infoblox

活用事例

Oxnard Union High School District、Infoblox のネットワークインテリジェンスを活用してプロアクティブなセキュリティを実現

概要

カリフォルニア州ベンチュラ郡に位置する Oxnard Union High School District（OUHSD、オックスナード合同高校区）は、9 年生から 12 年生までの生徒を対象とする 13 校で構成されています。

この地区はオックスナード平原にまたがり、オックスナード、ポートヒューニーメ、カマリロの各都市、およびエルリオ、ソミス、チャンネル諸島ビーチといった近隣の非法人コミュニティも管轄しています。

> *BloxOne Threat Defense を導入したことで、学区全体のユーザーとデバイスをサイバー攻撃から守り、インシデントを未然に防ぐ能力に自信を持てるようになりました。*
>
> **Juan Castano**
> **上級ネットワーク管理者、**
> **Oxnard Union High School District**

状況

統一されていないネットワーク運用

学区は、約 17,000 人の生徒と 1,900 人の教職員一人ひとりに、学習成果を最大化するために必要なテクノロジーとサポートを提供しています。OUHSD の上級ネットワーク管理者 Juan Castano 氏にとって、これは協力して取り組むべき課題です。「全員が協力してネットワークの課題に取り組むのです。」

同地区の学校は、生徒にChromebookまたはWindowsノートパソコンを提供し、インターネット接続、オンラインポータル、その他のデジタルサービスを提供しています。ネットワークとセキュリティの観点から、OUHSDは学生や教職員が日中に使用する多様なラップトップ、タブレット、その他の個人用電子機器にも対応しなければなりません。

このような背景の中で、地区の重要なネットワークサービス管理の環境は、時間の経過とともに進化し、Microsoft DNS や Active Directory、カスタムドメインコントローラーなどの異なるソリューションが導入されるようになりました。また、特定のネットワークゾーンでは Infoblox NIOS も使用されていました。セキュリティ面では、Castano 氏と彼が協力する 15 名の現場技術者には、セキュリティイベントを事前に検知して阻止するための信頼できる手段がありませんでした。

OXNARD UNION HIGH SCHOOL DISTRICT
Creating Prosperity through Equity, Inquiry, and Wellness

課題

DNS の競合と時間のかかるセキュリティ対策

2 年前に Castano 氏が現在の職務に就いたとき、OUHSD のネットワークインフラストラクチャが業務効率を妨げているのは明らかでした。業務の効率化を図るため、彼と同僚たちは旧式で不要になったサーバーやサービスの削減を始めました。しかし作業を進める中で障害が発生し、一部のサービスにアクセスできなくなる事態が起きました。「何をやってもうまくいきませんでした」と、彼は当時を振り返ります。

根本原因は、DNS、DHCP、IP アドレス管理（これらを総称して DDI と呼ぶ）に分断されたソリューションを使用していたことにあると、すぐに判明しました。これらは、現代のネットワーク通信に不可欠な基盤です。学区の IT インフラストラクチャは時間の経過とともに進化し、DNS トラフィックは Microsoft DNS サーバーおよび Infoblox NIOS サーバーへルーティングされるよう構成されていました。その結果として発生した DNS の競合が、ネットワークのパフォーマンスに影響を与えていました。さらに、ネットワーク機器の時刻を同期させる Network Time Protocol（NTP）などの基本機能も、複数のシステム上で動作していました。「すべてが相互に参照し合っている状態で、収拾がつかない状況でした」と Castano 氏は語ります。

ネットワーク管理上の課題に加えて、OUHSD は脅威の調査および対応に時間がかかることによる深刻なセキュリティの問題にも直面していました。Castano 氏と同僚がセキュリティアラートを受け取った際には、関係するデバイスの特定、脅威の詳細の解明、封じ込めやその他の対応措置の開始といった作業を、複数のツールを行き来しながら、手順を踏んで長時間かけて実施しなければなりませんでした。このプロセスは非常に時間がかかるだけでなく、完全に後手に回っていました。「すべての調査作業が終わった頃にはすでに手遅れで、応急処置を施すしかありませんでした」と Castano 氏は述べています。「ひとつのマルウェアを突き止めて調査するだけで、まるごと 1 フェーズ費やすことになりますし、それが単独のマルウェアであることを祈るしかないのです。平均的な調査時間は 4 時間にも及んでいました。」

このような反応的なセキュリティ体制は、以前から懸念されていたものの、米国国土安全保障省（DHS）からの連絡を受けたことで、その脆弱さがより一層明確になりました。当局からの通報によって、学区内のネットワーク上の 1 台の端末が、ランサムウェア攻撃の可能性を示す不審な活動を検知されたことが明らかになりました。ある生徒が、学校の課題で使用するテンプレートをダウンロードしようとビジネス向けのウェブサイトにアクセスしたところ、悪意のある実行ファイルが含まれていました。

OUHSD のセキュリティ対策ではこの活動を検知できなかったものの、FBI のシステムは検出しました。問題の端末は迅速に対応され、被害はありませんでしたが、この一件は学区に強い警鐘を鳴らすこととなりました。「まさに厳しい現実を突きつけられた出来事でした」と Castano 氏は述べています。

お客様： *Oxnard Union High School District（OUHSD）*
業種： *教育*
所在地： *カリフォルニア州オックスナード*

目的：

- DNS、DHCP、IPAM の複数のシステムによって生じるネットワークの競合の解決
- サーバーのスプロールの抑制と運用効率の向上
- ネットワークの管理および脅威調査に必要な手作業の削減

結果：

- DNS 管理を単一で使いやすいソリューションに統合
- トレーニング不要の Web インターフェースで、重要なネットワークサービスの管理を簡素化
- 脅威調査の平均所要時間を 4 時間から 20 分に短縮

製品：

- NIOS DDI
- BloxOne Threat Defense

解決策

DNS の統合、プロアクティブな脅威検知、包括的な可視性の実現

Castano 氏にとって、学区が抱える慢性的なネットワークの問題に対する答えは、DNS および NTP のすべての機能を、既に導入していた DDI に対応可能なソリューション、つまり Infoblox NIOS に統合することでした。「Windows マシンにあるレコードと Infoblox にある別のレコードを同期させるという複雑な構成をやめ、すべてを NIOS Grid に集約することにしたのです」と彼は振り返ります。

この移行では、Microsoft DNS および追加のドメインコントローラーに存在していた主要な DDI 機能を Infoblox に移す作業が含まれていました。Castano 氏は、移行を中断なくスムーズに進められたのは Infoblox プロフェッショナルサービスによる支援のおかげだと述べています。「サポートは本当に素晴らしく、移行も非常にスムーズに行えました」と語ります。現在、学区の DDI および NTP 機能は、2 台の仮想 NIOS サーバー上で稼働する NIOS Grid によって管理されています。ランサムウェアのインシデントを受けて、OUHSD は脅威の見落としを防ぐと同時に、Castano 氏とそのチームがよりプロアクティブに対応できるよう、攻撃の実行前に脅威を特定して無効化できるソリューションを模索しました。学区は、Infoblox プロフェッショナルサービスと連携し、BloxOne Threat Defense Advanced をバリュー検証（PoV）ベースで導入しました。このソリューションは、学区のネットワークインフラストラクチャに接続されたすべてのデバイスに対する集中管理と可視性、AI および機械学習による振る舞い検知、さらに包括的なイベント調査と対応機能を提供します。導入後すぐに、従来のマルウェア対策や脅威検出ツールでは見逃されていた脅威や異常の検出が始まりました。「本当に目から鱗でした。ユニークな検出数の多さには驚かされました」と Castano 氏は述べています。「私たちの目に見えていなかっただけで、実際には多くのことがずっと起こっていたのです。」

結果

効率性の向上とセキュリティの強化

不要なハードウェアを排除し、DDI 機能を Infoblox に統合したことで、学区のネットワークインフラストラクチャははるかにスリムかつ効率的になりました。現在、Castano 氏とネットワーク技術者たちは、各校のネットワークを単一のプラットフォームで管理しています。「今ではすべてが NIOS に集約されており、すべてのネットワークが一箇所にまとまっています。各ネットワークに簡単にアクセスして、予約済み IP、固定 IP、リースの情報をすぐに確認できます」と Castano 氏は述べています。

よりシンプルな環境に加え、NIOS は Castano 氏とその IT チームに、Web インターフェースを起点とした卓越した操作性と利便性を提供しています。「トレーニングは一切不要で、何が起きているのかすぐにわかります。新しい学校やサイトを追加する必要があるときでも、すぐに同じ設定を再現できるので本当に便利です。すべてが問題なくスムーズに動作します。」

Castano 氏にとって、学区のユーザーとデータを守る作業も、Infoblox によってはるかに効率的になりました。たとえば、BloxOne Threat Defense のフィルタリング機能により、生徒や教職員による悪意あるドメインへのアクセスが自動的にブロックされるため、OUHSD は国土安全保障省（DHS）に通報されるような事態を未然に回避できるようになっています。この機能は、Infoblox の膨大な DNS データと最新の脅威インテリジェンスを活用し、他のソリューションでは見逃されるセキュリティ問題を特定します。その結果、Castano 氏はハッキング、マルウェア、NX ドメイン、疑わしい IP アドレスに関連する宛先を、高精度かつ容易にブロックでき、正当なトラフィックが妨げられることなく流れることを保証できます。Infoblox フィルタリングのプロアクティブな性質は、Castano 氏に安心感を与えています。「BloxOne Threat Defense のおかげで、私たちは地区全体の各ユーザーとデバイスをサイバー攻撃から守り、インシデントを未然に防ぐ能力により自信を持てるようになりました。」

現在では、セキュリティイベントが発生した際に、Infoblox から得られる包括的な脅威の可視性によって、Castano 氏の対応時間は大幅に短縮されています。「これまで 4 時間かかっていた作業が、今では約 20 分で済むようになりました。」重要なデバイスのコンテキスト情報は、IPAM ソリューションから自動的に収集され、セキュリティアラートとともに提供されます。BloxOne Threat Defense の Dossier 機能は、これまで手間のかかっていた脅威調査の多くのステップを自動化し、脅威そのものや関与しているアクター、ホスティング元の WHOIS データなどを分析担当者が把握できるよう支援します。「必要な情報がすべて一か所に集約されて表示されるので、わざわざ手作業で探し回る必要がなく、本当に助かっています。大幅な時間の節約になっています。」

サイバーセキュリティやネットワーク管理において、時間は何よりも重要です。Infoblox のおかげで、Castano 氏とその同僚は、ネットワークとセキュリティのタスクを容易に切り替えられる単一の環境を通じて、さらに多くの時間を節約できています。これは、少人数で複数の役割をこなす必要がある中小規模の組織にとって大きなメリットです。たとえば、ネットワーク上の端末で不審な DNS アクティビティが発生した場合、Castano 氏はそのデバイスの DNS 履歴をすばやく調査し、不適切な動作や疑わしい Web アプリの利用、実際のサイバー脅威の活動を確認できます。NIOS から得られる豊富なデバイスデータにより、これらのイベントに関するユーザー情報やデバイス情報といった詳細なコンテキストが自動的に提供されます。「NIOS にすべての情報がきれいに整理されているおかげで、イベントの発生場所だけでなく、現場のどの建物で起きたのかまで、すばやく特定できるのです」と Castano 氏は述べています。サイバー脅威の活動が特定されると、チームは BloxOne Threat Defense の迅速な機能を活用して、該当するデバイスを自動的に隔離・修復することができます。

ネットワークとセキュリティを Infoblox に統合したことで、OUHSD はネットワークのパフォーマンスとセキュリティの強化に加え、Castano 氏とそのチームに革新のための自由ももたらしました。「毎日、すべてが正常に稼働しているかを確認するのに、多くの時間を費やす必要がなくなりました」と彼は語ります。「Infoblox のおかげで、将来を見据えた計画に時間を使えるようになりました。こうした時間の節約は非常に重要です。もしなければ、日々の業務に追われるだけで、何も前に進まなかったと思います。」

Infoblox株式会社
〒107-0062 東京都港区南青山2-26-37
VORT外苑前I
3F

03-5772-7211
www.infoblox.com

バージョン：20241004v1