ハイブリッドおよびマルチクラウドインフラストラクチャのためのSplunkセキュリティ

主要なメリット

- インフラストラクチャ全体で複数のクラウドテクノロジーを**導入、運用および保護**
- マルチクラウドサービス全体で**効果的にセキュリティを調査および分析**
- **マルチクラウド環境での可視性を高め**、効果的に調査、アラート生成、修復およびレポートを実行
- ハイブリッドとクラウドインフラストラクチャの両方で**データの正規化と管理**を行うことで、脅威の分析と検出を強化
- ビジネスニーズの増加に応じて**コストを管理し、セキュリティ規模を変更**

クラウドの導入がますます進む中で、企業は驚異的なスピードでハイブリッドおよびマルチクラウド環境に移行し始めています。マルチクラウドとは2つ以上のクラウドサービスで構成される単一のアーキテクチャであり、これが広く浸透してきたため、大半の企業がマルチクラウド戦略を導入しているとGartnerとFlexeraのレポートは伝えています。

しかし、多くの組織がマルチクラウドインフラストラクチャへの移行を進めるにつれ、クラウドセキュリティ戦略の機能強化と整備の必要性はますます高まっています。クラウドでは、管理と保護が必要な新しいデータストリーム、アプリケーション、およびサービスが導入されることで、攻撃対象は必然的に拡大します。そのため、内部および外部の脅威をリアルタイムでより効果的に特定および調査して対応を行うために、環境全体にわたってエンドツーエンドでの可視性を向上させる必要性が高まっています。

Splunkのメリット

統合された強力なクラウドセキュリティ戦略を策定することの重要性がこれまでになく高まっています。同時にその作業はこれまでになく困難でもあります。Splunkのセキュリティ運用スイートは、その強力な可視化機能によって、ハイブリッドとマルチクラウド環境全体にわたってSOCチームのデータ運用を支援します。Splunkの包括的なビューを使用すれば、マルチクラウド環境内の脅威の監視、調査、分析、検出をより迅速に行うことができます。複数のチームがインフラストラクチャの全体図を確認できる統合的な環境を構築して、クラウドセキュリティ体制の強化に役立てることができます。

また、Splunkの分析主導型ソリューションを使用すれば、マルチクラウドでのサイバーセキュリティに対して包括的にアプローチすることができ、環境内のデータを統合して効果的なセキュリティ体制を構築できます。Splunkは、アマゾン ウェブ サービス(AWS)、Azure、GCPを始めとするさまざまなCSP(クラウドサービスプロバイダー)や、プラットフォーム、アプリケーション、導入済みのその他の製品で生成される重要なデータの正規化と管理を行い、セキュリティの脆弱性や脅威を効果的に検出し防御します。

Splunkの機能

マルチクラウド環境の可視化

マルチクラウドのエコシステムは数多く存在し、ベンダー、アプリケーション、システムは多岐にわたります。一方で、マルチクラウド戦略を採用している企業は、インフラストラクチャ全体を可視化して、潜在的な脅威を迅速に特定してリスクを最小限に抑える必要があります。SplunkでRawイベントデータ、CSPネイティブのセキュリティツール、クラウド管理プラットフォームなどから取得されるデータを集約することで、セキュリティアナリストは一元化されたビューでシステム全体を見渡すことができます。この統合ビューにより、アナリストはより効果的な検証を行い、コンテキストに応じてアラートの優先順位を決定することができます。さらに、インシデント検出までの時間を短縮し、調査を最適化して迅速に対応することができます。

複数のクラウドプロバイダーに対応する柔軟性とツール

監視と監査に使用するツールがトラブルシューティングに使用するツールと異なっていると、必要以上に運用が複雑になり、セキュリティ対策が阻害要因となって、重大な問題への対応が遅くなります。Splunkをクラウドファーストで構築すれば、迅速な拡張が可能で、すべてのクラウド環境からあらゆるデータを取り込むことができます。さらに数多くのツールを単一のシンプルなソリューションに置き換えることができます。これによってサイロ化を防いで高速なリリースサイクルを実現し、全般的な運用効率を向上させる一方で、必要となる機能を同時に複数利用することができます。

脆弱性と設定ミスの監視、調査、検出

データプラットフォームと継続的監視の基盤が確立すると、セキュリティチームは既知の脅威を検出し、その他の疑わしいトラフィックパターンや、設定されたベースラインから逸脱する異常なアクティビティなどの脅威の兆候を見つけ出すことができます。Splunkのセキュリティソリューションはベンダーに依存しません。提供される統合ビューを使用して、複数のクラウドサービスにまたがる脆弱性と設定ミスを迅速に検出および調査して、修復することができます。

また、継続的に監視することでコンプライアンス要件への準拠を保証できます。そのためセキュリティチームは、Splunkを活用することで必要に応じてプロアクティブに対処することができます。Splunkには、クラウドプラットフォームから取得したセキュリティ関連のデータをチェックするための検出ライブラリが用意されており、Splunk Security EssentialsやEnterprise Security Content Updateなどの無料アプリケーションに加え、Splunk Enterprise Securityなどのプレミアムソリューションを通じて利用できます。

費用対効果を把握しROIを最大化

マルチクラウドとハイブリッド環境全体でのイベントを可視化できることで、チームはより有意義なタスクに注力してSOCを継続的に成長させることができるため、全般的なコストを削減し、俊敏性を高め、リスクを最小限に抑えることができます。組織はリアルタイムで支出を監視してコストを予測し、効率の低下が発生した場合はそれを特定することができます。その結果、より少ない初期費用で、より多くのビジネスニーズに対応できるセキュリティ運用に自信をもって移行することができます。

今すぐSplunk Enterprise Securityをお試しください

Splunk Enterprise Securityの機能をぜひお試しください。ダウンロード、ハードウェアのセットアップ、設定は不要です。Splunk Enterprise Security Online Sandboxは7日間利用できる評価環境です。クラウドでプロビジョニングされ、データは予め用意されています。この環境を使用して、データのサーチ、可視化、分析に加えて、セキュリティ関連のさまざまなユースケースにわたるインシデントの綿密な調査を行うことができます。詳細な手順を記載したチュートリアルが用意されており、Splunkソフトウェアが実現する効果的な可視化と分析をご紹介します。詳細についてはこちらをご覧ください。

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階
www.splunk.com/ja_jp
splunkjp@splunk.com

20-14609-SPLK-Splunk Security for Hybrid and Multicloud Infrastructures-A4-SG-JA-202012