

Cisco Security Monitoring Analysis and Response System

CS-MARS(Cisco Security Monitoring Analysis and Response System) は、ネットワーク上の脅威を管理および監視し、感染抑制対策を提供するハイ パフォーマンスかつスケーラブルなアプライアンス ファミリです。CS-MARS は、従来型のセキュリティ イベント 監視機能に、ネットワーク インテリジェンス、コンテキスト の関連付け、ベクトル分析、異常検出、ホットスポット 識別、自動感染抑制機能などを組み合わせることにより、ネットワーク デバイスおよびセキュリティ デバイスをより効率的に使用できるようにします。これにより、CS-MARS を使用する企業では、ネットワーク コンプライアンスを維持しながら、ネットワーク 攻撃を正確に識別して排除できます。

主な利点

中央集中型の監視機能

CS-MARS は、さまざまなデバイス ログ、アラート、および NetFlow コミュニケーションを使用して、ルータ、スイッチ、ファイアウォール、VPN コンセントレータ、エンドポイントデバイスといったネットワーク インフラストラクチャに関する詳細情報を提供します。これにより、CS-MARS は脅威に関する情報から IP、MAC アドレス、および攻撃に最も近いスイッチ ポートを識別し、ネットワーク内の攻撃経路を提供します。

中央のイベント リポジトリ

CS-MARS は、ファイアウォール、認証サーバ、ネットワーク侵入検知サービス、防御サービス、およびプロキシ サーバなどのセキュリティ デバイスによって生成されたすべてのイベントの中央リポジトリとして機能します。ネットワークデバイスで発生したイベントとともに、ワークステーションおよびサーバのログも収集されます。収集されたイベントはすべて、リアルタイムで相互に関連付けられます。

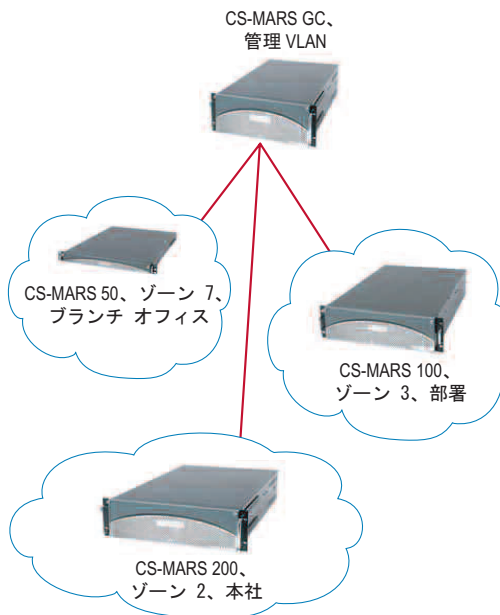
データの削減

CS-MARS を使用すると、数百万のセキュリティ イベントを、少数のネットワーク インシデントのレポートへと集約できます。

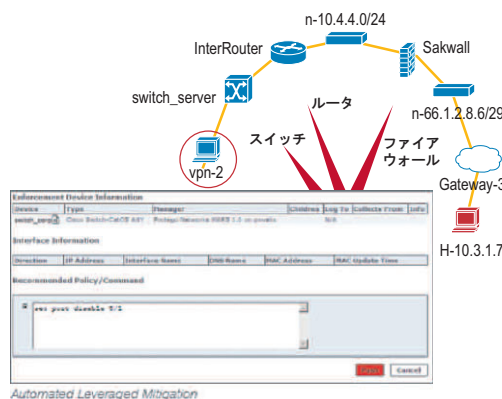
タイムリーな攻撃抑制

CS-MARS のシステムには、高度なパフォーマンスおよび専門的な対策機能の両方が搭載されているため、攻撃がネットワーク全体に拡散する前にそれらを認識し、推奨される感染抑制対策を提供することができます。

拡張性の高い展開



感染抑制に向けた投資の活用



詳細なレポート



エンドツーエンドのネットワーク認識

CS-MARS は、あらゆるタイプのネットワーク システムとエンド システムによる完全な構成を使用して Network Address Translation (NAT; ネットワーク アドレス変換)/Port Address Translation (PAT; ポート アドレス変換) および MAC アドレス情報を統合することにより、攻撃者、ターゲット、およびネットワーク ホット スポットをグラフィック形式で識別し、迅速な対応を行うことができます。また、NAT を実行する前後のアドレスの表示も可能です。

統合された脆弱性評価

CS-MARS は、ネットワーク攻撃が実際に起こる可能性があるか、またはフォールス ポジティブであるかを判断します。これにより、作成するアラームの数とアクションの実行に必要な時間を削減できます。

展開コストと運用コストの削減

システムの起動およびネットワークへの接続が完了すると、CS-MARS はトポロジの検出およびマッピングを行います。これにより、システムが短時間で稼働できるようになります。

感染抑制機能の自動化

自動感染抑制機能を使用すると、使用可能なチャックポイントデバイスの識別が攻撃経路に沿って行われ、ユーザは感染の脅威を軽減するための適切なデバイス コマンドを自動的に適用できるようになります。また、MAC アドレス、Windows ワークステーション名、VPN ユーザ名、物理的なファースト ホップ スイッチ ポートといった、感染抑制に不可欠な多数のアトリビュートも自動的に識別されます。これらの結果を使用することにより、攻撃を迅速かつ正確に阻止し、被害を最小限に抑えることができます。

ネットワーク インテリジェンスを備えたイベントの関連付け

CS-MARS は、ルータ、スイッチ、脆弱性分析ツール、およびファイアウォールからトポロジとデバイス構成を理解し、ネットワーク トラフィックのプロファイリングを行うことで、ネットワーク インテリジェンスを取得します。システムでは、統合型のネットワーク検出が行われ、デバイス構成と現在のセキュリティ ポリシーを含むトポロジ マップが作成されます。これにより、CS-MARS は、ユーザ ネットワーク上のパケット フローをモデル化します。アプライアンスはインラインでは動作せず、既存のソフトウェア エージェントの利用も最小限なため、ネットワークまたはシステム パフォーマンスには影響がありません。

SureVector 分析

SureVector 分析機能は、管理範囲の拡大、迅速な調査、および応答時間の短縮を可能にします。SureVector 分析を使用すると、攻撃経路の明白かつ正確な追跡、インシデントの発生に先立つ未処理イベントに関する詳細の取得、および異常な攻撃動作のソースの特定を管理者が行えるようになります。この結果、より詳細で正確な分析をリアルタイムで実行できるようになり、攻撃の阻止が実現します。

NetFlow 分析

CS-MARS は、毎秒 300,000 フローの速度でルータから NetFlow データを収集します。NetFlow およびファイアウォールのログを使用すると、ネットワークの使用状況の分析を特定のワークステーションに至るまで行うことができます。これにより、管理者は、ウイルスやワームの存在などの異常を検出して対策を実施できます。

コンテキストの関連付け

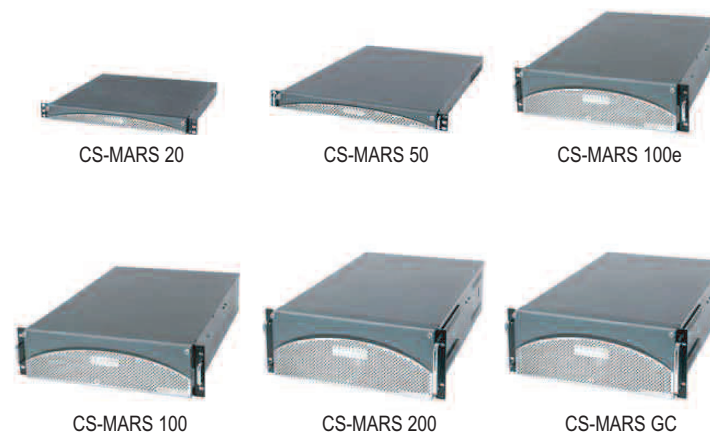
コンテキストの関連付け機能は、ネットワークレベルのインテリジェンスを利用して、複数のセキュリティ イベントおよび NAT 境界を越えて行われるネットワーク動作をセッション内でグループ化します。また、システムとユーザ定義された関連付けルールを複数のセッションに適用することで、有効なインシデントを識別します。CS-MARS は、出荷時に事

前定義済みのルールによって完全に補完されています。Protego によって頻繁にアップデートされるこれらのルールを使用することにより、さまざまな複合型の攻撃シナリオ、Day Zero 攻撃、およびワームの識別が可能になります。グラフィック形式のルール定義フレームワークを使用すると、あらゆるアプリケーション上でユーザ定義のカスタム ルールを容易に作成できます。コンテキストの関連付けにより、未処理のイベント データの大幅な削減、応答の優先順位付けの簡素化、および展開された対策の効果の最大活用が可能になります。

ハイパフォーマンスかつスケラブルなアーキテクチャ

CS-MARS は、単一のボックスで毎秒 10,000 個の速度でイベントをキャプチャします。単一のボックスでの対応が不可能な要件の場合には、CS-MARS Global Controller を中央サイトに導入できます。Global Controller は、個別の Local Controller からインシデントを集約します。このアーキテクチャでは、大半の処理がローカルに実行されるため、展開された各 Local Controller でのほぼりニアなパフォーマンスの向上が実現します。

シスコ製品番号 (Protego モデル)	パフォーマンス		ストレージ	フォームファクタ	電源装置
	イベント/秒	NetFlow/秒			
CS-MARS-20R-K9	50	1,500	120 GB (非 RAID)	1 RU × 16 インチ	300 W
CS-MARS-20-K9	500	15,000	120 GB (非 RAID)	1 RU × 16 インチ	300 W
CS-MARS-50-K9	1000	30,000	240 GB RAID 0	1 RU × 25.6 インチ	300 W
CS-MARS-100E-K9	3000	75,000	750 GB RAID 10 ホットスワップ対応	3 RU × 25.6 インチ	500 W デュアル冗長
CS-MARS-100-K9	5000	150,000	750 GB RAID 10 ホットスワップ対応	3 RU × 25.6 インチ	500 W デュアル冗長
CS-MARS-200-K9	10,000	300,000	1 TB RAID 10 ホットスワップ対応	4 RU × 25.6 インチ	500 W デュアル冗長
シスコ製品番号 (Protego Global Controller モデル)	分散モニタリング		ストレージ	フォームファクタ	電源装置
	サポートされるモデル	最大接続数			
CS-MARS-GCM-K9	MARS 20 または 50 のみ	5	1 TB RAID 10 ホットスワップ対応	4 RU × 25.6 インチ	500 W デュアル冗長
CS-MARS-GC-K9	任意	制限なし	1 TB RAID 10 ホットスワップ対応	4 RU × 25.6 インチ	500 W デュアル冗長





ハードウェア仕様

- 専用の 19 インチ ラックマウント アプライアンス — UL、FCC、CE、および VCCI 認証
- セキュリティ強化型 OS — 大半のネットワーク サービスは使用不可
- 10/100/1000 イーサネット インターフェイス × 2 — リカバリ メディア付属の DVD-ROM
- ストレージ — Cisco Security MARS 50 用の RAID 0、Cisco Security MARS 100、200、および Global Controller (GC) 用のホットスワップ対応 RAID 10
- 冗長ロードシェアリング — 500 W の電源、120/240 V の自動スイッチ

リアルタイムの調査とコンプライアンスに関するレポート

CS-MARS は、従来のセキュリティ ワークフローを簡素化する、使いやすい分析フレームワークを搭載しています。また、自動的な事例の割り当て、調査、エスカレーション、通知、および注釈機能を提供することにより、日常的な業務や特殊な監査に対応します。CS-MARS では、攻撃をグラフィック形式で再生したり、保存済みのイベント データを取得して過去のイベントを分析したりできます。また、リアルタイムまたは事後のデータ検索に対応した特殊なクエリーを完全にサポートしています。CS-MARS では、事前定義された多数のレポートを提供しており、運用要件を満たしながら Sarbox、GLBA、HIPAA、FISMA、Basel II などへの適合認定に対応することができます。また、わかりやすいレポート作成機能により、データ形式、トレンド形式、およびチャート形式を使用して、100 を超える標準レポートに変更を加えたり、多岐にわたる作成方法（実行プラン、復旧プラン、インシデント、ネットワーク アクティビティ、セキュリティ ポスチャ、監査、部門レポートなど）で新しいレポートを生成したりできます。CS-MARS では、バッチおよび E メール形式によるレポートにも対応します。

管理

- セキュアな Web インターフェイス (HTTPS)、ロールベースの管理、完全なユーザ監査証跡
- E メール、ポケットベル、Syslog、および SNMP (簡易ネットワーク プロトコル) を介したインシデントのエスカレーション、ワークフロー、および通知
- CS-MARS GC による複数の CS-MARS アプライアンスの階層型管理
- 検証済みの自動アップデート — デバイスのサポート、新規ルールおよび機能
- 未処理データの継続的な圧縮およびオフラインの Network File Sharing (NFS) ストレージへのインシデントのアーカイブ

クエリーとレポート

- GUI により、多数のデフォルト クエリーおよびカスタマイズされたクエリーをサポート
- 100 を超える通常レポート — 管理レポート、運用レポート、および適合認定レポート
- わかりやすいレポート生成機能により、さまざまなカスタマイズ形式のレポートに対応
- データ形式、チャート形式、およびトレンド形式により、HTML および CSV でのエクスポートをサポート
- レポート システム — 特殊、バッチ、テンプレート、および E メール転送

トポロジの検出

- レイヤ 3 およびレイヤ 2 — ルータ、スイッチ、ファイアウォール
- ネットワーク IDS — ブレードおよびアプライアンス
- 手動検出および定期的な検出
- SSH、SNMP、Telnet、およびデバイス固有のコミュニケーション
- 検出の代わりとなるシード ファイル

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。

この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービス マーク、登録商標、登録サービスマークです。

この資料に記載された仕様は予告なく変更する場合があります。