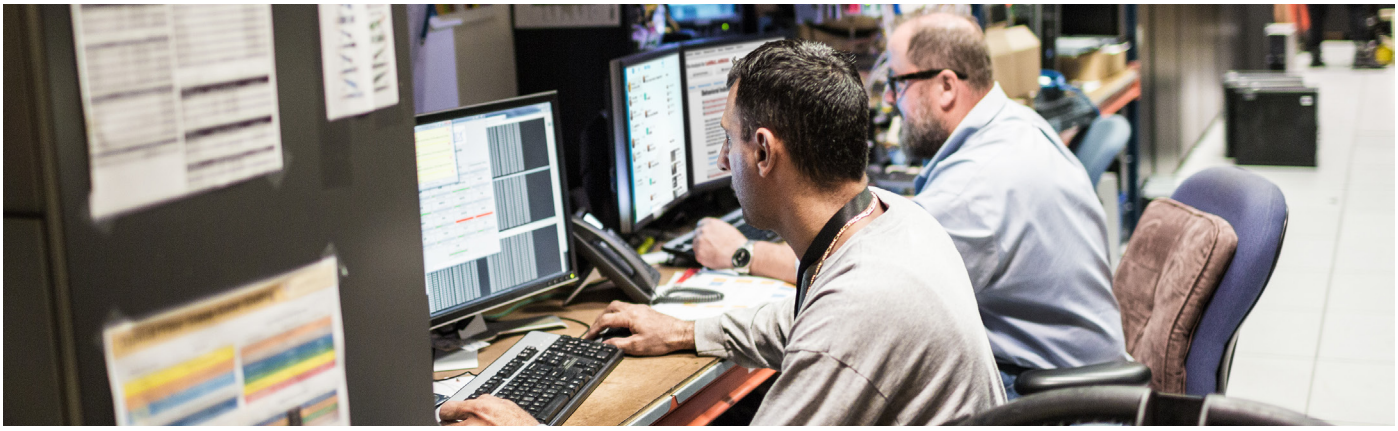
ケース スタディ

Shawmut 社では、セキュリティの強化と管理の簡素化を実現



概要

顧客名：Shawmut Design and Construction
規模：従業員数 1000 人以上
業界：建設
所在値：米国マサチューセッツ州ボストン（本社）。事業所を全国に展開

「Cisco Defense Orchestrator によって、重複したオブジェクト、未使用のオブジェクト、整合性のないオブジェクトを判別するプロセスが自動化され、オブジェクトの結合や削除が非常に簡単になりました。このソリューションによって、負担のかかる手動の作業に費やす日数が減り、有効なオブジェクトを誤って削除するリスクが大幅に削減されたのです」

- Chris Ryan 氏
Shawmut ネットワーク マネージャ

Shawmut Design and Construction 社では、建設プロジェクトやセキュリティにおける「想定外」は禁物です。同社で重視されるのは、プロアクティブに行動することです。

同社は従業員が所有するタイプの企業で、当事者意識、プロアクティブなソリューションの作成、そして将来を見据えた思考という企業文化を育成してきました。こうした理由から、同社は 12 米億ドル規模で全国展開し、非常に複雑かつ物流上の課題が多いプロジェクトを解決可能な企業として、多数の大手企業から高い評価を獲得してきました。また同社は、顧客やベンダーと継続的なパートナーシップを構築していることでも知られています。同社の受注の 80 % はリピート客から発注されており、Shawmut とシスコの関係は 2000 年代初頭から続いています。

同社は拡大し続けており、事業の方法も変わり続けていることから、社内の IT チームでは、事業をサポートするための新しい運営技術とアプリケーションをどう評価するかという課題を常に抱えています。優先順位が高い分野は、事業の運営や、会社の知的財産などの価値のあるデータを保護することです。Shawmut が日々直面している脅威に対処するためには、古いハードウェアを最新のセキュリティ制御を使用してアップグレードする必要があります。理想的なソリューションは、組織全体のセキュリティを IT チームが管理する方法を簡素化し、IT 部門の人員を増やすことなく、ビジネスをプロアクティブに保護するための統制を実現することです。

Shawmut の IT スタッフは、シスコと連携して、現状を評価し、シスコのセキュリティ ソリューションのポートフォリオを詳しく理解することにしました。

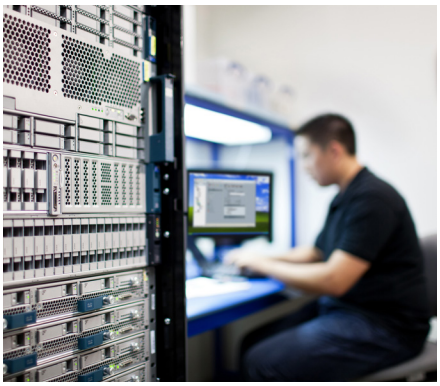
まず、マサチューセッツ州のボストンおよびウェストボローの事業所に設置されている既存の Cisco ASA 5500 シリーズ ファイアウォールは耐用期間を超えており、交換が必要でした。同社では、各データセンターで Cisco ASA 5500-X シリーズ次世代ファイアウォール製品群を高可用性構成（アクティブ/パッシブ モード）に置き換えることで、インフラストラクチャを刷新しました。

ネットワーク マネージャを務める Chris Ryan 氏は、ハードウェアにおけるアップグレードに加えて、基本的な設定とポリシー構造を最適化し、常に改善を続けることも同じように重要であることを認識していました。

Cisco Defense Orchestrator を導入することにより、Shawmut は以下を実現しています。

- ポリシーの自動検出および一貫性のある構造の構築

- すべてのデバイスを対象にした、セキュリティ ポリシーの一元的な管理



- セキュリティ体制の向上とトラブルシューティングの簡素化

Chris 氏は、「ビジネス上の要求と新しいアプリケーションに対応するためにポリシーの変更を何年も続けた結果、今日採用しているようなポリシー構造を簡素化する必要に迫られました。シンプルかつ一環したポリシーの設計により、トラブルシューティングに対するアプローチを合理化し、セキュリティ体制を全体的に強化できます」と説明しています。

最初のステップは、ASA デバイス全体における現在のポリシー構造を把握することでした。Chris 氏や彼のチームは、Cisco Defense Orchestrator を、現在導入済みのポリシーを検出するのに役立つプラットフォームだと考えています。

Defense Orchestrator は、シスコ セキュリティ製品全体に対するセキュリティ ポリシーの管理を簡素化します。この製品により、ネットワーク オペレーション チームは、一元的かつ一貫してポリシーをオーケストレーション/管理でき、最新の脅威から組織を保護できます。ポリシーは、デバイスのグループや条件（オブジェクト）に応じて適用できます。

Defense Orchestrator はクラウドベースのアプリケーションであることから、Chris とそのチームには 24 時間以内にシスコ アカウントが付与され、従来から使用している ASA ファイアウォールを数分間でオンボーディングできました。オンボーディング時に、Shawmut の IT チームは、以下のような一般的な問題について素早く確認できました。

重複したオブジェクト

これらは、命名スキームが異なる一方で、オブジェクト内のコンテンツは共通しているオブジェクトです。たとえば、あるオブジェクトを「Web プロキシ サーバ」と呼んでおり、別のオブジェクトを「コンテンツ サーバ」と呼んでいる場合でも、オブジェクトの詳細が完全に一致する場合などが想定されます。Defense Orchestrator では、名前を取捨選択し、オブジェクトをマージすることで、設定内のオブジェクト数を削減できます。

未使用のオブジェクト

これらは現在 ASA の設定内で使用されていないオブジェクトであり、トラブルシューティングおよびコンプライアンス上の問題となる可能性があります。非常に多い例は、お客様が Cisco Adaptive Security Device Manager を使用して ASA の設定を管理している場合です。デフォルトでは、Device Manager は「DM-Inline」というオブジェクトを作成しますが、これはお客様の設定では意味を成しません。Defense Orchestrator を使用することで、環境で使用されていないオブジェクトを削除し、設定をより簡素にできます。

一貫性のないオブジェクト

「一貫性のないオブジェクト」とは、ASA プラットフォーム間では名前が同じなのに、デバイス間ではコンテンツが異なるオブジェクトを指します。これはトラブルシューティング上の問題となるだけでなく、脆弱性の原因となる可能性もあります。たとえば、オブジェクト内で特定の国をブロックするために「国ブロック リスト」を使用しており、すべての ASA 次世代ファイアウォールで同じリストをブロックするようにしようとしている場合などが想定されます。Defense Orchestrator を使用することで、不整合を検出し、すべてのオブジェクトをマージして、プラットフォーム全体でオブジェクトの一貫性を確保できます。

Defense Orchestrator により、チームはこうした問題を素早く検出し、問題を数分間で修復できます。

関連情報

cdosales@cisco.com までご連絡ください。

製品とサービス

- Cisco Defense Orchestrator
- Cisco ASA 5500-X with FirePOWER サービス シリーズ

Chris 氏は、「Cisco Defense Orchestrator によって、重複したオブジェクト、未使用のオブジェクト、整合性のないオブジェクトを判別するプロセスが自動化され、オブジェクトの結合や削除が非常に簡単になりました。」「このソリューションによって、負担のかかる手動の作業に費やす日数が減り、有効なオブジェクトを誤って削除するリスクが大幅に削減されたのです」と述べています。

Shawmut 社では Defense Orchestrator を使用することで、安定したポリシー構造を素早く実現でき、自社のセキュリティ ポリシーをプロアクティブに管理できるようになりました。ポリシーを一元管理できるようになり、一貫性も確保しています。

Chris 氏は、「当社のセキュリティ ニーズは進化を続けており、使用するシスコ ソリューションのポートフォリオも拡大する可能性があります。Defense Orchestrator を利用することで、環境全体におけるセキュリティ ポリシーを一元的に、かつ一貫した方法で管理できます」と付け加えています。

Defense Orchestrator は、シスコのファイアウォール、次世代ファイアウォール、および OpenDNS と連携します。何千ものデバイスを対象にしたポリシー変更を、簡単かつ一元的にオーケストレーションできます。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C36-738171-00JA 17.07