



Microsoft Sentinel Incident experience

Public Preview

Microsoft Corporation



新しい「インシデント調査」ビューについて

- 2023/1/18よりPublic Preview
- SOCアナリストがインシデントに対しより効果的に対処するための新たなインシデント調査ビューを提供
- 新しいデザインを提供することの背景
 - アナリストは、セキュリティ インシデントのトリアージ、調査、対応を行う際に、多くの情報、アクション、ツールに迅速かつシームレスにアクセスする必要がある
 - 新しい調査ページでは、一つのビューでインシデントと侵害の範囲を把握するために必要な情報とツールをアナリストに提供
 - 多くのお客様/パートナー様、およびMS内SOCメンバーからのフィードバックを受けてデザインに反映し、Public Previewとして提供

• リソース

[【Microsoft Learn】 Navigate and investigate incidents in Microsoft Sentinel | Microsoft Learn](#)

[【ブログ】 The new incident experience is here! - Microsoft Community Hub](#)

[【デモ】 Announcing the New Microsoft Sentinel Incident Investigation Experience! - YouTube](#)

[概要] タブ

ホーム > Microsoft Sentinel > Microsoft Sentinel | インシデント >

Multi-stage incident involving Defense evasion & Discovery on one endpoint

インシデント ID 1283

最新の情報に更新 ログ タスク (プレビュー) アクティビティ ログ

This is the new, improved incident page (currently in preview). You can use the toggle to switch back.

中 重 大 度 新規 状態 未割り当て 所有者

Microsoft 365 Defender での調査

ワークスペース名

説明

製品名のアラート

- Microsoft Defender for Endpoint

証拠

該当なし 6 アラート 0 ブックマーク イベント

最終更新時間 12/15/2022, 11:07:49 AM 作成時刻 12/15/2022, 10:32:50 AM

エンティティ (23 個)

- powershell.exe
- explorer.exe
- notepad.exe
- win2019-asp2-3

すべて表示 >

戦術と手法

- Defense Evasion (3)
- Discovery (7)

インシデントブック

インシデントの概要

分析ルール

インシデントチーム

調査

インシデントのタイムライン

12月15日 10:41:12 中 A process was injected with potential...

12月15日 10:30:45 中 Unexpected behavior observed by a p...

12月15日 10:30:45 中 Suspicious process injection observed

12月15日 10:30:45 中 Suspicious process injection observed

12月15日 10:30:15 低 Suspicious Application Window Disco...

12月15日 10:30:15 低 Suspicious sequence of exploration ac...

エンティティ

powershell.exe

explorer.exe

notepad.exe

win2019-asp2-3

localadmin

5be67dad56e33cc

5394096a1cebfb81

a28438a1388f772

インシデントアクション

- プレイブックの実行
- オートメーション ルールの作成
- Team の作成 (プレビュー)

上位の分析情報

① 最初のアラートの前の過去 24 時間 ②

IP address remote connections

12/14/2022, 10:32:49 AM - 12/15/2022, 10:52:08 AM

204.79.197.203

Direction	IPAddress	Remote IP	Total
All	204.79.197.20	2 IPs	0

See All connections >

類似インシデント (プレビュー) ①

重大度	インシデント ID	タイトル	最終更新時間	状態	類似性の理由	最後の所有者
中	1286	A process was injected with potentially mal...	2022/12/15 10:52	新規	類似のエンティティ...	未割り当て
中	1282	Suspicious process injection observed	2022/12/15 10:34	新規	類似のエンティティ...	未割り当て
中	1275	Unexpected behavior observed by a proce...	2022/12/15 10:33	新規	類似のエンティティ...	未割り当て
中	1273	Suspicious process injection observed	2022/12/15 10:33	新規	類似のエンティティ...	未割り当て

【ご参考】旧画面

タイムライン、類似インシデント、アラート内容などタブを切り替える必要あり

ホーム > インシデント ...
インシデント ID 1283
最新の情報に更新 タスク (プレビュー)

Switch to the new, improved incident page (currently in preview).

Multi-stage incident involving Defense evasion & Dis...
インシデント ID: 1283
Microsoft 365 Defender での調査

未割り当て 新規 中
所有者 状態 重大度

製品名のアラート
Microsoft Defender for Endpoint

証拠
該当なし 6 アラート 0 ブックマーク
イベント

最終更新時間 作成時刻
22/12/15 11:07 22/12/15 10:32

エンティティ (23 個) (プレビュー)
localadmin win2019-asp2-3 204.79.197.203 powershell.exe
すべて表示 >

戦術と手法
Defense Evasion (3)
Discovery (7)

インシデント フック
インシデントの概要

タグ
+

インシデント リンク
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insig...

最後のコメント (合計: 0)

タイムライン 類似インシデント (プレビュー) 警告 ブックマーク エンティティ (プレビュー) コメント

検索 タイムライン コンテンツ: すべて 重大度: すべて 方針: すべて

Dec 15 10:41 AM A process was injected with potentially malicious code
中 | Microsoft Defender for Endpoint による検出 | 方針: Defense Evasion プレイバックの表示

Dec 15 10:30 AM Unexpected behavior observed by a process ran with no command line arguments
中 | Microsoft Defender for Endpoint による検出 | 方針: Defense Evasion プレイバックの表示

Dec 15 10:30 AM Suspicious process injection observed
中 | Microsoft Defender for Endpoint による検出 | 方針: Defense Evasion プレイバックの表示

Dec 15 10:30 AM Suspicious process injection observed
中 | Microsoft Defender for Endpoint による検出 | 方針: Defense Evasion プレイバックの表示

Dec 15 10:30 AM Suspicious Application Window Discovery
低 | Microsoft Defender for Endpoint による検出 | 方針: Discovery プレイバックの表示

Dec 15 10:30 AM Suspicious sequence of exploration activities
低 | Microsoft Defender for Endpoint による検出 | 方針: Discovery プレイバックの表示

Try the new experience

トグルで旧画面に切り替え

選択された項目なし
タイムラインから項目を選択して、詳細を表示してください

Investigate incidents with Microsoft Sentinel | Microsoft Learn

ログ分析クエリウインドウ

インシデント調査画面から直接クエリー実行結果を確認可能

「ログ」ボタンあるいは「アラート」からログクエリービューを確認

ホーム > Multi-stage incident involving Defense evasion & Discovery on one endpoint ...
インシデント ID 1283

最新の情報に更新 ログ タスク (プレビュー) アクティビティ ログ

This is the new, improved incident page (currently in preview). You can use the toggle to switch back.

中 重大度 新規 状態 未割り当て 所有者

Microsoft 365 Defender での調査

ワークスペース名

説明

製品名のアラート

- Microsoft Defender for Endpoint

証拠

該当なし 6 アラート 1 ブックマーク

最終更新時間 1/19/2023, 10:24:06 AM 作成時刻 12/15/2022, 10:32:50 AM

エンティティ (23 個)

- explorer.exe
- powershell.exe
- notepad.exe
- 6bcbce4a295c163791b60...

すべて表示 >

戦術と手法

- Defense Evasion (3)
- Discovery (7)

インシデントブック
インシデントの概要

分析ルール

インシデントチーム

調査

ログ
Sentinel-rkan2-azure-m365

実行 時間の範囲: カスタム

```
1 SecurityAlert
2 summarize arg_max(TimeGenerated, *) by SystemAlertId
3 where SystemAlertId in("51b67627-627c-2e2c-4c95-889d1c4ad512", "72094193-c5d4-1654-0b62-5799c31223cc",
"070977ed-8a0f-8777-230c-c186948c1afb", "c8f86a7c-ead6-5a6e-48d1-d67a2caf4509", "b3f469d5-1e96-a931-77ba-ab615944b153",
"a3d56f77-aa9d-bef5-f90d-4fef5da39d83")
```

結果 グラフ ブックマークの追加

SystemAlertId	TimeGenerated [UTC]	DisplayName	AlertName
<input checked="" type="checkbox"/> a3d56f77-aa9d-bef5-f90d-4fef5da39d83	2022/12/15 1:58:57.670	A process was injected with potentially malicious code	A process was injected with potentially m...
<input type="checkbox"/> b3f469d5-1e96-a931-77ba-ab615944b153	2022/12/15 2:08:29.190	Suspicious process injection observed	Suspicious process injection observed
<input type="checkbox"/> 51b67627-627c-2e2c-4c95-889d1c4ad512	2022/12/15 2:08:29.190	Suspicious process injection observed	Suspicious process injection observed
<input type="checkbox"/> 72094193-c5d4-1654-0b62-5799c31223cc	2022/12/15 2:08:29.190	Suspicious process injection observed	Suspicious process injection observed
<input type="checkbox"/> 070977ed-8a0f-8777-230c-c186948c1afb	2022/12/15 1:38:57.670	Suspicious process injection observed	Suspicious process injection observed
<input type="checkbox"/> c8f86a7c-ead6-5a6e-48d1-d67a2caf4509	2022/12/15 1:38:57.670	Suspicious process injection observed	Suspicious process injection observed

0s 870ms | 時刻の表示 (UTC+00:00) | 1 - 6 行目 (全 6 行)

完了

気になるクエリーはブックマーク追加、インシデントとの紐づけやエンティティとの紐づけ、Mitre戦術フェーズとの紐づけなど可能

ブックマーク紐づけ

The screenshot displays the Microsoft Sentinel 'Incident' page for an incident titled 'Multi-stage incident involving Defense evasion & Dis'. The interface includes a left sidebar with navigation options like 'Home', 'Incident ID 1283', and 'Latest information'. The main area shows the incident timeline with several alerts. A green box highlights a bookmark icon (a blue square with a white 'B') next to the first alert, 'SecurityAlert - Windows alert'. Another green box highlights the '1 Bookmark' button in the left sidebar. A third green box highlights the 'SecurityAlert - Windows alert' details pane, which shows the alert's raw result. A fourth green box highlights the 'Bookmark' button in the details pane. A fifth green box highlights the 'Bookmark' button in the 'Incident' table at the bottom. A sixth green box highlights the 'Bookmark' button in the 'Incident' table at the bottom. A seventh green box highlights the 'Bookmark' button in the 'Incident' table at the bottom. A eighth green box highlights the 'Bookmark' button in the 'Incident' table at the bottom. A ninth green box highlights the 'Bookmark' button in the 'Incident' table at the bottom. A tenth green box highlights the 'Bookmark' button in the 'Incident' table at the bottom.

インシデントに紐づけたブックマークはインシデントタイムラインに追加

紐づけられたブックマーク数

ブックマーク出力結果の全体を表示

タスク

タスクを使用してインシデントワークフローを表示。

定常的なタスクはオートメーションルールを使って自動的に割り当て可能

ホーム > Microsoft Sentinel > Microsoft Sentinel | インシデント >

[SAMPLE ALERT] Access from a suspicious IP to a storage blob container ...
インシデント ID 1357

最新の情報に更新 | インシデントの削除 | ログ | **タスク (プレビュー)** | アクティビティ ログ

This is the new, improved incident page (currently in preview). You can use the toggle to switch back.

情報提供 重大度 | 終了 状態 | 未割り当て 所有者

Microsoft Defender for Cloud での調査

ワークスペース名

説明
THIS IS A SAMPLE ALERT: Someone has accessed your Azure storage account 'Sample-Storage' from a suspicious IP address.

製品名のアラート
• Microsoft Defender for Cloud

Tasks (プレビュー)
1/3 completed. View full details

終了する理由
Undetermined
サンプルアラートのため、自動クローズ

証拠
該当なし 0 | 1 アラート | 0 ブックマーク

最終更新時間
1/19/2023, 10:23:58 AM

作成時刻
1/19/2023, 10:23:36 AM

エンティティ (2 個)
00.00.00.00
Sample-Storage

戦術と手法
Reconnaissance (0)

インシデントブック
インシデントの概要

調査

インシデントのタイムライン

エンティティ

類似インシデント (プレビュー)

重大度	インシデント ID	タイトル	最終更新時間	状態	類似性の理由
情報提供	1344	[SAMPLE ALERT] PREVIEW - Access from a ...	2023/1/19 10:22	終了 - 不明	類似のエンティティ...
情報提供	1354	[SAMPLE ALERT] Unusual upload of .cs pkg ...	2023/1/19 10:22	終了 - 不明	類似のエンティティ...
情報提供	1356	[SAMPLE ALERT] Unusual application acces...	2023/1/19 10:22	終了 - 不明	類似のエンティティ...

タスクの進行状況

インシデント タスク (プレビュー)

最新の情報に更新 + タスクの追加

3 件中 1 件完了

Search Status: All

1. インシデント管理部門に連絡する
作成元: Automation rule - インシデントへのタスク追加
2. ブラックリスト管理DBへの登録
作成元: Automation rule - インシデントへのタスク追加
3. 疑陽性、過検知の場合は、記録を残してください
作成元: Automation rule - インシデントへのタスク追加

割り当てられたインシデントタスクの詳細。
共通して実施が必要なタスクは
オートメーションルール化することで
実施漏れを防ぐ

(重大度や状態の変更、プレイブックのトリガー、追加されたアラートなど、手動または自動のインシデントのコメント追加など)
他のアナリストの活動状況確認によりコラボレーション、監査の目的で利用可能

インシデント アクティビティ ログ

×

Activity logs content : All

	OnMicrosoft.com	01/19/23, 11:34 AM		
	複数のデバイスにおける段階的な攻撃が確認されました。1時間後にチェックポイントを設けます。			
	Bookmark was changed	01/19/23, 10:24 AM		
	Bookmark e0e56684-5518-4a2e-980d-95fdafb65183 was added to the incident by MOD Administrator			
	Alert was changed	12/15/22, 10:57 AM		
	Alert a3d56f77-aa9d-bef5-f90d-4fef5da39d83 was added to the incident by Microsoft 365 Defender Alerts Logs			
	Incident was created	12/15/22, 10:32 AM		
	Incident was created			

↓

インシ
履歴、
(コメ
可能)

AM Normal ⚙ B I U S ☞ ≡ ≡ ≡ ↗ ↘

コメントを入力する...

閉じる コメント

インシデントに対するアクティビティの履歴、アナリスト間のコメントを確認
(コメントはリンクや画像を貼ることも可能)

エンティティ情報 (1/3)

インシデントで識別されたエンティティ情報を表示

ホーム > Multi-stage incident involving Defense evasion & Discovery on one endpoint ...

インシデント ID 1283

最新の情報に更新 | ログ | タスク (プレビュー) | アクティビティ ログ

This is the new, improved incident page (currently in preview). You can use the toggle to switch back. New experience

中 重 新 未 未
大 規 割 割
度 状 り 当
度 態 当 有
者 者 者

Microsoft 365 Defender での調査

ワークスペース名

説明

製品名のアラート

- Microsoft Defender for Endpoint

証拠

該当なし 6 ブックマーク
イベント アラート

最終更新時間 作成時刻
1/19/2023, 10:24:06 AM 12/15/2022, 10:32:50 AM

エンティティ (23 個)

- explorer.exe
- powershell.exe
- notepad.exe
- 6cbce4a295c163791b60...

すべて表示 >

戦術と手法

- Defense Evasion (3)
- Discovery (7)

インシデント ブック
インシデントの概要

分析ルール

インシデント チーム

調査

概要 エンティティ

インシデントのタイムライン

Search

フィルターの追加

- 12月15日 10:58:57 SecurityAlert - Windows alert MOD Administrator による作成
- 12月15日 10:41:12 A process was injected with potential... Microsoft Defender for Endp... 万...
- 12月15日 10:30:45 Unexpected behavior observed by a p... Microsoft Defender for Endp... 万...
- 12月15日 10:30:45 Suspicious process injection observed Microsoft Defender for Endp... 万...
- 12月15日 10:30:45 Suspicious process injection observed Microsoft Defender for Endp... 万...
- 12月15日 10:30:15 Suspicious Application Window Disco... Microsoft Defender for Endp... 万...

エンティティ

Search Type: All

- powershell.exe
- notepad.exe
- 6cbce4a295c163791b60...
- 7353f60b173907...
- de96a6e699443...
- 7a59c99173eb57...
- bbe3017916bf2d...
- 9e3bd0da2531cc...

上位の分析情報

① 最初のアラートの前の過去 24 時間 ①

IP address remote connections

12/14/2022, 10:32:49 AM - 12/15/2022, 10:52:08 AM

204.79.197.203

Direction	IP Address	Remote IP	Total
All	204.79.197.20	2 IPs	0

See All connections >

TI に追加 (プレビュー)

プレイブックの実行 (プレビュー)

類似インシデント (プレビュー) ①

重大度	インシデント ID	タイトル	最終更新時間	状態	類似性の理由	最後の所有者
中	1286	A process was injected with potentially mal...	2022/12/15 10:52	新規	類似のエンティティ...	未割り当て
中	1282	Suspicious process injection observed	2022/12/15 10:34	新規	類似のエンティティ...	未割り当て
中	1275	Unexpected behavior observed by a proce...	2022/12/15 10:33	新規	類似のエンティティ...	未割り当て

各エンティティについてTIに追加したり、プレイブックを実行することで追加のアクションを実行

エンティティ情報 (2/3)

エンティティタブからエンティティの一覧確認、エンティティに関する情報、分析を確認

The screenshot displays the Microsoft Defender portal interface. The main section is the 'Entity' tab, which lists various entities. A green box highlights the 'Entity tab' label. Another green box highlights the 'Details' view for a specific entity, showing location information, log activity, and data sources. A third green box highlights the 'Analysis' view, showing IP address remote connections and watchlist insights. A fourth green box highlights the 'MS analysis or insights from previous activities' section.

Entity tab

Entity details view

Entity analysis view

MS analysis or insights from previous activities

名前	種類
explorer.exe	ファイル
powershell.exe	ファイル
notepad.exe	ファイル
6cbce4a295c163791b60fc23d285e6d84f28ee4c(SHA1)	FileHash
7353f60b1739074eb17c5f4dddefe239(MD5)	FileHash
de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c(SHA256)	FileHash
7a59c99173eb57f9bb17a1ae27f628040b01af53(SHA1)	FileHash
bbe3017916bf2db64b5e6b251468082e(MD5)	FileHash
9e3bd0da2531cdfc3499c82c729b74fa9e49ab2397ca37fcd3d93d650c812ddd(SHA256)	FileHash
5be67dad56e33cddb1c327948ee70d43e69ed106(SHA1)	FileHash
5394096a1ceb8f1af24e993777caabf4(MD5)	FileHash
a28438e1388f272a52559536d99d65ba15b1a8288be1200e249851fd7ee6c7e(SHA256)	FileHash
localadmin	アカウント
win2019-asp2-3	ホスト
"powershell.exe"	プロセス
Explorer.EXE	プロセス
"notepad.exe"	プロセス
204.79.197.203	IP
userinit.exe	ファイル
f1874e3af4f277fd7fb75038ec4d702cf43e4650c(SHA1)	FileHash
dff836e6145c8cca28ddfc8f6ccbe78c9(MD5)	FileHash
d3f1cec588c2e0fd3cbd913b0af988a6e4ec2d700a52f3a3112d72506b75c7e2(SHA256)	FileHash
userinit.exe	プロセス

Entity details view (204.79.197.203 IP)

Location information

Organization: microsoft corporation

City: redmond

State: washington

Country: united states

Continent: north america

Log activity

Data sources

Log to recorded hosts

Entity actions

Entity analysis view (204.79.197.203 IP)

Initial alert history

IP address remote connections with T1 match

IP address remote connections

Watchlist insights (Preview)

Entity actions

エンティティ情報 (3/3)

エンティティの詳細から直近7日間のアクティビティ、関連アラートを確認可能

エンティティタイムライン。
同一エンティティのアクティビティや類似インシデント内のアラート発生タイミングを確認可能

ホーム > Microsoft Sentinel > Microsoft Sentinel | インシデント >
Rare subscription-level operations in Azure ...
インシデント ID 1358

最新の情報に更新 | インシデントの削除 | ログ | タスク (プレビュー) | アクティビティ ログ

This is the new, improved incident page (currently in preview). You can use the toggle to switch back. New experience

概要 エンティティ

ワークスペース名

説明
This query looks for a few sensitive subscription-level events based on Azure Activity Logs. Test
For example this monitors for the operation name 'Create or Update Snapshot' which is used for creating backups but could be misused by attackers to dump hashes or extract sensitive information from the disk.

製品名のアラート
• Microsoft Sentinel

Tasks (プレビュー)
0/3 completed. View full details

証拠
3 イベント 1 アラート 0 ブックマーク

最終更新時間 1/19/2023, 2:35:20 PM 作成時刻 1/19/2023, 2:35:20 PM

エンティティ (5 個)

戦術と手法
Credential Access (0)
Persistence (0)

調査

タイムライン

アカウント

過去 7 日間

- 1月19日 14:35:19 Rare subscription-level operations in Azure
低 Microsoft Sentinel による検出
- 1月18日 14:35:17 Rare subscription-level operations in A...
低 Microsoft Sentinel による検出
- 1月18日 13:16:14 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 203 time(s)
- 1月18日 10:27:59 SigninLogs - 0372b2efe75d
による作成
- 1月18日 10:24:08 SigninLogs - 5c39a0b56159
による作成
- 1月17日 14:35:16 Rare subscription-level operations in A...
低 Microsoft Sentinel による検出
- 1月17日 09:16:35 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 135 time(s)
- 1月16日 08:53:37 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 205 time(s)
- 1月13日 22:23:47 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 1 time(s)
- 1月12日 17:19:00 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 125 time(s)

すべての詳細を表示 | プレイブックの実行 (プレビュー)

過去のアラートを当該インシデント
に加えることができる

ホーム > Microsoft Sentinel > Microsoft Sentinel | インシデント >
Rare subscription-level operations in Azure ...
インシデント ID 1358

最新の情報に更新 | インシデントの削除 | ログ | タスク (プレビュー) | アクティビティ ログ

This is the new, improved incident page (currently in preview). You can use the toggle to switch back. New experience

概要 エンティティ

ワークスペース名

説明
This query looks for a few sensitive subscription-level events based on Azure Activity Logs. Test
For example this monitors for the operation name 'Create or Update Snapshot' which is used for creating backups but could be misused by attackers to dump hashes or extract sensitive information from the disk.

製品名のアラート
• Microsoft Sentinel

Tasks (プレビュー)
0/3 completed. View full details

証拠
3 イベント 1 アラート 0 ブックマーク

最終更新時間 1/19/2023, 2:35:20 PM 作成時刻 1/19/2023, 2:35:20 PM

エンティティ (5 個)

戦術と手法
Credential Access (0)
Persistence (0)

調査

Add alert to incident
The alert will become part of this incident.
OK キャンセル

過去 7 日間

- 1月19日 14:35:19 Rare subscription-level operations in Azure
低 Microsoft Sentinel による検出
- 1月18日 14:35:17 Rare subscription-level operations in A...
低 Microsoft Sentinel による検出
- 1月18日 13:16:14 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 203 time(s)
- 1月18日 10:27:59 SigninLogs - 0372b2efe75d
による作成
- 1月18日 10:24:08 SigninLogs - 5c39a0b56159
による作成
- 1月17日 14:35:16 Rare subscription-level operations in A...
低 Microsoft Sentinel による検出
- 1月17日 09:16:35 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 135 time(s)
- 1月16日 08:53:37 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 205 time(s)
- 1月13日 22:23:47 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 1 time(s)
- 1月12日 17:19:00 The user signed in to an Azure resource
The user signed in to Microsoft.aad1am 125 time(s)

すべての詳細を表示 | プレイブックの実行 (プレビュー)

類似インシデント

過去や現在に渡っての類似インシデント発生状況を確認。
大規模攻撃の一部である可能性の確認や類似インシデントでの過去の対応者から知見を得ることに活用。

Multi-stage incident involving Defense evasion & Discovery on one endpoint
インシデント ID 1283

最新の情報に更新 | ログ | タスク (プレビュー) | アクティビティ ログ

This is the new, improved incident page (currently in preview). You can use the toggle to switch back.

中
重大度

新規
状態

未割り当て
所有者

Microsoft 365 Defender での調査

ワークスペース名

説明

製品名のアラート

証拠

該当なし 6
イベント アラート ブックマーク

最終更新時間
1/19/2023, 11:34:54 AM

作成時刻
12/15/2022, 10:32:50 AM

エンティティ (23 個)

戦術と手法

インシデントブック

分析ルール

インシデント チーム

調査

概要 エンティティ

インシデントのタイムライン

エンティティ

類似インシデント (プレビュー)

- 類似インシデント（最大20件表示）
- 類似性の降順で並び替えられる
- 過去14日間のデータに基づいて計算