SplunkのCybersecurity Maturity Model Certification (CMMC)向けソリューション

サイバーセキュリティのミッションを支援

アメリカ国防総省(DoD)は、2018年の国家防衛戦略の更新時にサイバーセキュリティ戦略を改定しました。DoD調達案件を勝ち取るための条件として、これまではコスト、スケジュール、パフォーマンスの3つが掲げられていましたが、今回の改定により、4番目の条件としてサイバーセキュリティが加えられました。この戦略は、国防総省調達規則(DFARS)で定められた既存のサイバーセキュリティ要件が、国家のサイバーミッション達成には不十分であったことを示しています。調達と持続性のための国防次官室(OUSD A&S)はこの不足を埋めるため、業界関係者、国防総省、大学付属研究センター (UARC)、連邦出資研究開発センター (FFRDC)との協力のもと、サイバーセキュリティ成熟度モデル認証(CMMC)を策定しました。

CMMCは、技術要件についても、またDoDコントラクターとの「Trust, but verify(信頼する、しかし検証する)」の関係構築についても、DFARSを踏襲しています。これを達成するために、CMMCではすべてのDoDコントラクターに対して継続的な監査を義務付けています。継続的な監査は国家のサイバーミッションにとっては有益ですが、DoDコントラクターにとっては新たな課題となります。DoDコントラクターが新規契約条件を満たすには、DFARSのようにコンプライアンスを単発的に確立するのではなく、コンプライアンスとサイバーセキュリティの体制を定期的に実証しなければなりません。

大きな課題

サイバーセキュリティとコンプライアンスを実証するというCMMCの新たな継続的要件を満たすためには、DoDコントラクターがサイバーセキュリティと継続的監視に付随する4つの課題を克服する必要があります。

実装の長期化と複雑さ

DoDコントラクターは、継続的監視とCMMCで定義されたサイバーセキュリティプラクティスを実現するためのテクノロジーを速やかに配備および導入しなければなりません。これを達成するためには、簡単な調整によってそれぞれのユースケースの要件に対応できる、強力なプラットフォームが必要です。計画やデータモデリングなどの各種活動によってフェーズが分かれているウォーターフォール式の長期プロジェクトでは、初回の認証と履行をタイムラインどおりに実現できません。DoDコントラクターが認証を取得するには、反復的な調整と拡張によってCMMC要件特有のニーズに対応できる、実績のあるエンタープライズクラスのテクノロジーを利用しなければなりません。

センサーとデータソースのサイロ化

DoDコントラクターは、実装の複雑さを乗り越えるだけでなく、ツールやデータソースのサイロ化を解消して、監視、履行、監査準備を効率化する反復可能な統合プロセスを確立しなければなりません。システムインテグレーターの社内ネットワークは多様性に富んでいることが多く、ノートPCやネットワーク機器から産業用制御システムまで、さまざまなものが含まれています。こうしたネットワークでは、多種多様なツールが使用されているだけでなく、地方支社、データセンター、パブリッククラウド、工業設備など、環境が物理的に分散していることも少なくありません。DoDコントラクターは統合的なアプローチを採用して、自社環境を監視し、それに関連するアーティファクトを即座に供給できるようにする必要があります。

大量かつ高速なデータ

CMMCの範囲は包括的であるため、DoDコントラクターは大量のセンサーやアプリケーションからデータを収集して監視しなければなりません。マシンデータは高速で大量に生成され、しかもそのデジタル形式は限りなく多様です。また、こうした各種センサーやアプリケーションのデータにアクセスするには、ビジネスプロセスやコントロール、ときにはアナリストトレーニングまで必要とするため、事態はさらに複雑です。企業では各部門が日々、ギガバイト級からテラバイト級のデータを生成しており、時とともにデータの量と生成速度が飛躍的に上昇しているケースも少なくありません。DoDコントラクターには、こうした量や速度の上昇とさまざまな課題に応じて拡張できるプラットフォームが必要です。

成長の阻害要因となる厳格性

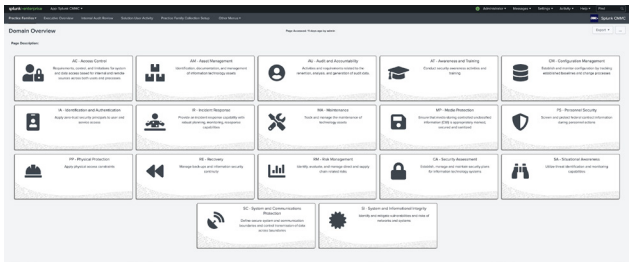
CMMCの要件を満たすために戦略的な意思決定をする際には、自らの成長を阻害しないアプローチを選択する必要があります。現代のネットワークは動的なエコシステムであり、ビジネスのニーズに応じて常に進化します。また、この課題を複雑化させるのが、CMMCが定めている複数の成熟度レベルです。これは、機密以外の重要情報(CUI)の取り扱いに対する期待に基づいて適用されます。はじめにCMMCレベルのいずれかを達成したとしても、ビジネスニーズによっては、成熟度レベルを上げて新規契約案件の条件を満たすために、さらに高度なサイバーセキュリティプラクティスを導入する必要が生じるかもしれません。DoDコントラクターは盤石な対応力で拡張性を維持するとともに、自社のビジネスと将来の契約獲得のために必要となるそれぞれのCMMCレベルに適応していく必要があります。

Splunkのアプローチ

Splunk®はオープンなData-to-Everythingプラットフォームを民間および公共セクターの19,000以上の組織に提供しています。米軍の4軍種すべて、国防総省の諸機関、防衛産業のコントラクター企業もSplunkを利用しています。Splunkを使用することで、前述の大きな課題を克服できます。Splunkは、国防総省の新しいサイバーセキュリティ成熟度モデル要件に対応できるように、CMMC向けのソリューションを開発しました。このソリューションを使用すれば、CMMCの5つの成熟度モデルで定義されている分野、機能、そして170以上のプラクティスに対応できます。

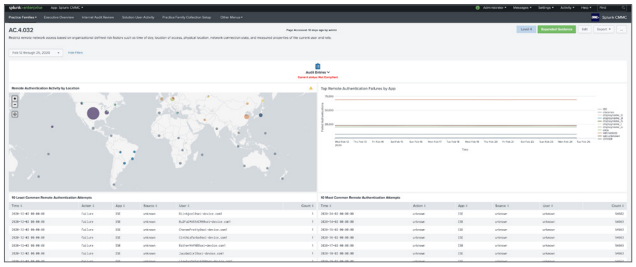
迅速な運用化

Splunkを使用してデータを活用することで、CMMCで求められるユースケースとワークフローを簡単に可視化でき、データに対する**調査、監視、分析、アクション**を1つの環境で行うことができます。Splunkでは、ほぼあらゆる形式のデータを取り込めるため、ワークフローと分析を反復的に実装でき、CMMCのレベル1 ～ 5で求められるサイバーセキュリティプラクティスに柔軟に対応できます。



データを一元的に表示できるビュー

Data-to-Everythingプラットフォームであるsplunkは、サイロ化したデータソースやセンサーを統合する中枢として機能します。Splunkはベンダーや場所に依存しないため、全社のツール、センサー、各地の拠点、さらにはクラウドやホスティングプロバイダーまでのデータを単一の画面に統合できます。Splunkの共通情報モデル(CIM)によりデータの正規化を効率化して、複数のデータソース間で標準化された分析を行うことができます。単一のビューを構築することで、サイロを解消してデータを可視化し、CMMCやサイバーセキュリティの継続的な監視をはじめとするさまざまな目的に役立てて、データの価値を最大限に引き出すことができます。



オンプレミスとクラウドでの拡張

オンプレミスのSplunk Enterprise、またはFedRAMP認定SaaSであるSplunk Cloudを使用すれば、エンタープライズデータのニーズに対応できます。日々、テラバイト規模のデータが生成されても簡単に処理し、毎秒数万件のイベントを処理して活用できるほか、組織の成長や変化するニーズに対応して柔軟にスケールアウトできます。これらの特性に加え、高可用性やディザスタリカバリなどの機能も備えているため、ビッグデータの課題にも対応できます。

堅牢性とミッションへの即応性

SplunkのCMMC向けソリューションは、カスタムアプローチであらゆる環境のニーズに合わせて導入およびスケーリングできるだけでなく、ミッションにおける必要性に応じて成熟度を高め、拡張機能を導入していくことができます。Splunk Enterpriseをベースとしたこのソリューションでは、他のSplunk機能からのデータを活用して、CMMCプラクティスへの対応に役立てることができます。Splunk Enterprise Security、Splunk Phantom、Splunk UBAのいずれも、CMMCで求められるプラクティスの自動化、合理化、実施のために利用できます。

今すぐ導入

サイバーセキュリティは、国家防衛戦略にとっても、組織の知的財産にとっても非常に重要です。サイバーセキュリティ成熟度モデル認証を獲得するための一歩を踏み出しましょう。

ソリューションがもたらす成果

- 環境を継続的に監視し、セキュリティとコンプライアンスの要件を達成および維持します。
- CMMCで求められるプラクティスの導入と達成を加速します。
- 一貫したエンタープライズデータ環境を利用することで、組織全体の効率化を実現します。
- 監査情報、トレーサビリティ、アクティビティを1つの環境にまとめて、複雑さを軽減します。
- 義務付けられたデータ収集と供給を自動化して、監査対応のための時間を短縮します。
- さらに上の成熟度認証レベルを取得するための道筋を示します。

サイバーセキュリティ成熟度モデル認証への対応にSplunkを活用できます。Splunk Enterpriseを長年ご利用の場合も、Splunkを初めて評価する場合も、**詳細についてお問い合わせください**。

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

20-13209-PUBSEC-Cybersecurity Maturity Model Certification (CMMC) Solution-A4-JA-202012