MarkLogic

サイバー状況認識ソリューション
分散されたサイバーデータを統合する

大規模で複雑な組織では、物理的なセキュリティとネットワークセキュリティを含む、複数のシステムが利用されています。データベース、サーバー、アプリケーション、メール、ファイアウォール、ルーターの各ログファイルと、建物へのアクセス、バッジリーダー、生体認証を始めとした物理的なセキュリティは、サイバー脅威を識別する際に把握する必要のあるほんの一部に過ぎません。長年にわたり多大な労力、イノベーション、インフラストラクチャが、マルウェア、脅威の検出、ログの記録に使われてきました。それでもインフラストラクチャ、分析、すべてのデータに関する重要情報を共有するためのベストプラクティスおよび規約が不足しているのが現状です。組織に対するサイバー攻撃を防止・分析するために必要な情報は、従業員の日常業務、受託業者、警備員室、企業リスク管理、従業員保護、一般的なセキュリティに埋もれている可能性があります。しかもこれらすべてが、各所に分散されて存在しているのです。

現在のサイバーシステムは、レガシーで融通の利かないRDBMS（リレーショナルデータベース管理システム）や、機能が過剰な扱いにくいオープンソースプラットフォームに大きく依存しています。このようなソリューションではソースの変更に容易には対応できず、集合データをもとの方法で利用することができません。セキュリティ運営やSIEM（セキュリティ情報イベント管理システム）、IDS（侵入検知システム）から出力されるデータはしばしばデバイス独自、システム独自の形式で保存されます。この点を認識した一部の組織では、分析やデータサイエンスのサポートにHadoopを重視したアーキテクチャと基本的なNoSQLプラットフォームに投資しています。このような種類のアーキテクチャには、得られたデータとインサイトを運用する機能が備わっておらず、イベントを静的に観測することしかできません。

現在のサイバーソリューションには次のような限界があります。

- サイバー脅威のすべての指標と警告が分散表示される。機関や組織は漏洩を示す指標、高度かつ執拗な脅威、サイバー警告、サイバー勧告、技術注記、システムに危害をおよぼすおそれのある個人/グループのつながりを見ることができません。
- 規制、ポリシー、ガバナンスに従ってサイバー脅威を表示できない。「ボックスチェック」によるサイバー防衛以上のものが必要となります。
- サイバー情報は主としてログファイルの調査に限定される。

変化する状況

機械学習やAIなどの新しい手法によるマルウェアやサイバー攻撃防御の高度な技術が、マルウェア対策シグネチャをサーバー、ワークステーション、ラップトップに手動でインストールするウィルス対策パッケージといった指紋技術の代わりに利用されるようになっています。攻撃の前後に発生するイベントを取得して特徴付けるイノベーションはまだありませんでした。

アメリカ国防総省のJIEDDO（統合即製爆発物対策機関）は、「Left of Boom」に重点を置いています。これは問題（IED、つまり即製爆発物）から自分たち自身をどう守るかではなく、問題をどう防止するかを重視していることを意味します（テロの資金収集を研究し、IEDを使うテロリストのネットワークを追跡）。サイバーセキュ

今日のサイバー状況認識

- CERTメッセージ
- 疑わしい行為のレポート
- インシデントレポート
- システムドキュメント
- メーカーからのバグ・パッチ・システム修復と履歴
- CMDB（構成管理データベース）
- サイバーアラート、通知
- テクニカルレポート
- リファレンスドキュメントとリサーチレポート
- 業界の制御システムのセキュリティと教育
- ハードウェアスキャンレポート（IRISスキャン）

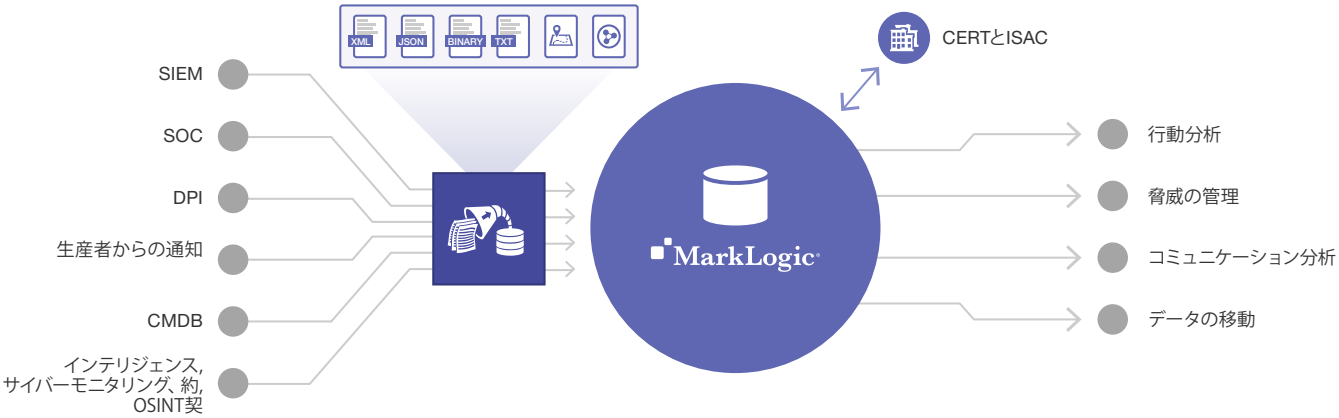
リティで同様のことを行うには、ソーシャルエンジニアリングを始めとしたサイバーや運用の脆弱性を完全に把握する必要があります。それにはサイバー脅威の領域について新たな見方をする必要があります。

国家安全保障や防衛産業は、「すべての発生元の」情報を保護するという課題に直面しています。これは情報の重要性ゆえに機関どうしの協力が困難な課題です。例えば運用における脅威や脆弱性の全体像を把握するには、信号処理でサイバー情報、人知 、地理情報といった情報を組み合わせる必要があります。現代のサイバー脅威への対応はすべての発生元で解決すべき課題であり、分散されているすべてのデータを簡単に統合できる柔軟なデータベースが必要です。

最新のサイバー状況認識ソリューション

MarkLogic®サイバー状況認識ソリューションは分散しているサイバーデータを統合し、さまざまなデータソースやフィード間、複数のコミュニティ間のトランザクションをサポートします。情報を引き出し分散する分析ツールで利用できる、統合化されたデータセットが出力されます。このソリューションを実装すると、すべてソースとダウンストリーム分析をポイントツーポイントで統合（および維持）するための費用と労力が大幅に削減されます。既存のSOAおよび各種のエンタープライズサービスバスを補完します。また、統合されたデータすべてを利用する新しいアプリケーションを構築しつつ、レガシーシステムおよび既存のシステムを引き続き運用できます。このソリューションではデータすべてに索引が付けられ、RESTfulなサービスを使ってデータが公開されるため、すべてのサイバーイベントの情報をセキュアに共有できる一方、統合のための費用が削減され、複雑さが軽減されます。サイバー状況認識ソリューションは、推奨のUS-CERTおよび同様の国際的な「トラフィック負荷の少ないプロトコル」に従って、配信および改訂を管理します。そのためには、警告、分類、コミュニティのようなタグごとに、セキュリティを細分化する必要があります。

MarkLogicサイバー状況認識ソリューションを導入することで 実装、運用、保守の各費用を削減しつつ、リアルタイムの分析が可能になり、運用機能が向上します。MarkLogicでは各産業と政府機関が、新しい情報共有・分析センターや統合サイバー脅威センターを設立する中、意味的、時間的、そして位置的コンテキストでサイバー状況認識のすべての側面をまとめる必要があると考えています。ISAC（セキュリティ情報共有組織）は先頃、サイバーデータの統合と共有を改善することを目的に、財務、医療、産業用制御システム、石油/ガス、電気、公共安全などの分野におけるサイバー脅威に関するコミュニティ固有の情報を共有することにしました。MarkLogicのソリューションはこのような重要な取り組みをサポートし、強化します。



MarkLogicのソリューションはオペレーショナルデータハブとして機能します。分散された複数のデータソースを読み取り・書き込み統合するとともに、索引を作成して検索、共有、分析、配信ができるようにします。

MarkLogic

MarkLogicサイバー状況認識ソリューションを実装すると、以下が実現されます。

- リアルタイム分析と遡及分析を統合し、情報を迅速に整理し共有する
- すべてのデータを公開。ドリルダウン、ファセット検索を使って簡単に検索できるようになる
- データサイエンスにより取得したインサイトを活用する
- 精密パケット検査機能を使用して、作成されたシグネチャとフィルターすべてに対して、柔軟で永続的なレイヤーとアラート方法を提供。
- 状況認識と調査の際に大変役に立つエンティティ・オブジェクトとして、漏洩、高度で執拗な脅威、ユーザー、アカウント、組織、IT資産などの価値の高いサイバー情報を指標表示。

豊富な実績

MarkLogicは運用市場とNoSQLデータベース市場における有数の企業として、多数の業界アナリストから評価されており、データ統合、検索、検出、分析、コンテンツ配信の各ソリューションを世界中の大規模組織に提供しています。これらの組織では、信頼性、柔軟性、セキュリティを備えた独自のソリューションを必要としており、それが実現可能なのはMarkLogicエンタープライズNoSQLプラットフォームだけです。

MarkLogicについて

10年以上にわたり、世界の多くの組織がMarkLogicの製品を使って革新的な情報アプリケーションを構築しています。MarkLogicは、分断されたデータの統合における世界的なエキスパートです。オペレーショナルでありトランズアクショナルな、基幹業務に対応したエンタープライズNoSQLデータベースのプラットフォームで、お客様のデータを統合して360度、あらゆる視点からデータを使うことができる次世代アプリケーションの構築を支援します。MarkLogicの本社は米国シリコンバレーにあり、その他のオフィスを米国、欧州、アジア、オーストラリアに展開しています。日本では東京渋谷にマークロジック株式会社を設立しています。

マークロジック株式会社 MARKLOGIC K.K.　150-0043 東京都渋谷区道玄坂 1-12-1渋谷マークシティウェスト 22 階
+81 3 4360 5354 | jp.marklogic.com | MarkLogic-JP@marklogic.com