

kaspersky

「Kaspersky Managed Detection and Response」のご紹介

2025年03月19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

V2.2

Kaspersky Managed Detection and Response (MDR)とは

サービス概要

■高度なシステムとKasperskyのSOCのエキスパートの分析による脅威検知サービス

24時間365日、お客様環境で発生したイベントを継続監視

インシデント発見時に、インシデント詳細と推奨の対応策(remediation)を提供

■様々な脅威を検知する2,000以上の脅威ハンティングルール

Kaspersky脅威インテリジェンスおよびMITRE ATT&CK Frameworkをベースに作成

攻撃の各フェーズで確認される攻撃手法を検知、攻撃が深刻化する前の対処を支援

■誤検知を防ぎ、「本物」のインシデントのみを報告

収集されたテレメトリーは機械学習ベースの自動分析システムによってリアルタイムで処理、

偽陽性のフィルタリング・アラートの優先順位付けを機械的に行うことで、攻撃開始から検知までの時間(MTTD)・

検知から対応完了までの時間(MTTR)の短縮を実現

システムによって怪しいと判定された行為は、KasperskyのSOCのエキスパートによる脅威ハンティングを実施

Kaspersky Managed Detection and Response (MDR)とは

サービス概要

■高度なEDR(Next EDR Expert または Next XDR Expert)の購入は不要

Next EDR Foundations / OptimumとMDRの購入でマネージドEDRサービスを提供
(最小購入ライセンス数: 150)

■推奨されたレスポンスを即時実行する「自動承認機能」

「自動承認」機能を有効にすることで、管理者の応答無しでレスポンスを24時間365日自動実行
ランサムウェア・ワーム・C&C通信といった緊急性の高い端末のネットワーク分離や調査・分析に必要な検体を
管理者の業務時間外に自動取得し、カスペルスキーのSOCエキスパートに送信

■他社エンドポイントセキュリティ環境へMDRサービスを提供(Windowsのみ)

収集されたテレメトリーは機械学習ベースの自動化システムによって処理
システムによって怪しいと判定された行為は、KasperskyのSOCのエキスパートによる脅威ハンティングを実施

MDRサービス概要

EPPを補完するマネージドサービス

- エンドポイントの挙動を24時間365日監視
- エキスパートによる脅威ハンティング
- 対象端末への 手動 or 自動レスポンス
SOCエキスパートへのダイレクトアクセス
- マニュアルでのインシデント作成

強化された可視性

- 使いやすいMDRポータル
のダッシュボード・レポート機能
- セキュリティヘルスチェックと
対象端末のステータス可視化

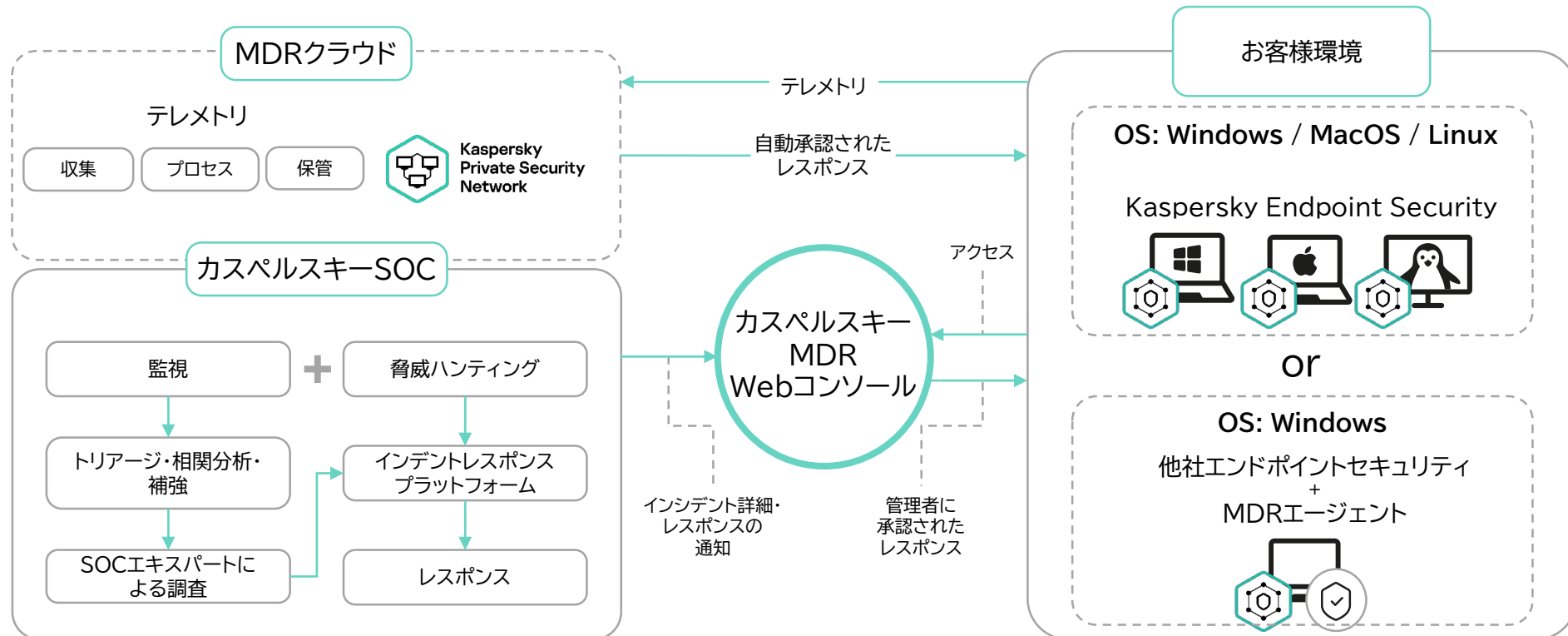
分析および調査のサポート

- APIでのインシデントデータ
ダウンロード
- ログ保持期間:3か月
- インシデント履歴保持期間:1年

Kaspersky Managed Detection and Response (MDR)とは

機械学習ベースの自動分析システム・SOCエキスパートの分析による脅威検知サービス

1. Kaspersky Endpoint Security(KES)がインストールされた端末からテレメトリを収集し、カスペルスキーのSOCへ転送（KESを「EDRエージェント」モードでインストールすることでサードパーティ製エンドポイントセキュリティ製品と同居可能）
2. 収集したテレメトリを自動分析システムによって分析、怪しいアクティビティを検知した場合、カスペルスキーのSOCエキスパートへ通知
3. SOCエキスパートがアラートをさらに調査し、お客様へアラート通知



テレメトリ

脅威の検出を目的とした、端末のログデータ収集

- ・エンドポイントが各端末のログをKasperskyのクラウドに送信
- ・送信されたログはルールに基づきストレージに保管→自動分析システム・KasperskyのSOCエキスパートによって分析

<収集される情報=テレメトリ>

- ファイルシステムイベント (ファイル作成・変更)
- プロセスイベント (プロセススタート、インジェクションなど)
- ネットワークイベント (コネクション、DNSクエリ、メール、
ファイルダウンロードなど)
- システムイベント (レジストリ、イベントログ、WMI、自動実行など)
- エンドポイントセキュリティイベント(マルウェア検知)
- サービスイベント

<サンプル>

```
"processcmdline": "\\C:\\WINDOWS\\system32\\WindowsPowerShell\\v1.0\\PowerShell.exe\" -NoLogo -N  
"processfilemd5": "0x234B54B8BB71EF6D13BDB51A6C464CD9",  
"processfilepath": "c:\\windows\\ccm\\systemtemp\\84c17278-7077-4826-96fd-ae3ad25d3305.ps1",  
"processlogonsessionid": "0x85FA3",  
"processlogontype": 2,  
"processpid": 10000,  
"processuniquepid": "0xDB0702CF60C5AEC3",  
"processuserid": "S-1-5-21-1430328663-2098613005-1233803906-143945",  
"processversioninfodescription": "Windows PowerShell",  
"processversioninfooriginalfilename": "PowerShell.EXE",  
"processversioninfoproductname": "microsoft\\u00ae windows\\u00ae operating system",  
"processversioninfovendorname": "Microsoft Corporation",  
"productinfo": "kes 11.3.0.773 Windows 10 RS5 x64",  
"statsource": 1,  
"storageaddedfiletype": 2,  
"type": "aps",  
"user_description": "mdr_iro23",
```

テレメトリ

監査ログをテレメトリに使用

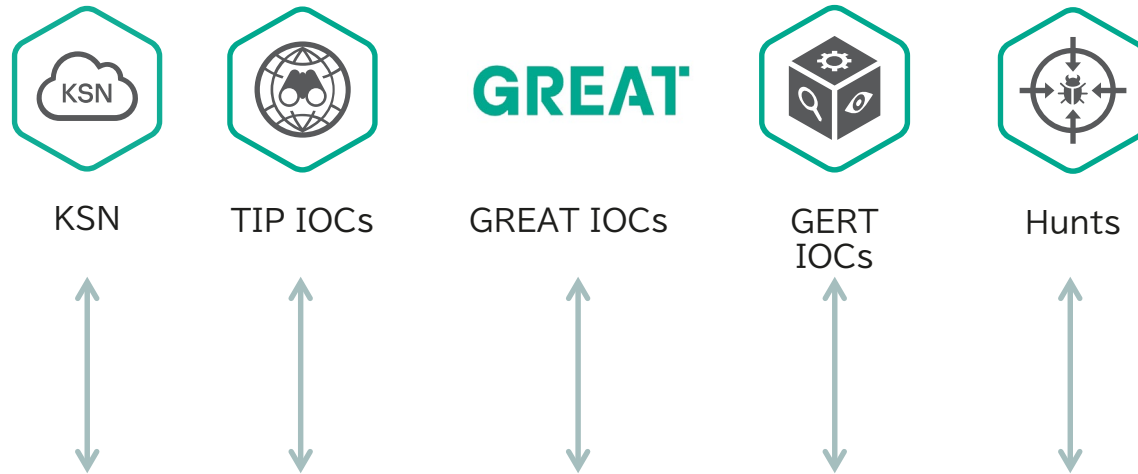
- ドメインポリシー(ローカル)とドメインコントローラーポリシーによる、コンピュータの監査
ログオン、特殊なログオン、重要な特権の使用、監査ポリシーの変更など、21のサブカテゴリの監査
- アクティブディレクトリのユーザー、グループの監査
Administrator、Administrators、Domain Admins、Group Policy Creator Ownersなど
20のユーザー、グループの監査
- アクティブディレクトリ証明書サービスの監査



テレメトリプロセスパイプライン

対象のテレメトリに関する多角的な脅威インテリジェンスや知見によって精度の高い分析

KSNに集まるレピュテーション、ボットネット監視、スパムトラップ、OSINTなどの脅威情報、グローバル調査解析チーム「GReAT」・グローバル緊急対応チーム「GERT」といったさまざまなソースの脅威インテリジェンス情報を使用



取得したテレメトリをさまざまな
脅威インテリジェンスの情報で強化

検知技術: 脅威ハンティングルール・IoA

オブジェクトではなく行為に着目した攻撃兆候の検出

■IoA(Indicators of Attack)とは？

犯罪者が攻撃準備の際に取りうる戦術、テクニック、行動に焦点を当てた

「攻撃の痕跡(IoA:Indicators of Attack)」による高度な標的型攻撃対策ソリューション

IoAは展開されたテクニックを追跡するものであり、使用されているツールがどんなものであるかは問わない

->マルウェアの動作と判断することが難しい正規ツールを用いた攻撃への対応が可能

■脅威ハンティングルールとは？

SOCエキスパートによって作成された脅威を検出するためのルール

ルールはカスペルスキーの脅威インテリジェンスとMITRE ATT&CKを基に作成

2,000以上のルールが設定されており、ルールは脅威インテリジェンスサービスの情報を基に定期的に更新



IoAとIoCの違い

マルウェアの動作と判断することが出来ない正規ツールを用いた攻撃への対応が可能

IoA : 攻撃の戦術、テクニック、行動に焦点を当てた「攻撃の指標」

IoC : 侵害の痕跡

IoC

IoA

IoC

ボリュームシャドウコピーを
削除するコマンド



ボリュームシャドウコピーを
削除する悪性プログラム



ファイル名、ハッシュ値などを用いて検出

ボリューム
シャドウコピーが
削除される行為



削除の
イベントログ



イベントログを
削除するコマンド

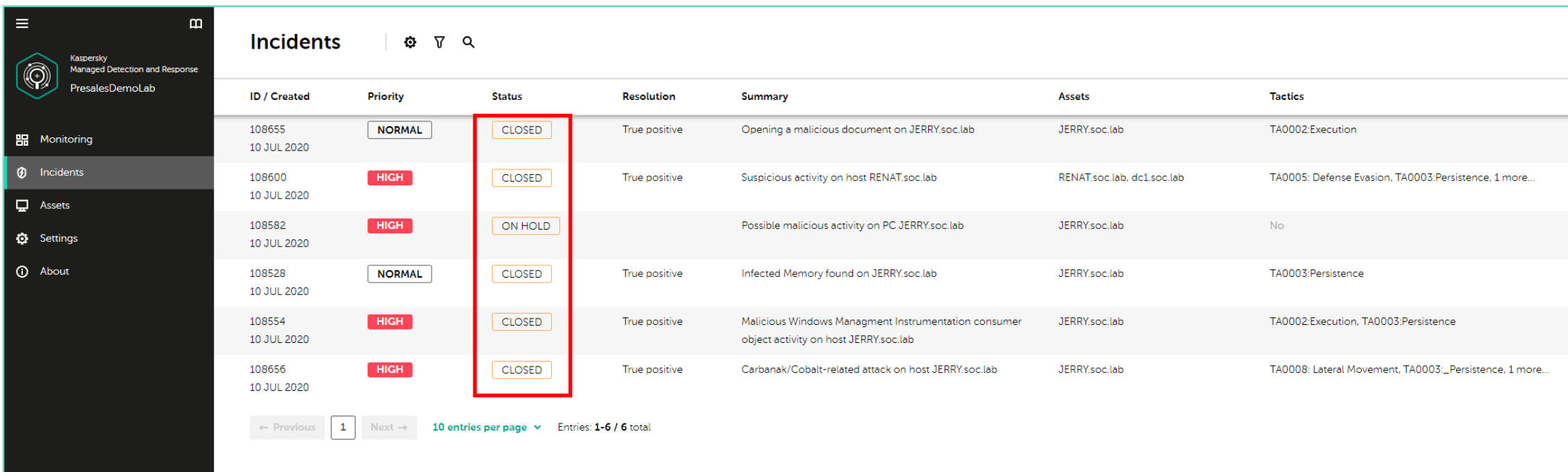


イベントログを
削除する悪性プログラム

ファイル名、ハッシュ値などを用いて検出

インシデント対応(レスポンス)

- ・インシデント発見時、インシデント詳細および推奨の対応策とレスポンスを通知



ID / Created	Priority	Status	Resolution	Summary	Assets	Tactics
108655 10 JUL 2020	NORMAL	CLOSED	True positive	Opening a malicious document on JERRY.soc.lab	JERRY.soc.lab	TA0002:Execution
108600 10 JUL 2020	HIGH	CLOSED	True positive	Suspicious activity on host RENAT.soc.lab	RENAT.soc.lab, dc1.soc.lab	TA0005: Defense Evasion, TA0003:Persistence, 1 more...
108582 10 JUL 2020	HIGH	ON HOLD		Possible malicious activity on PC JERRY.soc.lab	JERRY.soc.lab	No
108528 10 JUL 2020	NORMAL	CLOSED	True positive	Infected Memory found on JERRY.soc.lab	JERRY.soc.lab	TA0003:Persistence
108554 10 JUL 2020	HIGH	CLOSED	True positive	Malicious Windows Managment Instrumentation consumer object activity on host JERRY.soc.lab	JERRY.soc.lab	TA0002:Execution, TA0003:Persistence
108656 10 JUL 2020	HIGH	CLOSED	True positive	Carbanak/Cobalt-related attack on host JERRY.soc.lab	JERRY.soc.lab	TA0008: Lateral Movement, TA0003:_Persistence, 1 more...

インシデント詳細

Incident 861376

[← Previous](#) [Next >](#) [Receive a PDF summary by email](#)

Summary Responses (0) Communication (0) History (2)

Summary	Suspicious event logs cleaning on host webserv
Priority	HIGH
Status	ON HOLD
Status description	Recommendations: It is recommended to clarify the purpose and legitimacy of this activity.
Created	10/11/2023 21:11
Updated	10/16/2023 04:22
MITRE Tactics	TA0005: Defense Evasion
MITRE Techniques	T1070.001: Clear Windows Event Logs
Detection technology	KES

Summary: インシデントの概要・緊急度・ステータス・検知/更新日時
MITRE ATT&CK(戦術、手法)、検知技術など

Affected

Affected assets (1) Asset-based IOCs (2) Network-based IOCs (0)

Status	Asset name	Asset ID
🟢	WEBSRV	0xED590803CB8CE16932288C1C190A80B3

Affected: インシデントに関連する端末情報・IoC

Description

Additional telemetry analysis on the **webserv** host revealed the following activity:
A script was created on the host:

```
C:\Users\Administrator\AppData\Local\Temp\vmware-Administrator\VMwareDnD\76fd9c06\webserver\root\clear.ps1  
0xBA5CDEF939E4BED3F4C3AD2FDBCE5D80
```

This script was created by a chain of processes:

```
C:\Windows\explorer.exe  
->  
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr  
->  
C:\Users\Administrator\AppData\Local\Temp\vmware-Administrator\VMwareDnD\76fd9c06\webserver\root\clear.ps1
```

This activity was performed in the context of the user **WEBSRV\Administrator (SID: S-1-5-21-3443941371-2223888951-336872208-500)**.
Also, an activity was performed on the host to delete **Security** logs

```
wevtutil cl Security  
powershell clear-eventlog Security
```

Description: SOCのエキスパートの調査で分かったインシデント詳細

インシデント対応(レスポンス)

確認後、推奨されるレスポンスを承認することで対象の端末に対して自動で処理を実行

Incident 1034598 < Previous Next > [Receive a PDF summary by email](#)

Summary **Responses (2)** Communication (0) History (4)

	Status	Asset ID	Type	Details	Comment	Update time
<input checked="" type="checkbox"/>	NEW	0xf0a5703791ccb b04f0e2be50b30 d8b09	Get file	Infected file path: C:\temp\svchost.exe Maximum file size: 10 GB		08/15/2024 19:27
<input type="checkbox"/>	NEW	0xf0a5703791ccb b04f0e2be50b30 d8b09	Delete registry key	Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\System Value: C:\temp\svchost.exe		08/15/2024 19:28

Selected: 1

Accept
Reject

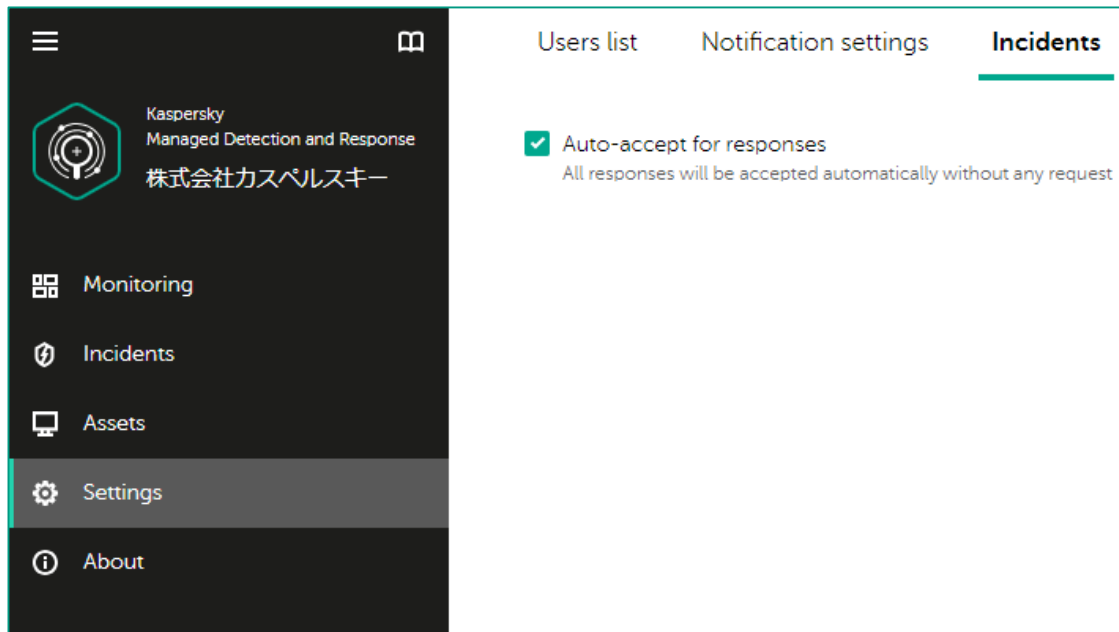
選択したレスポンスに対する許可・拒否を選択（複数選択可）

- Accept: 推奨されたレスポンスを実行
- Reject: レスポンスの実行を拒否

インシデント対応(レスポンス)

・「自動承認」機能をオンにした場合

SOCエキスパートから推奨されたアクションがお客様の承認無しで自動実行
->セキュリティ担当者の業務時間外に発生したインシデントにも対応可能



<SOCエキスパート実行レスポンス機能>

- ・ホストのネットワーク分離
- ・ネットワーク分離解除
- ・ファイル隔離
- ・ファイル隔離解除
- ・レジストリキーの削除
- ・対象ファイル取得
- ・メモリーダンプ
- ・プロセスの終了 (※)
- ・スクリプトの実行 (※)



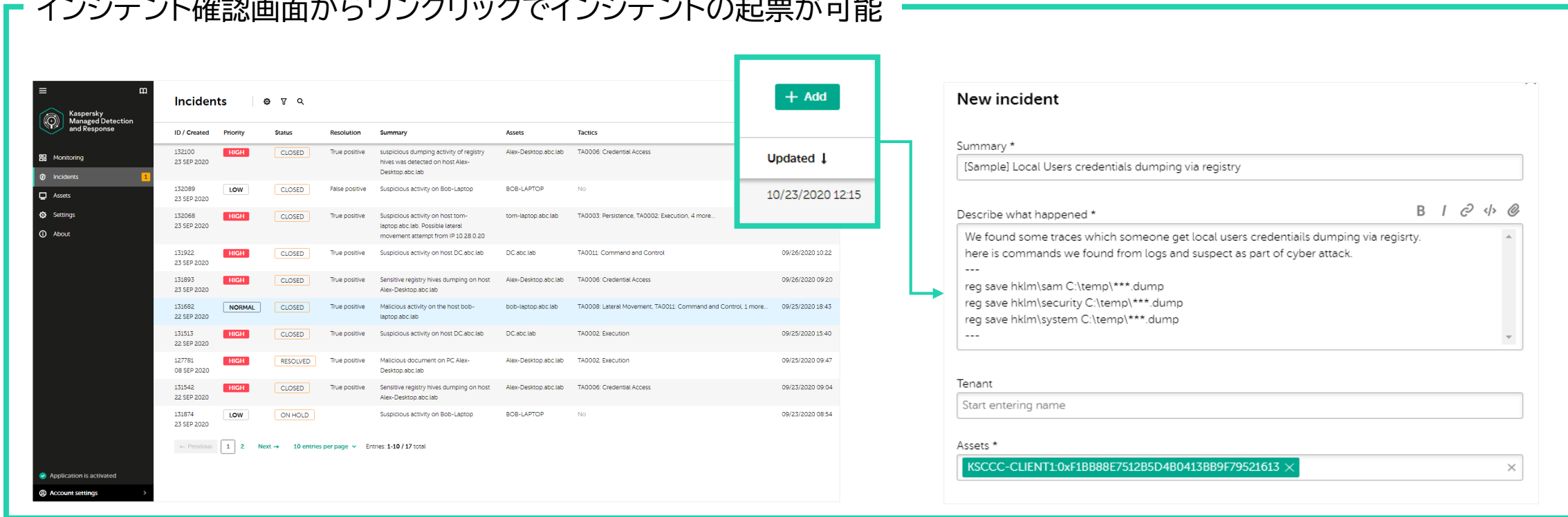
※Kaspersky Endpoint Security for Windowsのみ

脅威ハンティング・マニュアルでのインシデント生成

手動でインシデントを作成し、SOCエキスパートへ詳細の調査を依頼

- ・MDRによってインシデントが自動作成されなかったイベントを新しいインシデントとして手動で追加可能
- ・SOCエキスパートは追加されたインシデントを分析(収集したテレメトリから関連するアクションを調査など)、再評価

インシデント確認画面からワンクリックでインシデントの起票が可能



ID / Created	Priority	Status	Resolution	Summary	Assets	Tactics
132100 23 SEP 2020	HIGH	CLOSED	True positive	suspicious dumping activity of registry hives was detected on host Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0006: Credential Access
132089 23 SEP 2020	LOW	CLOSED	False positive	Suspicious activity on Bob-Laptop	BOB-LAPTOP	No
132068 23 SEP 2020	HIGH	CLOSED	True positive	Suspicious activity on host tom-laptop.abc.lab. Possible lateral movement attempt from IP 10.28.0.20	tom-laptop.abc.lab	TA0003: Persistence, TA0002: Execution, 4 more...
131922 23 SEP 2020	HIGH	CLOSED	True positive	Suspicious activity on host DC.abc.lab	DC.abc.lab	TA0011: Command and Control
131893 23 SEP 2020	HIGH	CLOSED	True positive	Sensitive registry hives dumping on host Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0006: Credential Access
131682 22 SEP 2020	NORMAL	CLOSED	True positive	Malicious activity on the host bob-laptop.abc.lab	bob-laptop.abc.lab	TA0008: Lateral Movement, TA0011: Command and Control, 1 more...
131513 22 SEP 2020	HIGH	CLOSED	True positive	Suspicious activity on host DC.abc.lab	DC.abc.lab	TA0002: Execution
127781 08 SEP 2020	HIGH	RESOLVED	True positive	Malicious document on PC Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0002: Execution
131542 22 SEP 2020	HIGH	CLOSED	True positive	Sensitive registry hives dumping on host Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0006: Credential Access
131874 23 SEP 2020	LOW	ON HOLD		Suspicious activity on Bob-Laptop	BOB-LAPTOP	No

New incident

Summary *

[Sample] Local Users credentials dumping via registry

Describe what happened *

We found some traces which someone get local users credentials dumping via registry. here is commands we found from logs and suspect as part of cyber attack.

```
reg save hklm\sam C:\temp\***.dump
reg save hklm\security C:\temp\***.dump
reg save hklm\system C:\temp\***.dump
```

Tenant

Start entering name

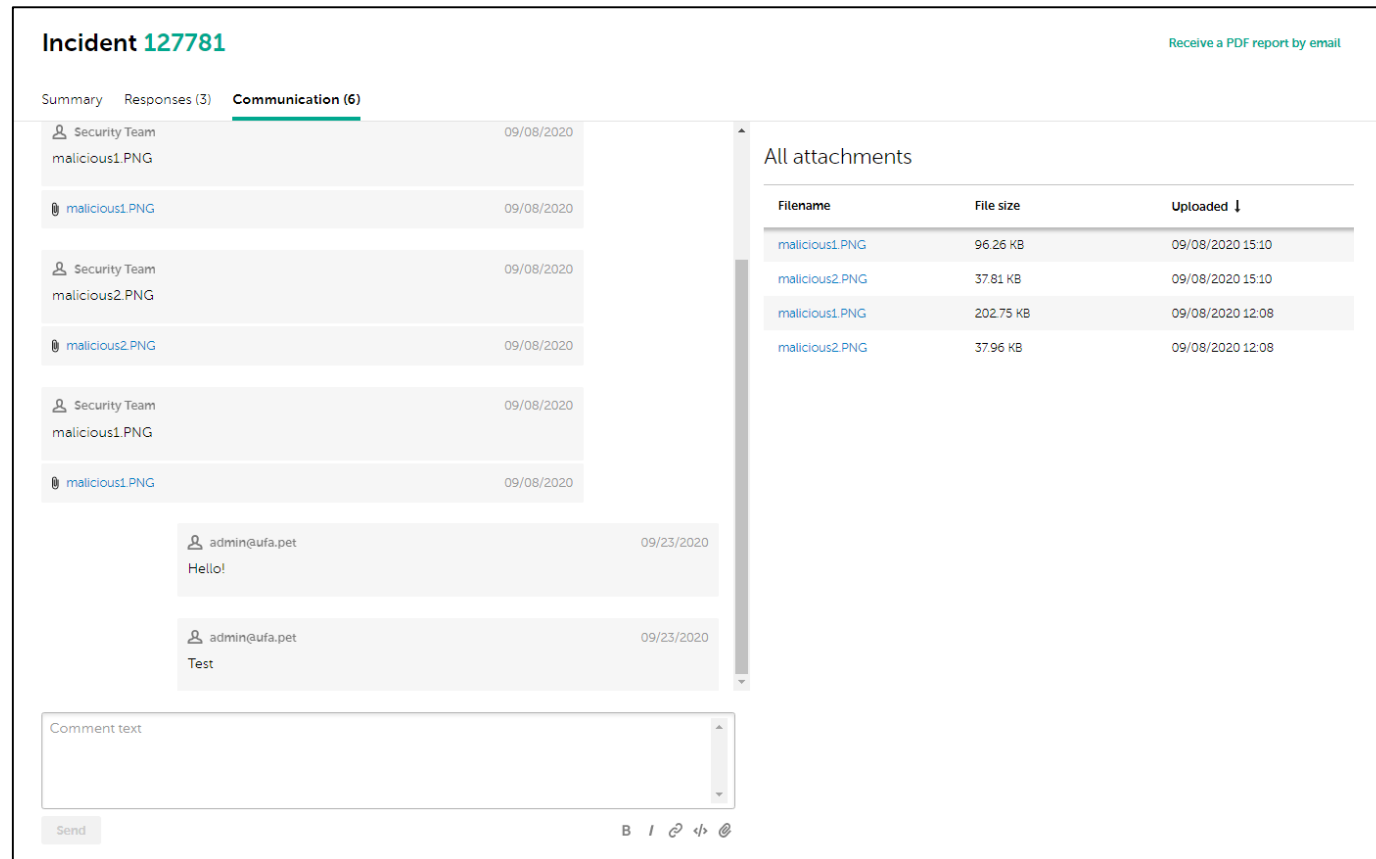
Assets *

KSCCCC-CLIENT1:0xF1BB88E7512B5D4B0413BB9F79521613

SOCエキスパートへのダイレクトアクセス

「今」起こっているインシデントを理解し、次のアクションへ繋げる

- ・レポートされたインシデントに関する質問をポータル上のチャットでSOCエキスパートに「直接」問い合わせ可能
- ・チャットではコメント以外にも画像やログファイルなどのファイル添付が可能（ファイルサイズ:10MBまで）



Incident 127781 Receive a PDF report by email

Summary Responses (3) **Communication (6)**

Security Team 09/08/2020
malicious1.PNG

malicious1.PNG 09/08/2020

Security Team 09/08/2020
malicious2.PNG

malicious2.PNG 09/08/2020

Security Team 09/08/2020
malicious1.PNG

malicious1.PNG 09/08/2020

admin@ufa.pet 09/23/2020
Hello!

admin@ufa.pet 09/23/2020
Test

Comment text

Send B I ↻ ↶ @

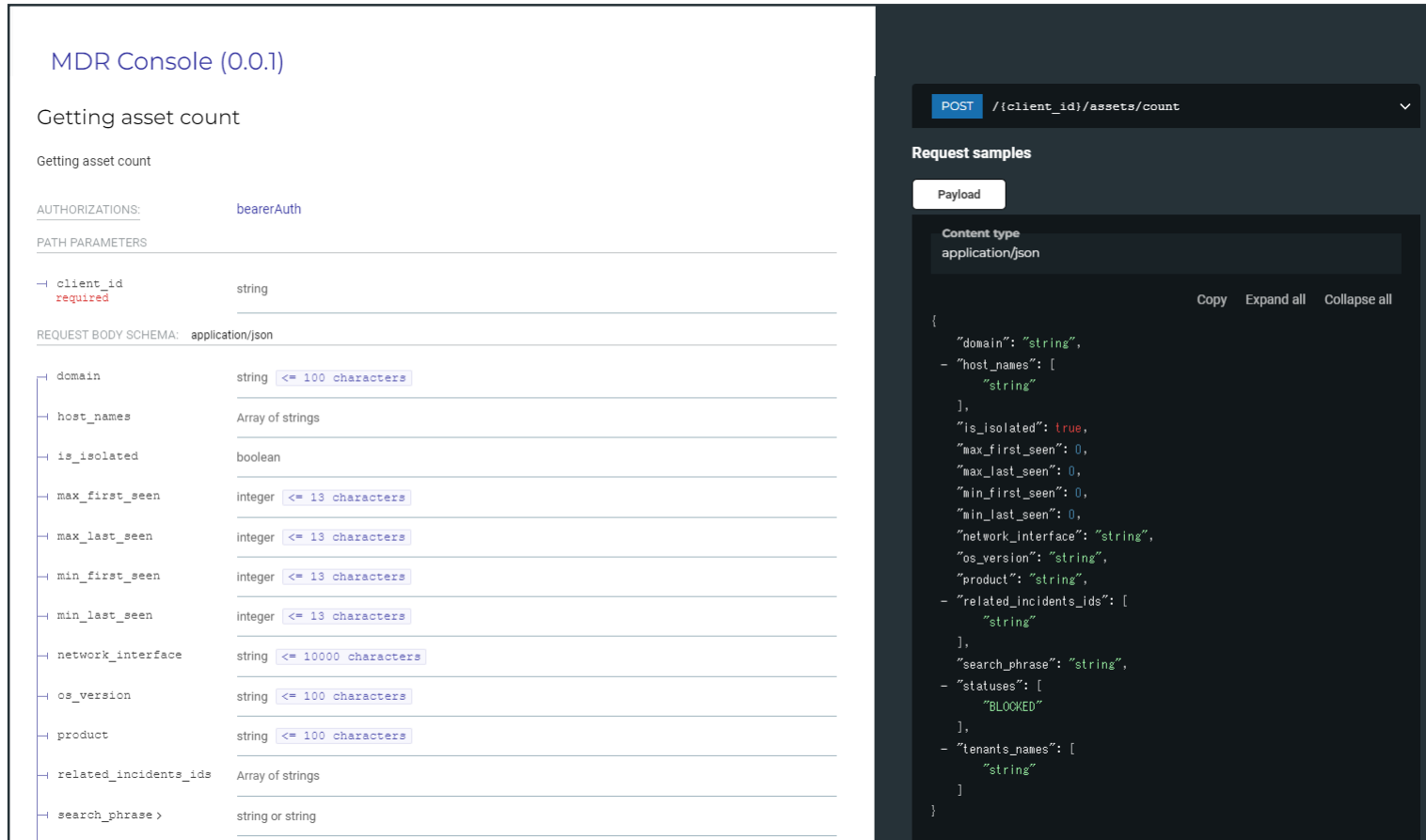
All attachments

Filename	File size	Uploaded ↓
malicious1.PNG	96.26 KB	09/08/2020 15:10
malicious2.PNG	37.81 KB	09/08/2020 15:10
malicious1.PNG	202.75 KB	09/08/2020 12:08
malicious2.PNG	37.96 KB	09/08/2020 12:08

APIでのデータダウンロード

REST API利用による運用効率化

- ・インシデントの詳細情報の取得やコメントの追加、インシデント対応状況の取得をREST APIで実行可能
- ・使用可能なパスパラメータおよびサンプルはすべてオンラインヘルプで提供



MDR Console (0.0.1)

Getting asset count

Getting asset count

AUTHORIZATIONS: [bearerAuth](#)

PATH PARAMETERS

client_id	string
required	

REQUEST BODY SCHEMA: [application/json](#)

domain	string	<= 100 characters
host_names	Array of strings	
is_isolated	boolean	
max_first_seen	integer	<= 13 characters
max_last_seen	integer	<= 13 characters
min_first_seen	integer	<= 13 characters
min_last_seen	integer	<= 13 characters
network_interface	string	<= 10000 characters
os_version	string	<= 100 characters
product	string	<= 100 characters
related_incidents_ids	Array of strings	
search_phrase	string or string	

Request samples

Payload

Content type
application/json

Copy Expand all Collapse all

```
{
  "domain": "string",
  "host_names": [
    "string"
  ],
  "is_isolated": true,
  "max_first_seen": 0,
  "max_last_seen": 0,
  "min_first_seen": 0,
  "min_last_seen": 0,
  "network_interface": "string",
  "os_version": "string",
  "product": "string",
  "related_incidents_ids": [
    "string"
  ],
  "search_phrase": "string",
  "statuses": [
    "BLOCKED"
  ],
  "tenants_names": [
    "string"
  ]
}
```

対象OS/管理サーバー・アプリケーション

OS・管理サーバー	アプリケーション	MDRサポート
 Windows	Kaspersky Security for Windows	Ver12.0以降
 MacOS	Kaspersky Security for Mac	Ver11.3以降
 Linux	Kaspersky Security for Linux	Ver11.4以降
 仮想マシン  (Windows、Linux)	Kaspersky Security for Virtualization Light Agent	Ver5.2以降
 管理サーバー オンプレミス	Kaspersky Security Center (Windows / Linux)	Windows:Ver14.2 Linux:Ver15.1
 管理サーバー クラウド	Kaspersky Security Center Expert View	N/A (クラウドでは常に最新版を提供)

緊急度	応答時間	目標値
High (例: 標的型攻撃・APT)	1時間以内	90%
Medium (例: 一般的なマルウェア)	4時間以内	90%
Low (例: アドウェア、リスクウェアなど)	24時間以内	90%

応答時間:

インシデントの検出からMDRポータル上でのアラート通知までの時間

目標値:

応答時間内にアラート通知が完了したインシデントの割合

kaspersky