Cisco SecureX タイルのリスト

初版：2020 年 6 月 26 日

最終更新：2022 年 10 月 13 日

概要

SecureX では、シスコの統合型セキュリティポートフォリオとお客様のセキュリティインフラストラクチャ全体とをつなぐことで、可視性が統一され、自動化が実現し、ネットワーク全体のセキュリティが強化されます。その結果、すでに存在しているソリューションに組み込まれたセキュリティがシンプルになります。セキュリティ環境全体を可視化し、脅威への対応を促進するため、SecureX ダッシュボード中央の [タイル（Tiles）] ペインには統合された製品のメトリックとデータが表示されます。統合を SecureX に追加すると、ダッシュボードをカスタマイズするときに、製品によって提供されるタイルを追加できるようになります。このドキュメントは、SecureX で使用できるタイルとその説明の補足リストです。

（注） このタイルリストは定期的に更新されますが、SecureX と統合されているすべての製品でタイルの完全なリストが反映されているとは限りません。

Cisco Defense Orchestrator（CDO）

タイル名	説明
CDO デバイスの概要（CDO Device Summary）	CDO デバイスステータスの概要。
CDO オブジェクトとポリシー（CDO Objects and Policies）	CDO オブジェクトとポリシーの概要。
CDO VPN	CDO VPN の要約。
CSDAC - 要素	CSDAC 要素の要約。
CSDAC - ソース コネクタ	タイプおよびステータス別の CSDAC コネクタ。
CSDAC - 変換先アダプタ	タイプおよびステータス別の CSDAC アダプタ。

タイル名	説明
CSDAC - ダイナミックオブジェクト	CSDAC ダイナミックオブジェクトとマッピング数。

クラウドメールボックス

タイル名	説明
Messages by Direction	電子メールトラフィックの合計が宛先別に表示されます。電子メールは、[送信（Outgoing）]、[混合（Mixed）]、[内部（Internal）]、および[受信（Incoming）]に分けられます。
Malicious & Phishing	悪意のある、またはフィッシングであると判定されたメッセージのスナップショットが表示されます。
Spam	スパムと判定されたメッセージのスナップショットが表示されます。
Graymail	グレイメールと判定されたメッセージのスナップショットが表示されます。

Duo

タイル名	説明
Duo Trust Monitor	Duo Trust Monitor からの統計を表示します。

Firepower Threat Defense（FTD）

この統合に関する重要な情報、および FTD デバイスから SSE にイベントを送信するようにシステムを構成するには、https://cisco.com/go/firepower-securex-documentation で入手可能な『Cisco Firepower and SecureX Integration Guide』を参照してください。

タイルに関する重要な情報

イベントのメトリックを示すタイルには、過去 7 日以内に FTD デバイスから Security Services Exchange（SSE）に送信されたイベントが表示されます。

正しい一連のイベントが表示されるようにするには、Security Services Exchange で自動昇格オプションを正しく構成する必要があります。詳細については、SSE のオンラインヘルプを参照してください。SSE にアクセスするには、[イベントの概要（Event Summary）] タイルで概要値をクリックします。

一部のタイルは、Firepower Device Manager（FDM）によって管理される展開にではなく、Firepower Management Center（FMC）によって管理されるシステムにのみ適用されます。

これらのタイルからの一部のリンクを使用すると、FMC アプライアンスに移動します。ブラウザが内部ネットワークに接続できる限り、SecureX 内から FMC にアクセスできます（SecureX は企業のネットワークに接続する必要はありません）。

SecureX のタイルから FMC を相互起動するには、FMC の名前が完全修飾ドメイン名（FQDM）である必要があります。FMC の名前を変更するには、FMC Web インターフェイスの **[システム（System）] > [構成（Configuration）] > [情報（Information）]** に移動し、[名前（Name）] フィールドを変更します。

[イベントの概要（Event Summary）] タイル

このタイルには、選択したタイムフレーム（最大 7 日間）内に発生した SSE の FTD イベントがまとめられています。

このタイルのメトリックをクリックすると、Security Services Exchange（SSE）でイベントの詳細を表示できます。SSE は別のブラウザウィンドウに開きます。

[インシデント昇格理由（Incident Promotion Reason）] タイル

このタイルには、選択したタイムフレーム（最大7日間）内にインシデントに昇格した Security Services Exchange（SSE）の FTD イベントがまとめられています。

タイルには、イベントがインシデントに昇格した理由が表示されます。これには、次のようなものがあります。

- システムにより自動的に。（[Talos処理（Talos Disposition）]）

  Talos IP レピュテーションスコアが低い IP アドレスに関係する侵入イベントが自動的にインシデントに昇格します。SSE でマルウェアイベントの自動昇格を有効にしている場合、このメトリックには、送信元 IP レピュテーションスコアが低いマルウェアイベントも含まれます。

- SSE で組織が構成した自動昇格設定に基づいて自動的に。

  これらの設定は、SSE で **[クラウドサービス（Cloud Services）] > [イベント（Eventing）] >** ⚙ **> [イベントの自動昇格（Auto-Promote Events）]** の順にクリックするとあります。

  セキュリティ インテリジェンス カテゴリ（DNS、URL、および IP アドレス）には、Talos 脅威インテリジェンスデータに基づいた一致に基づいて昇格されたイベントが含まれ、カスタム セキュリティ インテリジェンス リストおよびフィードに基づいてイベントを自動的に昇格するように SSE が構成されている場合は、それらのイベントも含まれます。

その他の構成可能な自動昇格の理由は、[侵入ルールカテゴリ（Intrusion Rules Category）]、[マルウェア脅威スコア（Malware Threat Score）]、および [カスタムIPアドレス（Custom IP Address）] です。

- SSE の [イベント（Events）] ページからユーザーが手動で。（ユーザー昇格）

チェックボックスを選択または選択解除して、グラフ表示を変更します。

イベントのインシデントへの昇格については、SSE のオンラインヘルプを参照してください。

[Talos IPレピュテーション（Talos IP Reputation）] タイル

このタイルには、選択したタイムフレーム（最大 7 日間）内に FTD から Security Services Exchange（SSE）に送信された侵入およびマルウェアイベントに関連付けられたパブリック IP アドレスの Talos レピュテーションスコアがまとめられています。

この値は、[インシデント昇格理由（Incident Promotion Reason）] タイルの [Talos処理（Talos Disposition）] 値と同じ脅威データに基づきますが、カウントは計算方法によって異なる場合があります。たとえば、[Talos IPレピュテーション（Talos IP Reputation）] は送信元と宛先の IP アドレスを別々にカウントしますが、[Talos処理（Talos Disposition）] の値は、送信元と宛先の両方の IP アドレスのレピュテーションが低くても、インシデントごとに 1 回だけ増加します。

SSE からインシデントにイベントを昇格させるために使用される [Talos IPレピュテーション（Talos IP Reputation）] 脅威メトリックは、FTD デバイスでは使用されません。これは、ネットワークのセキュリティ インテリジェンス データと似ているようで異なります。

このタイルのメトリックをクリックすると、Security Services Exchange（SSE）でイベントの詳細を表示できます。SSE は別のブラウザウィンドウに開きます。

SSE に表示されるイベントの数は、タイルに表示されるイベントの数と異なる場合があります。重複するイベントはSSEから自動的に削除され、SSEの構成によってイベントが自動的に除外される場合があります。SecureX タイルには、SSE でそのようなアクションが実行される前のイベント数が表示されます。

[侵入の上位攻撃者（Intrusion Top Attackers）] タイル

FTD デバイスから SSE に送信された、組織で発生した侵入イベントの上位攻撃者のリスト。

ダッシュボードの上部でより長いタイムフレームが選択されている場合でも、このタイルには最大7日分のデータが表示されます。タイル自体で選択されたタイムフレームを確認してください。

[侵入の上位ターゲット（Intrusion Top Targets）] タイル

FTD デバイスから SSE に送信された、組織で発生した侵入イベントの上位ターゲットのリスト。

ダッシュボードの上部でより長いタイムフレームが選択されている場合でも、このタイルには最大7日分のデータが表示されます。タイル自体で選択されたタイムフレームを確認してください。

[侵入の上位シグニチャ（Intrusion Top Signatures）] タイル

FTD デバイスから SSE に送信された、組織で発生した侵入イベントの上位シグニチャのリスト。

ダッシュボードの上部でより長いタイムフレームが選択されている場合でも、このタイルには最大7日分のデータが表示されます。タイル自体で選択されたタイムフレームを確認してください。

[デバイスインベントリ（Device Inventory）] タイル

重要 このタイルを使用するには、それぞれの FMC で Cisco Success Network を有効にする必要があります。FMC の [システム（System）]>[スマートライセンス（Smart Licenses）] ページでこの機能を有効にします。不明な点がある場合は、FMC オンラインヘルプで「Cisco Success Network」を検索してください。

このタイルには、FMC による展開からのデータのみが表示されます。FDM によって管理されるデバイスは、このタイルに反映されません。

このタイルは、SecureX に登録されている FMC アプライアンスとその管理対象デバイスが、少なくとも推奨ソフトウェアバージョンを実行しているかどうかを示します。この最小バージョンは、入手可能な最新のソフトウェアバージョンではない可能性があります。代わりに、ソフトウェアの品質、安定性、および使用可能期間に基づいてシスコが決定します。

最適な保護のためには、すべての FMC とすべての管理対象デバイスが、少なくとも推奨バージョンを実行している必要があります。アップグレード手順については、https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.html にある『Cisco Firepower Management Center Upgrade Guide』を参照してください。

[推奨バージョン（Suggested version）] リンクをクリックすると、仮想アプライアンスのダウンロード用に Cisco.com の [ソフトウェアダウンロード（Software Downloads）] ページに移動します。同じダウンロードをすべての仮想アプライアンスとハードウェア FMC アプライアンスに使用できます。

[アップグレードが必要な管理対象デバイス（Managed devices needing upgrade）] 列のゼロ（0）は、この FMC のすべての管理対象デバイスが最新であることを示します。

[セキュリティ更新状況（Security Update Status）] タイル

重要 このタイルを使用するには、それぞれの FMC で Cisco Success Network を有効にする必要があります。FMC の [システム（System）]>[スマートライセンス（Smart Licenses）] ページでこの機能を有効にします。不明な点がある場合は、FMC オンラインヘルプで「Cisco Success Network」を検索してください。

このタイルには、FMC による展開からのデータのみが表示されます。FDM によって管理されるデバイスは、このタイルに反映されません。

効果的な保護のために、システムでは常に最新の脅威インテリジェンスを使用する必要があります。

このタイルに展開が最新でないことが表示されている場合は、最新の更新をダウンロードしてインストールします。

これらの更新、オプション、およびそれらを手動または自動でインストールする手順については、FMC オンラインヘルプの「System Updates」の章を参照してください。

[セキュリティ機能（Security Capabilities）] タイル

重要 このタイルを使用するには、それぞれの FMC で Cisco Success Network を有効にする必要があります。FMC の [システム（System）]>[スマートライセンス（Smart Licenses）] ページでこの機能を有効にします。不明な点がある場合は、FMC オンラインヘルプで「Cisco Success Network」を検索してください。

このタイルには、FMC による展開からのデータのみが表示されます。FDM によって管理されるデバイスは、このタイルに反映されません。

このタイルは、セキュリティ機能をどの程度広範囲に使用しているかを示します。具体的には次のとおりです。

- ライセンスの各タイプが割り当てられた、それぞれの FMC が管理するデバイスの数。
- それぞれの FMC が管理するデバイスに展開される、ライセンスの各タイプを必要とするルールの数。

  簡単な例として、3 つの URL フィルタ処理ルールを持つ 1 つのアクセス コントロール ポリシーがあり、そのポリシーを 4 つの管理対象デバイスに展開した場合、ルールの数は 12 です。

トラブルシューティング

このドキュメントで問題に対する回答が見つからない場合は、https://cisco.com/go/firepower-securex-documentation で入手可能な『Cisco Firepower and SecureX Integration Guide』を参照してください。

Orbital

タイル名	説明
ユーザークエリと結果の統計	ユーザークエリと結果を説明する一連のメトリック。
組織クエリと結果の統計	組織クエリと結果を説明する一連のメトリック。

タイル名	説明
ユーザーカタログの統計	このユーザーが最も頻繁に使用するカタログクエリを説明する一連のメトリック。
組織カタログの統計	この組織が最も頻繁に使用するカタログクエリを説明する一連のメトリック。

Secure Client

タイル名	説明
コンピュータの概要（Computer Summary）	コンピュータの数とそれぞれの問題（インスタンスキーが競合している、インスタンスキーがない、パッケージのインストールに失敗した、パッケージの再構成に失敗した、ID がないなど）を表示します。
ユニファイドコネクタの統計	ユニファイドコネクタの数と統計（キーが競合している、キーがない、インストールに失敗した、再構成に失敗した、ID がないなど）を表示します。

Secure Cloud Analytics

Secure Cloud Analytics（旧称 Stealthwatch Cloud）は、オンプレミスおよびクラウドベースのネットワーク展開をモニターする Software as a Service（SaaS）ソリューションです。ネットワークトラフィックに関する情報を収集することによって、トラフィックに関する観測内容（ネットワーク上の動作に関する事実）が作成され、トラフィックパターンに基づいてネットワークエンティティのロールが自動的に識別されます。観測内容それ自体は、それらが表すものの事実を超えた意味を持ちません。観測内容、ロール、およびその他の脅威インテリジェンスの組み合わせに基づいて Secure Cloud Analytics が生成するアラートは、潜在的な悪意のある動作をシステムによって識別されたものとして表す実用的な項目です。

Secure Cloud Analytics は、興味深い動作の観測内容（ハイライトされた観測内容）も識別します。これは、ポータル UI から確認できます。これらの観測内容は、それ自体は悪意のある動作を意味するものではありませんが、ネットワーク上の注目すべきトラフィックを表している可能性があります。

以下では、SecureX で表示できる Secure Cloud Analytics タイルについて説明します。これは、Secure Cloud Analytics の結果を表します。

タイル名	説明
アラート概要チャート（Alert Overview Chart）	選択したタイムフレームに基づいて、マルチレベルの円グラフを表示します。外側のリングの内容は次のとおりです。 • タイムフレーム内に作成された新しい Secure Cloud Analytics アラート • タイムフレームの前に作成され、タイムフレーム内にまだクローズしていない未解決の Secure Cloud Analytics アラート • タイムフレーム中にクローズされた解決済みの Secure Cloud Analytics アラート そして、内側のリングの内容は次のとおりです。 • 割り当てられた Secure Cloud Analytics アラート • 未割り当ての Secure Cloud Analytics アラート
アラートクイックビュー（Alert Quick View）	未解決の Stealthwatch Cloud アラートと未割り当ての Stealthwatch Cloud アラートの現在の数を表示します。
デバイス数チャート（Device Count Chart）	Stealthwatch Cloud が特定のタイムフレーム中にネットワーク上でトラフィックの送信を検出した一意のエンティティの数を、縦棒チャートとして表示します。
監視数（Observation Count）	Stealthwatch Cloud が特定のタイムフレームに生成した観測内容の合計数と、そのタイムフレームでハイライトされた観測内容の合計数を表示します。[観測内容（Observations）] および [ハイライトされた観測内容（Highlighted Observations）] リンクをクリックすると、Stealthwatch Cloud ポータル UI に移動して、これらの観測内容に関する詳細情報を表示できます。
Sensor Status	構成済みの Stealthwatch Cloud センサーのリストと、それらがアクティブか非アクティブかを表示します。

タイル名	説明
トラフィック時系列チャート（Traffic Over Time Chart）	選択したタイムフレームで Stealthwatch Cloud によって監視されたインバウンドトラフィック、インバウンド暗号化トラフィック、アウトバウンドトラフィック、およびアウトバウンド暗号化トラフィックの量を積み上げ棒チャートとして表示します。

Secure Email Appliance

受信 E メールのメトリック

タイル名	説明
Secure Endpoint によって処理される受信ファイル（Incoming Files Handled by Secure Endpoint）	受信メールの Secure Endpoint 分析を要約した一連のメトリック。
着信メール サマリー	メールフローアクティビティを要約した一連のメトリック。
受信脅威メッセージの概要（Incoming Threat Messages Summary）	脅威アクティビティを要約した一連のメトリック。
E メールの概要（Email Summary）	メールフローアクティビティを要約した一連のメトリック。
受信メール接続数の上位（国別）（Top Incoming Mail Connections by Country）	国別に上位の受信メール接続数を要約した一連のメトリック。
受信脅威メッセージ総数別の上位送信者（ドメイン）（Top Senders (Domains) by Total Incoming Threat Messages）	受信脅威メッセージ総数別に上位送信者（ドメイン）を要約した一連のメトリック。
受信脅威メッセージ総数別の上位送信者（IP アドレス）（Top Senders (IP Addresses) by Total Incoming Threat Messages）	受信脅威メッセージ総数別に上位送信者（IP アドレス）を要約した一連のメトリック。
検出した受信ウイルスタイプの上位（Top Incoming Virus Types Detected）	検出した上位の受信ウイルスタイプを要約した一連のメトリック。
上位URLスパムメッセージ（Top URL Spam Messages）	上位の URL スパムメッセージを要約した一連のメトリック。

送信 E メールのメトリック

タイル名	説明
発信メール サマリー	送信メールフローアクティビティを要約した一連のメトリック。
送信脅威メッセージ総数別の上位送信者ドメイン（Top Outgoing Sender Domains by Total Outgoing Threat Messages）	送信脅威メッセージ総数別に上位送信者ドメインを要約した一連のメトリック。
送信脅威メッセージ総数別の上位送信者 IP アドレス（Top Sender IP Addresses by Total Outgoing Threat Messages）	送信脅威メッセージ総数別に上位送信者 IP アドレスを要約した一連のメトリック。

Secure Endpoint

タイル名	説明
検出された侵害（Compromises detected）	AMP によって検出された侵害を要約した一連のメトリック。
コンピュータの概要（Computers Summary）	AMP コンピュータの状態を要約した一連のメトリック。
要約	AMP の検出と応答を要約した一連のメトリック。
隔離	時間別に AMP 検疫を要約した一連のメトリック。
検出された MITRE ATT&CK の戦術（MITRE ATT&CK Tactics detected）	AMP によって検出された MITRE ATT&CK の戦術を要約した一連のメトリック。
脅威ハンティング（Threat Hunting）	脅威ハンティング送信による脅威ハンティングインシデント。
上位のエンドポイント侵害（Top Endpoint Compromises）	シビラティ（重大度）スコア別の上位の侵害。
上位の動的脅威（Top Dynamic Threats）	上位の動的脅威。
上位マルウェア脅威（Top Malware Threats）	検出名で集計された侵害検出別の上位の脅威。
上位の侵害の観測対象（Top Compromise Observables）	上位の侵害の観測対象。

Secure Malware Analytics

タイル名	説明
脅威スコア	脅威スコア範囲別の送信のカウント。
結果別の総送信数（Total Submissions by Result）	ステータス別の送信のカウント。
脅威スコア別の合計送信数（Total Submissions by Threat Score）	脅威スコア範囲別の送信のカウント。
合計有害判定数（Total Convictions）	有害であると判定された送信のカウント。
結果別の送信の送信元（Submissions Source by Result）	送信の送信元別にグループ化された、ステータス別の送信のカウント。
脅威スコア別の送信の送信元（Submission Source by Threat Score）	送信の送信元別にグループ化された、脅威スコア範囲別の送信のカウント。
送信環境（Submission Environments）	環境別にグループ化された、有害であると判定された送信と有害ではないと判定された送信のカウント。
送信ファイルタイプ（Submission File Types）	ファイルタイプ別の送信のカウント。
権限付与 API サンプル送信（Entitlement API Sample Submissions）	送信とレート制限された送信のカウント。
送信ネットワークの出口（Submission Network Exits）	分析中に使用されたネットワーク出口別の送信のカウント。
上位のタグ（Top Tags）	タグ別の送信のカウント。
上位の IP アドレス（Top IP Addresses）	分析中に参照された IP 別の送信のカウント。
上位ドメイン	分析中に参照されたドメイン別の送信のカウント。
上位の動作指標	送信中にトリガーされたカウントインジケータ。

Secure Network Analytics

タイル名	説明
カテゴリ別のホストのアラーム	最後のリセット時間以降のアラームカテゴリ内にあるホストの数。
ネットワークの可視性	ホスト数とトラフィック量の統計情報。
上位のアラームホスト	最後のリセット時以降ネットワーク上でアクティブになっていて、アラームシビラティ（重大度）別にソートされた上位 7 位までの内部ホスト。
カウント別の上位のアラーム	カウント別の上位 10 位のアラーム。
トラフィック別の上位の内部ホストグループ	トラフィック別の上位 10 位の内部ホストグループ。
トラフィック別の上位のホストグループ	トラフィック別の上位 10 位の外部ホストグループ。
可視性アセスメント	可視性アセスメントカテゴリのホスト数。

Cisco Secure Web Appliance

タイル名	説明
AMP によって分析される受信ファイル（Incoming Files Analyzed by AMP）	AMPによって分析された受信ファイルを要約した一連のメトリック。
HTTPSレポート（HTTPS Reports）	HTTP および HTTPS トラフィックの Web トランザクションを要約した一連のメトリック。
上位ドメイン	Web トランザクションの上位のドメインを要約した一連のメトリック。
上位マルウェアカテゴリ（Top Malware Categories）	Web トランザクションの上位のマルウェアカテゴリを要約した一連のメトリック。
上位URLカテゴリ（Top URL Categories）	Web トランザクションの上位の URL カテゴリを要約した一連のメトリック。

SecureX Threat Response

タイル名	説明
インシデントのステータスと割り当てられた従業員（Incident Statuses and Assignees）	インシデントのステータスに基づいて、現在ログインしているユーザーなどに割り当てられているインシデントを表示します。このタイルを使用すると、インシデントのステータスと割り当てられた従業員をすばやく確認できます。
影響の大きいインシデント（High Impact Incidents）	インシデントマネージャが認識している上位の侵害を表示します。これらのインシデントは、SecureX Threat Response Incident Manager の [影響大（High Impact）] リストまたは SecureX リボンの Incidents アプリに表示されるものです。

セキュリティ管理アプライアンス（E メール）

受信 E メールのメトリック

タイル名	説明
Secure Endpoint によって処理される受信ファイル（Incoming Files Handled by Secure Endpoint）	受信メールの Secure Endpoint 分析を要約した一連のメトリック。
着信メール サマリー	メールフローアクティビティを要約した一連のメトリック。
受信脅威メッセージの概要（Incoming Threat Messages Summary）	脅威アクティビティを要約した一連のメトリック。
E メールの概要（Email Summary）	メールフローアクティビティを要約した一連のメトリック。
受信メール接続数の上位（国別）（Top Incoming Mail Connections by Country）	国別に上位の受信メール接続数を要約した一連のメトリック。
受信脅威メッセージ総数別の上位送信者（ドメイン）（Top Senders (Domains) by Total Incoming Threat Messages）	受信脅威メッセージ総数別に上位送信者（ドメイン）を要約した一連のメトリック。

タイル名	説明
受信脅威メッセージ総数別の上位送信者（IP アドレス）（Top Senders (IP Addresses) by Total Incoming Threat Messages）	受信脅威メッセージ総数別に上位送信者（IP アドレス）を要約した一連のメトリック。
検出した受信ウイルスタイプの上位（Top Incoming Virus Types Detected）	検出した上位の受信ウイルスタイプを要約した一連のメトリック。
上位URLスパムメッセージ（Top URL Spam Messages）	上位の URL スパムメッセージを要約した一連のメトリック。

送信 E メールのメトリック

タイル名	説明
発信メール サマリー	送信メールフローアクティビティを要約した一連のメトリック。
送信脅威メッセージ総数別の上位送信者ドメイン（Top Outgoing Sender Domains by Total Outgoing Threat Messages）	送信脅威メッセージ総数別に上位送信者ドメインを要約した一連のメトリック。
送信脅威メッセージ総数別の上位送信者 IP アドレス（Top Sender IP Addresses by Total Outgoing Threat Messages）	送信脅威メッセージ総数別に上位送信者 IP アドレスを要約した一連のメトリック。

セキュリティ管理アプライアンス（Web）

タイル名	説明
HTTPS レポート（HTTPS Reports）	HTTP および HTTPS トラフィックの Web トランザクションを要約した一連のメトリック。
Secure Endpoint によって分析される受信ファイル（Incoming Files Analyzed by Secure Endpoint）	Secure Endpoint によって分析された受信ファイルを要約した一連のメトリック。
上位ドメイン	Web トランザクションの上位のドメインを要約した一連のメトリック。
上位マルウェアカテゴリ（Top Malware Categories）	Web トランザクションの上位のマルウェアカテゴリを要約した一連のメトリック。
上位URLカテゴリ（Top URL Categories）	Web トランザクションの上位の URL カテゴリを要約した一連のメトリック。

Tetration

タイル名	説明
Tetration 監視対象インベントリメトリック（Tetration Monitored Inventory Metrics）	現在学習されているインベントリを説明するメトリック。
Tetration ポリシーメトリック（Tetration Policy Metrics）	構成されたセグメンテーションポリシーを説明するメトリック。
Tetration ソフトウェアエージェントの概要（Tetration Software Agents Summary）	接続されたソフトウェアエージェントを説明するメトリック。

Umbrella

タイル名	説明
コマンドアンドコントロール カテゴリ別のセキュリティブロック（Security Blocks by Command-and-Control Category）	コマンドアンドコントロール カテゴリ別にセキュリティブロックを要約した一連のメトリック。
仮想通貨マイニングカテゴリ別のセキュリティブロック（Security Blocks by Cryptomining Category）	仮想通貨マイニングカテゴリ別にセキュリティブロックを要約した一連のメトリック。
マルウェアカテゴリ別のセキュリティブロック（Security Blocks by Malware Category）	マルウェアカテゴリ別にセキュリティブロックを要約した一連のメトリック。
フィッシングカテゴリ別のセキュリティブロック（Security Blocks by Phishing Category）	フィッシングカテゴリ別にセキュリティブロックを要約した一連のメトリック。
クラウドマルウェアの概要（Cloud Malware Summary）	承認されたアプリケーションのクラウドマルウェアを要約した一連のメトリック。
リクエストの概要（Request Summary）	Umbrella リクエストを要約した一連のメトリック。
ファイアウォールセッションとブロックの総数（Firewall Sessions and Blocks）	ファイアウォールセッションとブロックの総数。
プロキシセッションとブロックの総数（Proxy Sessions and Blocks）	プロキシセッションとブロックの総数。
プロキシ セキュリティ ブロック（Proxy Security Blocks）	プロキシ セキュリティ ブロックの総数。

SecureX タイルリストの変更履歴

製品	変更日	タイル	説明
Secure Client	10/13/2022	コンピュータのサマリー、ユニファイドコネクタの統計	これら 2 つの新しいタイルを追加しました。
Secure Malware Analytics	10/13/2022	上位の動作指標	この 1 つの新しいタイルを追加しました。
Orbital	10/13/2022	ユーザーのクエリと結果の統計、組織のクエリと結果の統計、ユーザーカタログの統計、組織カタログの統計	タイルの名前と説明を更新しました。
Duo	10/13/2022	Duo Trust Monitor	新しいタイルを 1 つ備えた新しい Duo 統合モジュールを追加しました。
Cisco Defense Orchestrator	10/13/2022	CDO VPN、CSDAC 要素、CSDAC ソースコネクタ、CSDAC 変換先アダプタ、CSDAC ダイナミックオブジェクト	これら 5 つの新しいタイルを追加しました。
Umbrella	10/13/2022	ファイアウォールセッションとブロック、プロキシセッションとブロック、プロキシ セキュリティ ブロック	これら 3 つの新しいタイルを追加しました。

製品	変更日	タイル	説明
Secure Endpoint	10/13/2022	上位の動的脅威（Top Dynamic Threats）	この 1 つの新しいタイルを追加しました。
クラウドメールボックス	2022/03/25	[宛先別メッセージ（Messages by Direction）]、[悪意あり&フィッシング（Malicious&Phishing）]、[スパム（Spam）]、[グレイメール（Graymail）]	これら 4 つの新しいタイルを備えた新しい Cloud Mailbox 統合モジュールを追加しました。
Orbital、SecureX Threat Response、Secure Malware Analytics	2022/03/10	—	Secure Malware Analytics および Orbital のタイルを更新しました。SecureX Threat Response タイルの新しいトピックを追加しました。
Firepower	2021/03/03	[セキュリティ更新状況（Security Update Status）]	新しい [セキュリティ更新状況（Security Update Status）] タイルは、システムがネットワークを保護するために最新の脅威インテリジェンスを使用しているかどうかを示します。
Firepower	2021/03/03	Security Capabilities	新しい [セキュリティ機能（Security Capabilities）] タイルには、ライセンスの数と使用中のルールの数によって、システムが使用しているセキュリティ機能がまとめられています。
Firepower	2021/03/03	デバイスインベントリ（Device Inventory）	新しい [デバイスインベントリ（Device Inventory）] タイルには、アップグレードする必要があるアプライアンスとデバイスがまとめられています。

製品	変更日	タイル	説明
Firepower	2020/07/23	[未処理のイベントサマリー（Raw Event Summary）]	このタイルは、[イベントの概要（Event Summary）] タイルになりました。 以前の説明は次のとおりです。 このタイルには、選択したタイムフレーム（最大 7 日間）内に SSE に送信されたすべてのイベントがまとめられています。 SSE に表示されるイベントの数は、タイルに表示されるイベントの数と異なる場合があります。重複するイベントはSSEから自動的に削除され、SSEの構成によってイベントが自動的に除外される場合があります。SecureX タイルには、SSE でそのようなアクションが実行される前のイベント数が表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。