

## WideAngle マネージドSOAR 対処除外設定リスト作成時の留意事項

1. 対処除外設定リストは、サービスを新規で契約する際、自動対処の除外対象(ホスト、アカウント、アラート\*情報のリスト指定)を記入いただくリストです。対処除外対象としたホスト、アカウント、アラートに対しては、自動対処(自動パスワードリセット、自動隔離)の対象外とします。対処除外設定を不要とする場合や、リスト指定以外の設定(全ホスト、全アカウント指定)の場合は、お客さまからの提示は不要です。
2. 対処除外設定リストは「ホスト指定用(Host.csv)」と「アカウント指定用(Account.csv)」、「アラート指定用(Alert.csv)\*」の3種類あります。新設時のヒアリングシートの「サービス開通時の自動対処除外設定条件」の指定内容に合わせて、対処除外設定リストを添付いただきます。サービス開通後は、お客さまのカスタマーポータル画面より、作業依頼にてお申し込みください。なお、カスタマーポータル上では、以下の名称で登録されております。
  - ・ホスト指定用: No-Action-Host\_N番\_yyyymmdd.csv(旧Host.csv)
  - ・アカウント指定用: No-Action-Account\_N番\_yyyymmdd.csv(旧Account.csv)
  - ・アラート指定用: Exclusion-Alert\_N番\_yyyymmdd.csv(旧Alert.csv)
 \* アラートのリスト指定につきましては、作業依頼のみでの受付となります。
3. 対処除外設定リストの記載方法は下記のイメージの通りです。

### 【対処除外設定リストの記載例】

#### ・ホスト指定用(Host.csv)

```

Hostname
以下に除外対象とするHostnameを記載
host1
host2
.
.
.
    
```

- ・・・1行目はヘッダー(固定) ※削除しないでください。
- ・・・2行目は説明文(固定) ※削除しないでください。
- ・・・3行目以降に除外したい端末のホスト名を記載

#### ・アカウント指定用(Account.csv)

```

DisplayName
以下に除外対象とするDisplayNameを記載
User1
User2
.
.
.
    
```

- ・・・1行目はヘッダー(固定) ※削除しないでください。
- ・・・2行目は説明文(固定) ※削除しないでください。
- ・・・3行目以降に除外したいアカウントの表示名を記載

#### ・アラート指定用(Alert.csv)

```

AlertName
以下に除外対象とするAlertNameを記載
Automated investigation started manually
EDR_NCS_
アラート名1
アラート名2
.
.
.
    
```

- ・・・1行目はヘッダー(固定) ※削除しないでください。
- ・・・2～4行目は説明文(固定) ※削除しないでください。
- ・・・5行目以降に除外したいアラート名を記載

4. 対処除外設定リスト(CSVファイル)の文字コード/エンコード方式について  
「ホスト指定用(Host.csv)」と「アカウント指定用(Account.csv)」、「アラート指定用(Alert.csv)」はすべて文字コードが「UTF-8」となっています。ファイルの文字コードがUTF-8以外の場合にはSentinelへの登録ができないため、こちら記載・保存いただく際はCSVファイルの文字コードをUTF-8以外に変更されないようお願いします。
5. 自動隔離除外設定の制限事項について  
ホストの指定には、端末のホスト名(Host Name)を使用します。したがって、お客さまのAzure環境にてホスト名の重複がある場合は、WatchListに登録されたホスト名を持つ全てのホストについて、隔離を行いません。  
(対象デバイス: Microsoft Defender for Endpoint、Microsoft Defender for Business、Microsoft Defender for Endpoint連携を行うデバイス)
6. 自動パスワードリセット除外設定の制限事項について  
アカウントの指定には、Microsoft Entra ID上の表示名(Display Name)を使用します。したがって、お客さまのMicrosoft Entra IDに登録されているアカウントにおいて表示名の重複がある場合は、WatchListに登録された表示名を持つ全てのアカウントについて、パスワードリセットを行いません。  
(対象デバイス: Microsoft Entra ID P1、Microsoft Entra ID P2、Microsoft Defender for Identity、Microsoft Defender for Cloud Apps)