7000 シリーズ

シリーズ 3 の管理対象デバイスグループ。このシリーズのデバイスには、70xx ファミリ（3D7010/7020/7030/7050 モデル）および 71xx ファミリ（3D7110/7120/3D7115/3D7125 および AMP7150 モデル）が含まれます。

8000 シリーズ

シリーズ 3 の管理対象デバイスグループ。このシリーズのデバイスには、81xx ファミリ（3D8120/8130/8140 および AMP8150 モデル）、82xx ファミリ（3D8250/8260/8270/8290 モデル）、83xx ファミリ（3D8350/8360/8370/8390 モデル）、および AMP83xx ファミリ（AMP8350/AMP8360/AMP8370/AMP8390 モデル）が含まれます。8000 シリーズ デバイスは、通常 7000 シリーズデバイスより高性能です。

ASA FirePOWER

Cisco ASA with FirePOWER Services の省略名。

banner

サーバ バナーを参照してください。

Blue Coat X-Series 向け Cisco NGIPS

仮想デバイスのほとんどの機能を提供する、Blue Coat のスケーラブルなシャーシベースのシステム上に構築されたソフトウェアベースのアプリケーション。

CA

認証局を参照してください。

CAC 認証および許可

共通アクセス カード（CAC）によって提供されたクレデンシャルのみを使用してアプライアンスの Web インターフェイスにログインすることをユーザに許可する LDAP 認証の種類。

certificate

公開キー証明書を参照してください。

Cisco ASA with FirePOWER Services

ASA FirePOWER モジュールがインストールされた Cisco 適応型セキュリティ アプライアンス（ASA）管理対象デバイスのグループ。このシリーズのデバイスには、ASA5506-X、ASA5506H-X,ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、および ASA5585-X-SSP-60 モデルが含まれます。

Cisco Cloud

Collective Security Intelligence クラウドを参照してください。

CLI

コマンド ライン インターフェイス(CLI)を参照してください。

Collective Security Intelligence クラウド

防御センターが最新の関連情報(マルウェア、セキュリティ インテリジェンス、および URL フィルタリング データなど)を取得できる、シスコがホストする外部サーバ。*クラウド サービス*または*シスコ クラウド*とも呼ばれます。マルウェア クラウド ルックアップと FireAMP プライベート クラウドも参照してください。

Context Explorer

モニタリング対象のネットワークに関する詳細でインタラクティブなグラフィカル情報を表示するページ。明確に区切られたセクションには、鮮明な線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で情報が、詳細リストとともに表示されます。分析を調整するためにカスタム フィルタを簡単に作成および適用できます。また、グラフ エリアをクリックするかまたはカーソルを置くと、データ セクションの詳細を確認できます。高度にカスタマイズ可能で、細分化され、リアルタイムで更新されるダッシュボードとは対照的に、Context Explorer は手動で更新され、より広範囲に及ぶデータのコンテキストを提供するように設計されています。また、ユーザが積極的に調査することができるようにレイアウトは 1 つの一貫した設計になっています。

Control ライセンス

ユーザ制御およびアプリケーション制御を実装できるようにするライセンス。スイッチングおよびルーティング(DHCP リレーと NAT を含む)などのハードウェアベースのタスク、VPN、およびデバイス クラスタリングを実行するように、サポートされている管理対象デバイスを設定することもできます。

CRL

証明書失効リスト(CRL)を参照してください。

disposition

マルウェアの性質を参照してください。

eStreamer

防御センターまたは管理対象デバイスから外部クライアント アプリケーションにイベント データをストリーミングできるようにする FireSIGHT システムのコンポーネント。

FireAMP

シスコ のエンタープライズ クラスのエンドポイントをベースとした高度なマルウェア分析およびマルウェア対策ソリューション。マルウェアの感染、継続的に発生する脅威、標的型攻撃を検出、認識し、ブロックします。組織に FireAMP サブスクリプションがある場合、個々のユーザがエンドポイント(コンピュータ、モバイル デバイス)にインストールした軽量の FireAMP コネクタが Collective Security Intelligence クラウドと通信します。これにより、マルウェアを瞬時に識別して検疫するだけでなく、マルウェアの発生を識別し、その伝搬経路を追跡し、その影響を把握して、正常に回復する方法を知ることができます。FireAMP ポータルを使用して、カスタム保護を作成したり、特定のアプリケーションの実行をブロックしたり、カスタム ホワイトリストを作成したりすることもできます。ネットワーク ベースの高度なマルウェア防御と比較してください。

FireAMP コネクタ

サブスクリプションベースの FireAMP 展開のユーザがコンピュータやモバイル デバイスなどのエンドポイントにインストールする軽量のエージェント。コネクタは Collective Security Intelligence クラウドと通信し、情報を交換します。これにより、組織全体でマルウェアを迅速に特定して検疫できます。また、エンドポイントのホストで侵害の兆候（IOC）も識別できます。

FireAMP サブスクリプション

組織が FireAMP を高度なマルウェア防御（AMP）ソリューションとして使用できるようにする個別購入サブスクリプション。ネットワークベースの AMP を実行するために管理対象デバイスで有効にする Malware ライセンスと比較してください。

FireAMP プライベート クラウド

モニタ対象ネットワークと FireAMP ベース（ファイルおよびマルウェア）の機能の Collective Security Intelligence クラウドの間のセキュアなメディエータとして機能する FireAMP が提供する仮想マシン。クラウドへのすべての接続は、ネットワーク上の個々のエージェントやアプライアンスからではなく、プライベート クラウドの匿名化されたプロキシ接続上で発生します。

FireAMP ポータル

組織のサブスクリプションベースの FireAMP 展開を設定できる Web サイト（http://amp.sourcefire.com/）。

FireSIGHT ライセンス

防御センターのデフォルト ライセンス。これにより、ホスト、アプリケーション、およびユーザ ディスカバリを実行できます。FireSIGHT ライセンスは、防御センターとその管理対象デバイスを使用してモニタできるホストとユーザの数、およびユーザ制御を実行するためにアクセス コントロール ルールで使用できるアクセス制御ユーザの数を決定します。

FireSIGHT 推奨ルール

侵入ポリシーの情報に基づいて、ネットワーク マップでどのルールを有効/無効にしたらよいかを推奨する機能。推奨に基づくルール状態の変更をシステムに許可することができます。この場合、システムは読み取り専用の FireSIGHT 推奨レイヤを追加します。

FireSIGHT 推奨レイヤ

FireSIGHT 推奨ルール機能によって推奨される状態にルール状態を変更することをシステムに許可している場合に存在する侵入ポリシーの組み込みレイヤ。

GeoDB

地理位置情報データベース（GeoDB）を参照してください。

GID

ジェネレータ ID（GID）を参照してください。

HA リンク インターフェイス

ハイ アベイラビリティ リンク インターフェイスとも呼ばれ、デバイス間でヘルス情報を共有するため冗長通信チャネルとして機能するデバイスのクラスタ化されたペアの各メンバーに対して設定される物理インターフェイス。

HTTP 応答ページ

ユーザの HTTP 要求がアクセス制御によってブロックされた場合に、システムに表示されるように設定できる Web ページ。シスコ提供の汎用応答ページを表示するか、カスタム HTML を提供できます。インタラクティブ ブロック ルールによって要求がブロックされる場合、ユーザが応答ページのボタンをクリックして、要求元のサイトに戻って続行できるようにすることができます。

ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する、新しいパッシブ オペレーティング システムまたはサーバの ID がシステムによって報告されると発生する競合。

LDAP 認証

ユーザ クレデンシャルを Lightweight Directory Access Protocol（LDAP）ディレクトリ サーバに保存されている LDAP ディレクトリと比較することによって、ユーザ クレデンシャルを確認する外部認証の形式。

Lights-Out Management（LOM）

アウトオブバンド Serial over LAN（SoL）管理接続を使用して、アプライアンスの Web インターフェイスにログインせずに、特定のアプライアンスをリモートでモニタまたは管理できるシリーズ 3 の機能。シャーシのシリアル番号の表示や、ファンの速度や温度などの設定のモニタリングといった、限られたタスクを実行できます。

Link Aggregation Control Protocol（LACP）

システムおよびポート情報の交換方法を提供する IEEE 802.3ad 仕様のコンポーネント。複数の物理ポートのバンドリングを制御して、Link Aggregation Group（LAG）と呼ばれる単一の論理データ チャネルを形成できます。LACP を有効にすると、チャネルの一方の端の各デバイスは、LACP を使用して集約でアクティブに使用されるリンクを特定します。

Link Aggregation Group（LAG）

管理対象デバイスの複数の物理イーサネット インターフェイスを単一の論理リンクにグループ化できるシリーズ 3 の機能。ネットワーク間のパケット スイッチングを提供するレイヤ 2 展開、またはインターフェイス間のトラフィックをルーティングするレイヤ 3 展開で設定します。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。

list

セキュリティ インテリジェンス リストを参照してください。

Malware ライセンス

ネットワーク トラフィックで高度なマルウェア防御（AMP）を実行することができるライセンス。ファイル ポリシーを使用して、管理対象デバイスによって検出された特定のファイル タイプについてマルウェア クラウド ルックアップを実行するようにシステムを設定できます。FireAMP サブスクリプションと比較してください。

NAT

ネットワーク アドレス変換。プライベート ネットワーク上の複数のホストで単一のインターネット接続を共有するために最も一般的に使用される機能。ディスカバリを使用して、システムはネットワーク デバイスをロード バランサとして識別できます。また、FireSIGHT システムのレイヤ 3 展開では、NAT ポリシーを使用して NAT によるルーティングを設定できます。

NAT ポリシー

NAT ルールを使用して NAT によるルーティングを実行するポリシー。

NAT ルール

ネットワーク トラフィックを評価し、条件に一致するトラフィックの変換方法を指定する一連の設定と条件。NAT ルールは、NAT を使用してルーティングを実行するために既存の NAT ポリシーに追加されます。

NetFlow

Cisco IOS 対応機器で実行するためにシスコによって開発された、IP トラフィック情報を収集するための公開されている独自のネットワーク プロトコル。NetFlow 対応デバイスによって収集された情報は、FireSIGHT システムによって収集されたディスカバリ データと接続データを補足したり、管理対象デバイスがカバーしないネットワークをモニタしたりするために使用できます。

NetMod

管理対象デバイスのシャーシにインストールするモジュール。これには、そのデバイスのセンシング インターフェイスが含まれます。

Nmap

Network Mapper。ホストで実行しているオペレーティング システムとアプリケーション プロトコルを検出するために使用できるオープン ソースのアクティブ スキャナ。Nmap スキャンを実行すると、検出された情報がネットワーク マップに追加されます。

PKI

公開キー インフラストラクチャ（PKI）を参照してください。

PKI オブジェクト

公開キー証明書およびペアの秘密キーを表す再利用可能なオブジェクト。

Protection ライセンス

侵入検知と防御、ファイル制御、およびセキュリティ インテリジェンスフィルタリングを実行できるライセンス。ライセンスがなくても、シリーズ 2 のデバイスでは、セキュリティ インテリジェンス以外の Protection 機能を自動的に使用できます。

RADIUS 認証

Remote Authentication Dial In User Service。ネットワーク リソースへのユーザ アクセスの認証、認可、およびアカウンティングに使用されるサービスです。外部認証オブジェクトを作成して、FireSIGHT システム ユーザが RADIUS サーバを介して認証できるようにすることができます。

RSA 暗号化

大きい数字を 2 つの素数に分解することに基づく暗号化方式。楕円曲線（EC）暗号化とは対照的な暗号です。

SFP モジュール

71xx ファミリ デバイスのネットワーク モジュールに挿入される小型フォーム ファクタ トランシーバ。SFP モジュールのセンシング インターフェイスでは設定可能なバイパスは許可されていません。

SHA-256 ハッシュ値

マルウェア クラウド ルックアップを実行するファイルを表す 32 ビット文字列。SHA256 と略記されることもあります。ハッシュ値は、暗号ハッシュ関数を使用して計算されます。複数のファイルの SHA-256 値が同じであれば、コンテンツが同じである可能性が非常に高くなります。

SID

シグネチャ ID（Sid）を参照してください。

Snort

IP ネットワークでのリアルタイム トラフィック分析およびパケット ロギングを実行するオープン ソースの侵入検知システム。Snort は、プロトコル分析、コンテンツ検索、およびコンテンツ マッチングを実行できます。また、さまざまな攻撃やプローブを検出できます。Snort では、柔軟なルールの言語を使用して、収集または通過させるべきネットワーク トラフィックを示します。FireSIGHT システムは、Snot を使用して、デコーダ、プリプロセッサ、および侵入ルールに照らしてパケットをテストします。

Spero 分析

マルウェア分析のために、Collective Security Intelligence クラウドにファイル構造特性を送信する方法。結果は動的分析を補足します。

SSL

セキュア ソケット レイヤ（SSL）を参照してください。

SSL インスペクション

ネットワークを通過する暗号化されたトラフィックを検査し、復号し、ログに記録することができる機能。復号しないように選択したトラフィックと復号されたトラフィックの両方を、アクセス制御でさらに検査できます。

SSL ポリシー

親アクセス コントロール ポリシーの一部として適用するポリシー、およびポリシー ターゲット デバイスでモニタする暗号化されたトラフィックに対して SSL インスペクションを実行するポリシー。SSL ポリシーには、複数の SSL ルールを含めることができます。また、これらのルールの基準を満たさないトラフィックの処理とロギングを決定するデフォルト アクションも指定します。SSL ポリシーでは、CA の公開キー証明書に基づき、復号できないトラフィックの処理方法、および信頼できる暗号化トラフィックを指定することもできます。

SSL ルール

システムが暗号化されたトラフィックを調査するために使用し、SSL インスペクションの実行を可能にする一連の条件。SSL ポリシーに組み込まれる SSL ルールは、簡単な IP アドレスのマッチングを実行したり、異なるユーザ、アプリケーション、ポート、URL、および暗号化されたセッション特性が関係する複雑な接続の特性を示したりすることがあります。SSL ルール アクションは、ルールの条件を満たすトラフィックをシステムがどのように処理するかを決定します。その他のルール設定によって、接続をログに記録する方法(および記録するかどうか)が決定されます。

SSL ルール アクション

システムが SSL ルールの条件を満たす暗号化されたネットワーク トラフィックをどのように処理するかを決定する設定。一致するトラフィックをブロックできます(接続の再設定はすることもしないこともできます)。また、暗号化されたトラフィックを復号せず、アップロードされた秘密キーを使用して着信トラフィックを復号したり、再署名された公開キー証明書を使用して発信トラフィックを復号したり、追加の SSL ルールを使用してトラフィックのモニタを続行したりすることもできます。

SVID

脆弱性 ID を参照してください。

TLS

Transport Layer Security を参照してください。

Transport Layer Security

セキュア ソケット レイヤ(SSL) プロトコルの後を継ぐ暗号化アプリケーション層プロトコル。SSL インスペクション機能を使用することにより、TLS プロトコルで暗号化されたトラフィックを復号できます。

URL オブジェクト

個々の URL を表す再利用可能なオブジェクト。

URL カテゴリ

URL の一般的な分類(マルウェア、ソーシャル ネットワーキングなど)。

URL フィルタリング

モニタ対象ホストによって要求された URL に基づいて、ネットワークを通過できるトラフィックを決定するアクセス コントロール ルールを作成できる機能。防御センターによって Collective Security Intelligence クラウドから取得される、それらの URL の URL カテゴリおよび URL レピュテーションの情報に相関します。許可またはブロックする個々の URL または URL のグループを指定することで、Web トラフィックに対するきめの細かいカスタム コントロールを実現できます。

URL フィルタリング(URL Filtering) ライセンス

URL カテゴリおよび URL レピュテーションの情報に基づいて URL フィルタリングを実行することができるライセンス。URL フィルタリング(URL Filtering) ライセンスは期限が切れることがあります。

URL レピュテーション

組織のセキュリティ ポリシーに反する目的のために Web サイトが使用される可能性を表します。Collective Security Intelligence クラウドによって判定されます。

UTC 時間

協定世界時。UTC は世界のあらゆる場所で共通の標準時間です。グリニッジ標準時（GMT）とも呼ばれます。FireSIGHT システム は UTC を使用しますが、タイムゾーン機能を使用して現地時間を設定することもできます。

VDB

脆弱性データベースを参照してください。

VLAN

仮想ローカル エリア ネットワーク（VLAN）を参照してください。

VLAN タグ オブジェクト

個々の 仮想ローカル エリア ネットワーク（VLAN）タグを表す再利用可能なオブジェクト。

VPN

FireSIGHT システムの管理対象デバイスの仮想ルータ間にセキュアな VPN トンネルを構築できる機能。

VPN ライセンス

FireSIGHT システムの管理対象デバイスの仮想ルータ間にセキュアな VPN トンネルを構築できるようにするライセンス。

VRT

シスコ VRT を参照してください。

使用してパケットの送信先を決定します。

VRT 分析レポート

動的分析のために送信されたキャプチャされたファイルのシスコ VRT 分析のレコード。動的分析サマリー レポートで提供される情報および動的分析中に検出された追加の情報の詳細を示します。

Web アプリケーション

HTTP トラフィックの内容または HTTP トラフィックに対して要求された URL を表すアプリケーション タイプ。

X-シリーズ

Blue Coat X-Series 向け Cisco NGIPS の省略名。

アクション

特定の基準を満たす(または満たさない)ネットワーク トラフィックを、システムが処理、検査、または記録する方法を決定する設定。アクションはポリシーのデフォルト アクションとして、特定のポリシーだけでなくさまざまなタイプのルールに関連付けられます。

アクセス コントロール ポリシー

管理対象デバイスがモニタするネットワーク トラフィックに対してアクセス制御を実施するために、それらのデバイスに適用するポリシー。アクセス コントロール ポリシーには、複数のアクセス コントロール ルールが含まれる場合があります。これらのルールの基準を満たさないトラフィックの処理とロギングは、同じくアクセス コントロール ポリシーによって指定されるデフォルト アクションによって決定されます。アクセス コントロール ポリシーのその他の設定は、セキュリティ インテリジェンス、SSL インスペクション、パフォーマンス オプション、プリプロセッサ オプションなどの詳細設定を制御します。

アクセス コントロール ルール

FireSIGHT システムがモニタリング対象のネットワーク トラフィックを検査し、きめ細かなアクセス制御を実現するために使用する一連の条件。アクセス コントロール ポリシーに組み込まれるアクセス コントロール ルールで、簡単な IP アドレスのマッチングを実行したり、さまざまな基準が関係する複雑な接続の特性を示したりすることができます。アクセス コントロール ルール アクションは、ルールの条件を満たすトラフィックをシステムがどのように処理するかを決定します。その他のルール設定により、接続をログに記録する方法(およびログに記録するかどうか)と、ルールによって許可されたトラフィックを侵入ポリシーまたはファイル ポリシーのどちらで検査するかが決定します。

アクセス コントロール ルール アクション

システムがアクセス コントロール ルールの条件を満たすネットワーク トラフィックをどのように処理するかを決定する設定。一致するトラフィックを*ブロック*することができます(接続の再設定はしてもしなくても構いません)。HTTP トラフィックでは、ブロックをバイパスするオプションを提供できます。また、トラフィックを*信頼*して、追加のインスペクションなしで通過させることも、一致するトラフィック(必要に応じて侵入ポリシーとファイル ポリシーを使用して検査することが可能)を*許可*することも、または追加のアクセス コントロール ルールを使用してトラフィックを*モニタ*し続けることもできます。

アクセス リスト

アプライアンスにアクセス可能なホストを表す IP アドレスのリスト。システム ポリシーで設定されます。デフォルトでは、すべてのユーザがポート 443(HTTPS)を使用してアプライアンスの Web インターフェイスにアクセスでき、ポート 22(SSH)を使用してコマンド ラインにアクセスできます。また、ポート 161 を使用する SNMP アクセスを追加できます。

アクセス制御

ネットワークを通過するトラフィックの指定、検査、記録を可能にする FireSIGHT システムの機能。アクセス制御は、セキュリティ インテリジェンス、SSL インスペクション、プリプロセッサ オプション、侵入検知と防御、ファイル制御、高度なマルウェア防御を呼び出します。また、ディスカバリで検査できるトラフィックを決定します。

アクセス制御ユーザ

アクセス制御によってネットワーク利用を制御されるユーザ。Microsoft Active Directory サーバと防御センターの間の接続を設定する場合は、アクセス制御ユーザが所属する必要のある LDAP グループを指定します。ユーザ エージェントがアクセス制御ユーザによるログインをレポートする場合、それらのユーザは IP アドレスと関連付けられます。これにより、ユーザ条件が指定されたアクセス コントロール ルールのトリガーが可能になります。非アクセス制御ユーザと比較してください。

アクティブ検出

アクティブ ソースを使用したホスト、アプリケーション、およびユーザ情報の検出。アクティブ ソースには、Nmap のようなスキャナ、システムの Web インターフェイスへのユーザ入力、またはコマンド ラインやサードパーティのアプリケーション API コールを使用したネットワーク マップへのホスト入力が含まれます。パッシブ検出と比較してください。

アダプティブ プロファイル

ディスカバリ データを使用して、パケットのターゲット ホストのオペレーティング システムを判別するアクセス コントロール ポリシーの詳細設定(パッシブ展開に推奨)。ネットワーク分析ポリシー内の対象を絞ったプロファイルによって、ターゲット ホストのオペレーティング システムと同じ方法で IP パケットが最適化され、ストリームが再構成されます。次に、侵入ポリシーが宛先ホストで使用されるものと同じ形式でデータを分析します。

アプライアンス

FireSIGHT システム、防御センター、管理対象デバイス、Cisco ASA with FirePOWER Services、または Blue Coat X-Series 向け Cisco NGIPS。物理アプライアンスとソフトウェアベースのアプライアンスがあります。

アプライアンス統計情報

稼働時間、システム メモリの使用率、負荷平均、ディスク使用率、システム プロセスのサマリーなど、アプライアンスに関する取得可能な情報。また、防御センターではデータ コリレータプロセスに関する情報。

アプリケーション

検出されたネットワーク アセット、通信方法、または HTTP コンテンツ。システムは、アプリケーション プロトコル、クライアント アプリケーション、Web アプリケーションの 3 種類のアプリケーションを検出します。

アプリケーション カテゴリ

アプリケーションの最も本質的な機能を示す一般分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

アプリケーション タイプ

アプリケーションが、アプリケーション プロトコル、クライアント アプリケーション、Web アプリケーションのいずれであるか。

アプリケーション タグ

アプリケーション カテゴリでカバーされない、アプリケーションに関する情報。たとえば、ビデオ ストリーミングの Web アプリケーションには、「高帯域幅」および「ディスプレイ広告」というタグが付けられることがよくあります。アプリケーションには任意の数のタグを付けることができます(タグなしも可能)。

アプリケーション ディテクタ

ネットワーク上のアプリケーションを識別するためにシステムが使用するツール。アプリケーション ディテクタは、パケット ヘッダー内の ASCII または 16 進数のパターンか、トラフィックが使用するポート、あるいはその両方を使用して、アプリケーションを識別します。シスコでは、システム更新、脆弱性データベースの更新、またはインポート/エクスポート機能を介して追加のディテクタを提供することがあります。独自のアプリケーション プロトコル ディテクタを作成することもできます。

アプリケーション フィルタ

アプリケーション リスク、ビジネスとの関連性、種類、カテゴリ、およびタグに関連した基準に従ってグループ化された 1 つ以上のアプリケーション。アプリケーション フィルタはオブジェクト マネージャで作成します。

アプリケーション プロトコル

サーバとホスト上のクライアント アプリケーションの間の通信で検出されたアプリケーション プロトコル トラフィックを表すアプリケーションのタイプ(例:SSH、HTTP など)。

アプリケーション リスク

アプリケーションの使用方法が組織のセキュリティ ポリシーに違反している可能性。アプリケーションのリスクは、Very Low から Very High までの範囲です。

アプリケーション制御

アクセス制御の一部として、どのアプリケーション トラフィックがネットワークを通過可能であるかどうかを指定できる機能。

アプリケーションのビジネスとの関連性

ビジネスとの関連性を参照してください。

アラート

システムが特定のイベントを生成したことを示す通知。侵入イベント(影響を含む)、ディスカバリ イベント、ネットワークベースのマルウェア イベント、相関ポリシー違反、ヘルス ステータスの変更、および記録された接続に基づいてアラートを発行できます。通常は電子メール、Syslog、または SNMP トラップでアラートを発行できます。

アラート応答

システムが電子メール、Syslog、または SNMP トラップでアラートを送信することを許可する一連の設定。単一のアラート応答を使用して複数のタイプのイベントについてのアラートを受けることができます。

暗号スイート リスト

トラフィックの暗号化に使用される複数の暗号スイートを表す再利用可能なオブジェクト。

イベント

ワークフローを使用して、イベント ビューアで表示できる特定のオカレンスに関する詳細の集合。イベントは、ネットワークに対する攻撃、検出されたネットワーク アセットの変更、組織のセキュリティおよびネットワーク利用のポリシーの違反などを表します。システムは、アプライアンスのヘルス ステータスの変更、Web インターフェイスの使用状況、ルール更新、および起動された修復に関する情報を含むイベントも生成します。また、「イベント」が特定のオカレンスを表していない場合でも、システムはイベントとして他の特定の情報を表示します。たとえば、イベント ビューアを使用して、検出されたホスト、アプリケーション、およびそれらの脆弱性に関する詳細情報を表示することができます。

イベント ストリーマ

eStreamer を参照してください。

イベント トラフィック チャネル

トラフィック チャネルを参照してください。

イベント ビューア

イベントの表示および操作を可能にするシステムのコンポーネント。イベント ビューアは、ワークフローを使用して、広範なイベント ビューや、目的のイベントだけを含む絞り込まれたイベント ビューを表示します。ワークフローをドリルダウンするか、または検索を使用して、イベント ビューのイベントを制限できます。

イベントしきい値

指定した時間内にイベントが生成される回数に基づいて、システムがログを記録したり、侵入イベントを表示したりする回数を制限する機能。同一のイベントが大量に発生して悩まされている場合には、イベントしきい値を使用します。

イベント抑制

特定の IP アドレスまたは IP アドレスの範囲によって侵入ルールがトリガーとして使用された場合に、抑制侵入イベントを使用できるようにする機能。イベント抑制は、誤検出を低減するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを送信する電子メール サーバがある場合、そのサーバによってトリガーとして使用されるルールのイベントを抑止することにより、本物の攻撃に対するイベントのみが表示されるようにすることができます。

インシデント

予想されるセキュリティ ポリシーの違反に関与している疑いのある 1 つ以上の侵入イベント。システムには、インシデントの調査に関連した情報の収集および処理に使用できるインシデント処理機能が備えられています。

インタラクティブ ブロック

ユーザが HTTP 応答ページのボタンをクリックして、最初にブロックされた Web サイトを続行できるようにするアクセス コントロール ルール アクション。

インテリジェンス フィード

シスコ VRT によりレピュテーションが低いと判定される IP アドレスのリストの集合。リストは定期的に更新されます。インテリジェンス フィードの各リストは特定のカテゴリ（オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）など）を表しています。アクセス コントロール ポリシーでは、セキュリティ インテリジェンスを使用して、すべてまたはいずれかのカテゴリをブラックリストに登録できます。インテリジェンス フィードは定期的に更新されるため、インテリジェンス フィードを使用することで、システムがネットワーク トラフィックのフィルタリングに最新の情報を使用することが保証されます。

インポート

アプライアンス間で各種設定を転送するために使用できる手法。同じ種類の別のアプライアンスから以前にエクスポートされた設定をインポートできます。

インライン インターフェイス

インライン展開でトラフィックを処理するように設定されたセンシング インターフェイス。インライン インターフェイスをインライン セットにペアで追加する必要があります。

インライン セット

インライン インターフェイスの 1 つ以上のペア。

インライン展開

管理対象デバイスがネットワーク上にインラインで配置される FireSIGHT システムの展開。この設定では、デバイスがネットワーク トラフィック フローに影響を与える可能性があります。トラフィック フローに影響を与えずに分析および応答できるパッシブ検出とは異なります。

ウィジェット（widget）

ダッシュボード ウィジェットを参照してください。

影響

侵入イベントに関する、侵入データ、ディスカバリ データ、および脆弱性の間の相関関係を示す番号付きインジケータ。たとえば、影響レベル 1（赤色の影響アイコン）は、ターゲット ホストが、侵入イベントによって表される攻撃に対して*脆弱*であることを意味します。影響レベル 2（オレンジ色の影響アイコン）は、*潜在的に脆弱*であることを意味します。ネットワーク検出ポリシーによってモニタされていないネットワーク上のホストに向けられた攻撃は、影響レベル 0（灰色の影響アイコン）になります。これは、防御センターがイベントの影響を判別できないことを示しています。

エクスポート

アプライアンスからアプライアンスへのさまざまな設定（ポリシーなど）を転送するために使用できる方法。1 つのアプライアンスから設定をエクスポートしたら、同じタイプの別のアプライアンスにその設定をインポートできます。

エンドポイント

ユーザが組織の高度なマルウェア防御戦略の一部として FireAMP コネクタをインストールするコンピュータまたはモバイル デバイス。

応答

相関ポリシー違反に対する反応（アラートまたは修復）。

侵害の兆候（IOC）

システムが FireAMP エンドポイント データをモニタ対象ネットワーク上のホストに関連付けるための機能。ネットワーク検出ポリシーで設定します。侵害を受けた可能性のあるホストには、そのステータスを示すタグが付けられます。このタグは、ホスト プロファイルや関連するイベント ビューで表示されます。

オブジェクト

名前を値（IP アドレスまたは URL など）に関連付ける再利用可能な設定。Web インターフェイスでその値を使用するときは、その名前のオブジェクトを代わりに使用できます。オブジェクト マネージャを使用してオブジェクトを作成します。ネットワーク オブジェクト、セキュリティ インテリジェンス オブジェクト、ポート オブジェクト、VLAN タグ オブジェクト、URL オブジェクト、アプリケーション フィルタ、変数セット、ファイル リスト、HA リンク インターフェイス、セキュリティ ゾーン、暗号スイート リスト、識別名オブジェクト、および PKI オブジェクトも参照してください。

オブジェクト マネージャ

オブジェクトおよびオブジェクト グループを管理する Web インターフェイスのページ。

オペレーティング システムのアイデンティティ

オペレーティング システム ベンダーと、ホスト上のオペレーティング システムのバージョンの詳細。

外部認証

ユーザが FireSIGHT システム アプライアンスにログインする際、外部に保存されたユーザ クレデンシャルを使用してユーザ名とパスワードを認証する方法（LDAP 認証や RADIUS 認証など）。内部認証と比較してください。

カスタム テーブル

FireSIGHT システムによって提供される事前定義された 2 つ以上のテーブルからのフィールドを組み合わせた、ユーザが構築できるテーブル。たとえば、新しいコンテキストで接続データを調べるために、ホスト属性テーブルのホストの重要度情報と接続データ テーブルの情報を組み合わせることができます。

カスタム トポロジ

ホスト、モバイル デバイス、およびネットワーク デバイス ネットワーク マップのサブネットを意味ある仕方で編成および識別することを可能にする機能。

カスタム フィンガープリント

フィンガープリントを参照してください。

カスタム ユーザ ロール

特殊なアクセス権限が付与されているユーザ ロール。カスタム ユーザ ロールには一連のメニューベースのアクセス許可およびシステム アクセス許可を含めることができます。またカスタム ユーザ ロールは完全に独自に作成することも、事前定義ユーザ ロールを基にすることもできます。

カスタム ワークフロー

組織の固有のニーズを満たすために作成するワークフロー。

カスタム検出リスト

SHA-256 ハッシュ値で表されたファイルのリスト。システムはこのリストにあるファイルを検出した場合、Collective Security Intelligence クラウドでのそのファイルの disposition が [クリーン(Clean)] であっても、そのファイルをマルウェアと見なしてマルウェア クラウド ルックアップを実行しません。

仮想 防御センター

仮想ホスティング環境の各自の機器に展開できる 防御センター。

仮想スイッチ

ネットワークを通過する着信トラフィックおよび発信トラフィックを処理するスイッチド インターフェイスのグループ。レイヤ 2 展開では、論理セグメントにネットワークを分割しながら、スタンドアロン ブロードキャスト ドメインとして機能するように管理対象デバイスで仮想スイッチを設定できます。仮想スイッチは、ホストからの Media Access Control(MAC)アドレスを使用してパケットの送信先を決定します。

仮想デバイス

仮想ホスティング環境の各自の機器に展開できる管理対象デバイス。仮想デバイスは、ハイ アベイラビリティ、クラスタリング、スタッキング、NAT、VPN、高速パス ルールなどのハードウェア ベースの機能をサポートしません。また、仮想デバイスを仮想スイッチまたは仮想ルータとして設定することはできません。

仮想ルータ

レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループ。レイヤ 3 展開環境では、宛先 IP アドレスに基づいてパケット転送を決定してパケットをルーティングするように、仮想ルータを設定できます。スタティック ルートを定義し、Routing Information Protocol(RIP)および Open Shortest Path First(OSPF)ダイナミック ルーティング プロトコルを設定し、ネットワーク アドレス変換(NAT)を実装できます。

仮想ローカル エリア ネットワーク(VLAN)

VLAN では、地理的な場所ではなく、部門や主な用途などの基準に基づいてホストがマッピングされます。モニタ対象ホストのホスト プロファイルには、そのホストに関連付けられた VLAN 情報が示されます。最も内側の VLAN タグの情報もさまざまなイベントに含まれます。システムでは、接続の VLAN タグに基づいて、アクセス制御を含む複数のタイプのトラフィック処理を実行できます。レイヤ 2 およびレイヤ 3 の展開では、VLAN タグ付きトラフィックを適切に処理するように、管理対象デバイスで仮想スイッチおよび仮想ルータを設定できます。

カテゴリ（category）

アプリケーション カテゴリ、ファイル カテゴリ、または URL カテゴリを参照してください。

監査イベント

FireSIGHT システムの特定のユーザ インタラクションを示すイベント。各監査イベントには、タイムスタンプ、イベントを生成したアクションを実行したユーザのユーザ名、送信元 IP アドレス、イベントを説明するテキストが含まれます。監査イベントは、監査ログに記録されます。

監査ログ

システムとのユーザ インタラクションの記録。監査ログは、監査イベントで構成されます。

管理インターフェイス

FireSIGHT システム アプライアンスを管理するために使用するネットワーク インターフェイス。ほとんどの展開環境では、管理インターフェイスが内部保護されたネットワークに接続されます。センシング インターフェイスと比較してください。仮想 防御センターおよびすべてのシリーズ 3 アプライアンスで、パフォーマンスを向上させるためにトラフィックをチャネルに分割するか、防御センターが異なるネットワークにトラフィックを分離できるように追加ネットワークへのルートを作成するよう、複数の管理インターフェイスを設定できます。また、別個のネットワークにトラフィック チャネルをルーティングして、スループット キャパシティを増やすこともできます。

管理対象デバイス

デバイスを参照してください。

管理トラフィック チャネル

トラフィック チャネルを参照してください。

基本ポリシー

カスタム ポリシーの基本ポリシー階層として機能する侵入ポリシーまたはネットワーク分析ポリシー。

基本ポリシー階層

侵入ポリシーまたはネットワーク分析ポリシーの最下層である組み込みレイヤ。基本ポリシーによって基本ポリシー階層の設定が決まるため、ポリシーのデフォルト設定となります。

キャプチャされたファイル

ネットワーク トラフィックで検出され、動的分析または Spero 分析用に Collective Security Intelligence クラウドへ送信するため、あるいはデバイスへのファイル ストレージのためにデバイスによってコピーされるファイル。

脅威スコア

ファイルを動的分析のために、Collective Security Intelligence クラウドに送信した結果としてファイルに割り当てられ、ファイルにマルウェアが含まれる可能性の尺度となる 1 ～ 100 の評価。

共通アクセス カード（CAC）

CAC 認証および許可に使用される米国国防総省発行の ID カード。

共有オブジェクトのルール

C ソース コードからコンパイルされたバイナリ モジュールとして提供される侵入ルール。共有オブジェクトのルールを使用して、標準テキスト ルールでは不可能な方法で攻撃を検出できます。共有オブジェクトのルールのルール キーワードおよび引数は変更できません。できるのは、ルールで使用される変数を変更したり、送信元と宛先のポートや IP アドレスなどの側面を変更したり、カスタム共有オブジェクトのルールとしてルールの新規インスタンスを保存したりすることに限られます。共有オブジェクト ルールのジェネレータ ID（GID）は 3 です。

共有レイヤ

その他のポリシーによる使用が許可された侵入ポリシーまたはネットワーク分析ポリシーのレイヤ。共有レイヤを使用するポリシーは、共有レイヤでの変更がコミットされたときに更新されます。共有レイヤは、その共有を許可するポリシーでのみ変更できます。共有レイヤを使用するポリシーでは共有レイヤは読み取り専用になります。

組み込みレイヤ

侵入ポリシーまたはネットワーク分析ポリシーの読み取り専用レイヤ。これらのポリシーには、常に組み込み基本ポリシー階層が含まれます。侵入ポリシーには組み込み FireSIGHT 推奨レイヤを含めることもできます。

クライアント

1 つのホストで実行され、一部の操作を別のホスト（サーバ）で実行するアプリケーション。クライアント アプリケーションとも呼ばれます。たとえば、電子メール クライアントでは電子メールを送受信できます。あるホスト上のユーザが別のホストにアクセスするために特定のクライアントを使用していることをシステムが検出すると、クライアントの名前とバージョン（該当する場合）などを含めてその情報をホスト プロファイルとネットワーク マップでレポートします。

クライアント アプリケーション

クライアントを参照してください。

クラウド サービス

Collective Security Intelligence クラウドを参照してください。

クラスタリング

2 つのピア シリーズ 3 デバイス間またはピア スタック間でネットワーキング機能と設定データの冗長性を実現する機能。クラスタリングによって、ポリシー適用、システム更新、および登録のための単一の論理システムが作成されます。冗長防御センターの設定を可能にするハイ アベイラビリティと比較してください。

クリーン リスト

SHA-256 ハッシュ値で表されたファイルのリスト。システムはこのリストにあるファイルを検出した場合、Collective Security Intelligence クラウドでのそのファイルの disposition が [マルウェア（Malware）] であっても、そのファイルをクリーンとして見なしてマルウェア クラウド ルックアップを実行しません。

クリップボード

後からインシデントに追加できる侵入イベントを最大 25,000 個までコピーできる保存エリア。

グローバル ブラックリスト

すべてのアクセス コントロール ポリシーのセキュリティ インテリジェンス ブラックリストにデフォルトで含められるセキュリティ インテリジェンス オブジェクト。グローバル ブラックリストはすべてのセキュリティ ゾーンに適用されます。ダッシュボード、Context Explorer、および多くのイベント ビューア ページで、IP アドレスのコンテキスト メニューを使用して個々の IP アドレスをグローバル ブラックリストに追加できます。

グローバル ホワイトリスト

すべてのアクセス コントロール ポリシーのセキュリティ インテリジェンス ホワイトリストにデフォルトで含められるセキュリティ インテリジェンス オブジェクト。グローバル ホワイトリストはすべてのセキュリティ ゾーンに適用されます。ダッシュボード、Context Explorer、および多くのイベント ビューアページで、IP アドレスのコンテキスト メニューを使用して個々の IP アドレスをグローバル ホワイトリストに追加できます。

現在のアイデンティティ

システムによって、特定のネットワーク アセットに対して正しい可能性が最も高いと見なされるオペレーティング システムまたはサーバのアイデンティティ。システムは多くの方法でこのデータを使用します。たとえば、統計の計算、脆弱性情報の割り当て、攻撃の影響の評価、および相関ルールの評価のために使用します。

現在のユーザ

システムがホストと関連付けるユーザ。ユーザがアクセス制御ユーザである場合、システムはそのホストとの間のトラフィックに対してユーザ制御を実行できます。ホストに関連付けられたアクセス制御ユーザがいない場合は、非アクセス制御ユーザがホストの現在のユーザとなることができます。ただし、アクセス制御ユーザがホストにログインした後は、別のアクセス制御ユーザがログインした場合のみ、現在のユーザが変更されます。

検出ポリシー

ネットワーク検出ポリシーを参照してください。

検出ルール

ネットワーク検出ポリシー内で、モニタするネットワークとゾーン、それらをモニタするために使用するデバイス（NetFlow 対応デバイスを含む）、およびモニタリング対象から除外するポートを指定します。各ルールは、モニタ対象ネットワークでホスト、ユーザ、またはアプリケーションを検出するかどうかも指定します。

公開キー

すべてのユーザが使用できる公開キー証明書に関連付けられた暗号キー。公開キーおよびペアにされた秘密キーは、セキュア ソケット レイヤ（SSL）と Transport Layer Security の暗号化および復号に使用されます。

公開キー インフラストラクチャ（PKI）

認証局が公開キー証明書およびペアにされた秘密キーを個々のユーザに対して発行する方法を管理するシステム。

公開キー証明書

証明書に保存された公開キーがそのユーザに属していることを裏付ける、認証局によって個々のユーザに対して発行されるデジタル ドキュメント。

高速パス ルール

限定された条件を使用して、分析の必要がないトラフィックが処理をバイパスできるようにデバイスのハードウェア レベルで設定するルール。

高度なマルウェア防御

略語は AMP。FireSIGHT システム のネットワーク ベースのマルウェア検出およびマルウェア ブロッキング機能です。FireAMP サブスクリプションが必要なシスコのエンドポイントベースの AMP ツールである FireAMP とこの機能を比較してください。

コマンド ライン インターフェイス(CLI)

シリーズ 3 および仮想デバイスの制限付きテキストベース インターフェイス。CLI ユーザが実行できるコマンドは、ユーザに割り当てられているアクセス レベルによって異なります。

コンテキスト メニュー

FireSIGHT システムの他の機能にアクセスするためにショートカットとして使用できる、Web インターフェイスの多くのページで使用可能なポップアップ メニュー。メニューの内容は、表示しているページ、調べている特定のデータ、ユーザ ロールなどの複数の要因によって異なります。

コンプライアンス ホワイトリスト

相関ルールと同様、ネットワーク トラフィックが相関ポリシーに違反していると見なされる場合に満たしているべき基準を指定する方法の 1 つ。どのオペレーティング システム、アプリケーション、およびプロトコルが特定のサブネットのホスト上で実行できるかを指定するコンプライアンス ホワイトリストは、防御センターを使用して設定できます。ホワイトリストに違反した場合に、アラートや修復のような応答を起動するように 防御センター を設定することもできます。コンプライアンス ホワイトリストは他のタイプのホワイトリストとは関連付けられないことに注意してください。

コンプライアンス ホワイトリスト イベント

ホワイトリスト イベントを参照してください。

コンプライアンス ホワイトリスト違反

ホワイトリスト違反を参照してください。

サードパーティの脆弱性

サードパーティから取得された脆弱性データ。組織でスクリプトを作成するか、またはコマンド ライン インポート ファイルを作成して、サードパーティ アプリケーションからネットワーク マップ データをインポートできる場合、システムの脆弱性データを補強するために、ホスト入力機能を使用してサードパーティの脆弱性データをインポートすることができます。

サーバ

アプリケーション プロトコル トラフィックで識別されるホスト上にインストールされたサーバ アプリケーション(クライアント アプリケーションと比較してください)。

サーバ アイデンティティ

ホスト上のサーバのアプリケーション プロトコルの種類、ベンダー、バージョンの詳細。

サーバ バナー

サーバの識別に役立つ追加情報を提供するサーバに関して検出された最初のパケットの最初の 256 バイト。システムは、初めてサーバが検出されたときに、一度だけサーバ バナーを収集します。

サーバ証明書

認証局によって発行される暗号化された証明書。サーバ アイデンティティの変更できない確認を提供します。任意の認証局に証明書を要求し、そのカスタム証明書をアプライアンスにアップロードできます。

最適化ポリシー

IP 最適化プリプロセッサ（ネットワーク分析ポリシーで設定）が、ターゲット ホストのオペレーティング システムに基づいて、フラグメント化された IP パケットを再構成する方法を示すサブポリシー。アダプティブ プロファイルは適応型最適化ポリシーを使用することに注意してください。

サブサーバ

同じホスト上の別のサーバによって呼び出されるサーバ。

ジェネレータ ID（GID）

システムのどのコンポーネントが侵入イベントを生成したかを示す番号。GID は、ルールのシグネチャ ID（Sid）が、ルールをトリガーとして使用するパケットのコンテキストを提供するのと同じ方法でイベントの種類を分類することによって、より効率的にイベントを分析するのに役立ちます。

時間枠

任意のイベント ビューにおけるイベントの時間的制約。それぞれのイベント ビューには、ユーザ設定に応じた異なるデフォルトの時間枠がある場合があります。すべてのイベント ビューが時間で制約されるわけではないことに注意してください。

しきい値

イベントしきい値を参照してください。

識別名オブジェクト

公開キー証明書のサブジェクトまたは発行元の識別名を表す再利用可能なオブジェクト。

シグネチャ ID（Sid）

各侵入ルールに割り当てられた固有の識別番号（別名 Snort ID）。新しいルールを作成するか、既存の標準テキスト ルールを変更すると、1,000,000 かそれより大きな SID が割り当てられます。FireSIGHT システムで提供される共有オブジェクトのルールおよび標準テキスト ルールの SID は、1,000,000 より小さくなります。また、プリプロセッサおよびデコーダは、SID を使用して、検出するさまざまな種類のパケットを識別します。

シスコ VRT

シスコ の脆弱性調査チーム。

システム ポリシー

メール リレー ホスト設定や時刻同期設定のような、展開内の複数のアプライアンスで同じになる可能性のある設定。システム ポリシーは、防御センターを使用して、Defense Center 自体または管理対象デバイスに適用します。

自動アプリケーション バイパス（AAB）

インターフェイスを通過するパケットを処理する時間を制限し、時間が超過したときにパケットが処理をバイパスすることを可能にする高度なデバイス設定。

修復

システムに対して行われる可能性のある攻撃の影響を軽減するアクション。修復を設定し、相関ポリシー内でそれらを相関ルールおよびコンプライアンス ホワイトリストと関連付けることにより、それらがトリガーとして使用されるときに、防御センターによって修復が起動されるようにすることができます。これにより、ユーザが攻撃に即時に対処できない場合でも攻撃の影響を自動的に緩和でき、またシステムが組織のセキュリティ ポリシーに準拠し続けるようにすることができます。防御センターには事前定義された修復モジュールが付属しています。柔軟性のある API を使用して、カスタム修復を作成することもできます。

修復インスタンス

修復モジュールの一連の設定。モジュールごとに複数のインスタンスを設定できます。たとえば、異なる相関ポリシーの違反に対し、同一のモジュールの、設定の違う異なるインスタンスを使用して対応することができます。修復インスタンスがトリガーとして使用されると、その結果実行されるアクションを修復と呼びます。

修復ステータス イベント

修復が起動すると、生成されるイベント。

修復モジュール

修復インスタンスと呼ばれる一連の設定を使用して修復を起動するプログラム。FireSIGHT システムには各種アクションを実行する複数の修復モジュールが付属しています。また、柔軟性のある API を使用して独自のモジュールを作成することもできます。

状態共有

デバイスまたはスタックのいずれかに障害が発生した場合に、ピアがトラフィック フローを中断することなく引き継ぐことができるようにするために、クラスタ化されたデバイスまたはスタックを同期できる機能。状態共有によって、厳密な TCP の適用、単方向のアクセス コントロール ルール、ブロッキングの永続化、および動的 NAT の適切なフェールオーバーが確実化されます。

証明書失効リスト(CRL)

アプライアンスのユーザ証明書を発行した認証局によって取り消された証明書のリスト。これによって、クライアント ブラウザの証明書チェックを使用して FireSIGHT システム Web インターフェイスへのアクセスを制限することができます。ユーザが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。SSL インスペクション中、デバイスは CRL の公開キー証明書を検出できますが、暗号化されたトラフィックを信頼しません。

シリーズ 2

FireSIGHT システムアプライアンスモデルの 2 番目のシリーズ。リソース、アーキテクチャ、ライセンス制限のため、シリーズ 2 アプライアンスでサポートされる機能セットは限定されています。シリーズ 2 デバイスには、3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500 および 3D9900 が含まれます。シリーズ 2 防御センターには、DC500、DC 1000、および DC3000 が含まれます。

シリーズ 3

FireSIGHT システムアプライアンスモデルの 3 番目の シリーズ。シリーズ 3 アプライアンスには、7000 シリーズおよび 8000 シリーズのデバイスと、DC750、DC1500、DC2000、DC3500 および DC4000 の防御センターが含まれます。

侵入

ネットワークで発生したセキュリティ違反、攻撃、またはエクスプロイト。

侵入イベント

侵入ポリシー違反を記録するイベント。侵入イベント データには、日付、時刻、エクスプロイトのタイプ、および攻撃とそのターゲットに関するコンテキスト情報が含まれます。

侵入検知と防御

ネットワーク トラフィックのセキュリティ ポリシー違反のモニタリング、およびインライン展開で悪意のあるトラフィックをブロックまたは変更する機能。FireSIGHT システムでは、ネットワーク分析ポリシーでトラフィックを前処理してから、侵入ポリシーをアクセス コントロール ルールまたはデフォルト アクションに関連付けるときに侵入検知および防御を実行します。

侵入ポリシー

侵入およびセキュリティ ポリシー違反についてネットワーク トラフィックを検査するために設定できる各種のコンポーネント。ネットワーク トラフィックがアクセス コントロール ルールの条件を満たす場合、侵入ポリシーでそのトラフィックを検査できます。また、侵入ポリシーをアクセス コントロール ポリシーのデフォルト アクションに関連付けることもできます。侵入ポリシーの主要コンポーネントは、トラフィックを検査する侵入ルール、およびネットワーク分析ポリシーで関連付けられたプリプロセッサ オプションのイベントを生成するプリプロセッサ ルールです。センシティブ データを検査したり、特別な侵入イベント処理を実行したりする詳細設定が可能なだけでなく、必要に応じて FireSIGHT 推奨レイヤを追加することもできます。侵入ポリシーは常に変数セットと組み合わせて使用します。

侵入ルール

モニタ対象のネットワーク トラフィックに適用される場合に、潜在的な侵入、セキュリティ ポリシー違反、およびセキュリティ違反を識別する一連のキーワードおよび引数。システムはルール条件に照らしてパケットを比較します。パケット データが条件に一致すると、ルールがトリガーされ、侵入イベントが生成されます。侵入ルールには、廃棄ルールとパス ルールが含まれます。

スイッチ

マルチポート ブリッジとして機能するネットワーク デバイス。システムはネットワーク検出を使用して、スイッチをブリッジとして識別します。また、管理対象デバイスを、2 つ以上のネットワークの間でパケット スイッチングを実行する仮想スイッチとして設定できます。

スイッチド インターフェイス

レイヤ 2 展開環境でトラフィックを切り替えるために使用するインターフェイス。タグなし 仮想ローカル エリア ネットワーク（VLAN）トラフィックを処理するための物理スイッチド インターフェイスと、指定の VLAN タグが付いたトラフィックを処理するための論理スイッチド インターフェイスを設定できます。

スケジュール タスク

1 回実行するか、または繰り返し定期的に実行するようにスケジュールできる管理タスク。

スタッキング

スタック構成の設定で 2 ～ 4 台の物理デバイスを接続することによって、ネットワーク セグメントで検査されるトラフィックの量を増加させることができる機能。スタック構成を確立するときに、各スタック構成のデバイスのリソースを 1 つの共有構成に統合します。

スタック

検出リソースを共有する、2 ～ 4 台の接続されたデバイス。

スヌーズ期間

相関ルールがトリガーとして使用された後に、システムがそのルールのトリガーを停止する間隔（秒、分、時間単位で指定される）。そのルールが再度違反されても、この期間内はトリガーしません。スヌーズ期間が終了したら、ルールを再びトリガーできるようになります（そしてトリガーとして使用された時点から新しいスヌーズ期間が開始します）。非アクティブな期間も参照してください。

脆弱性

ホストが影響を受けやすい特定のセキュリティ侵害を指す表現。防御センターは、それぞれのホストが影響を受けやすい脆弱性に関する情報をホストのホスト プロファイルに示します。また、脆弱性ネットワーク マップを使用して、モニタ対象ネットワーク全体でシステムが検出した脆弱性の概要を把握できます。ホストが特定のセキュリティ侵害に対して脆弱ではなくなったと判断した場合は、特定の脆弱性を非アクティブ化するか、または無効としてマークできます。

脆弱性 ID

特定の脆弱性に関連付けられた ID 番号。シスコの脆弱性データベースおよびサードパーティの脆弱性データベース（Bugtraq や CVE など）では、異なる脆弱性 ID の番号付け方式が使用されています。

脆弱性データベース

ホストが影響を受けやすい既知の脆弱性のデータベース。VDB とも呼ばれます。ユーザが特定のホストでネットワークのセキュリティ侵害のリスクが大きくなっているかどうかを判断できるように、システムは各ホストで検出されたオペレーティング システム、アプリケーション プロトコル、およびクライアントを VDB に関連付けます。VDB 更新には、新規の脆弱性と更新された脆弱性、および新規アプリケーション ディテクタと更新されたアプリケーション ディテクタが含まれることがあります。

脆弱性の詳細

脆弱性ワークフローの最後のページ。脆弱性の詳細には、技術的な詳細と既知のソリューションを含む特定の脆弱性に関する情報が示されます。

脆弱性マッピング

ディスカバリ データとの脆弱性情報の関連付け。これにより、影響の相関を実行できます。

正常性ポリシー

展開環境内のアプライアンスの正常性を検査するときに使用される条件。正常性ポリシーは、ヘルス モジュールを使用して、システムのハードウェアおよびソフトウェアが正しく動作しているかどうかを示します。デフォルトの正常性ポリシーを使用するか、または独自のポリシーを作成できます。

セキュア ソケット レイヤ(SSL)

Transport Layer Security プロトコルの基になった暗号化アプリケーション層プロトコル。SSL インスペクション機能を使用することにより、SSL プロトコルで暗号化されたトラフィックを復号できます。

セキュリティ インテリジェンス

送信元または宛先の IP アドレスに基づいて、アクセス コントロール ポリシーごとにネットワークを通過できるトラフィックを指定できる機能。特に、アクセス コントロール ルールによってトラフィックが分析される前に、特定の IP アドレスをブラックリストに登録する(アドレス間で送受信されるトラフィックを拒否する)必要がある場合に役立ちます。必要に応じて、セキュリティ インテリジェンス フィルタリングのモニタ設定を使用して、システムでブラックリストに追加された接続を分析し、さらにブラックリストとの一致を記録させることができます。

セキュリティ インテリジェンス イベント

セキュリティ インテリジェンス ブラックリストによってブロックまたはモニタされるトラフィックが生成する接続イベント。通常の接続イベントとは別に、セキュリティ インテリジェンス イベントを表示および対話操作できます。

セキュリティ インテリジェンス オブジェクト

1 つ以上の IP アドレスを表す単一の設定。これは、アクセス コントロール ポリシーのセキュリティ インテリジェンス ブラックリストおよびセキュリティ インテリジェンス ホワイトリストに追加します。セキュリティ インテリジェンス オブジェクトには、セキュリティ インテリジェンス リスト、セキュリティ インテリジェンス フィード、およびネットワーク オブジェクトとグループが含まれます。グローバル ブラックリスト、グローバル ホワイトリスト、およびインテリジェンス フィードのカテゴリは、セキュリティ インテリジェンス オブジェクトと見なされます。

セキュリティ インテリジェンス フィード

セキュリティ インテリジェンス オブジェクトの種類の 1 つ。ユーザが設定する間隔で、システムが定期的にダウンロードする IP アドレスの動的なコレクション。フィードは定期的に更新されるため、フィードを使用することで、システムがセキュリティ インテリジェンス機能を使用したネットワーク トラフィックのフィルタリングに最新の情報を使用することが確実化されます。インテリジェンス フィードも参照してください。

セキュリティ インテリジェンス ブラックリスト

アクセス コントロール ポリシーで、トラフィックをアクセス コントロール ルールによって分析する前に、対象のホストとの間のトラフィックを拒否できるようにする IP アドレスのリスト。ブラックリストはセキュリティ インテリジェンス オブジェクトで構成されます。これには、グローバル ブラックリストも含まれます。アクセス コントロール ポリシーのセキュリティ インテリジェンス ホワイトリストは、ブラックリストよりも優先されます。

セキュリティ インテリジェンス ホワイトリスト

アクセス コントロール ポリシーで、アクセス コントロール ルールを使用するホストとの間のトラフィックがポリシーによって検査されるように強制する（つまり、セキュリティ インテリジェンスを使用してトラフィックを拒否しないようにする）ための IP アドレスのリスト。ポリシーのホワイトリストはセキュリティ インテリジェンス ブラックリストよりも優先されるため、ブラックリストの微調整に使用できます。ホワイトリストは、グローバル ホワイトリストで構成されます。これには、セキュリティ インテリジェンス オブジェクトも含まれます。

セキュリティ インテリジェンス リスト

ユーザがセキュリティ インテリジェンス オブジェクトとして防御センターに手動でアップロードする IP アドレスのシンプルで静的なコレクション。セキュリティ インテリジェンス フィード、グローバル ブラックリスト、およびグローバル ホワイトリストを補強および微調整するために、このリストを使用します。

セキュリティ ゾーン

さまざまなポリシーおよび設定でトラフィック フローを管理および分類するために使用できる 1 つ以上のインライン、パッシブ、スイッチド、またはルーテッド インターフェイスのグループ。単一ゾーンのインターフェイスは、複数デバイスのにまたがる場合があります。単一のデバイスに対して複数のセキュリティ ゾーンを設定することもできます。トラフィックをセキュリティ ゾーンと照合するには、少なくとも 1 つのインターフェイスをそのセキュリティ ゾーンに割り当てる必要があり、各インターフェイスは 1 つのゾーンのみに属することができます。

セキュリティ ポリシー

ネットワークを保護するための組織のガイドライン。たとえば、セキュリティ ポリシーではワイヤレス アクセス ポイントの使用が禁止されることがあります。セキュリティ ポリシーにはアクセプタブル ユース ポリシー（AUP）も含まれていることがあります。AUP は、組織のシステムの使用方法に関するガイドラインを従業員に提供します。

セキュリティ ポリシー違反

セキュリティ違反、攻撃、エクスプロイト、またはその他のネットワークの不正使用。

接続

2 台のホスト間のモニタ対象セッション。NetFlow 対応デバイスからのインポート接続データだけでなく、FireSIGHT システム管理対象デバイスによって検出された接続もログに記録できます。

接続イベント

システムがモニタ対象ホストとその他のホストの間で接続を検出したときに生成されるイベント。セキュリティ インテリジェンス イベントは、特別な種類の接続イベントです。接続イベントには、検出されたトラフィックに関する情報が含まれます。さまざまな設定を使用して、記録する接続とタイミング、およびそのデータの保存先に関するきめ細かい制御が可能です。管理対象デバイスによって接続が検出された場合、ブロック解除された接続のログは開始時および終了時に記録できますが、ブロックされた接続の多くについては開始時にのみ記録できます。これらの接続のログは、防御センター データベースに記録できます。ルールまたはデフォルト アクションに応じて、接続イベントのログを外部 Syslog または SNMP トラップ サーバに記録することもできます。NetFlow レコードには接続の終了が記録され、常にデータベースに保存されます。

接続グラフ

グラフ形式で接続イベントを表示する方法。

接続サマリー

5 分間隔で集約される接続データ。システムは接続サマリーを使用して接続グラフとトラフィック プロファイルを作成します。データが集約されるためには、複数の接続が接続の終了を表し、送信元と宛先の IP アドレスが同じで、応答側（宛先）ホストで同じポートを使用している必要があります。それらは同じプロトコル（TCP または UDP）とアプリケーション プロトコルを使用している必要があります。また、同じ管理対象デバイスによって検出されるか、同じ NetFlow 対応デバイスによってエクスポートされている必要があります。

接続トラッカー

ルールの最初の基準が満たされた後、システムが特定の接続の追跡を開始するように、相関ルールを制約する 1 つ以上の条件。次にルールがトリガーされるのは、追跡された接続がさらに基準を満たした場合のみです。

接続ログ

接続イベントを参照してください。

設定（インポートまたはエクスポート用）

ポリシーやカスタム ワークフローなどの一連の設定。アプライアンス上に作成され、そのアプライアンスからエクスポートしたり、別のアプライアンスがインポートしたりできます。

設定可能なバイパス

バイパス モードを設定できるようにするインライン セットの特性。

センシング インターフェイス

ネットワーク セグメントのモニタリングに使用するデバイス上のネットワーク インターフェイス。管理インターフェイスと比較してください。

相関

ネットワークの脅威にリアルタイムで対応する相関ポリシーを構築するために使用できる機能。相関の修復コンポーネントは、ポリシー違反に対応する独自のカスタム修復モジュールを作成してアップロードすることを可能にする柔軟な API を提供します。

相関イベント

相関ルールがトリガーとして使用されると、防御センターよって生成されるイベント。ホワイトリスト イベント（ホワイトリスト違反より生成される）は、特別な種類の相関イベントであることに注意してください。

相関ポリシー

相関ルールおよびコンプライアンス ホワイトリストを使用して、セキュリティ ポリシー違反に相当するネットワーク アクティビティを示すポリシー。ポリシー内の各ルールまたはホワイトリストに対する応答を指定できます。

相関ルール

コンプライアンス ホワイトリストと同様、ネットワーク トラフィックが相関ポリシーに違反していると見なされる場合に満たしているべき基準を指定する方法の 1 つ。防御センターを使用して、特定のイベントが発生したとき、またはネットワーク トラフィックがトラフィック プロファイルに示された通常のネットワーク トラフィック パターンから逸脱しているときにトリガーとして使用される（かつ相関イベントを生成する）相関ルールを設定できます。ホスト プロファイル条件、接続トラッカー、スヌーズ期間、および非アクティブな期間で相関ルールを制約できます。相関ルールのトリガー時にアラートや修復などの応答を起動するように防御センターを設定することもできます。

ゾーン

セキュリティ ゾーンを参照してください。

ターゲット デバイス

ポリシー ターゲットを参照してください。

楕円曲線（EC）暗号化

有限フィールドのランダムな楕円曲線上にある計算ポイントに基づく暗号化方式。RSA 暗号化とは対照的な暗号です。

タグ（アプリケーション）

アプリケーション タグを参照してください。

タスク キュー

アプライアンスが実行する必要があるジョブのキュー。ポリシーを適用し、ソフトウェア更新をインストールし、他の長時間かかるジョブを実行すると、ジョブがキューに入れられ、ジョブのステータスが [タスクのステータス（Task Status）] ページに表示されます。[タスクのステータス（Task Status）] ページにはジョブの詳細なリストが表示され、ジョブのステータスを更新するために 10 秒ごとに更新されます。

ダッシュボード

現在のシステム ステータスを一目で理解できるビューを提供するディスプレイ。これには、システムによって収集され、生成されるイベントに関するデータが含まれます。システムによって提供されるダッシュボードを補強するために、選択したダッシュボード ウィジェットを組み込んだ複数のカスタム ダッシュボードを作成できます。モニタ対象のネットワークの状態と機能を、幅広の簡潔かつカラフルな図で示す Context Explorer と比較してください。

ダッシュボード ウィジェット

FireSIGHT システムの状況を把握するための小型の自己完結型ダッシュボード コンポーネント。

タップ モード

ネットワーク トラフィック フローがデバイスを通過する代わりに、各パケットのコピーが分析され、ネットワーク トラフィック フローが影響を受けない、シリーズ 3 デバイスおよび 3D9900 で使用可能な拡張インライン セットオプション。パケット自体ではなくパケットのコピーを処理するため、トラフィックをドロップ、変更、またはブロックするようにアクセス制御および侵入ポリシーを設定している場合でも、デバイスはパケット ストリームに影響しません。

地理位置情報

モニタリング対象のネットワークのトラフィックで検出されたルーティング可能な IP アドレスの位置情報ソースに関するデータ（接続タイプ、インターネット サービス プロバイダーなど）を提供する機能。イベントおよびホスト プロファイルで地理位置情報を表示し、アクセス コントロール ポリシーまたは SSL ポリシーのトラフィック フィルタリングに使用できます。

地理位置情報データベース（GeoDB）

ルーティング可能な IP アドレスに関連付けられた既知の地理位置情報データを格納し、定期的に更新されるデータベース。

ディスカバリ

管理対象デバイスを使用してネットワークをモニタし、ネットワークの完全で永続的なビューを提供する、FireSIGHT システムのコンポーネント。ネットワーク検出は、ネットワーク上のホスト（ネットワーク デバイスとモバイル デバイスを含む）の数と種類、およびそれらのホストのオペレーティング システム、アクティブなアプリケーション、オープン ポートを判別します。ネットワーク上のユーザ アクティビティをモニタするように管理対象デバイスを設定することもできます。これにより、ポリシー違反、攻撃、またはネットワークの脆弱性の源を識別できます。

ディスカバリ イベント

新しいアセットまたは既存のアセットに対する変更のディスカバリの詳細を示すイベント。ホスト入力イベントは、特別な種類のディスカバリ イベントです。「ディスカバリ イベント」は、ディスカバリ データまたは脆弱性の情報を意味する場合があります。

ディスカバリ データ

ディスカバリ機能を使用して収集されるネットワーク アセットとトラフィック フローを絞り込むための、ホスト、ユーザ、およびアプリケーションの情報。

データ コリレータ

システムによって収集されたデータを使用して、防御センター上でイベントを生成し、ネットワーク マップを作成するプログラム。

データベース アクセス

サードパーティ クライアントによる防御センターデータベースへの読み取り専用アクセスを許可する機能。

テーブル ビュー

イベント情報を表示するワークフローページの 1 つの種類。データベース テーブルの各フィールドに対して 1 列があります。イベント分析を実行する際は、目的のイベントに関する詳細を表示するテーブル ビューに移動する前に、ドリルダウン ページを使用して、調査するイベントを制約できます。多くの場合、テーブル ビューはシステム付属のワークフローの最後から 2 番目のページです。

適用

ポリシーまたはそのポリシーに対する変更を反映するために実行するアクション。ほとんどのポリシーは、防御センターから管理対象デバイスに適用します。ただし、相関ポリシーは管理対象デバイスの設定への変更に関与しないため、このポリシーはアクティブにしたり非アクティブにしたりします。

デコーダ

スニッフィングされたパケットをプリプロセッサが認識できる形式に変換する侵入検知と防御のコンポーネント。ネットワーク分析ポリシーで設定されます。

デバイス

物理的にフォールトトレラントな専用アプライアンス（Cisco ASA with FirePOWER Services を含む）。スループットの範囲内、または同じ多くの機能があるソフトウェアベースの展開で使用できます。デバイスで有効にするライセンス機能に応じて、これらを使用してトラフィックを受動的にモニタし、ネットワーク アセット、アプリケーション トラフィック、およびユーザ アクティビティの全体的なマップを作成したり、アクセス制御を実行したりすることができます。また、多くのデバイスでスイッチング、ルーティング（DHCP リレーと NAT を含む）、および VPN を実行できます。デバイスは 防御センター を使用して管理する必要があります。

デバイス クラスタリング

クラスタリングを参照してください。

デバイス スタッキング

スタッキングを参照してください。

デフォルト アクション

アクセス コントロール ポリシーまたは SSL ポリシーの一部で、ポリシーのモニタ以外のルールの条件を満たさないトラフィックを処理、検査、および記録する方法を指定するアクション。

動的分析

マルウェア分析のために、デバイスから Collective Security Intelligence クラウドにキャプチャされたファイルを送信する方法。クラウドはテスト環境でファイルを実行し、脅威スコアと動的分析サマリー レポートを防御センターに返します。動的分析サマリー レポートから、VRT 分析レポートも表示できます。

動的分析サマリー レポート

Collective Security Intelligence クラウドが脅威スコアをファイルに割り当てた理由（動的分析時に発見されたすべての脅威、およびファイルをテスト環境で実行したときに検出された追加のプロセスを含む）のサマリー。ここから、VRT 分析レポートを表示することもできます。

動的ルール状態

ルールに一致するトラフィックで検出されたレートの異常に応答して一定期間設定される侵入ルール状態。

トラフィック チャネル

管理トラフィックまたはイベント トラフィックのいずれかを伝送するため、シリーズ 3 のアプライアンスまたは仮想 防御センターの管理インターフェイスで設定できる接続。イベント トラフィック チャネルは、管理対象デバイスのネットワーク セグメントで生成されたイベント データだけを伝送し、管理トラフィック チャネルは内部で生成されたトラフィック（つまり、防御センターとデバイス間の管理トラフィック）だけを伝送します。管理インターフェイスを参照してください。

トラフィック プロファイル

指定した期間にログに記録される接続イベントに基づいた、ネットワーク上のトラフィックのプロファイル。モニタ対象ネットワーク セグメントのすべてのトラフィックを使用してプロファイルを作成することも、より対象を絞ってプロファイルを作成することもできます。次に、相関機能を使用し、既存のプロファイルに照らして新しいトラフィックを評価することによって、異常なネットワーク トラフィックを検出することができます。

トランスペアレント インライン モード

デバイスが「Bump In The Wire」として動作できるようにし、また認識するすべてのネットワーク トラフィックを、その送信元と宛先に関係なく転送できるようにする拡張インライン セットオプション。

ドリルダウン ページ

イベント ビューを制約するために使用される中間ワークフローページ。通常、ドリルダウン ページは、ページまたはテーブル ビューをさらに詳細に絞り込むために選択できる制約を提供します。

ドロップ イベント

廃棄ルールがトリガーとして使用されると生成される侵入イベント。イベント ビューアでは、ドロップ イベントは黒色の下矢印でマークされます。

内部認証

アプライアンス上のローカル データベースにユーザ クレデンシャルを保存する認証方式。ユーザがアプライアンスにログインする際に、ユーザ名およびパスワードが、データベース内の情報と照合されます。外部認証と比較してください。

認証オブジェクト

FireSIGHT システムの Web インターフェイスに対する外部認証（RADIUS または LDAP）を有効にするため、外部認証サーバに接続できるようにする設定の集合。

認証局

サーバ証明書またはユーザの公開キー証明書の作成に使用される証明書発行元。サーバおよびユーザの証明書によって、サーバ アイデンティティまたはユーザ アイデンティティの追加確認が行われます。

ネットワーク オブジェクト

1 つ以上の IP アドレス、CIDR ブロック、またはプレフィックス長を表す再利用可能なオブジェクト。

ネットワーク デバイス

FireSIGHT システムで、ブリッジ、ルータ、NAT デバイス、またはロード バランサとして識別されるホスト。

ネットワーク ファイル トラジェクトリ

ホストがネットワークでファイルを転送する際のファイル パスのビジュアル表現。SHA-256 ハッシュ値に関連付けられたファイルの場合、伝搬経路マップには、ファイルを転送したすべてのホストの IP アドレス、ファイルが検出された時間、ファイルのマルウェアの性質、関連するファイル イベント、マルウェア イベントなどが表示されます。

ネットワーク マップ

ネットワークを詳細に表現したもの。ネットワーク マップによって、ネットワークで実行するホスト、モバイル デバイス、およびネットワーク デバイス、またそれらに関連するホスト属性、アプリケーション プロトコル、および脆弱性の観点からネットワーク トポロジを表示することができます。

ネットワーク検出

ディスカバリを参照してください。

ネットワーク検出ポリシー

システムが特定のネットワーク セグメント（NetFlow 対応デバイスによりモニタされるネットワークを含む）について収集する、ディスカバリ データの種類（ホスト、ユーザ、およびアプリケーションデータを含む）を指定するポリシー。ネットワーク検出ポリシーは、ID の競合の解決設定、アクティブ検出のソースの優先度、および侵害の兆候（IOC）も管理します。

ネットワーク分析ポリシー

侵入ポリシーによって後で分析できるように、ネットワーク トラフィックをデコード、標準化、および前処理するように設定できるさまざまなプリプロセッサ。デフォルトでは、システム付属の 1 つのネットワーク分析ポリシーが、アクセス コントロール ポリシーによって処理されたすべてのトラフィックを前処理します。ただし、この前処理を実行するカスタム ネットワーク分析ポリシーを選択することもできます。上級ユーザは、複数のカスタム ネットワーク分析ポリシーでセキュリティ ゾーン、ネットワーク、または VLAN タグに基づいてトラフィックを前処理できる、ネットワーク分析ルールを使用できます。

ネットワーク分析ルール

FireSIGHT システムの上級ユーザが複数のカスタム ネットワーク分析ポリシーを使用して対象を絞った前処理を実行するために使用できる一連の条件。ネットワーク分析ルールは、アクセス コントロール ポリシーの詳細オプションとして設定します。

ハイ アベイラビリティ

デバイスのグループを管理するように冗長物理防御センターを設定できる機能。イベント データは管理対象デバイスから両方の防御センターにストリームされ、ほとんどの設定要素が両方の防御センターに保持されます。プライマリ防御センターに障害が発生した場合は、セカンダリ

防御センターを使用して、中断することなくネットワークをモニタできます。冗長なデバイスを指定できるクラスタリングと比較してください。

廃棄ルール

ルール状態が [ドロップしてイベントを生成する(Drop and Generate Events)] に設定された侵入ルール。悪意のあるパケットによってインライン展開のルールがトリガーとして使用された場合、ユーザが適用した侵入ポリシーが [インライン時にドロップ(drop when inline)] に設定されていれば、システムはそのパケットをドロップし、侵入イベント(具体的には、ドロップ イベント)を生成します。

バイパス モード

インライン セットのセンシング インターフェイスが何らかの理由で失敗し場合に、トラフィックがフローを続行することを許可するインライン セットの特性。

ハイブリッド インターフェイス

システムが仮想ルータと仮想スイッチの間のトラフィックをブリッジングできるようにする、管理対象デバイス上の論理インターフェイス。

パケット ビュー

侵入ルールをトリガーしたパケット、または侵入イベントを生成したプリプロセッサに関する詳細情報を提供する、ワークフローページの 1 つの種類。パケット ビューは、侵入イベントに基づくワークフローの最後のページです。

パス ルール

トリガーとして使用されたときに、侵入イベントを生成せず、またルールをトリガーしたパケットの詳細を記録しない侵入ルール。侵入ルールを無効にする代わりに、パス ルールを使用することによって、特定の状況で特定の基準を満たすパケットがイベントを生成しないようにできます。廃棄ルールと比較してください。

派生フィンガープリント

システムにより、パッシブに収集されたすべてのホストのフィンガープリントから作成されるオペレーティング システムのフィンガープリント。収集された各フィンガープリントの信頼値と、アイデンティティ間の裏付けとなるフィンガープリント データの量を使用して最も可能性の高いアイデンティティを計算する式を適用することにより作成されます。

パッシブ インターフェイス

パッシブ展開環境でトラフィックを分析するように設定されているセンシング インターフェイス。

パッシブ検出

管理対象デバイスによってパッシブに収集されたトラフィックの分析によるディスカバリ データのコレクション。アクティブ検出と比較してください。

非アクセス制御ユーザ

ユーザ エージェントまたは管理対象デバイスのいずれかによって検出された、アクセス制御には使用されないユーザ。非アクセス制御ユーザは、ホストにログインしているアクセス制御ユーザがいない場合のみ、そのホストの現在のユーザになることができます。

非アクティブな期間

相関ルールがトリガーとして使用されない間隔。非アクティブな期間の時間、頻度、および期間を設定できます。スヌーズ期間も参照してください。

ビジネスとの関連性

アプリケーションが、娯楽目的ではなく、組織の事業運営のコンテキスト内で使用される可能性。アプリケーションのビジネスとの関連性は、Very Low から Very High までの範囲です。

非バイパス モード

インライン セットのセンシング インターフェイスが何らかの理由で失敗し場合に、トラフィックをブロックするインライン セットの特性。

秘密キー

ペアにされた公開キー証明書の所有者にのみ知らされる暗号キー。公開キーおよび秘密キーは、セキュア ソケット レイヤ（SSL）と Transport Layer Security の暗号化および復号に使用されます。

標準テキスト ルール

ルール エディタで使用可能な ID、キーワード、および引数に基づいて作成された侵入ルール。独自のカスタム標準テキスト ルールを作成し、シスコが提供する標準テキスト ルールを変更できます。標準テキスト ルールのジェネレータ ID（GID）は 1 です。

ファイル イベント

管理対象デバイスによってネットワーク トラフィックで検出されるファイルを表すイベント。

ファイル カテゴリ

グラフィック、実行可能ファイル、アーカイブなど、ファイル タイプの一般的な分類。

ファイル キャプチャ

キャプチャされたファイルを参照してください。

ファイル ストレージ

保存済みファイルを参照してください。

ファイル タイプ

PDF、EXE、MP3 など、特定のファイル形式タイプ。

ファイル トラジェクトリ

ネットワーク ファイル トラジェクトリを参照してください。

ファイル ポリシー

システムがファイル制御とネットワークベースの高度なマルウェア防御を実行するために使用するポリシー。ファイル ルールが組み込まれたファイル ポリシーは、アクセス コントロール ポリシー内のアクセス コントロール ルールによって呼び出されます。

ファイル リスト

クリーン リストおよびカスタム検出リスト を参照してください。

ファイル ルール

ネットワーク トラフィックを調べるために、FireSIGHT システムが使用するファイル ポリシー内の一連の基準。送信されたファイルがルールの基準と一致した場合、ルールがトリガーとして使用され、ファイル イベントが生成されます。ファイル ルール アクションによって、(ファイル タイプまたはマルウェアの性質に基づいて) ファイルをブロックするか、単純にファイルを通過させて送信をログに記録するかが決まります。

ファイル ルール アクション

システムがファイル ルールの条件を満たすファイルをどのように処理するかを決定する設定。特定のファイル タイプを検出してそれについてのアラートを出すことや、それらのファイルの送信をブロックすることができます。これらのファイル タイプのサブセットでマルウェア クラウド ルックアップを実行することも、マルウェアの性質に基づいてこれらのファイルの送信をブロックすることもできます。

ファイル制御

アクセス制御の一部であり、ネットワークを通過できるファイル タイプを指定し、ログに記録できるようにする機能。

ファイルの性質

マルウェアの性質を参照してください。

フィード

セキュリティ インテリジェンス フィードを参照してください。

フィンガープリント

ホストのオペレーティング システムを識別するために、システムが特定のパケット ヘッダー値やネットワーク トラフィックのその他の固有データと比較する確立された定義。システムがホストのオペレーティング システムを誤って識別したり、識別できなかったりする場合は、ホストを識別するカスタム フィンガープリントを作成できます。

フェールセーフ

内部トラフィック バッファがいっぱいになった場合に、パケットが処理をバイパスして、そのデバイスの終わりまで続行することを可能にするインライン セットの特性。

複雑な制約

特定のイベントのすべての条件を使用してイベントのクエリを制約するイベント ビューまたはイベント検索の制約セット。

ブックマーク

イベント分析の特定の場所と時間への保存されたリンク。ブックマークは、使用しているワークフロー、表示しているワークフローの一部、表示しているワークフロー内のページ数、選択した時間枠、無効にした列、および課した制約に関する情報を保持します。

物理インターフェイス

NetMod の物理ポートを表すインターフェイス。

不明なホスト

システムによってトラフィックが分析されたが、既知のどのフィンガープリントにもオペレーティング システムが一致しないホスト。未確認ホストと比較してください。

プライベート検索

ユーザ アカウントに関連付けられた特定のテーブルの検索基準の名前付きセット。ユーザ自身か管理者アクセス権を持つユーザのみがそのユーザのプライベート検索を使用できます。

ブラックリスト

ヘルス モニタ ブラックリストまたはセキュリティ インテリジェンス ブラックリストを参照してください。

プリプロセッサ

侵入およびエクスプロイトに関してさらに検査するようにトラフィックを準備するシステムのコンポーネント。プリプロセッサはトラフィックを正規化し、不適切なヘッダー オプションの特定、IP データグラムの最適化、TCP ステートフル インスペクションおよびストリーム再構成の提供、チェックサムの検証によって、ネットワーク層プロトコルおよびトランスポート層プロトコルの異常を特定するのに役立ちます。プリプロセッサは、特定の種類のパケット データを、システムが分析できる形式に変換することもできます。これらのプリプロセッサは、データ正規化のプリプロセッサ、またはアプリケーション層プロトコル プリプロセッサと呼ばれます。アプリケーション層プロトコル エンコーディングを正規化することで、システムは、データを表す方法が異なるパケットに同じコンテンツ関連侵入ルールを効果的に適用し、有意義な結果を得ることができます。プリプロセッサは、パケットがユーザが設定したプリプロセッサ オプションをトリガーとして使用するたびに、プリプロセッサ イベントを生成します。プリプロセッサの設定には特定の専門知識が必要で、通常はほとんどまたはまったく変更する必要がありません。さらに、すべての展開環境に共通するものではありません。

プリプロセッサ イベント

パケットが指定されたプリプロセッサオプションをトリガーとして使用すると生成される侵入イベントの 1 つの種類。プリプロセッサ イベントは、異常なプロトコルのエクスプロイトを検出するのに役立ちます。

プリプロセッサ ルール

プリプロセッサまたはポートスキャン フロー ディテクタに関連付けられている侵入ルール。イベントが生成されるようにするには、プリプロセッサ ルールを有効にする必要があります。プリプロセッサ ルールにはプリプロセッサ固有のジェネレータ ID（GID）があります。

ヘルス イベント

展開内のいずれかのアプライアンスがヘルス モジュールで指定されたパフォーマンス基準を満たす（または満たしていない）ときに生成されるイベント。ヘルス イベントによっても、アラートが生成される場合があります。

ヘルス モジュール

展開内のアプライアンスの特定のパフォーマンスの側面（CPU 使用率や利用可能なディスク容量）のテスト。正常性ポリシーでユーザが有効にするヘルス モジュールは、ユーザがモニタするパフォーマンスの側面が特定のレベルに達した場合に、ヘルス イベントを生成します。

ヘルス モニタ

展開内のアプライアンスのパフォーマンスを継続的にモニタする機能。ヘルス モニタは、適用された正常性ポリシー内のヘルス モジュールを使用して、アプライアンスをテストします。

ヘルス モニタ ブラックリスト

不要なヘルス イベントの生成を防止するため、ヘルス モニタリングを部分的に一時無効にする設定。アプライアンスのグループ、単一のアプライアンス、または特定のヘルス モジュールのモニタリングを無効にすることができます。

変更調整レポート

過去 24 時間に行われたシステム変更すべての詳細レポート。新しい設定が保存されるたびに作成されるスナップショットに基づきます。毎日指定した時間に、それらのレポートを電子メールで送信するようにシステムを設定できます。

変数

侵入ルールで一般に使用される値の表現。FireSIGHT システムは、変数セットに編成された事前設定済みの変数を使用してネットワークおよびポート番号を定義します。複数のルールでこれらの値をハードコーディングするのではなく、ネットワーク環境を正確に反映するようにルールを調整するには、変数の値を変更できます。

変数セット

各侵入ポリシーで有効になっている侵入ルールをネットワーク トラフィックに厳密に一致させるために調整できるよう、侵入ポリシーにリンクさせる変数設定の集合。

防御センター

デバイスを管理し、それらが生成したイベントを自動的に集約し、関連付けることができる一元管理ポイント。

ポート オブジェクト

トランスポート層プロトコル（TCP、UDP、ICMP など）を使用するオープン ポートを表す再利用可能なオブジェクト。

保護されたネットワーク

ファイアウォールなどのデバイスによって他のネットワークのユーザから保護されている組織の内部ネットワーク。システムによって提供される侵入ルールの多くは、変数を使用して保護されたネットワークと保護されていない（または外部）ネットワークを定義します。

ホスト

一意の IP アドレスが割り当てられているネットワーク接続デバイス。FireSIGHT システム では、ホストとは、特定されたホストのうち、モバイル デバイス、ブリッジ、ルータ、NAT デバイス、またはロード バランサのいずれにも分類されないものです。

ホスト ビュー

ディスカバリ イベントまたはネットワーク アセットを表示するワークフローの最後のページ。ホスト ビューは、表示しているイベントやアセットに関連するホストのホスト プロファイルを表示します。

ホスト プロファイル

特定の検出されたホストに関する収集された情報。これには、ホストの名前やオペレーティング システム、またホストで実行されているプロトコルやアプリケーションなどのホストに関する一般情報が含まれます。ホスト プロファイルには、そのホストに関するユーザ履歴、ホスト属性、仮想ローカル エリア ネットワーク(VLAN)情報、該当するホワイトリスト違反、検出された脆弱性、侵害の兆候(IOC)、およびスキャン結果も含まれる場合があります。

ホスト プロファイル条件

トラフィック プロファイルまたは相関ルールで設定される制約。相関ルール内のホスト プロファイル条件は、ホストが特定の基準を満たす場合のみ、防御センターが相関イベントを生成することを指定します。トラフィック プロファイル内のホスト プロファイル条件は、プロファイルが作成されるホストを制限します。

ホスト属性

システムで検出されるホストに関する情報を提供し、ネットワーク環境で重要になる方法でそれらのホストを分類するために使用できるツール。システムには、2 種類の事前定義されたホスト属性(ホストの重要度とメモ)と、それぞれのアクティブなコンプライアンス ホワイトリストとの各ホストのコンプライアンスを示すホスト属性があります。独自のホスト属性を作成することもできます。

ホスト入力

ネットワーク マップの情報を増やすために、スクリプトまたはコマンド ライン ファイルを使用してサードパーティ ソースからデータをインポートできる機能。Web インターフェイスは、いくつかのホスト入力機能を提供します。オペレーティング システムやアプリケーション プロトコル ID の変更、脆弱性の有効化または無効化、ネットワーク マップからのさまざまな項目(クライアントとサーバのポートなど)の削除を実行できます。

ホスト入力イベント

ホスト入力機能を使用するときに生成される、ディスカバリ イベントの一種。ホスト入力イベントとパッシブ ディスカバリ イベントは相関ルールを作成するときには区別されますが、通常は、これらのイベントは同じように処理されます。

ホストの重要度

システムによって検出される特定のホストのビジネス重要度(重要性)を示すホスト属性。

ホスト履歴

ユーザ アクティビティの過去 24 時間のグラフィカル表示。ユーザのユーザ詳細で表示できるホスト履歴には、棒グラフで表現されるおおよそのログインおよびログアウトの時間とともに、ユーザがログインしたホストの IP アドレスが表示されます。

保存済みファイル

デバイスのハード ドライブまたはマルウェア ストレージ パック（インストールされている場合）に保存されたキャプチャされたファイル。保存済みファイルは後でダウンロードし、分析することができます。

ポリシー

設定を（ほとんどの場合アプライアンス）に適用するためのメカニズム。アクセス コントロール ポリシー、相関ポリシー、ファイル ポリシー、正常性ポリシー、侵入ポリシー、ネットワーク分析ポリシー、ネットワーク検出ポリシー、SSL ポリシー、およびシステム ポリシーを参照してください。

ポリシー ターゲット

ポリシーを適用するアプライアンスまたはゾーン。ポリシーは、複数のターゲットを持つ場合があります。

保留中（アプリケーション プロトコル）

システムがアプリケーション プロトコルを肯定的にも否定的にも識別できないときにアプリケーション プロトコル ID に与えられる設定。多くの場合、システムが保留中のアプリケーション プロトコルを識別するには、より多くのデータを収集して分析する必要があります。

ホワイトリスト

修復で、ある種のアクションから IP アドレスを除外するために設定できるコンプライアンス ホワイトリスト、セキュリティ インテリジェンス ホワイトリスト、HA リンク インターフェイス、または IP アドレスのリスト。

ホワイトリスト イベント

有効なターゲット ホストがコンプライアンス ホワイトリストに準拠しなくなったことをシステムが検出したときに生成されるイベント。ホワイトリスト イベントは、特別な種類の相関イベントです。

ホワイトリスト違反

ホストがコンプライアンス ホワイトリストにどのように準拠していないか詳細を示す、イベント ビューアで確認できる情報。

マルウェア イベント

シスコ の高度なマルウェア防御ソリューションの 1 つにより生成されるイベント。ネットワークベースのマルウェア イベントは、Collective Security Intelligence クラウドがネットワーク トラフィックで検出されたファイルに対してマルウェアの性質を返すと、生成されます。レトロスペクティブ マルウェア イベントは、その性質が変更されたときに生成されます。エンドポイントベースのマルウェア イベント（展開されている FireAMP コネクタが脅威を検出するか、マルウェアの実行をブロックするか、マルウェアを検疫するか、マルウェアの検疫に失敗した場合に生成されるイベント）と比較してください。

マルウェア クラウド ルックアップ

ファイルの SHA-256 ハッシュ値に基づいて、ネットワーク トラフィックで検出されたファイルのマルウェアの性質を決定するために、防御センターが Collective Security Intelligence クラウドと通信するプロセス。

マルウェア ストレージ パック

キャプチャされたファイルを保存するために特定のデバイスにインストールできるシスコが提供するセカンダリ ソリッド ステート ドライブ。これにより、イベントおよび設定ストレージのためにデバイスのプライマリ ハード ドライブに空き領域が確保されます。

マルウェア ブロッキング

シスコ のネットワーク ベースの高度なマルウェア防御(AMP)ソリューションのコンポーネント。インライン展開で、マルウェア検出によって検出されたファイルのマルウェア disposition が生成された場合、または検出されたファイルがカスタム検出リストにある場合は、ファイルをブロックしたり、ファイルのアップロードやダウンロードを許可したりすることができます。FireAMP サブスクリプションが必要なシスコのエンドポイントベースの AMP ツールである FireAMP とこの機能を比較してください。

マルウェア検出

シスコ のネットワーク ベースの高度なマルウェア防御(AMP)ソリューションのコンポーネント。全体的なアクセス制御設定の一部として管理対象デバイスに適用されたファイル ポリシーにより、ネットワーク トラフィックが検査されます。防御センターは、検出された特定のファイル タイプに対してマルウェア クラウド ルックアップを実行し、ファイルのマルウェアの性質に対するアラートを発行するイベントを生成します。その後 AMP マルウェア ブロッキングが実行され、ファイルをブロックするか、ファイルのアップロードまたはダウンロードを許可します。FireAMP サブスクリプションが必要なシスコのエンドポイントベースの AMP ツールである FireAMP とこの機能を比較してください。

マルウェアの性質

ファイルにマルウェアが含まれているかどうかについての Collective Security Intelligence クラウド による判定。判定はファイルの SHA-256 ハッシュ値、脅威スコア、およびファイルがクリーン リストまたはカスタム検出リストのいずれにあるかに基づいて行われます。

マルウェアの性質キャッシュ

ファイルのマルウェアの性質および脅威スコアを保存する防御センターのキャッシュ。パフォーマンスの向上のために、システムがすでに SHA-256 ハッシュ値に基づいてファイルの性質または脅威スコアを認識している場合、防御センターはマルウェア クラウド ルックアップを実行する代わりにキャッシュ情報を使用します。特定の期間が経過したら、キャッシュの情報がタイムアウトすることにより、キャッシュ データが古くならないようになっています。

マルウェア防御

高度なマルウェア防御を参照してください。

未確認ホスト

システムがホストに関する十分な情報をまだ収集していないため、オペレーティング システムを識別できないホスト。不明なホストと比較してください。

モニタ

一致するトラフィックをログに記録する方法。接続をすぐに許可またはブロックせずに、システムが引き続き評価できるようにします。セキュリティ インテリジェンス ブラックリストに違反するトラフィックや、アクセス コントロール ルールまたは SSL ルールの基準の組み合わせに一致するトラフィックをモニタできます。

モバイル デバイス

FireSIGHT システム では、ディスカバリ機能によりモバイル ハンドヘルド デバイス（携帯電話やタブレットなど）として識別されるホスト。多くの場合、モバイル デバイスがジェイルブレイクされているかどうかをシステムが検出できます。

ユーザ

管理対象デバイスまたはユーザ エージェントによって検出されたネットワーク アクティビティのユーザ。

ユーザ アイデンティティ

ユーザを参照してください。

ユーザ アクティビティ

システムがユーザ ログインまたはログオフ（失敗したログイン試行を含む場合があります）、または防御センターデータベースでのユーザ レコードの追加または削除を検出すると生成されるイベント。

ユーザ エージェント

ネットワークにログインするとき、またはその他の何らかの理由で Active Directory 資格情報に対して認証するときに、ユーザをモニタするためにサーバにインストールされるエージェント。アクセス制御ユーザによるアクティビティは、ユーザ エージェントによって報告される場合のみ、アクセス制御に使用されます。

ユーザ レイヤ

ポリシーの設定を変更できる侵入ポリシーのレイヤ。

ユーザ ロール

FireSIGHT システム のユーザに付与されたアクセスのレベル。たとえば、イベントアナリスト、FireSIGHT システムを管理する管理者、サードパーティ ツールを使用して防御センターデータベースにアクセスするユーザなどに対し、Web インターフェイスへの各種アクセス権限を付与できます。また、特殊なアクセス権限を含むカスタム ロールを作成できます。

ユーザ ロール エスカレーション

カスタム ユーザ ロールに付与すると、ログイン セッション中に、ユーザがパスワードを入力して別のユーザ ロールのアクセス許可を取得することが可能になる特権。

ユーザ詳細

ユーザ アイデンティティおよびユーザ アクティビティのワークフローの最後のページ。ユーザ詳細には、ユーザに関する一般情報とともに、ホスト履歴も表示されます。これは、過去 24 時間のユーザ アクティビティのグラフィカル表示です。

ユーザ証明書

FireSIGHT システム Web サーバに対してユーザのブラウザを識別する暗号化された証明書。サーバでユーザ アイデンティティのセカンダリ検証を実行できるようにします。証明書は、アプライアンスのサーバ証明書の発行元と同じ認証局によって発行される必要があります。

ユーザ制御

アクセス制御の一部であり、ネットワークを通過できるユーザ関連トラフィックの指定およびログ記録を可能にする機能。

ユーザ認識

組織が脅威、エンドポイント、ネットワーク インテリジェンスをユーザ アイデンティティ情報に関連付けることができる機能。また、この機能によってユーザ制御を実行することができます。

ユーザ認識オブジェクト

ネットワーク トラフィックまたはユーザ エージェントでアクティビティが検出されたユーザのメタデータを取得するために、LDAP サーバへの接続を可能にする設定の集合。組織が Microsoft Active Directory を使用している場合、ユーザ認識オブジェクトによってアクセス制御ユーザを指定することもできます。

ユーザ履歴

ホストに関する過去 24 時間のユーザ アクティビティのグラフィカル表示。ホストのホスト プロファイルに表示されるユーザ履歴には、棒グラフで表されるおおよそのログインおよびログアウトの時間とともに、そのホストにログインしたことが検出されたユーザのユーザ名が表示されます。

ユニファイド ファイル

イベントデータをログに記録するため FireSIGHT システムが使用するバイナリ ファイル形式。

抑制

イベント抑制を参照してください。

リスク

アプリケーション リスクを参照してください。

リンク ステートの伝達

インライン セットのインターフェイスの 1 つが停止したときに、ペアの 2 番目のインターフェイスを自動的に停止させる、バイパス モードのインライン セットのオプション。停止したインターフェイスが再び起動すると、2 番目のインターフェイスも自動的に起動します。つまり、ペアの 1 つのインターフェイスのリンク ステートが変化すると、もう一方のインターフェイスのリンク ステートも、その状態に一致するように自動的に変更されます。

ルータ

ゲートウェイに配置され、ネットワーク間でパケットを転送するネットワーク デバイス。システムはネットワーク検出を使用することでルータを検出できます。また、管理対象デバイスを 2 つ以上のインターフェイス間のトラフィックをルーティングする仮想ルータとして設定できます。

ルーテッド インターフェイス

レイヤ 3 展開環境でトラフィックをルーティングするインターフェイス。タグなし 仮想ローカル エリア ネットワーク（VLAN）トラフィックを処理するための物理ルーテッド インターフェイスと、指定の VLAN タグが付いたトラフィックを処理するための論理ルーテッド インターフェイスを設定できます。また、ルーテッド インターフェイスに静的な Address Resolution Protocol（ARP）エントリを追加できます。

ルール

ネットワーク トラフィックの検査で照合する基準を提供する構成要素。通常、ポリシーに含まれています。アクセス コントロール ルール、相関ルール、検出ルール、高速パス ルール、ファイル ルール、侵入ルール、ネットワーク分析ルール、プリプロセッサ ルール、および SSL ルールも参照してください。

ルール アクション

システムがルールの条件を満たすネットワーク トラフィックをどのように処理するかを決定する設定。アクセス コントロール ルール アクション、ファイル ルール アクション、および SSL ルール アクションも参照してください。

ルール更新

新規および更新された標準テキスト ルール、共有オブジェクトのルール、およびプリプロセッサ ルールを含む、必要に応じた侵入ルールの更新。ルール更新では、ルールの削除、デフォルトの侵入ポリシー、ネットワーク分析ポリシー、および高度なアクセス コントロール ポリシーの設定の変更、デフォルト変数およびルール カテゴリの追加や削除が実行されることもあります。

ルール状態

侵入ルールが侵入ポリシー内で有効であるか([イベントを生成する(Generate Events)] または [ドロップしてイベントを生成する(Drop and Generate Events)] に設定)、または無効であるか([無効(Disable)] に設定)。有効にされたルールはネットワーク トラフィックの評価に使用され、無効にされたルールは使用されません。

レイヤ

侵入ポリシーまたはネットワーク分析ポリシー内の設定一式。ポリシー内の組み込みレイヤにカスタム ユーザ レイヤを追加できます。上位レイヤの設定により、下位レイヤの設定がオーバーライドされます。

レート フィルタリング

一致するトラフィック レートに基づいて、ルールの新しい侵入ルール状態を設定する異常検出の形式。

レトロスペクティブ マルウェア イベント

以前に検出されたファイルのマルウェアの性質が変更されると生成されるネットワークベースのマルウェア イベント。このことが発生すると、システムは、そのレトロスペクティブ イベントの SHA-256 ハッシュ値を共有するファイルやマルウェアの性質も更新します。

レピュテーション(IP アドレス)

セキュリティ インテリジェンスを参照してください。

レピュテーション(URL)

URL レピュテーションを参照してください。

レポート テンプレート

レポートおよびそのセクションに対してデータの制約と形式を指定するテンプレート。

ロード バランサ

パフォーマンスとリソース使用を最適化するためにトラフィックを配信するネットワーク デバイス。ディスカバリを使用することで、システムはロード バランサを識別できます。

論理インターフェイス

特定の 仮想ローカル エリア ネットワーク（VLAN）タグ付きトラフィックが物理インターフェイスを通過するときに、そのトラフィックを処理するために定義する仮想サブ インターフェイス。

ワークフロー

イベント データの幅広いビューから、ユーザが関心のあるイベントだけが含まれた、より的が絞られたビューに移動することで、イベントを表示および評価するためにユーザが使用できる一連のページ。ワークフローには、それぞれが固有の機能を実行する 3 種類のページ（ドリルダウン ページ、テーブル ビュー、および最終ページ）を含めることができます。ワークフローの種類に応じて、最後のページは、テーブル ビュー、パケット ビュー、ホスト ビュー、脆弱性の詳細、ユーザ詳細のいずれかになることが考えられます。