kaspersky

Kaspersky EDR Optimum 2.1
製品紹介

2022年5月11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

先ずは、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

組織的課題

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。

kaspersky

Optimum セキュリティ と Expert セキュリティ

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

kaspersky

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

kaspersky

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

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。

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。

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。

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

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。

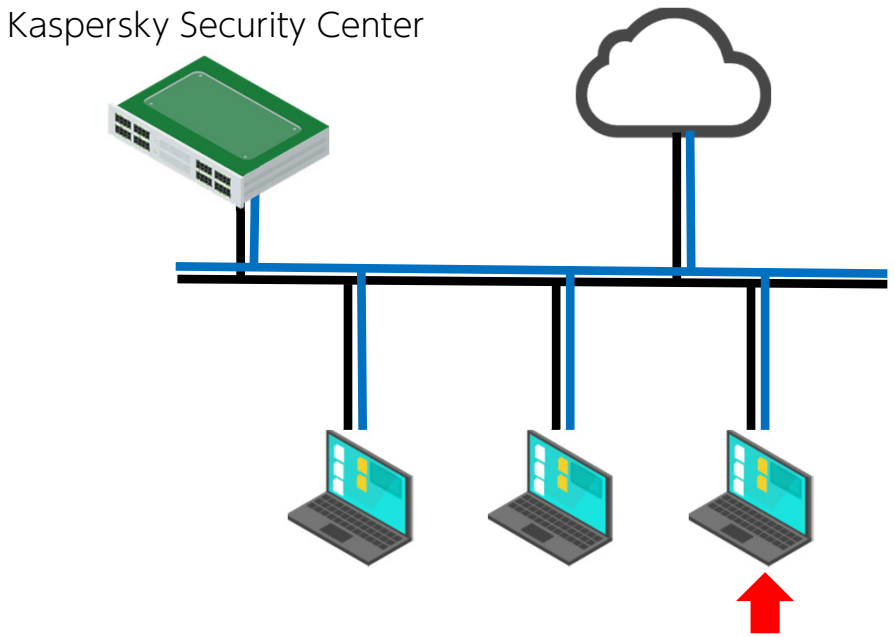
  プログラムの起動禁止、ファイルの隔離。

- IOCスキャン

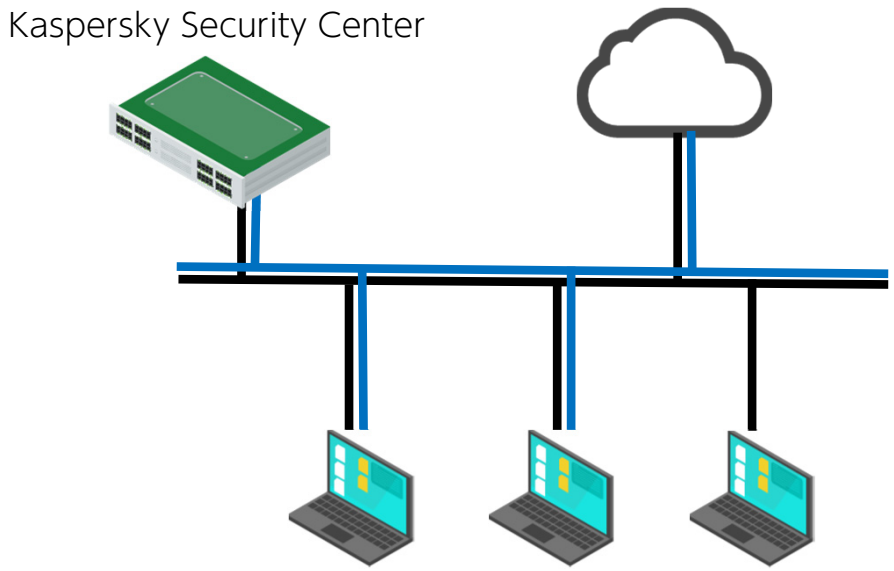
  セキュリティ侵害の痕跡を調査する。

kaspersky

コンピューターをネットワークから分離する



インシデントカードから
分離を実行



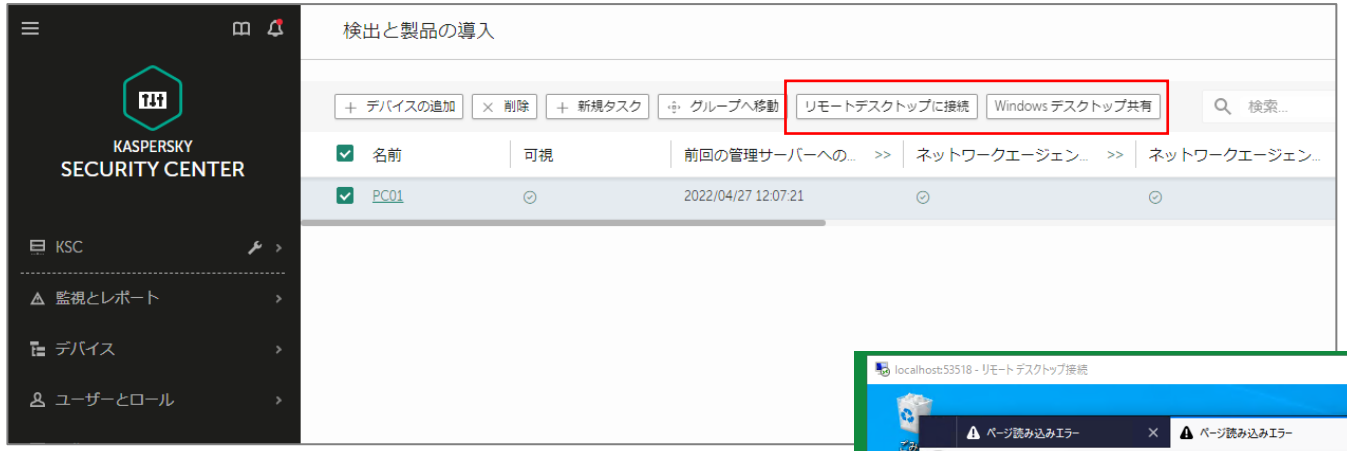
遠隔から論理的に
ネットワークを切断

物理的な接続

論理的な接続

物理的に切り離さないため、
管理操作は継続可能。

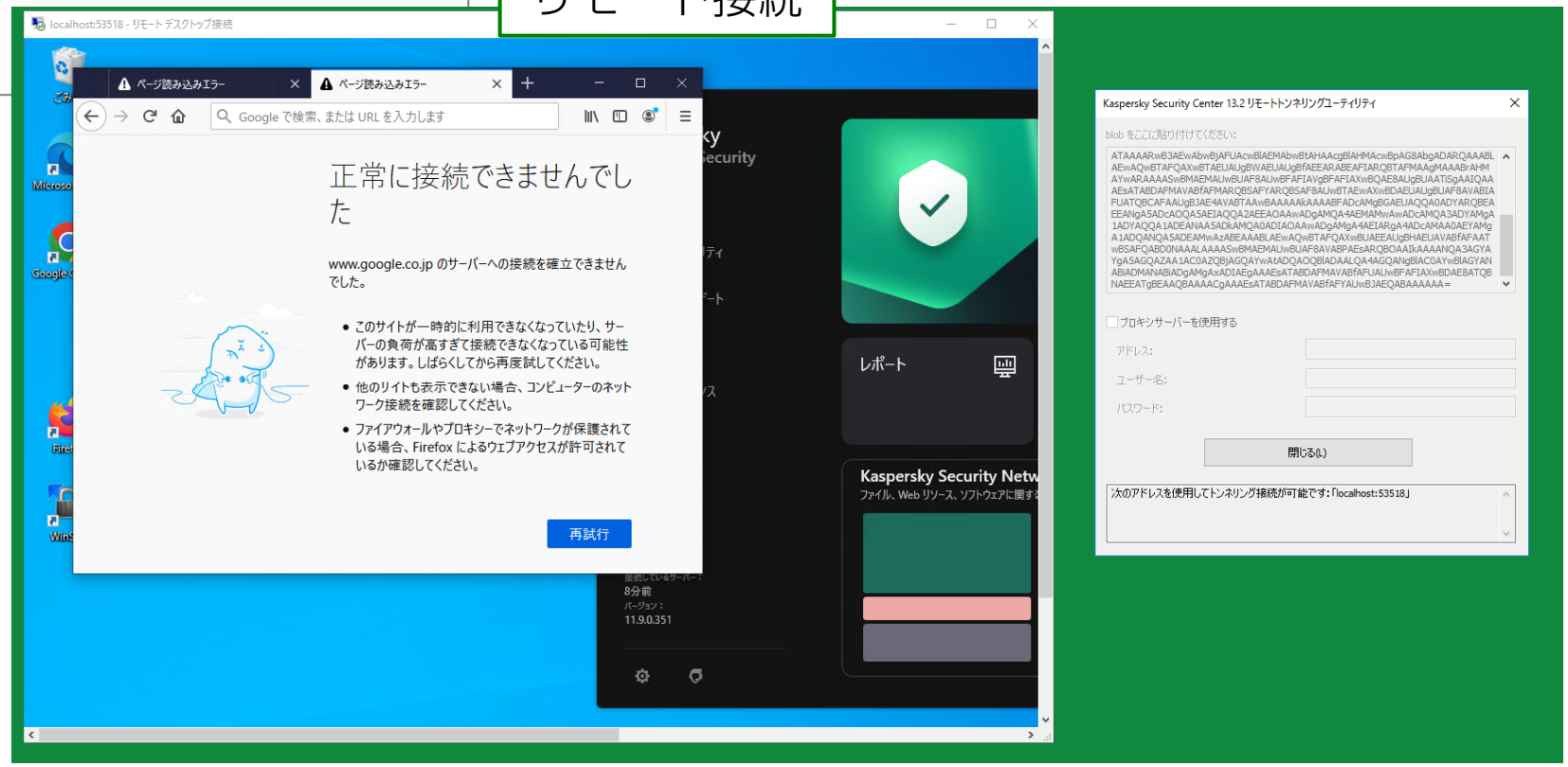
コンピューターをネットワークから分離する



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

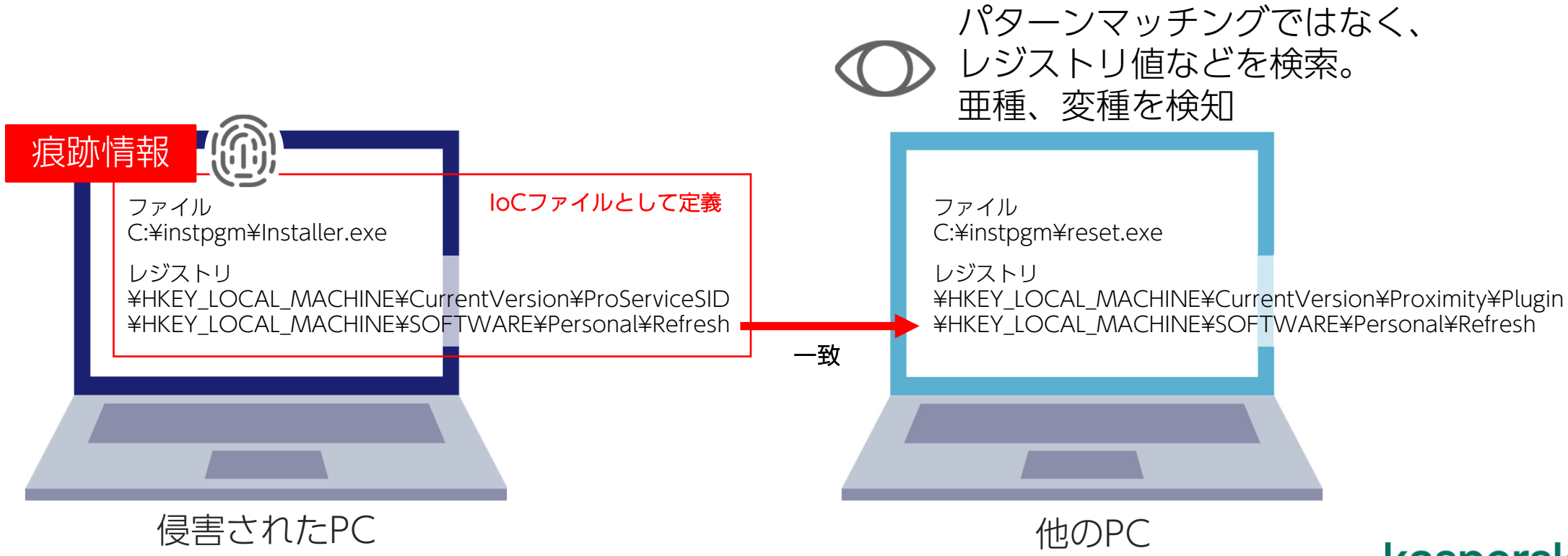


IOC スキャン

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。

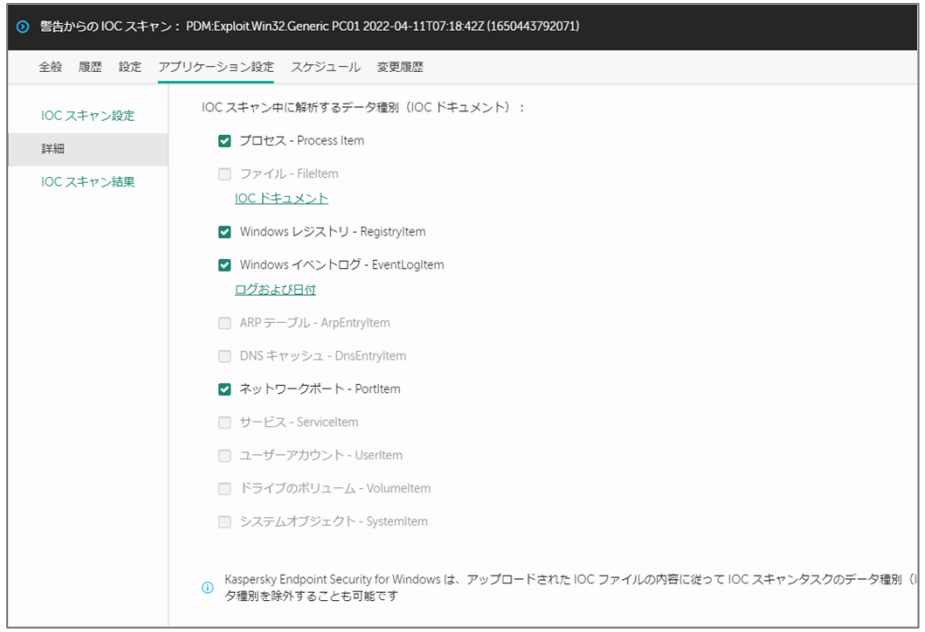
痕跡には、マルウェア本体のハッシュ値、マルウェアが生成するファイル、
レジストリ値などがあります。こうした情報を記述したファイルがIOCファイルです。



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/11.9.0/ja-JP/220828.htm
https://support.kaspersky.com/Help/KESWin/11.9.0/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/11.9.0/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:Exploit.Win32.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/remoteIP" 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="RegistryItem" search="RegistryItem/ValueName" type="endpoint">
```

実行防止（実行をブロック）

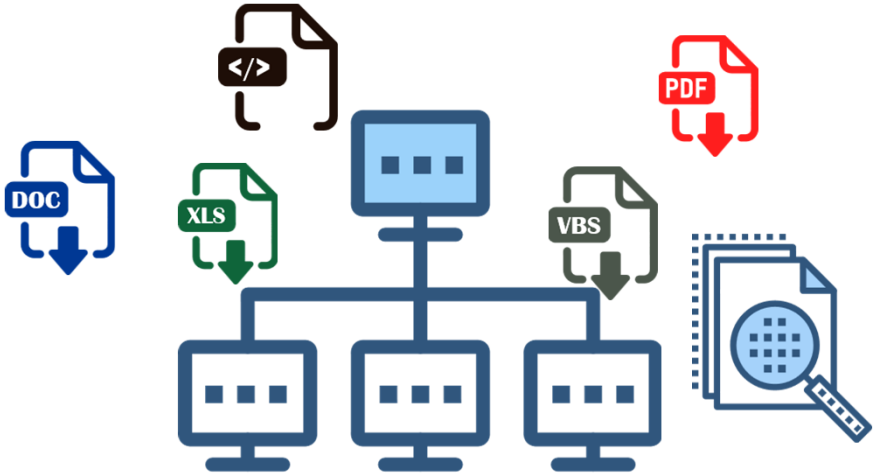
実行ファイルだけでなく、スクリプトの実行や
Office 形式のファイルオープンをブロックすることができます。

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/11.8.0/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/11.8.0/ja-JP/220826.htm



kaspersky

構成

EDR Optimum 2.1 構成

管理サーバー
Kaspersky Security Center 13.2
Kaspersky Security Center Cloud Console 2.1

エージェント
Kaspersky Endpoint Security for Windows 11.9以降
（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
300ライセンス以上を保有している場合に使用出来ます。

EDR Optimum 2.1 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 Security for Virtualization 5.2 Light Agent (Windows)

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

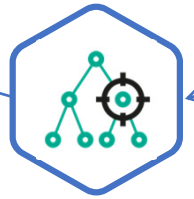
インシデントハンドリングプロセス

インシデントの特定

インシデントカード

封じ込め（対話式対応）

実行をブロック（プログラム起動防止）
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
IOCスキャンタスクの作成
プロセスの終了



根 絶

IOC スキャン

リカバリー

切り離した端末の復帰

誤検知時のファイル復帰

知見のまとめ

IOCスキャンタスクの統合

kaspersky

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　　フィルター

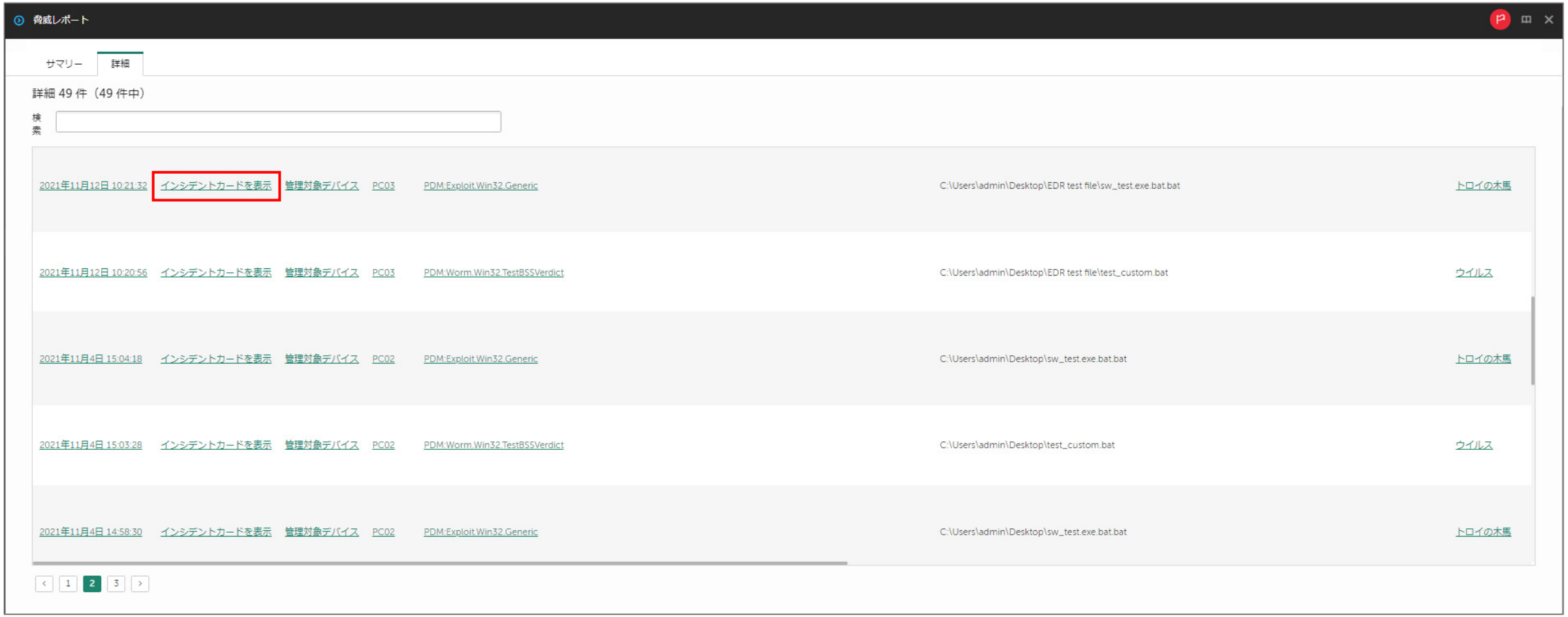
ルール名	通信方向	プロトコル	ソース
DNS	受信	TCP	
DNS	受信	UDP	
Large numbered TCP ports, randomly assigned by the RPC service	受信	TCP	
RPC Endpoint Mapper	受信	TCP	
DNS client	送信	TCP	
DNS client	送信	UDP	
DHCP server	受信 / 送信	UDP	
DHCP client	受信 / 送信	UDP	
MADCAP	受信	UDP	
DHCP failover	受信	TCP	

kaspersky

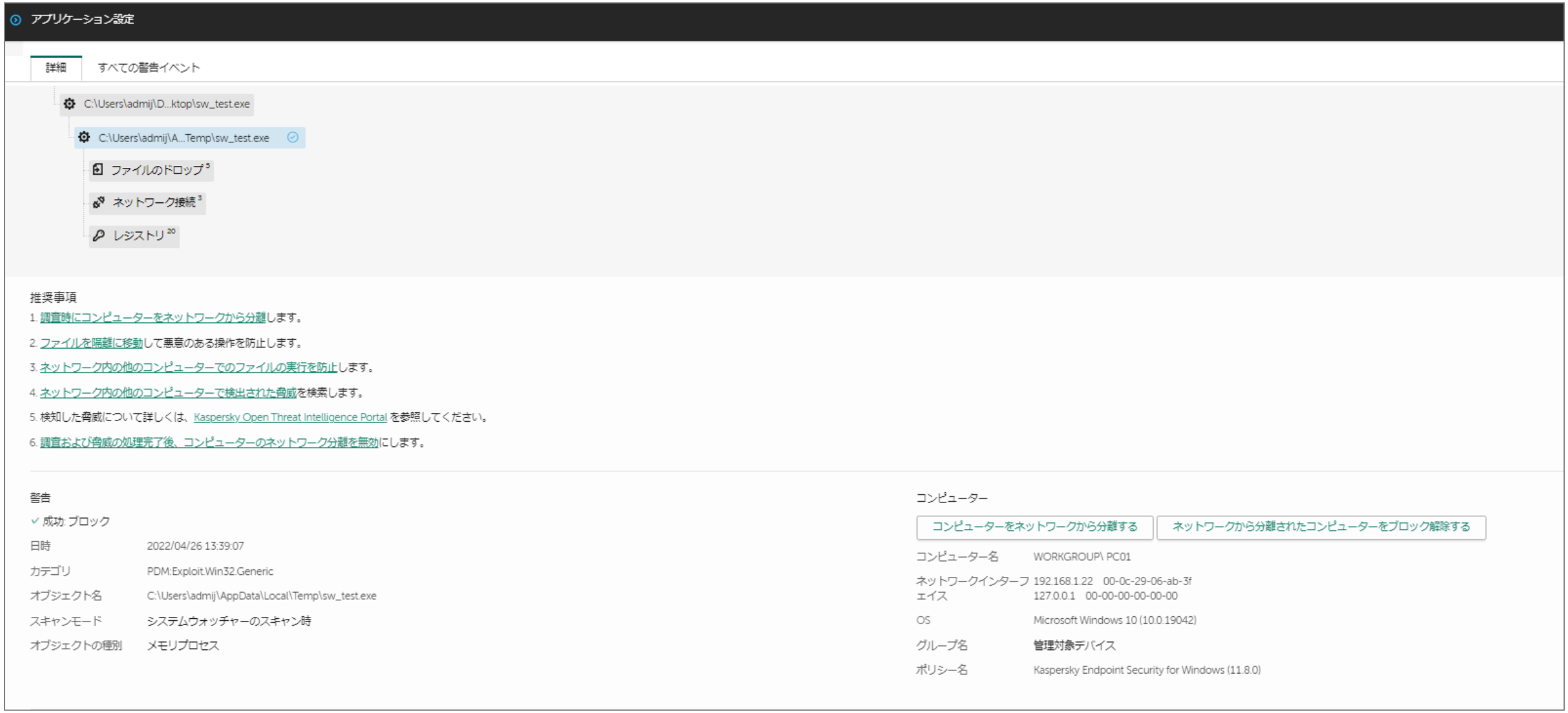
インシデント対応：特定フェーズ

Kaspersky EDR Optimum 操作起点

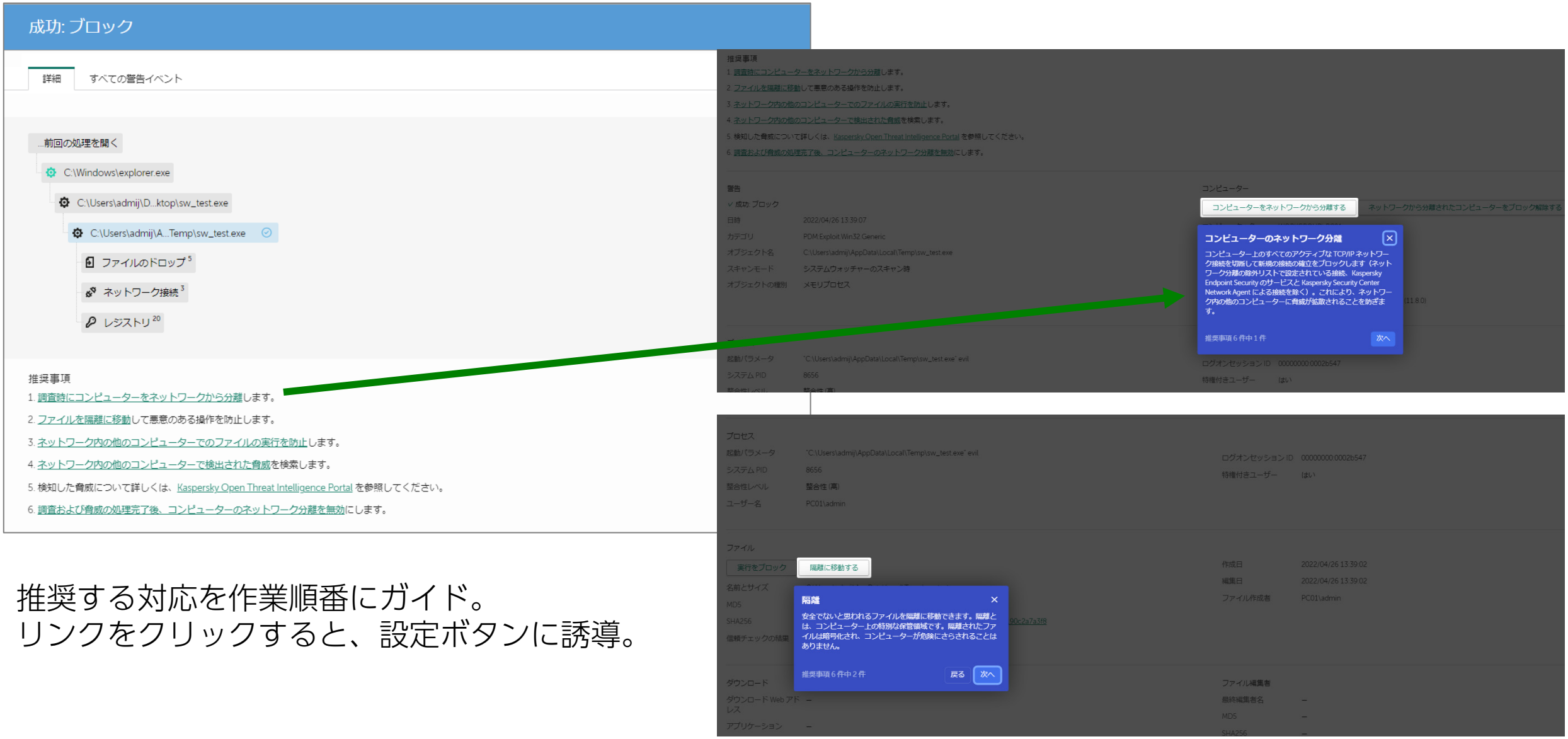
「脅威レポート」から解析レポートを展開、インシデント対応を実行



「インシデントを開く ー インシデントカードを表示」からアプリケーション設定＝インシデントカードを展開
詳細レポート



推奨事項（Guided Response）



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。

「インシデントを開く ー インシデントカードを表示」からアプリケーション設定＝インシデントカードを展開
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

時刻	種別	オブジェクト
2021/11/29 16:20:12	プロセスの開始	C:\Users\admij\AppData\Local\Temp\sw_test.exe
2021/11/29 16:20:11	プロセスの開始	C:\Users\admij\Desktop\sw_test.exe
2021/11/12 11:11:22	プロセスの開始	C:\Windows\explorer.exe
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
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
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile1
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile2
2021/11/29 16:20:18	ファイルのドロップ	C:\TestBssExploitBlockingDetectAction.tst
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\sw_test.exe
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
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile1
2021/11/29 16:20:12	ファイルのドロップ	C:\Users\admij\AppData\Local\Temp\droppedfile2
2021/11/29 16:20:18	ファイルのドロップ	C:\TestBssExploitBlockingDetectAction.tst

インシデントカード （詳細） レポート

KESのアクション

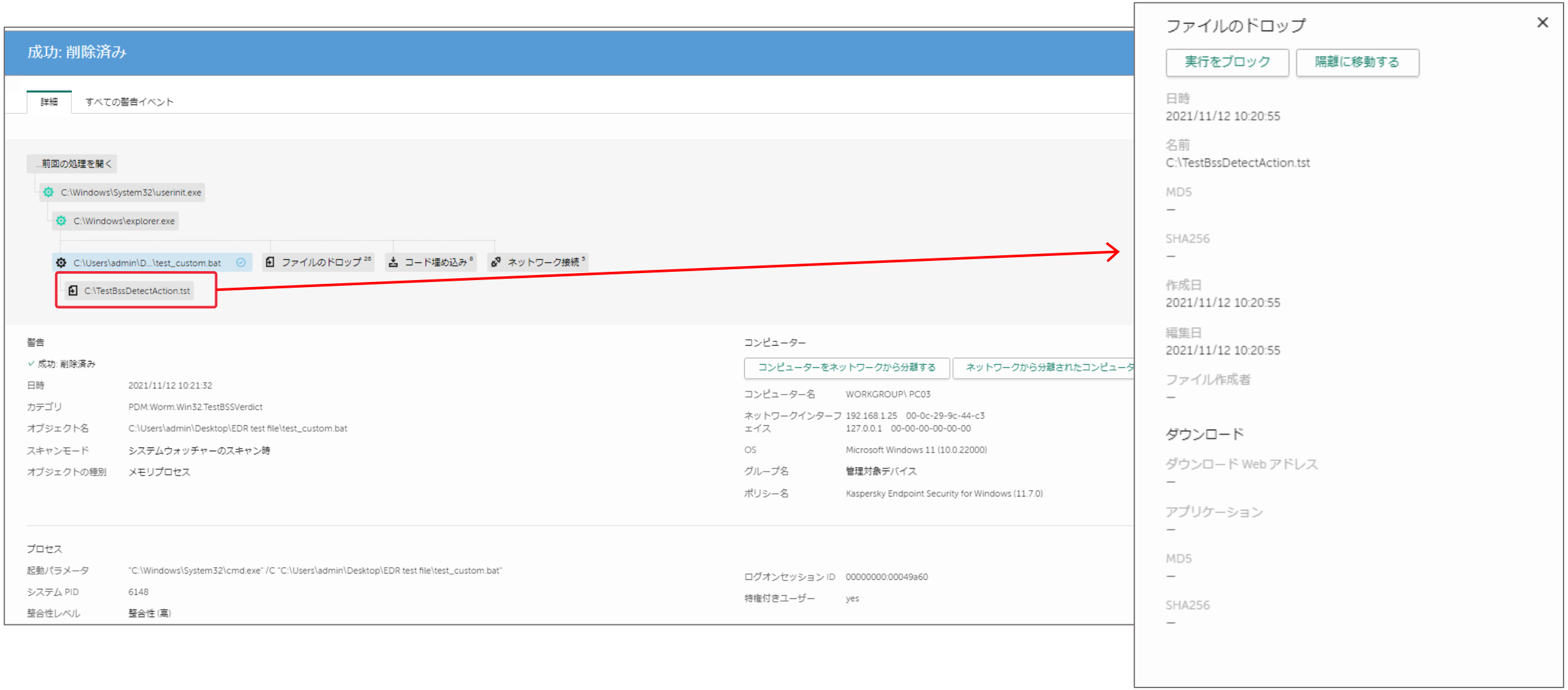
脅威プロセスの連鎖

インシデント詳細

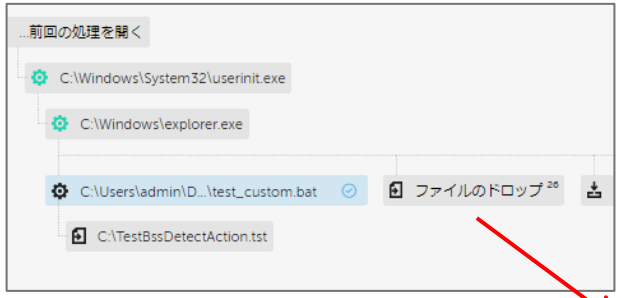
検知したオブジェクトの詳細

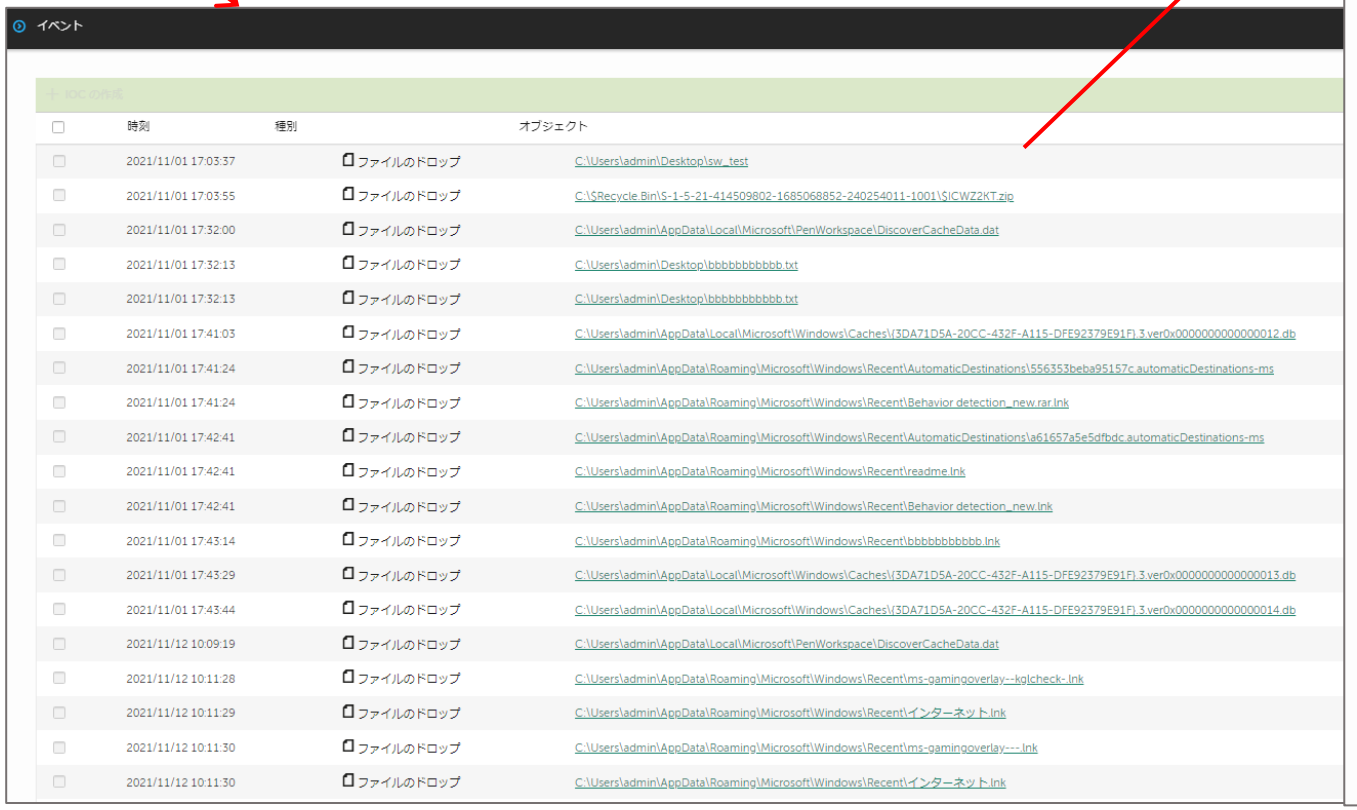
インシデントカード: ファイルのドロップ

攻撃によって作成されたファイルの情報



インシデントカード: ファイルのドロップ





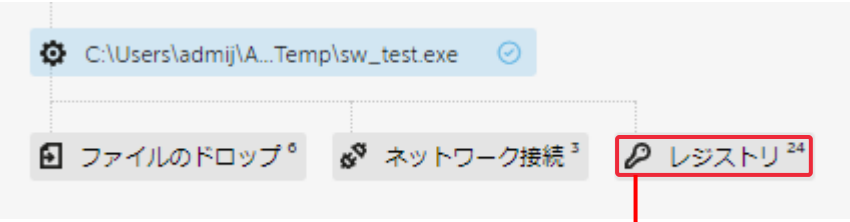
インシデントカード: コード埋め込み、ネットワーク接続の情報

+ IOC の作成

	時刻	種別	オブジェクト
☑	2021/11/29 16:20:11	コード埋め込み	C:\Users\admij\Desktop\sw_test.exe
☐	2021/11/29 16:20:11	コード埋め込み	C:\Users\admij\Desktop\sw_test.exe

	時刻	種別	オブジェクト
☐	2021/11/29 16:20:12	ネットワーク接続	93.184.216.34:80
☐	2021/11/29 16:20:15	ネットワーク接続	5.255.255.5:80
☐	2021/11/29 16:20:15	ネットワーク接続	5.255.255.5:443

インシデントカード: レジストリ



IOC の作成　フィルター

	時刻	種別	オブジェクト
	2022/04/11 16:18:30	レジストリ	\registry\user\s-1-5-21-3603613330-4022074072-375812484-1001\software\microsoft\windows\curren
	2022/04/11 16:18:30	レジストリ	\registry\user\s-1-5-21-3603613330-4022074072-375812484-1001\software\microsoft\windows\curren
	2022/04/11 16:18:30	レジストリ	\registry\user\s-1-5-21-3603613330-4022074072-375812484-1001\software\microsoft\windows\curren
	2022/04/11 16:18:30	レジストリ	\registry\user\s-1-5-21-3603613330-4022074072-375812484-1001\software\microsoft\windows\curren
	2022/04/11 16:18:30	レジストリ	\registry\user\s-1-5-21-3603613330-4022074072-375812484-1001\software\microsoft\windows\curren

レジストリ

日時
2022/04/11 16:18:30

レジストリキー
\registry\user\s-1-5-21-3603613330-4022074072-375812484-1001\software\microsoft\windows\currentversion\run

名前
sw_test

値
"C:\Users\admij\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、インシデントカード上のボタンやタスクで実行します。

インシデン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

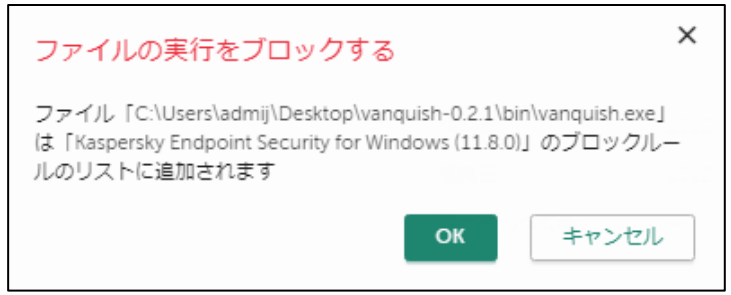
タスクから実行

- “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

kaspersky

“実行をブロック”

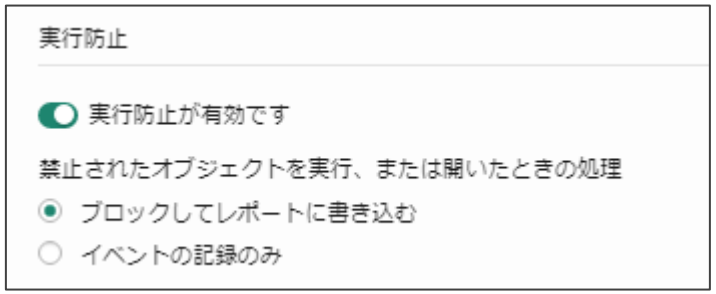
① インシデントカードから、起動停止したいプロセスで、「実行をブロック」をクリック。



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。

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。



“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 インシデントカードから、「 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。

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

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
アダプティブアノマリーコントロール
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ー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

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。

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。

“IOCの作成”

ファイルを選択し、「IOCの作成」をクリック

IoCスキャンによる痕跡検知時に取る、
アクションの設定