

kaspersky

Kaspersky EDR Optimum 2.3

製品紹介

2022年11月09日

株式会社カスペルスキー

セールスエンジニアリング本部

Kaspersky EDR ラインナップ

EDRとは？

EDR = Endpoint Detection & Response

- 意外とコンセンサスがない、EDRが果たす役割。

EP：エンドポイントプロテクション

マルウェアの実行防止。リアルタイム検知が主な役割。

重要な技術：ヒューリスティック検知、ふるまい検知、機械学習エンジン。

Endpoint Detection and Response

脅威を検知し、対応を支援するのが主な役割。

特にIoCによる検知、脅威ハンティング機能が特徴。

マルウェアの実行後、侵入後に使用するイメージで捉えられている。

Detection

ファイル名、変更日時、親プロセス、レジストリキー、Windowsイベントなど、痕跡を調べる。

Response

プロセスの停止、ファイル削除など。

エンドポイントの重要性

まずは、エンドポイントの対策を行うことが重要。

エンドポイント



最も脆弱な要素とITインフラへの一般的な攻撃起点のポイント



防御するのに十分な基準がない場合、効果的なインシデント調査のためのデータの重要なソース



TLS 1.3の採用により、エンドポイントによりフォーカス（ネットワークトラフィックの解読が困難）



76%

記録されたセキュリティイベントの76%がエンドポイントによって生成

84%

84%のインシデントにおいて、サーバー/ワークステーションが関与していた

Source: The SANS 2018 Endpoint Protection and Response Survey

kaspersky



すべての企業において、
複雑な脅威の防御が必要…



…しかしながら、
ITセキュリティ担当者と専門知識が不足

- ✓ 使いこなせるツールの選択。
- ✓ 昨今の脅威状況に合わせ、エンドポイントセキュリティの見直し。

KES Cloud Plus

- 脅威の分析
- シンプルさ
- 手ごろなコスト

Cloud

KES Cloud Pro

- 脅威の分析
- バランスの取れた自動化機能
- シンプルさ
- 手ごろなコスト

Cloud

Kaspersky EDR Optimum

- 脅威の分析
- バランスの取れた自動化機能
- シンプルかつ多くのレスポンス機能
- 手ごろなコスト

オンプレミス

Cloud

Kaspersky EDR Expert

- 検出技術の幅広いリスト、IOAなど
- 遡及的分析 (脅威ハンティング機能)

オンプレミス

Cloud

Kaspersky EDR Expert の2タイプのIOAルール:

- Kasperskyの専門家によるルール (除外設定も可能);
- ユーザー定義によるルール

カスペルスキーが提案する成熟度モデル

専門のセキュリティ
人員はいない。



**Kaspersky
Endpoint
Security for
Business**



**Kaspersky
Endpoint
Security
Cloud、Plus、
Pro**

- IT 部門がある。
- セキュリティ担当は IT 部門内にある。

セキュリティ専門性を
強化中。



**Kaspersky
EDR
Optimum**

- セキュリティ担当は IT 部門内にある。
- 小規模なセキュリティ部門がある。
- セキュリティ専任者は雇用する予定がない。

セキュリティ専門性を
強化中。



**Kaspersky
EDR Expert
On-premises、
Cloud**

セキュリティ部門が
確立している



**Kaspersky
EDR
Expert**



**Kaspersky
Anti Targeted
Attack
Platform
(XDR)**

- 必要十分なセキュリティ部門
- SOC/CERT/CSIRT
- 脅威ハンティンググループ

EDRラインナップ

	対応規模	特徴	Cloud対応	オンプレミス	EDRレベル
KES Cloud	5 ライセンス以上 999まで	Cloud Discoveryなど 付加機能。	対応	無し	無し
KES Cloud Plus	5 ライセンス以上 999まで	Cloud Discoveryなどの 付加機能、 Microsoft365の保護。	対応	無し	マルウェアの挙動を調査
KES Cloud Pro	5 ライセンス以上 999まで	Cloud Discoveryなどの 付加機能、 Microsoft365の保護。	対応	無し	マルウェアの挙動を調査 IOCスキャン 端末の隔離 など
KESB (Select、Advanced)	10ライセンス以上		300ライセンス 以上で対応	対応	無し
EDR-Optimum	10ライセンス以上	ライセンスにはKESB Advancedを含む。	300ライセンス 以上で対応	対応	マルウェアの挙動を調査 IOCスキャン 端末の隔離 など
EDR-Expert	250ライセンス以上	ライセンスにはKESB Advancedを含む。	300ライセンス 以上で対応	対応	マルウェアの挙動を調査 脅威ハンティング TAAによる検知 IOCスキャン 端末の隔離 など

Kaspersky EDR Optimumの価値

必要不可欠なセキュリティのその先に。

Optimumとは、「最適な」という意味。

Kaspersky EDR Optimumは、Endpoint Securityを含んだ統合ツール。

昨今の複雑な攻撃に対応する、高度のセキュリティを兼ね備えるだけでなく、攻撃を可視化、簡単な調査ツールやおよび自動応答オプションを提供します。

即座に脅威に対応しビジネスの中断を防ぐことを目的として、脅威を検出するだけでなく、その全範囲と発生源を明らかにします。

本資料は、Kaspersky Endpoint Security for Windows を使用した構成で説明しています。
Kaspersky Security for Virtualization Light Agent、
Kaspersky Security for Windows Serverでは、機能が異なります。

Kaspersky EDR Optimumの価値



マルチレベルの検知

様々な検知機能

定義、ヒューリスティック、レピュテーションから、
アダプティブアノマリコントロール、機械学習、
ふるまい検知、脆弱性攻撃、ネットワーク攻撃、
暗号化攻撃、ファイルレスマルウェアブロックなど。



根本原因解析

インシデントカードで何が行われたかを調査。

エンドポイントセキュリティの検知結果だけでは分からない、マルウェアの動きを可視化。

多くのリソースを必要とせず、あらゆる組織でのインシデント調査を可能にする。



強固な防御

高度なセキュリティを付加。

脆弱性管理・パッチ配信

アプリケーションコントロール

IoCベース検知を付加。

サードパーティー製 IoC ファイルも使用可能。



自動化された対応

すばやく簡単な対応。応答はインシデントカードからワンクリックで完了。

管理サーバーからクライアントへの対応指示が自動化される。

Kaspersky EDR Optimumの機能特徴

推奨事項 (Guided Response) 下記の操作をGUI上でガイドする新インターフェイス。

- インシデントカードによるマルウェア挙動を可視化。

- ファイル生成

- スクリプトの起動

- マルウェアのネットワーク通信

- マルウェアを自動起動させるレジストリの作成

- ワンクリック 簡単対応

- 端末の論理的切り離しを遠隔から実行。物理的に切り離さないため、管理操作は継続可能。

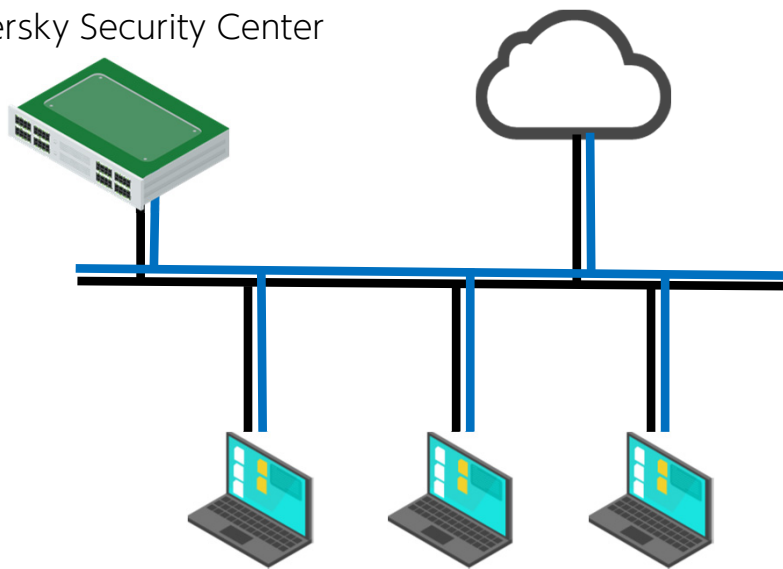
- プログラムの起動禁止、ファイルの隔離。

- IOCスキャン

- セキュリティ侵害の痕跡を調査する。

コンピューターをネットワークから分離する

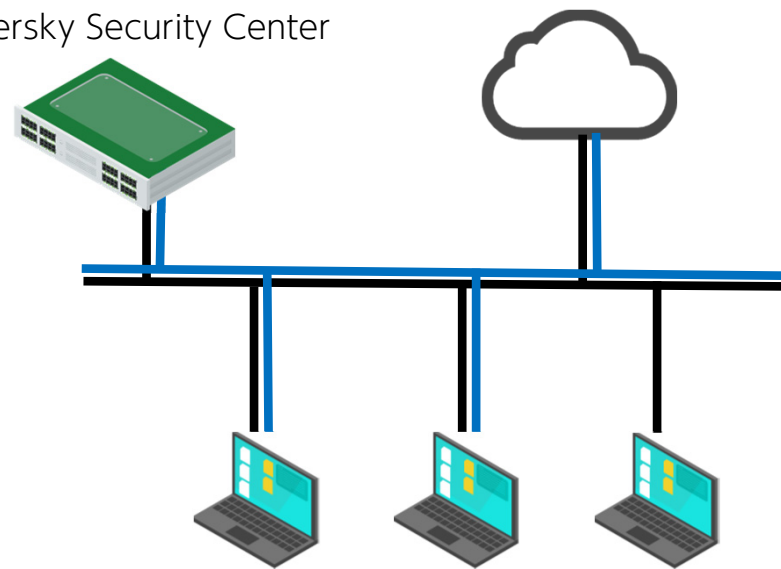
Kaspersky Security Center



インシデントカードから
分離を実行

— 物理的な接続
— 論理的な接続

Kaspersky Security Center



遠隔から論理的に
ネットワークを切断

物理的に切り離さないため、
管理操作は継続可能。

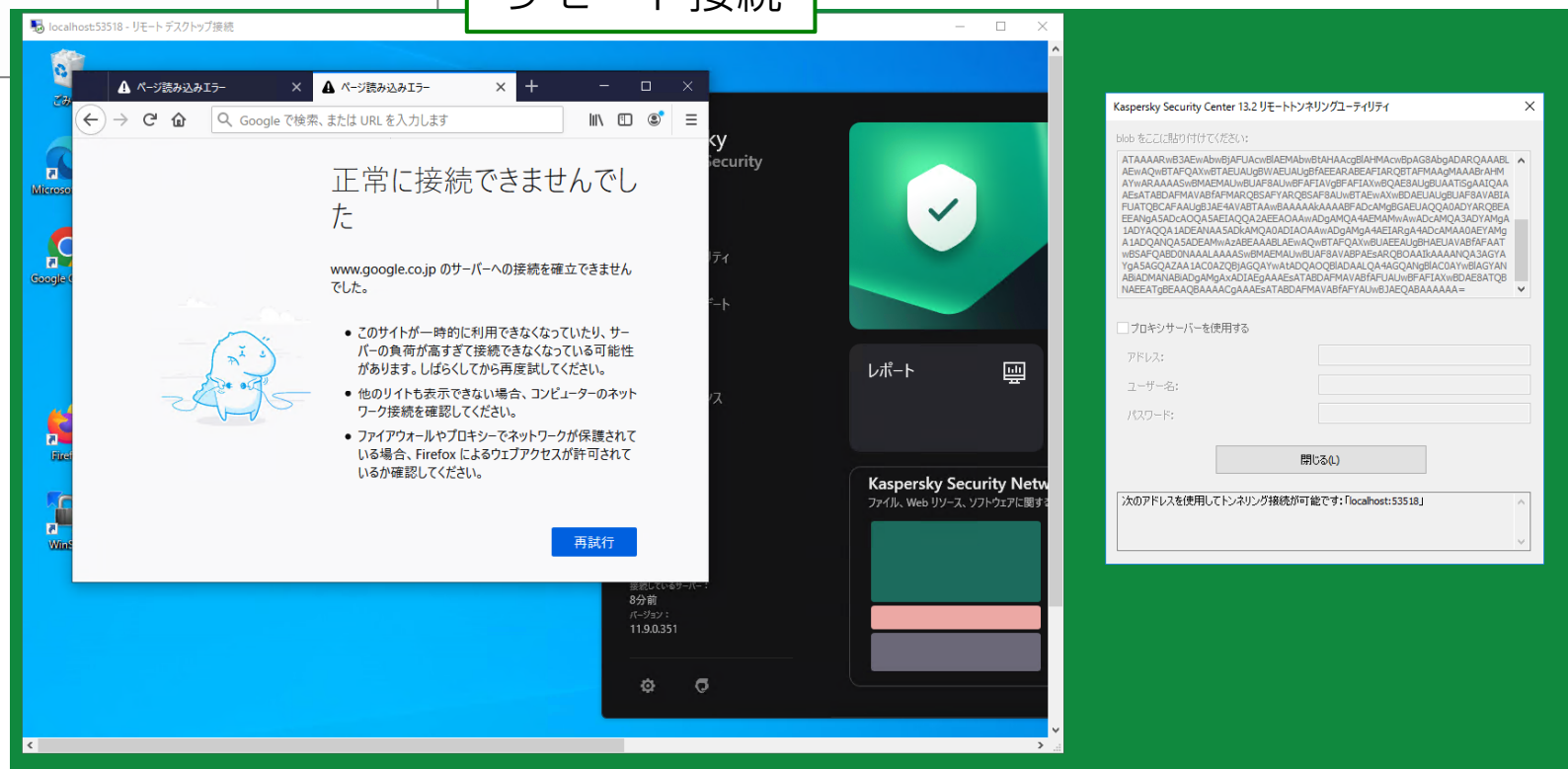
コンピューターをネットワークから分離する



物理的に切り離さないため、
ネットワーク切断された状態でも、
KSCからリモート接続が可能。

注 KSC Cloud Consoleでは
リモート接続は使用出来ません。

リモート接続

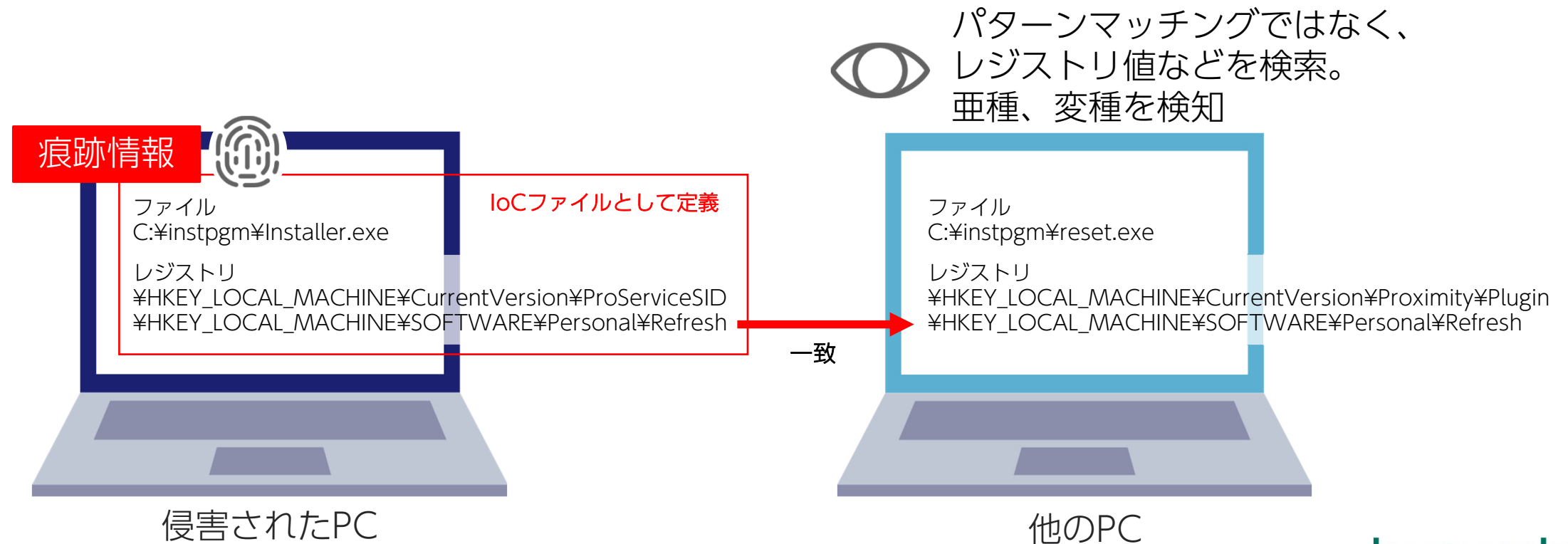


IOC スキャン

IOC : Indicators of Compromise (インディケート オブ コンプロマイズ) とは

Indicators : 痕跡 Compromise : セキュリティ侵害
IOCとは、セキュリティ侵害の痕跡のこと。

痕跡には、マルウェア本体のハッシュ値、マルウェアが生成するファイル、レジストリ値などがあります。こうした情報を記述したファイルがIOCファイルです。



IOC ファイルの作成 二つの方法

- インシデントカードからIOCファイルを作成。
- IOC作成ツールからIOCファイルを作成。

使用出来る項目

<https://support.kaspersky.com/help/KESWin/11.11.0/ja-JP/220828.htm>

https://support.kaspersky.com/Help/KESWin/11.11.0/IOC_Terms/IOC_TERMS.xlsx



使用可能なIOC項目

ArpEntryItem
DnsEntryItem
EventLogItem
FileItem
PortItem
ProcessItem
RegistryItem
ServiceItem
UserItem
VolumeItem
SystemInfoItem

IOCスキャンがスキャンするレジストリキー 一覧

<https://support.kaspersky.com/help/KESWin/11.11.0/ja-JP/221708.htm>

IOCスキャン結果の確認

警告からの IOC スキャン : PDM:ExploitWin32.Generic PC01 2022-04-11T07:18:42Z (1650443792071)

全般履歴設定アプリケーション設定スケジュール変更履歴

IOC スキャン設定

詳細

IOC スキャン結果

コンピューター

すべてのコンピューター

ステータス	コンピューター	時刻	結果
	PC01	2022/4/27 12:49:35	IOC が検出されました
	PC01	2022/4/26 13:54:28	IOC が検出されました
	PC01	2022/4/25 15:28:51	IOC が検出されました
	PC01	2022/4/20 17:47:36	IOC が検出されました

警告の詳細

結果 : 5f765bcb-de28-459a-ad5b-20c851708987.ioc

UUID

5F765BCB-DE28-459A-AD5B-20C851708987

説明

IPand EventLog

Windows イベントログ

イベント ID

4625

ソース

Microsoft-Windows-EventSystem

ログの名前

Application

時刻

2022-04-26T04:30:55Z

Windows イベントログ

イベント ID

4625

ソース

Microsoft-Windows-Security-Auditing

ログの名前

Security

時刻

2022-04-26T04:26:01Z

IOC

```
<OpenIOC xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="5f765bcb-de28-459a-ad5b-20c851708987" last-modified="2022-04-21T08:14:37Z" published-date="0001-01-01T00:00:00" xmlns="http://openioc.org/schemas/OpenIOC_1.1">
  <metadata>
    <short_description>IPand EventLog</short_description>
    <authored_date>2022-04-21T07:47:31Z</authored_date>
    <links />
  </metadata>
  <criteria>
    <Indicator operator="OR" id="0ce4d71f-3060-4b1e-91a3-ae5207a07780">
      <IndicatorItem id="8bf4d6d3-c718-4909-8cb0-3becd0697d06" condition="contains" preserve-case="false" negate="false">
        <Context document="PortItem" search="PortItem/remotelIP" type="endpoint">
          </Context>
        <Content type="IP">192.168.1.1</Content>
      </IndicatorItem>
      <IndicatorItem id="88e526b1-d273-4d00-ae92-99650cb169d3" condition="contains" preserve-case="false" negate="false">
        <Context document="ProcessItem" search="ProcessItem/path" type="endpoint">
          </Context>
        <Content type="string">notepad.exe</Content>
      </IndicatorItem>
      <IndicatorItem id="826ac4fe-f2cb-4a02-aa34-b2db7f467d95" condition="is" preserve-case="false" negate="false">
        <Context document="EventLogItem" search="EventLogItem/EID" type="endpoint">
          </Context>
        <Content type="int">4625</Content>
      </IndicatorItem>
      <IndicatorItem id="72aee7b4-95d6-4258-b595-9614767c682c" condition="contains" preserve-case="false" negate="false">
        <Context document="Registritem" search="Registritem/ValueName" type="endpoint">
          </Context>
        <Content type="string">notepad.exe</Content>
      </IndicatorItem>
    </Criteria>
  </IOC>
```

実行防止（実行をブロック）

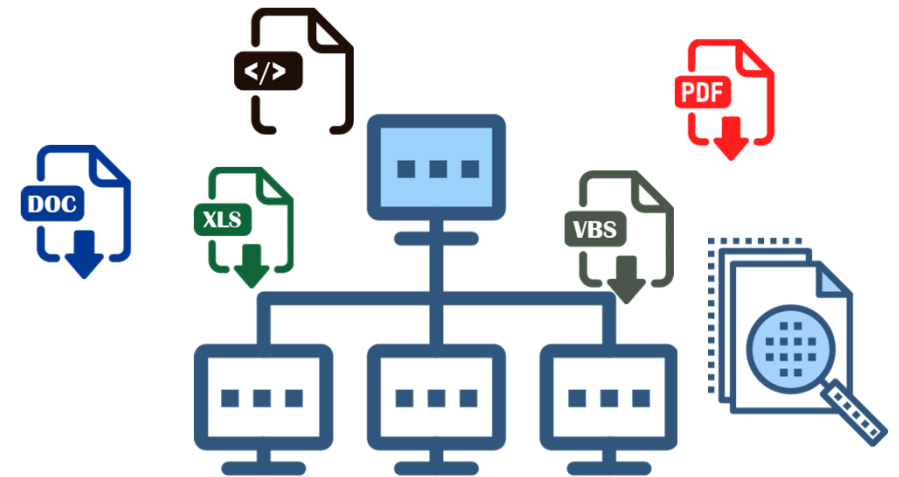
実行ファイルだけでなく、スクリプトの実行や
Office 形式のファイルオープンをブロックすることができます。

Adobe Acrobat、Microsoft Edge、Google Chrome、Mozilla Firefox、Tor Browserからの
PDFオープンをブロック。

AutoHotkey、cmd.exe、cscript.exe、wscript.exe、msiexec.exe、perl.exe、powershell.exe、
python.exeなどのスクリプトインタープリターをサポート。

実行防止でサポートされるファイルの拡張子
<https://support.kaspersky.com/KESWin/11.11.0/ja-JP/220820.htm>

サポートされるスクリプトインタープリター
<https://support.kaspersky.com/KESWin/11.11.0/ja-JP/220826.htm>



重要ファイルの誤削除防止

ファイルの隔離、実行防止などにより、Windows OSとKaspersky Endpoint Securityの実行に必要なファイルを、誤って削除してしまうことを防ぎます。

2022/11/02 11:34:36 に実行した 最近のイベントの結果					
<div>リストの更新 × 削除 ファイルへのエクスポート カテゴリへ割り当て 変更履歴</div> <div>検索...</div>					
<input type="checkbox"/>	イベントの発生日	デバイス	イベント	説明	管理グループ
<input type="checkbox"/>	2022/11/02 11:34:20	PC20	監査 (オブジェクトの変更)	ポリシー 「Kaspersky Endpoint Security for Wi... >>	管理対象デバイス
<input type="checkbox"/>	2022/11/02 11:31:09	PC20	失敗	ファイルはシステム上重要なオブジェクトに分類されており、隔離に移動できません	管理対象デバイス
<input type="checkbox"/>	2022/11/02 11:31:10	PC20	オブジェクトは隔離されません... >>	イベント種別: オブジェクトは隔離されませんでした (Endpoint Detection and Response) コンポーネント: Endpoint Detection and Response タスク名: Quarantine object from alert details C:\Windows\System32\svchost.exe [11fae7d6-2d6a-473c-a039-a4072638a49e] ファイルパス: C:\Windows\System32\svchost.exe MD5: b7f884c1b74a263f746ee12a5f7c9f6a エラー: ファイルはシステム上重要なオブジェクトに分類されています	管理対象デバイス
<input type="checkbox"/>	2022/11/02 11:31:09	PC20	実行中		管理対象デバイス
<input type="checkbox"/>	2022/11/02 11:29:09	PC20	実行中		管理対象デバイス
<input type="checkbox"/>	2022/11/02 11:25:47	PC20	監査 (管理サーバーへの接続)	管理サーバーにユーザー 「NWCSvcUser_3322... >>	管理対象デバイス

構成



EDR Optimum 2.3 構成

管理サーバー

Kaspersky Security Center 13.2、14。（KES 11.11のプラグインを使用）
Kaspersky Security Center Cloud Console

エージェント

Kaspersky Endpoint Security for Windows 11.7~11.11
（従来使用していたKaspersky Endpoint Agentは使用しません。KESに機能を内包しています）

Kaspersky Security for Virtualization 5.2 Light Agentと使用する場合は、
Kaspersky Endpoint Agentを使用。

Kaspersky Security 11.0.1 for Windows Serverと使用する場合は、
Kaspersky Endpoint Agentを使用。

Kaspersky Security Center Cloud Consoleは
KESB 300ライセンス以上を保有している場合など、
使用条件があります。詳しくはKaspersky Security Center
Cloud Consoleのヘルプをご確認ください。

EDR Optimum 2.3 構成

- EDR Optimumには、EDR Optimum(Bundle)と、 EDR Optimum add-onの2製品がある。
 - EDR Optimumは Kaspersky Endpoint Security for Business Advancedを含んだフル機能製品。
 - EDR Optimum Add-onは 以下の2製品にEDR Optimum 機能を追加する製品。
単独での購入は不可。
一部の端末でのみEDR -Optimumを使用する場合に購入する製品。

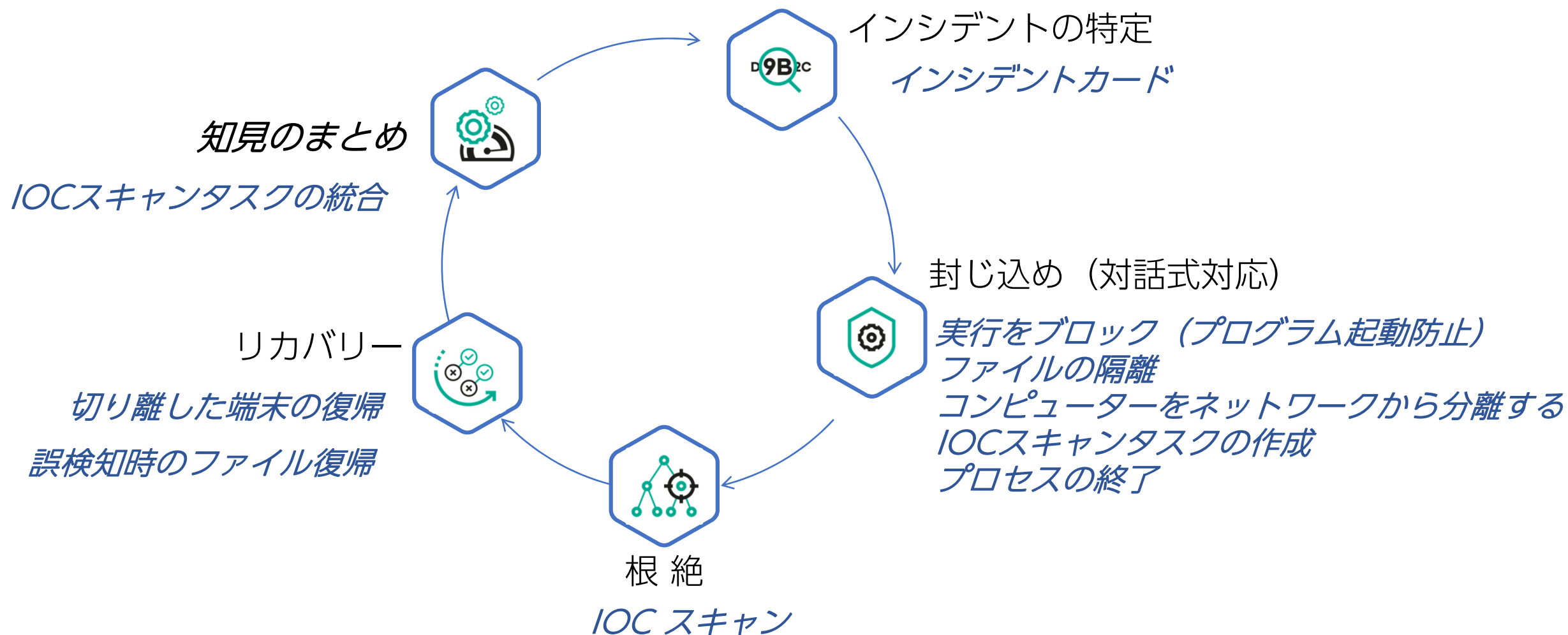
Add-onの対象ライセンス

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

注 Kaspersky Security for Virtualization 5.2 Light Agentを使用出来る、
Kaspersky Hybrid Cloud SecurityライセンスをCPUライセンスで購入している場合、
EDR Optimum add-onは、保護したい仮想マシン数で購入します。

インシデント対応

インシデントハンドリングプロセス



インシデント対応：
準備

コンピューターのネットワーク分離時のネットワーク許可ルール

ネットワーク分離は論理的切断のため、インターネット、メール、ファイル共有などは遮断し、基幹業務だけ許可するなど、設定が可能。

ネットワーク分離の除外リスト

ネットワーク分離が自動で有効化された後、コンピューターでブロックされないネットワーク接続です。

+ 追加 + プロファイルから追加 × 削除 設定 フィルター				
<input type="checkbox"/>	ルール名	通信方向	プロトコル	ソース
<input type="checkbox"/>	DNS	受信	TCP	
<input type="checkbox"/>	DNS	受信	UDP	
<input type="checkbox"/>	Large numbered TCP ports, randomly assigned by the RPC service	受信	TCP	
<input type="checkbox"/>	RPC Endpoint Mapper	受信	TCP	
<input type="checkbox"/>	DNS client	送信	TCP	
<input type="checkbox"/>	DNS client	送信	UDP	
<input type="checkbox"/>	DHCP server	受信 / 送信	UDP	
<input type="checkbox"/>	DHCP client	受信 / 送信	UDP	
<input type="checkbox"/>	MADCAP	受信	UDP	
<input type="checkbox"/>	DHCP failover	受信	TCP	

インシデント対応：
特定フェーズ

Kaspersky EDR Optimum 操作起点

「脅威レポート」から解析レポートを展開、インシデント対応を実行

脅威レポート

編集更新エクスポート

サマリー詳細

詳細 13 件 (13 件中)

検索

検知日時	アラートを開く	グループ	デバイス	IP アドレス	処理	オブジェクト種別	Cloud Sandbox による検知	ファイルのパス
11月 9, 2022 12:38:50	アラートの表示	管理対象デバイス	WIN2019	192.168.1.22	結果の説明: ブロック 種別: トロイの木馬 名前: PDM.Exploit.Win32.Generic ユーザー: WIN2019\admin (イニシエーター) オブジェクト: C:\Users\admin\AppData\Local\Temp\sw_test.exe 理由: 危険な動作 定義データベースの公開日時: 2022/11/09 2:59:00 SHA256: 9F0E9367E1D24528E50FE78C335625049FFA588B4E68806F2B057190C2A7A3F8 MD5: B292CB6A44CF82C6D4D14EED5F02FCAB	トロイの木馬	いいえ	C:\Users\admin\AppData\Local\Temp\sw_test.exe
11月 9, 2022 12:36:26	アラートなし	管理対象デバイス	WIN2019	192.168.1.22	イベント種別: オブジェクトのスキャン結果はサードパーティ製品に送信されました 名前: powershell.exe アプリケーションのパス: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe プロセス ID: 3920 ユーザー: WIN2019\admin (イニシエーター) コンポーネント: AMSI 保護 結果の説明: 未処理 種別: トロイの木馬 名前: HEUR:Trojan.Multi.AmsiKdbDetect.gen 危険性: 完全一致 精度: 高 オブジェクトの種別: 文字列 オブジェクトのパス: uid:// オブジェクトの名前: amsi_stream_9 理由: イベントを記録しました SHA256: 5F853D3B102811BBCA1B9912C44D8AA627D0E91ED2900602CE96C73E085BFA8A MD5: 51ABC9906AFC84933FC4D471CECF9560	トロイの木馬	いいえ	uid://amsi_stream_9

「アラートの表示」 からアラートカードを展開 “詳細”レポート

成功: ブロック

詳細

すべての警告イベント

```
graph LR; Start[+] --> Explorer[explorer.exe]; Explorer --> SWTest1[sw_test.exe]; SWTest1 --> SWTest2[sw_test.exe]; SWTest2 --> Registry[レジストリ]; SWTest2 --> FileDrop[ファイルのドロップ]; SWTest2 --> Network[ネットワーク接続];
```

推奨事項

1

調査時にコンピューターをネットワークから分離します。

2

ファイルを隔離に移動して悪意のある操作を防止します。

3

ネットワーク内の他のコンピューターでのファイルの実行を防止します。

4

ネットワーク内の他のコンピューターで検出された脅威を検索します。

5

検知した脅威について詳しくは、[Kaspersky Open Threat Intelligence Portal](#) および [Kaspersky Threat Intelligence Portal](#) を参照してください。

6

調査および脅威の処理完了後、コンピューターのネットワーク分離を無効にします。

警告

成功: ブロック

日時2022/10/12 09:46:32

カテゴリPDM: Exploit.Win32.Generic

オブジェクト名C:\Users\ladmin\AppData\Local\Temp\sw_test.exe

スキャンモードシステムウォッチャーのスキャン時

オブジェクトの種別メモリプロセス

コンピューター

コンピューターをネットワークから分離する

コンピューターの分離を解除する

コンピューター名WORKGROUP\PC20

ネットワークインターフェイス192.168.1.28 00-0c-29-ad-69-e5
127.0.0.1 00-00-00-00-00-00

OSMicrosoft Windows 10(10.0.19043)

グループ名管理対象デバイス

ポリシー名Kaspersky Endpoint Security for Windows (11.11.0)

kaspersky

29

推奨事項 (Guided Response)

成功: ブロック

詳細 全ての警告イベント

```
graph LR; Explorer[explorer.exe] --> SWTest1[sw_test.exe]; SWTest1 --> SWTest2[sw_test.exe]; SWTest2 --> Registry[レジストリ]; SWTest2 --> Files[ファイルのドキュメント]; SWTest2 --> Network[ネットワーク];
```

推奨事項

- 調査時にコンピューターをネットワークから分離します。
- ファイルを隔離に移動して悪意のある操作を防止します。
- ネットワーク内の他のコンピューターでのファイルの実行を防止します。
- ネットワーク内の他のコンピューターで検出された脅威を検索します。
- 検出した脅威について詳しくは、[Kaspersky Open Threat Intelligence Portal](#) および [Kaspersky Threat Intelligence Portal](#) を参照してください。
- 調査および脅威の処理完了後、コンピューターのネットワーク分離を無効にします。

推奨事項

- 調査時にコンピューターをネットワークから分離します。
- ファイルを隔離に移動して悪意のある操作を防止します。
- ネットワーク内の他のコンピューターでのファイルの実行を防止します。
- ネットワーク内の他のコンピューターで検出された脅威を検索します。
- 検出した脅威について詳しくは、[Kaspersky Open Threat Intelligence Portal](#) を参照してください。
- 調査および脅威の処理完了後、コンピューターのネットワーク分離を無効にします。

警告

成功: ブロック

日時 2022/04/26 13:39:07

カテゴリ PDM Exploit Win32 Generic

オブジェクト名 C:\Users\admin\AppData\Local\Temp\sw_test.exe

スキャンモード システムウォッチャーのスキャン時

オブジェクトの種類 メモリプロセス

プロセス

起動/パラメータ "C:\Users\admin\AppData\Local\Temp\sw_test.exe" evil

システム PID 8656

ログオンセッション ID 00000000.00026547

特権付きユーザー はい

コンピュータ

コンピューターをネットワークから分離する ネットワークから分離されたコンピューターをブロック解除する

コンピューターのネットワーク分離

コンピューター上のすべてのアクティブな TCP/IP ネットワーク接続を切断して新規の接続の確立をブロックします (ネットワーク分離の除外リストで設定されている接続、Kaspersky Endpoint Security のサービスと Kaspersky Security Center Network Agent による接続を除く)。これにより、ネットワーク内の他のコンピューターに脅威が伝播されることを防ぎます。

推奨事項 6 件中 1 件

次へ

推奨する対応を作業順番にガイド。
リンクをクリックすると、設定ボタンに誘導。

プロセス

起動/パラメータ "C:\Users\admin\AppData\Local\Temp\sw_test.exe" evil

システム PID 8656

整合性レベル 整合性 (高)

ユーザー名 PC01\admin

ログオンセッション ID 00000000.00026547

特権付きユーザー はい

ファイル

実行をブロック 隔離に移動する

隔離

安全でないと思われるファイルを隔離に移動できます。隔離とは、コンピューター上の特別な保管領域です。隔離されたファイルは暗号化され、コンピューターが危険にさらされることはありません。

推奨事項 6 件中 2 件

戻る 次へ

名前とサイズ

MDS

SHA256 90c2a7a3f8

信頼チェックの結果

ダウンロード

ダウンロード Web アドレ

レス

アプリケーション

作成日 2022/04/26 13:39:02

編集日 2022/04/26 13:39:02

ファイル作成者 PC01\admin

ファイル編集者

最終編集者名

MDS

SHA256

「アラートの表示」からアラートカードを展開 “全ての警告イベント”レポート

成功: ブロック

詳細

すべての警告イベント

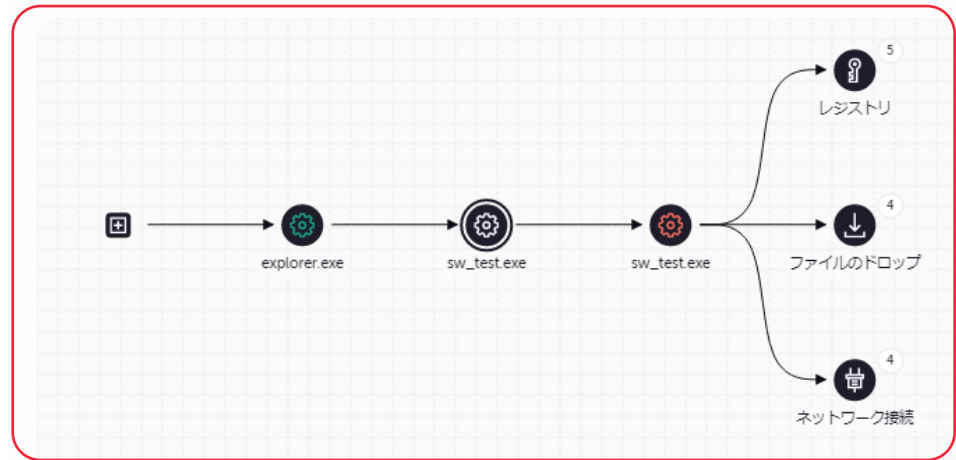
+ IOC の作成

<input type="checkbox"/>	時刻	種別	オブジェクト
<input type="checkbox"/>	2021/11/29 16:20:12	⚙ プロセスの開始	C:\Users\admij\AppData\Local\Temp\sw_test.exe
<input type="checkbox"/>	2021/11/29 16:20:11	⚙ プロセスの開始	C:\Users\admij\Desktop\sw_test.exe
<input type="checkbox"/>	2021/11/12 11:11:22	⚙ プロセスの開始	C:\Windows\explorer.exe
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\sw_test.exe.log
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile1
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile2
<input type="checkbox"/>	2021/11/29 16:20:18	📁 ファイルのドロップ	C:\TestBssExploitBlockingDetectAction.tst
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\sw_test.exe.log
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile1
<input type="checkbox"/>	2021/11/29 16:20:12	📁 ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile2
<input type="checkbox"/>	2021/11/29 16:20:18	📁 ファイルのドロップ	C:\TestBssExploitBlockingDetectAction.tst

アラートカード (詳細) レポート

成功: ブロック

詳細 全ての警告イベント



成功: ブロック

日時

2022/10/12 09:46:32

カテゴリ

PDM:Exploit.Win32.Generic

オブジェクト名

C:\Users\admin\AppData\Local\Temp\sw_test.exe

スキャンモード

システムウォッチャーのスキャン時

オブジェクトの種別

メモリプロセス

KESのアクション

脅威プロセスの連鎖

インシデント詳細

コンピューター

コンピューターをネットワークから分離する

コンピューターの分離を解除する

コンピューター名

WORKGROUP\PC20

ネットワークインターフェイス

192.168.1.28 00-0c-29-ad-69-e5

エイス

127.0.0.1 00-00-00-00-00-00

OS

Microsoft Windows 10(10.0.19043)

グループ名

管理対象デバイス

ポリシー名

Kaspersky Endpoint Security for Windows (11.11.0)

プロセス

起動パラメータ

"C:\Users\admin\AppData\Local\Temp\sw_test.exe" evil

システム PID

1800

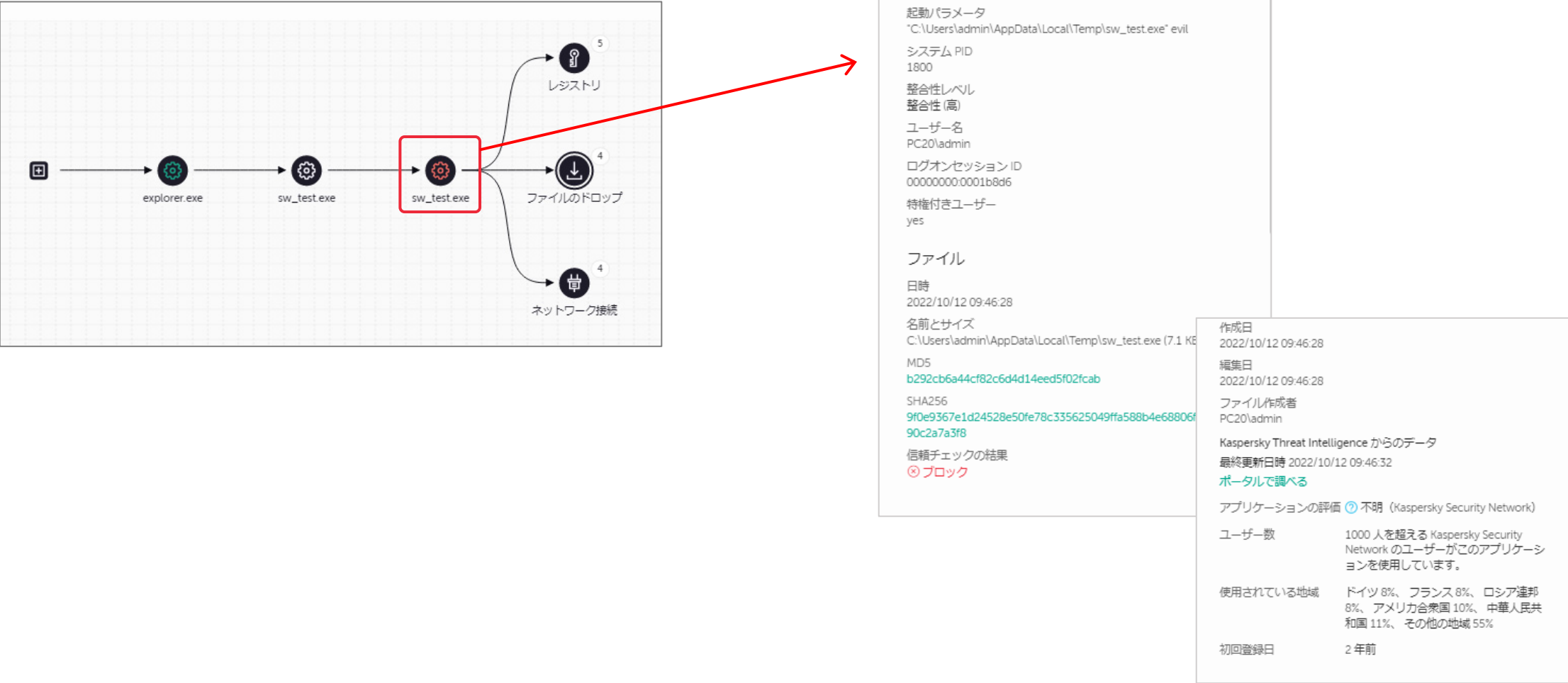
整合性レベル

整合性 (高)

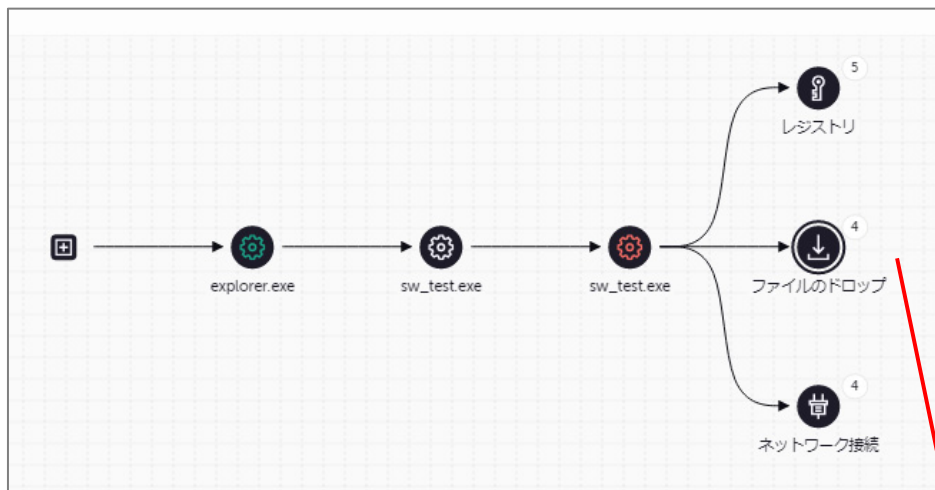
ユーザー名

PC20\admin

アラートカード



アラートカード: ファイルのドロップ



イベント			
+ IOC の作成			
<input type="checkbox"/>	時刻	種別	オブジェクト
<input type="checkbox"/>	2022/10/12 09:46:28	↓ ファイルのドロップ	C:\Users\admin\AppData\Local\Temp\sw_test.exe
<input type="checkbox"/>	2022/10/12 09:46:28	↓ ファイルのドロップ	C:\Users\admin\AppData\Local\Temp\droppedfile1
<input type="checkbox"/>	2022/10/12 09:46:28	↓ ファイルのドロップ	C:\Users\admin\AppData\Local\Temp\droppedfile2
<input type="checkbox"/>	2022/10/12 09:46:31	↓ ファイルのドロップ	C:\TestBssExploitBlockingDetectAction.tst

ファイルのドロップ

実行をブロック 隔離に移動する

ファイル

日時
2022/10/12 09:46:28

名前とサイズ
C:\Users\admin\AppData\Local\Temp\sw_test.exe (7.1 KB)

MD5
[b292cb6a44cf82c6d4d14eed5f02fcab](#)

SHA256
[9f0e9367e1d24528e50fe78c335625049ffa588b4e68806f2b057190c2a7a3f8](#)

作成日
2022/10/12 09:46:28

編集日
2022/10/12 09:46:28

ファイル作成者
-

Kaspersky Threat Intelligence からのデータ

最終更新日時 2022/10/12 09:46:32

[ポータルで調べる](#)

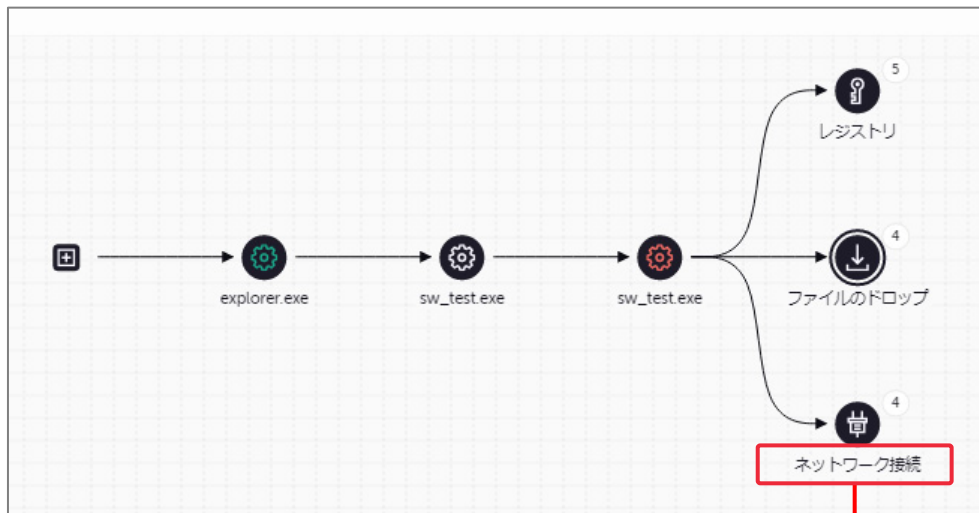
アプリケーションの評価 不明 (Kaspersky Security Network)

ユーザー数
1000 人を超える Kaspersky Security Network のユーザーがこのアプリケーションを使用しています。

使用されている地域
ドイツ 8%、フランス 8%、ロシア連邦 8%、アメリカ合衆国 10%、中華人民共和国 11%、その他の地域 55%

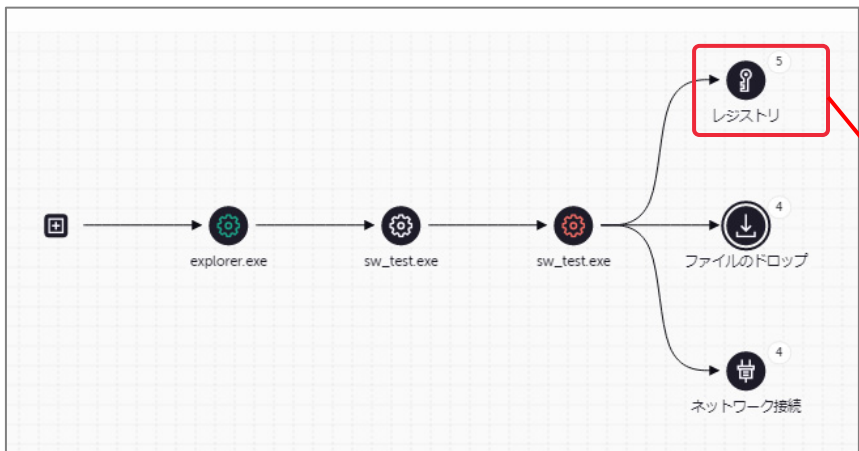
初回登録日
2 年前

アラートカード: ネットワーク接続の情報



イベント			
+ IOC の作成			
フィルター			
<input type="checkbox"/>	時刻	種別	オブジェクト
<input type="checkbox"/>	2022/10/12 09:46:28	ネットワーク接続	93.184.216.34:80
<input type="checkbox"/>	2022/10/12 09:46:29	ネットワーク接続	77.88.55.50:80
<input type="checkbox"/>	2022/10/12 09:46:29	ネットワーク接続	62.217.160.2:443
<input type="checkbox"/>	2022/10/12 09:46:30	ネットワーク接続	213.180.204.24:443

アラートカード: レジストリ



悪意あるプログラムが自動実行するようにレジストリが作成されています。

イベント

時刻	種別	オブジェクト
2022/10/12 09:46:28	レジストリ	\registry\user\s-1-5-21-3407934368-3318140685-4219265482-
2022/10/12 09:46:28	レジストリ	\registry\user\s-1-5-21-3407934368-3318140685-4219265482-
2022/10/12 09:46:28	レジストリ	\registry\user\s-1-5-21-3407934368-3318140685-4219265482-
2022/10/12 09:46:28	レジストリ	\registry\user\s-1-5-21-3407934368-3318140685-4219265482-
2022/10/12 09:46:28	レジストリ	\registry\user\s-1-5-21-3407934368-3318140685-4219265482-

レジストリ

日時
2022/10/12 09:46:28

レジストリキー
\registry\user\s-1-5-21-3407934368-3318140685-4219265482-1000\software\microsoft\windows\currentversion\run

名前
sw_test

値
"C:\Users\admin\AppData\Local\Temp\sw_test.exe" evil

自動実行ポイント
はい

インシデント対応：レスポンス
封じ込め・対話式対応

レスポンス

以下のアクションを、アラートカード上のボタンやタスクで実行します。

アラートカードからのレスポンス

- “実行をブロック”：プログラムの起動禁止
- “隔離に移動する”：ファイルの隔離
- “コンピューターをネットワークから分離する”： 端末をネットワークからの論理的に切断
- “IOCの作成”： IOCスキャンタスクの作成

タスクから実行

- “プロセスの終了”：既に起動しているプロセスの停止
- “プロセスの開始”：任意のプログラムを実行
- “ファイルの削除”：任意のファイルを削除
- “ファイルの取得”：任意のファイルを取得（元のファイルは残ります）
- “ファイルの隔離”：任意のファイルを隔離（隔離領域に移動しアクセス不可になります）
- “IOCスキャン”： IOCスキャンの実行

“実行をブロック”

① アラートカードから、起動停止したいプロセスで、「実行をブロック」をクリック。

ファイル

実行をブロック 隔離に移動する

名前とサイズ C:\Users\admin\AppData\Local\Temp\sw_test.exe (7.1 KB)

MD5 b292cb6a44cf82c6d4d14eed5f02fcab

SHA256 9f0e9367e1d24528e50fe78c335625049ffa588b4e68806f2b057190c2a7a3f8

信頼チェックの結果 ブロック

作成日 2022/11/09 12:41:10

編集日 2022/11/09 12:41:10

ファイル作成者 WIN2019\admin



ファイルの実行をブロックする

ファイル「C:\Users\admin\AppData\Local\Temp\sw_test.exe」は「Kaspersky Endpoint Security for Windows (11.11.0)」のブロックルールの一覧に追加されます

OK キャンセル

② ダイアログボックスで、OKをクリック

③ KES for Windows ポリシーの中に、ルールが作成されます。

+ 追加 編集 削除 フィルター

<input type="checkbox"/>	ステータス	名前	種別	オブジェクトのパス
<input type="checkbox"/>	有効	[KillChain] md5 for C:\Users\admin\j\Desktop\vanquish-0.2.1\bin\vanquish.exe	実行ファイル	

実際にブロックするか、
記録するのみにするか
予めポリシーを決定しておきます。

実行防止

実行防止が有効です

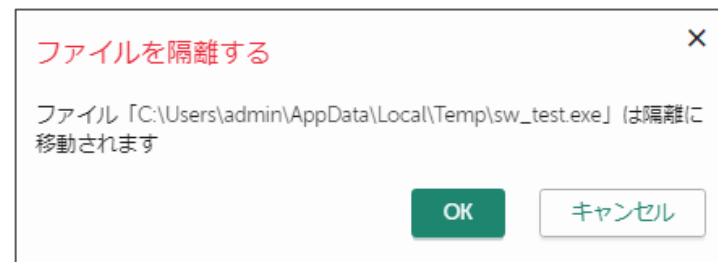
禁止されたオブジェクトを実行、または開いたときの処理

☒ ブロックしてレポートに書き込む

☐ イベントの記録のみ

“隔離に移動する”

① 隔離したいプロセスで、「隔離に移動する」をクリック。



② ダイアログボックスで、OKをクリック

③ レポジトリの隔離に、隔離されます。



既に削除が完了している、ブロックしたためファイルがない場合など、隔離が行われない場合があります。

バックアップに既にファイルが存在する場合もありますので、ご確認ください。

”コンピューターをネットワークから分離する”

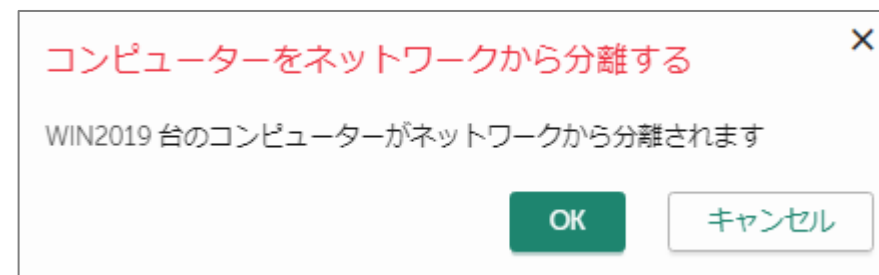
- ① アラートカードから、「コンピューターをネットワークから分離する」をクリック。

コンピューター

コンピューターをネットワークから分離する

コンピューターの分離を解除する

コンピューター名	WORKGROUP\WIN2019
ネットワークインターフェイス	192.168.1.22 00-0c-29-49-14-ed
エイス	127.0.0.1 00-00-00-00-00-00
OS	Microsoft Windows Server 2019(10.0.17763)
グループ名	管理対象デバイス
ポリシー名	Kaspersky Endpoint Security for Windows (11.11.0)



- ② ダイアログボックスで、OKをクリック

- ③ 端末(host)に、「ISOLATED FROM NETWORK」のタグが付与され、端末が隔離されます。
隔離された状態では、ポリシーの設定で指定した、Isolation時のネットワーク許可ルールに基づき動作します。

「ISOLATED FROM NETWORK」 タグが付与され、隔離された端末の確認

デバイス / タグ / デバイスのタグ

[自動タグルールの設定](#)
デバイスに割り当てられたタグがリスト表示されます。

+ 追加 × 削除

検索...

タグ | 使用中 | 割り当て先

☐ [ISOLATED FROM NETWORK](#) [デバイスの表示](#)

< 戻る 1 次へ > 20 結果: 1-1 / 1 合計

検出と製品の導入

+ デバイスの追加 × 削除 + 新規タスク グループへ移動

検索...

<input type="checkbox"/> 名前	可視	前回の管理サーバーへの接続	ネットワークエージェン...	ネットワークエージェン...
<input type="checkbox"/> PC01	☑	2022/04/20 16:59:12	☑	☑

< 戻る 1 次へ >

レポート

ファイル脅威対策

ウェブ脅威対策

メール脅威対策

ファイアウォール

ネットワーク脅威対策

有害 USB 攻撃ブロック

AMSI 保護

セキュリティコントロール

アダプティブアンチマルウェアコントロール

アプリケーションコントロール

デバイスコントロール

ウェブコントロール

タスク

定義データベースのアップデート

スキャン

整合性チェック

Detection and Response

Endpoint Detection and Response

Endpoint Detection and Response

アップデート

レポートを保存する

重要度:

検索

時刻:

すべて

<

2021/04/06

2022/04/21

>

イベントの日付	イベント	アプリケーション名	アプリケーションのパス
今日 (2022/04/20 16:36:19)	ネットワーク分離		
今日 (2022/04/20 16:35:44)	アプリケーションの設定が変更されました	avp.exe	C:\Program Files (x86)\K
今日 (2022/04/20 15:00:29)	オブジェクトが削除されました		
今日 (2022/04/20 15:00:29)	オブジェクトが隔離されました		
今日 (2022/04/20 14:59:47)	タスクを開始しました	avp.exe	C:\Program Files (x86)\K
今日 (2022/04/20 14:50:07)	タスクが停止しました	avp.exe	C:\Program Files (x86)\K

今日 (2022/04/20 16:36:19) ネットワーク分離

イベント: ネットワーク分離

ユーザー種別: 未定義

コンポーネント: Endpoint Detection and Response

クライアントID: 833029775

ページ読み込みエラー

←

→

🏠

🔍 https://www.youtube.com

⋮

🔒

☆

🖨

📄

👤

☰

正常に接続できませんでした

www.youtube.com のサーバーへの接続を確立できませんでした。

このサイトが一時的に利用できなくなっていたり、サーバーの負荷が高すぎて接続できなくなっている可能性があります。しばらくしてから再度試してください。

他のサイトも表示できない場合、コンピューターのネットワーク接続を確認してください。

ファイアウォールやプロキシでネットワークが保護されている場合、Firefox によるウェブアクセスが許可されているか確認してください。

再試行

43

kaspersky

“プロセスの終了”：起動しているプロセスの停止


① プロセスの終了タスクを作成します。

新規タスク

アプリケーション
Kaspersky Endpoint Security for Windows (11.7.0)

タスク種別
プロセスの終了

タスク名
プロセスの終了

タスクを割り当てるデバイスの選択 

☒ 管理グループにタスクを割り当てる

☐ デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする

☐ デバイスの抽出にタスクを割り当てる

② プロセスの終了タスクのプロパティに、ファイルパスをペーストします。

🕒 プロセスの終了

全般 履歴 設定 アプリケーション設定 スケジュール 変更履歴

プロセスの終了

処理を終了するファイルを指定してください

パスとハッシュを使用したプロセスの強制終了

完全パスを使用したプロセスの強制終了

パスとハッシュを使用したプロセスの強制終了

MD5

ファイルのチェックサム

プロセスのファイルまたはフォルダーの完全パス

☐ パスの大文字小文字を区別する

“IOCの作成”

ファイルを選択し、「IOCの作成」をクリック

+ IOC の作成				フィルター
<input type="checkbox"/>	時刻	種別	オブジェクト	
<input checked="" type="checkbox"/>	2022/04/11 16:24:35	プロセスの開始	C:\Users\admij\Desktop\bsstest_amsi.ps1	
<input type="checkbox"/>	2022/04/11 16:25:41	プロセスの開始	C:\Program Files\7-Zip\7zG.exe	
<input type="checkbox"/>	2022/04/11 16:26:02	プロセスの開始	C:\Program Files\7-Zip\7zG.exe	
<input type="checkbox"/>	2022/04/11 16:35:34	プロセスの開始	C:\Program Files\7-Zip\7zG.exe	
<input checked="" type="checkbox"/>	2022/04/11 16:35:40	プロセスの開始	C:\Users\admij\Desktop\SniffPass.exe	
<input checked="" type="checkbox"/>	2022/04/11 16:42:15	プロセスの開始	C:\Users\admij\Desktop\hookanlz.exe	
<input type="checkbox"/>	2022/04/11 16:43:37	プロセスの開始	C:\Program Files\7-Zip\7zG.exe	
<input checked="" type="checkbox"/>	2022/04/13 11:28:51	プロセスの開始	C:\Users\admij\Desktop\Po2_Keyboard_Polling\kbd.exe	
<input type="checkbox"/>	2022/02/04 16:38:16	プロセスの開始	C:\Windows\System32\winlogon.exe	
<input type="checkbox"/>	2022/02/04 16:54:43	ファイルのドロップ	C:\Users\admij\AppData\Roaming\Microsoft\Windows\Recent\sw_test.zip.lnk	
<input type="checkbox"/>	2022/02/04 16:54:56	ファイルのドロップ	C:\Users\admij\Desktop\sw_test	

IoCスキャンによる痕跡検知時に取る、
アクションの設定



IOC スキャンタスク

スキャン条件

☒ OR (見つかった IOC のいずれか)
☐ AND (見つかった IOC すべて)

IOC データ :

名前 : Trojan-PSW.Win32.XShadow.b
説明 : Trojan-PSW.Win32.XShadow.b PC01 2022-04-13T02:28:59Z
文書 : FileItem
IOC: FileItem/Md5sum

IOC コレクションのエクスポート...

IOC 検知時の処理

☒ コンピューターをネットワークから分離する
☐ 簡易スキャンを実行する
☐ コピーを隔離に移動し、オブジェクトを削除する

タスクの作成