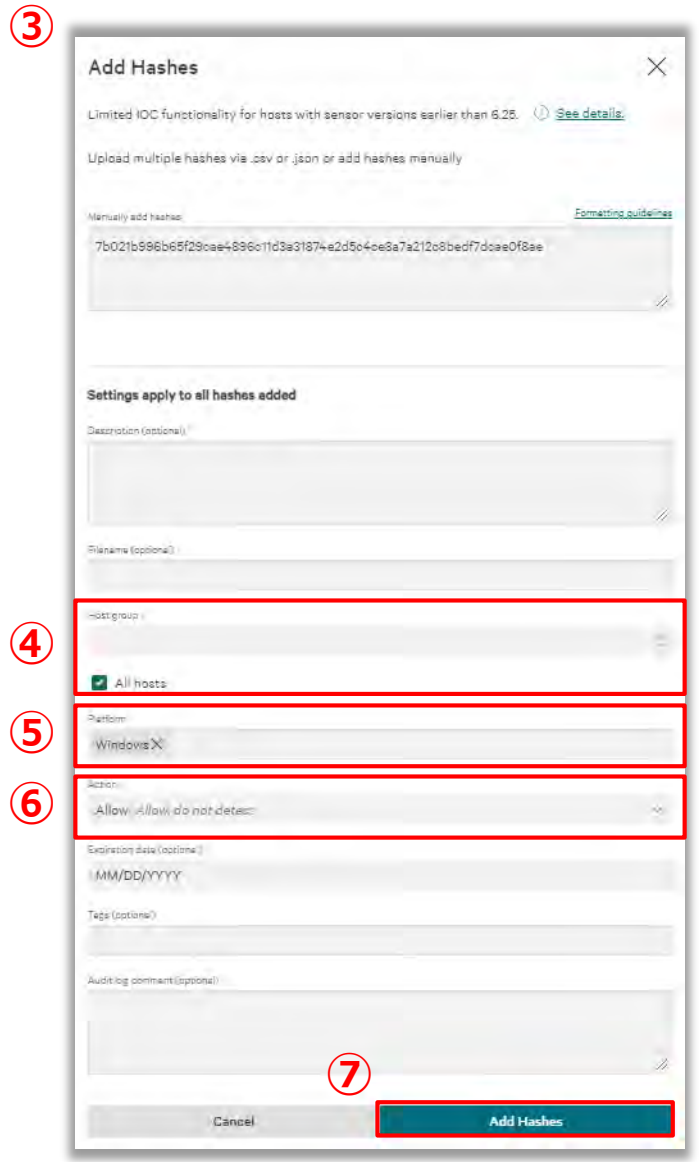
Activity > Detections > 対象アラート > IOC Management action

1. Detectionページに表示されている対象検知からホワイトリスト登録したいプロセスをクリックします。
2. 画面右側の「EXECUTABLE SHA256」にあるノートアイコンをクリックします。
   （IOC Management ページへ遷移します。）

①IOC Management（ハッシュ値による登録）

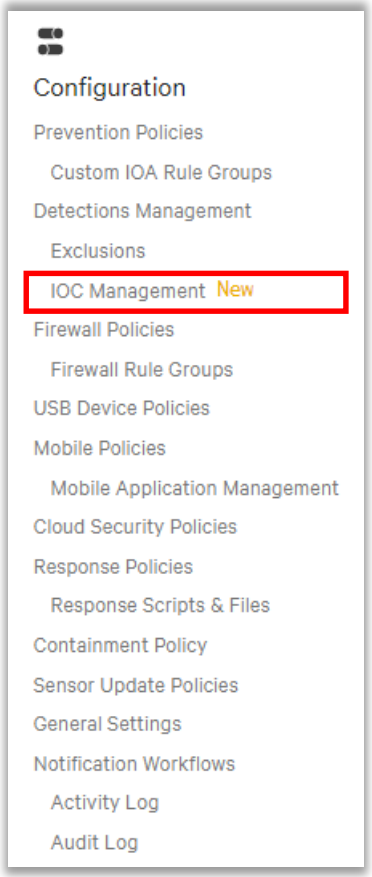
3. IOC Managementページ上に右図のようなウィンドウを確認
4. Host group から適用したいグループを選択
   ※全ホストに適用したい場合は「All hosts」を選択
5. Platformを選択（Windows, Mac, Linuxから複数選択可）
6. Actionから「Allow」を選択
7. 「Add Hashes」をクリックし、登録完了

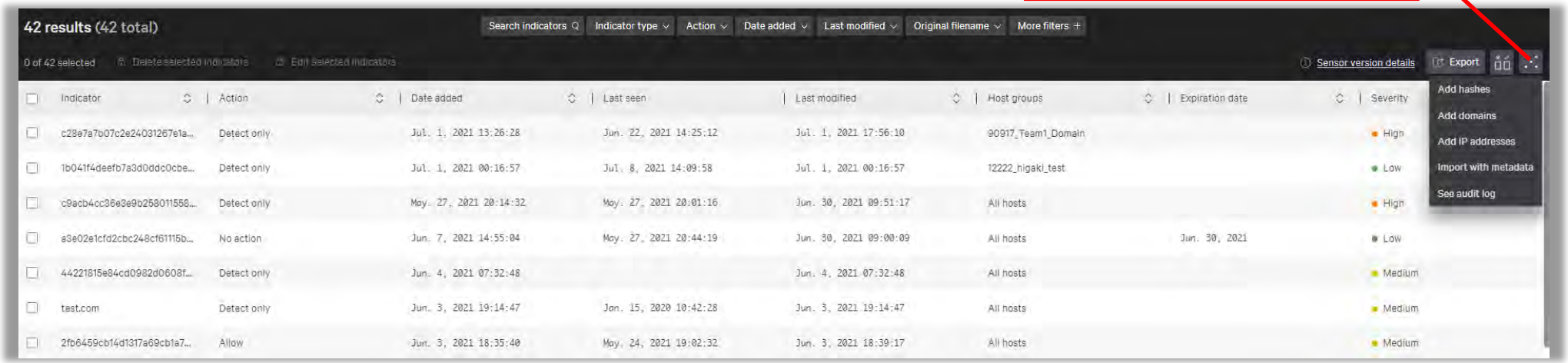
※他にもオプションの項目が用意されていますが、必要に応じてご利用ください。



【補足】IOC Managementページについて

Configuration > IOC Management では、ハッシュ値だけでなくドメインやIPアドレスを設定することが可能です。
IOCが記載されたjson/CSVファイルをアップロードすることで一括登録も可能です。





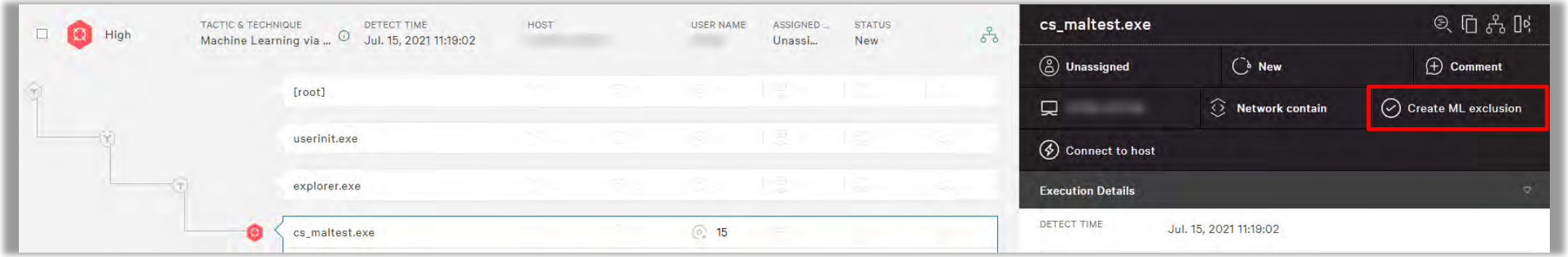
各IOCで設定可能なアクション

アクション	詳細	ハッシュ値	IPアドレス	ドメイン名
Block	ブロック	○	×	×
Detect Only	検知のみ	○	○	○
Allow	許可リストに登録し検知はされません	○	×	×
None	IOCの登録のみでアクションを行いません	○	○	○

②ML Exclusion（ファイルパスによる登録）

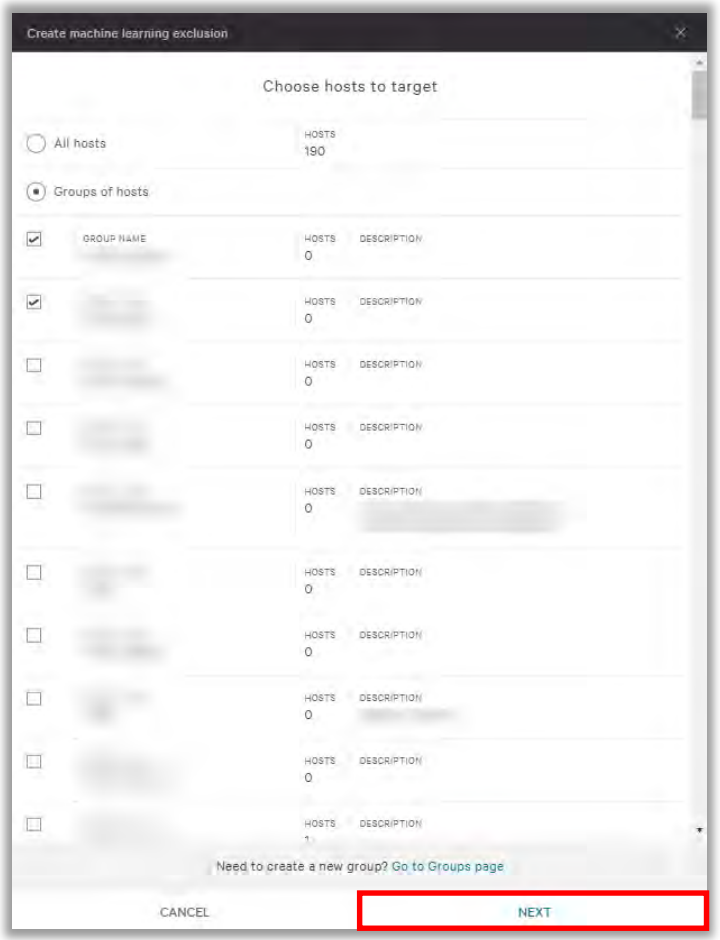
Activity > Detections > Create ML exclusion

1. Detectionページより対象検知を選択し、画面右側の「Create ML exclusion」のリンクをクリックします。
（IOC Management ページへ遷移します。）

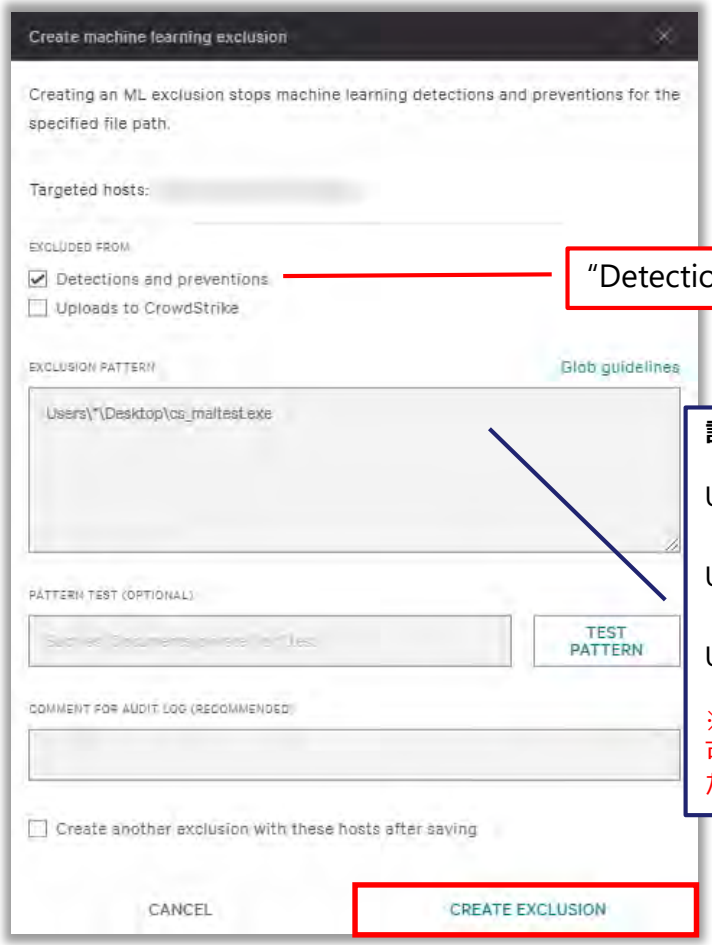


②ML Exclusion（ファイルパスによる登録）

2. 全ての端末（All hosts）、あるいは特定のグループ（Groups of hosts）に適用させるか選択し、“NEXT”をクリックします。



3. EXCLUSION PATTERN内を確認/記入し、”CREATE EXCLUSION” をクリックし、登録完了となります。



“Detections and preventions” を選択

記入例

・特定ファイル名を除外したい場合
Users¥Macnica¥Desktop¥cs_maltest.exe

・特定ファイルパスを除外したい場合
Users¥Macnica¥Desktop¥**

・特定ファイル拡張子を除外したい場合
Users¥Macnica¥Desktop¥*.ps1

※ワイルドカード「*」の利用は可能ですが、可能な限り除外範囲を絞り込むようご注意ください。

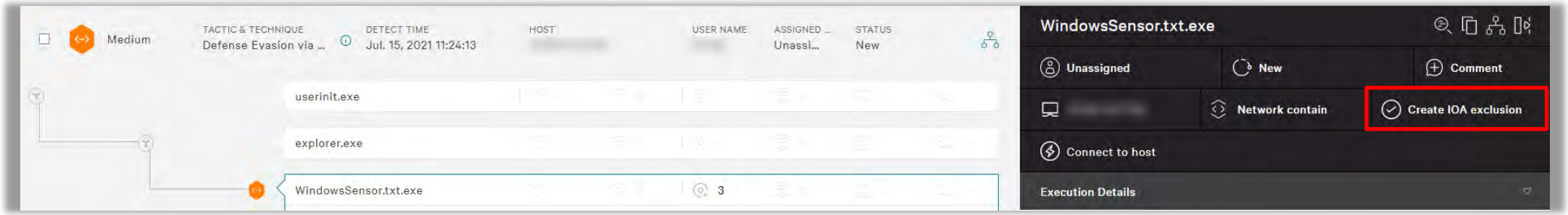
【補足】ワイルドカード

ワイルドカード	説明	記載例	マッチする例	マッチしない例
*	0文字以上の文字列にマッチします。この文字列には、ファイルパスの一部分を区切る"¥"または"/"などの区切り文字は含まれません。	Crowd*	Crowdstrike Crowd	Crowdstrike/Doc.ps1
**	0文字以上の文字列にマッチします。この文字列には、ファイルパスの一部分を区切る"¥"または"/"などの区切り文字は含まれます。	Crowd**	CrowdStrike Crowd/Strike.ps1 CrowdStrike/Doc.ps1	BigCrowd Crow wd
?	任意の1文字にマッチします。	DO?	DOC DOS DOs	doc docs DO
[abc]	角括弧で囲まれた任意の1文字にマッチします。	version[a1]	versiona version1	version version2
[!abc]	角括弧で囲まれた文字以外の任意の1文字にマッチします。	do[!ck]	dot	doc dok do
[a-z]	角括弧で囲まれた範囲内の任意の1文字にマッチします。範囲は[1-9]のように昇順で記載しなければなりません。	Version[0-9].bat	Version1.bat Version9.bat	Version10.bat
[!a-z]	角括弧で囲まれた範囲にはない任意の1文字にマッチします。範囲は[!1-9]のように昇順で記載しなければなりません。	Program[!2-4].exe	Program1.exe Programs.exe	Program2.exe Program3.exe

③IOA Exclusion（IOAによる登録）

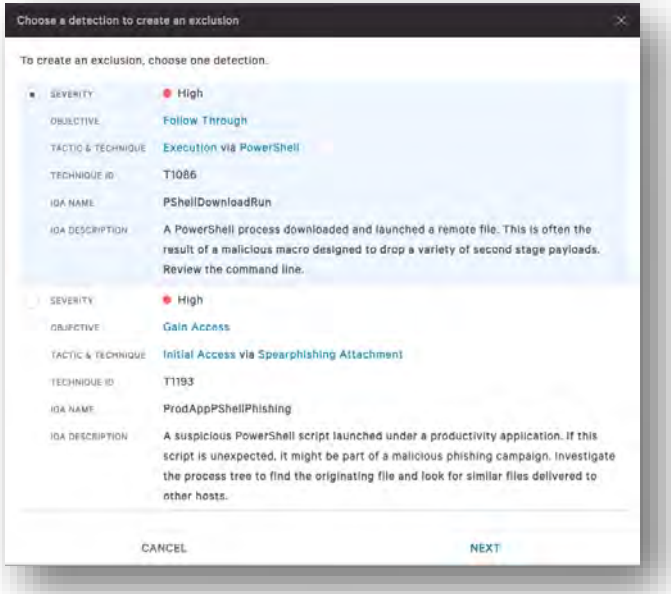
Activity > Detections > Create IOA exclusion

1. Detectionページより対象検知を選択し、画面右側の「Create IOA exclusion」のリンクをクリックします。



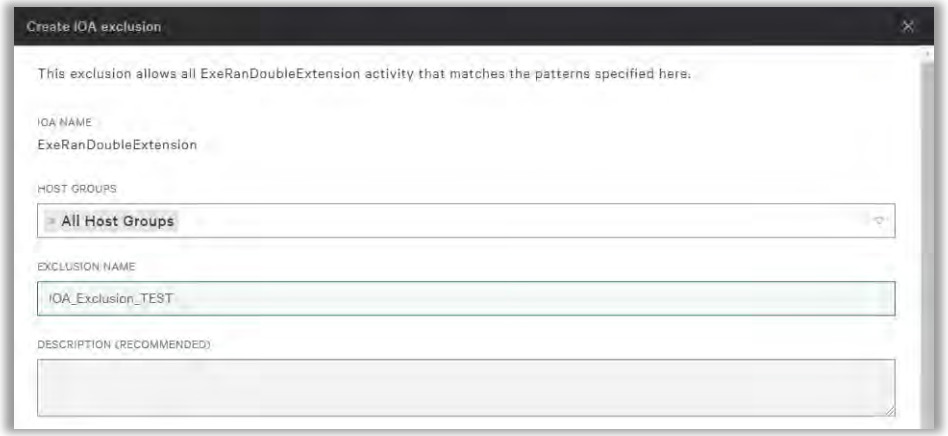
2. 下記のように複数検知が表示される場合は、除外したい検知を選択し”NEXT”をクリックします。

（表示されない場合は読み飛ばしてください。）

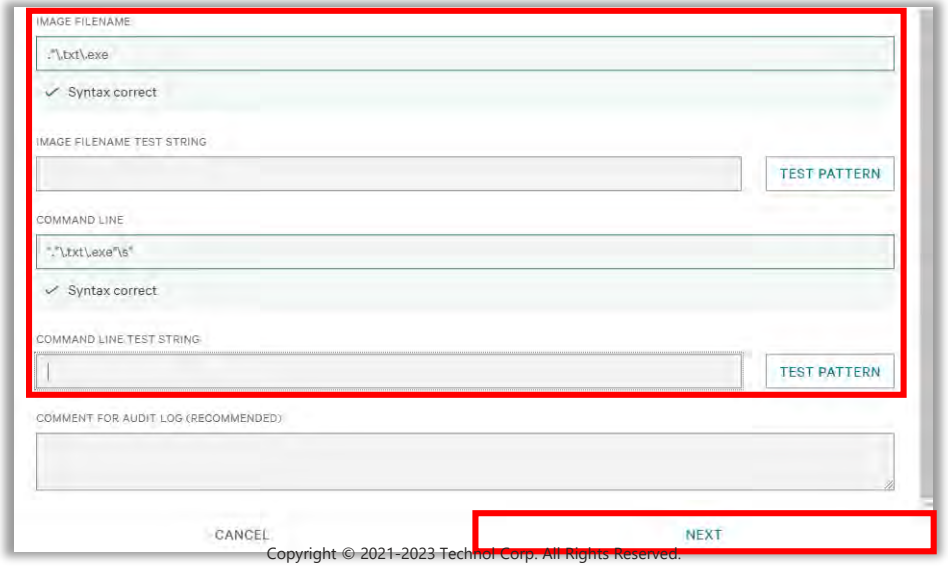


③IOA Exclusion（IOAによる登録）

3. HOST GROUPS よりルールを適用したいグループを選択（全体適用の場合はALL Host Groupsを選択）

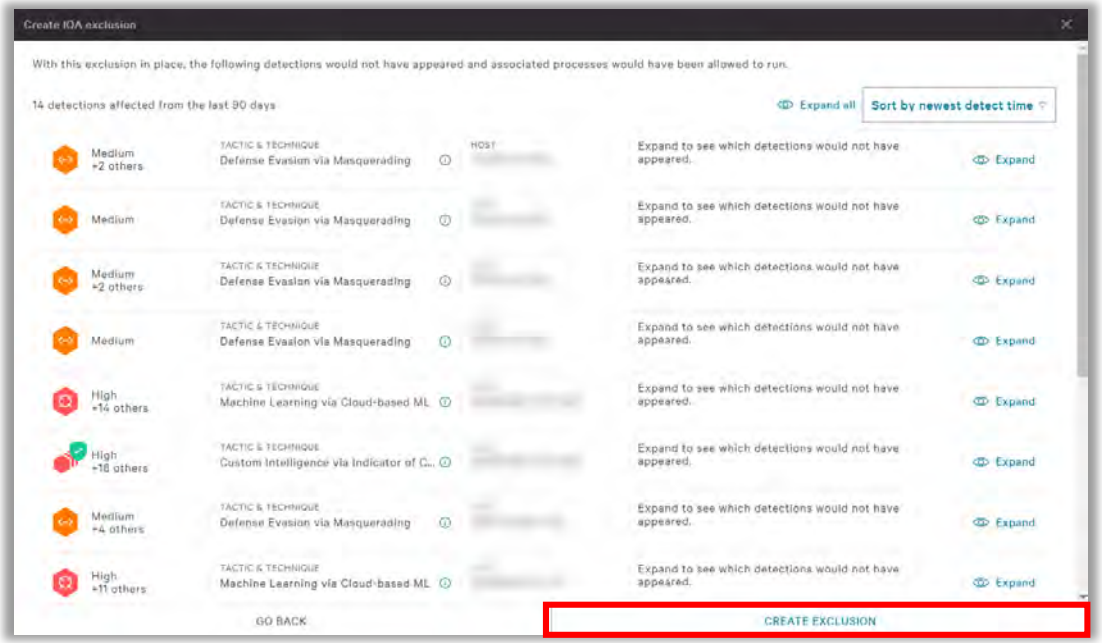


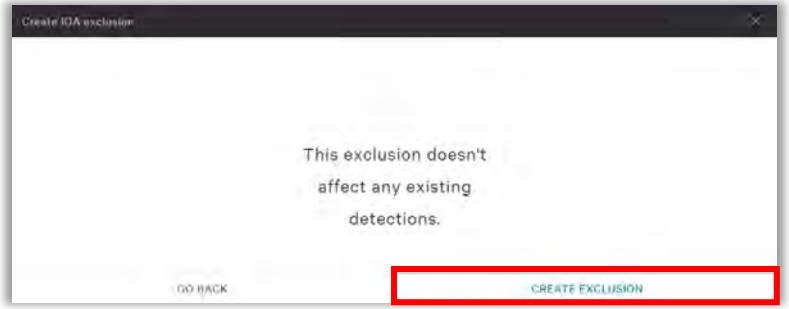
4. EXCLUSION NAMEにルール名を入力し、FILENAMEやCOMMAND LINEを確認した上で「NEXT」をクリック。



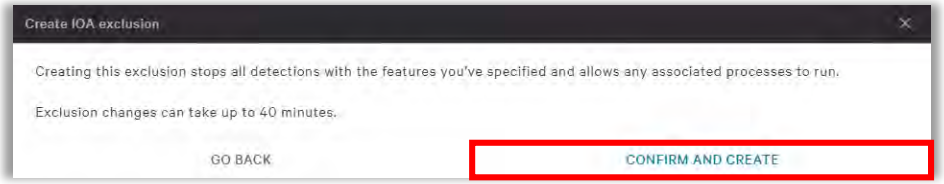
③IOA Exclusion（IOAによる登録）

5. 除外ルールの影響を受ける検知が存在する場合は左側の画面が表示される為、問題ないことを確認の上「CREATE EXCLUSION」をクリックします。影響を受ける検知がない場合は右側画面で「CREATE EXCLUSION」をクリックします。



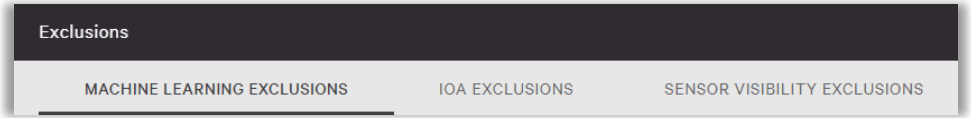


6. 確認画面が表示されるので「CONFIRM AND CREATE」をクリックし登録完了となります。



【補足】Exclusionsページについて

Configuration > Exclusionsでは、Falconセンサーの特定の機能の対象からファイルを除外（ホワイトリスト）するための3つのタブが用意されております。
こちらのページから登作成したルールの閲覧や除外ルールの新規作成/編集/削除を行うことが可能です。



■Machine Learning Exclusions（ML検知/ブロック除外）
指定されたファイルパスでの機械学習による検知やブロックのホワイトリストを設定できます。
過検知を軽減するために使用されます。

■IOA Exclusions（IOA検知/ブロック除外）
指定されたIOA（ファイル名及びコマンドライン）による検知やブロックのホワイトリストを設定できます。
過検知を軽減するために使用されます。

■Sensor Visibility Exclusions（センサーの可視性の除外）
指定されたファイルパスにおいて、センサーによるイベントデータの収集をバイパスします。
センサーの動作によるパフォーマンスへの影響を軽減するために使用されます。

④テクノルへ登録依頼（UI上から登録できない場合）

Activity > Detections

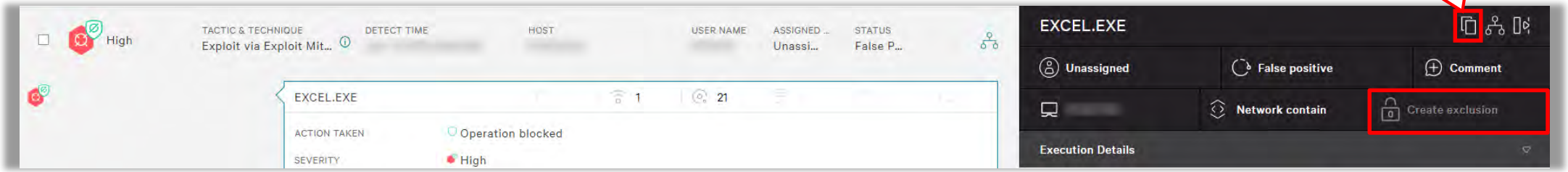
「Create exclusion」のリンクがグレーアウトしている場合は、Falcon UIからのIOAホワイトリストは不可です。
その場合は下記情報を取得いただき、弊社までご連絡ください。（CrowdStrike社へホワイトリスト登録依頼をさせていただきます。）
ただし、お客様の環境が脆弱にならないかCrowdStrike社にて精査された上で登録される為、ホワイトリストできない場合がございますので予めご了承ください。
また、内容によってはどのようなツールの影響によるものかなど確認をさせて頂く可能性がございますのでご了承ください。

✓対象テナントのCID情報

✓Detection情報（取得方法は下記ご参照ください）

✓過検知と判断された理由

検知対象を選択し、詳細情報上部にある「Copy detection to clipboard」ボタンをクリックすることで、検知情報がクリップボードにコピーされます。



お問合せ

【本件についてのお問合せ先】

株式会社テクノル

MR-EDサポート 担当

Mail: mred-support@technol.co.jp

TEL: 0178-38-6520