

Elements Security Center のセキュリティイベント

Elements ではサービス管理を行う Elements Security Center がご利用いただけます。「セキュリティイベント」ビューでは各サービスで確認された脅威情報が表示されます。これらの情報はセキュリティコンサルティングサービスや EDR によるさらなる脅威分析のソースとなります。このビューに表示される脅威情報は多岐にわたり、またセキュリティトレンドにより常に変化します。その為この情報を元に脅威状況を把握するには専門的な知識が必要となります。しかしながら脅威分析が可能なパートナーや専門家に心当たりがない場合、Withsecure ではそういったご要望にお応えする為、“緊急インシデント対応”(有償) / “WithSecure にエスカレーション”(有償) / “AI 分析”を提供させていただいております。状況に応じてご利用を検討ください。なお製品サポートでは脅威分析は提供させていただいておりませんのでご了承ください。

セキュリティイベントビュー

日時	深刻度	ソース	対象	詳細
50 minutes ago 2025/02/28, 11:57:16	① 情報	システムイベント	DESKTOP-A395F4C	An a
2 hours ago 2025/02/28, 10:57:11	② 情報	システムイベント	DESKTOP-A395F4C	An a
3 hours ago 2025/02/28, 9:57:07	③ 情報	システムイベント	DESKTOP-A395F4C	An a
3 hours ago 2025/02/28, 9:57:06	① 情報	システムイベント	DESKTOP-A395F4C	An a
4 hours ago 2025/02/28, 8:57:03	① 情報	システムイベント	DESKTOP-A395F4C	An a
4 hours ago 2025/02/28, 8:55:50	① 情報	システムイベント	DESKTOP-A395F4C	An a
5 hours ago 2025/02/28, 7:55:51	① 情報	システムイベント	DESKTOP-A395F4C	An a
6 hours ago 2025/02/28, 6:55:08	① 情報	システムイベント	DESKTOP-A395F4C	An a
7 hours ago 2025/02/28, 5:55:06	① 情報	システムイベント	DESKTOP-A395F4C	An a

- **緊急インシデント対応(有償)**

<https://www.withsecure.com/jp-ja/about-us/company-contacts/24-7-incident-hotline>

※ 英語対応のみとなります。

※セキュリティコンサルタントによるウイルス感染/サイバー攻撃の状況分析/アドバイス。

- **AI 分析(無償)**

分析対象企業を表示し下記ボタン押下で分析が動的生成されます。

セキュリティイベント + 概要の作成 ⋮ i

星印はLLMで生成されたコンテンツを表します

サンプル(直近7日間のみの分析となります)

セキュリティイベントの概要

この概要はAIが作成したものであり、慎重に扱う必要があることに注意してください。すべての脅威に完全に対処するためには、さらなる調査と専門家による相談が必要な場合があります。

以下は、2025年2月21日から2025年2月28日までの測定期間、1台のデバイスと6件のイベントで2025年2月28日に生成された会社「」のセキュリティイベントの概要です。

- 2025年2月25日、manualScanning エンジンが DESKTOP-6B8T8M7 デバイスで EICAR_Test_File の感染を2件検出しました。ソース: [1] eicar.com
推奨アクション: ファイルをより詳しく分析し、必要に応じてデバイスのプロファイルで除外設定を行うことを検討してください。
- 2025年2月26日、manualScanning エンジンが DESKTOP-6B8T8M7 デバイスで EICAR_Test_File の感染を1件検出しました。ソース: [1] eicar.com
推奨アクション: ファイルをより詳しく分析し、必要に応じてデバイスのプロファイルで除外設定を行うことを検討してください。
- 2025年2月27日、manualScanning エンジンが DESKTOP-6B8T8M7 デバイスで EICAR_Test_File の感染を3件検出しました。ソース: [1] eicar.com
推奨アクション: ファイルをより詳しく分析し、必要に応じてデバイスのプロファイルで除外設定を行うことを検討してください。

エグゼクティブサマリー: 2025年2月25日から27日にかけて、DESKTOP-6B8T8M7 デバイスでEICAR_Test_Fileの感染が合計6件検出されました。感染は同一のソース([1] eicar.com)から発生しており、manualScanning エンジンによって検出されています。同一デバイスで複数の感染が確認されたため、より詳細な分析と適切な対応が必要と考えられます。

● WithSecure にエスカレーション(EDR /有償)

Broad Context Detection

Broad Context Detection イベント検索

検出リストに戻る

Broad Context Detection 1 of 79

ID: 4304815-3943, カテゴリ: 異常なプロセス

デバイスモスキャン 概要 処理ツ

フォレンジックパッケージを収集する

タスクを列挙する

プロセスを列挙する

詳細 応答アクション 詳細 プロセスの詳細から入手できます。

WithSecureにエスカレーション

エスカレーション

会社名

テスト株式会社

※弊社日本営業所よりトークンを購入いただきます。

● BCD イベントに対する AI 分析(EDR/無償)

ステータス ⓘ

新規

クイックアクション

Luminenで分析する

影響されているデバイスを隔離

BCD 10363624-1055 概要

この概要はAIが作成したものであり、慎重に扱うべきであることに留意されたい。すべての脅威に完全に対処するためには、さらなる調査と専門家による相談が必要な場合があります。

要約:

2025年1月6日午前9時12分14秒(06.01.2025 17:12:14 UTC+08:00)、DESKTOP-OOAADA6ホストのユーザー のアカウントで、EICAR Anti Malware Testfileがダウンロードされ、7-Zipで実行されました(T1204.002 - User Execution: Malicious File)。この検出は中程度の重大度(severity.level=MEDIUM)と評価されています。

主な出来事:

- 06.01.2025 17:12:14 UTC+08:00: ユーザー のDESKTOP-OOAADA6ホストで、EICAR Anti Malware Testfileが7-Zipで実行された