infoblox

ÉTUDE DE CAS

Le district scolaire d'Oxnard Union s'appuie sur l'intelligence réseau pour assurer une sécurité proactive avec Infoblox

LE RÉSUMÉ

Le district scolaire d'Oxnard Union High (OUHSD), situé dans le comté de Ventura, en Californie, se compose de 13 écoles qui accueillent des élèves de la 9e à la 12e année du système scolaire américain.

Elle englobe la plaine d'Oxnard, y compris les villes d'Oxnard, Port Hueneme et Camarillo, ainsi que les communautés non constituées voisines d'El Rio, Somis et Channel Islands Beach.

LA SITUATION

Opérations réseau disparates

La circonscription fournit à chacun de ses quelque 17 000 étudiants et 1 900 membres du corps enseignant et du personnel, la technologie et le soutien dont ils ont besoin pour maximiser les résultats d'apprentissage. Pour Juan Castano, administrateur réseau principal de OUHSD, il s'agit d'un projet collaboratif. « Tout le monde travaille ensemble pour faire avancer les choses. »

Les écoles de la circonscription fournissent aux élèves des Chromebooks ou des ordinateurs portables Windows, ainsi qu'une connectivité Internet, des portails en ligne et d'autres services numériques. Du point de vue du réseau et de la sécurité, OUHSD doit également tenir compte de la diversité d'ordinateurs portables, de tablettes et d'autres appareils électroniques personnels utilisés par les élèves et le corps enseignant tout au long de la journée.

Dans ce contexte, le paysage dans lequel s'inscrit la gestion des services réseau essentiels de la circonscription a évolué au fil du temps pour inclure des solutions disparates, y compris Microsoft DNS et Active Directory, ainsi que des contrôleurs de domaine personnalisés. La circonscription a également utilisé Infoblox NIOS pour certaines zones de réseau. Sur le plan de la sécurité, M. Castano et les 15 techniciens de terrain avec lesquels il travaille ne disposaient d'aucun moyen fiable pour détecter et bloquer les événements de sécurité avant qu'ils ne se produisent.

> *« Depuis que nous bénéficions de BloxOne Threat Defense, nous nous sentons beaucoup plus confiants dans notre capacité à protéger chaque utilisateur et chaque appareil de la circonscription contre les cyberattaques et à empêcher les incidents avant qu'ils ne se produisent »*
>
> **Juan Castano**
> **Administrateur réseau senior,**
> **Oxnard Union High School District**

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

LES DÉFIS

Conflits DNS et sécurité chronophage

Lorsque M. Castano a accédé à son rôle actuel il y a deux ans, il était clair que l'infrastructure réseau de la circonscription OUHSD entravait son efficacité. Pour rationaliser les opérations, lui et ses collègues ont commencé à éliminer les serveurs et services considérés comme obsolètes. Cependant, ils ont rencontré dès le début des défaillances et ont remarqué que certains services étaient devenus inaccessibles. « Rien ne fonctionnait tout simplement », se souvient-il.

La cause profonde a rapidement été attribuée à des solutions disparates pour le DNS, le DHCP et la gestion des adresses IP (que l'on appelle collectivement le DDI), qui rendent possibles toutes les interactions réseau modernes. Au fil de l'évolution de l'infrastructure informatique de la circonscription, le trafic DNS a été configuré pour être dirigé vers les serveurs DNS de Microsoft et les serveurs NIOS d'Infoblox, mais les conflits DNS résultants ont affecté les performances du réseau. En outre, des fonctionnalités de base, telles que le protocole de temps réseau (NTP), qui synchronise les horloges des ordinateurs sur les appareils du réseau, étaient exécutées sur plusieurs systèmes. « Rien n'était fait correctement. C'était un vrai chaos », déclare M. Castano.

Outre les préoccupations liées à la gestion du réseau, la circonscription OUHSD a également dû faire face à des problèmes de sécurité urgents en raison de processus d'investigation et de réponse aux menaces chronophages. Lorsque M. Castano et son équipe recevaient une alerte de sécurité, ils devaient se lancer dans une longue et complexe enquête, passant d'un outil à l'autre pour identifier le ou les appareils concernés, obtenir des informations sur la menace, et engager des mesures de confinement ou d'autres actions de réponse. En plus d'être chronophage, ce processus était très réactif. « Une fois l'enquête terminée, il était déjà trop tard et nous avons dû improviser une solution, »se souvient M. Castano. « Une phase entière était consacrée à la recherche et à la découverte d'un seul malware, si bien que vous espériez qu'il n'y en ait pas d'autres. En moyenne, une enquête nous prenait quatre heures. »

La stratégie de sécurité réactive de la circonscription, qui était déjà source de préoccupation, est devenue évidente lorsque le Département de la Sécurité intérieure des États-Unis (DHS) est intervenu. Celui-ci a alerté la circonscription que l'une des machines de son réseau avait été signalée pour une activité indiquant une attaque potentielle par ransomware. Pour réaliser un devoir, un élève avait accédé à un site web pour télécharger un modèle qui contenait un fichier exécutable malveillant.

Si les mesures de sécurité de OUHSD n'avaient pas repéré l'activité, le FBI lui ne l'avait pas manquée. La machine concernée a été rapidement remise en état, sans qu'il n'y ait de dommages, mais l'incident a attiré l'attention de la circonscription. « Nous avons été brutalement rappelés à la réalité », déclare Juan Castano.

Client : *Oxnard Union High School District*
Secteur : *Éducation*
Lieu : *Oxnard, Californie, États-Unis*

LES OBJECTIFS :

- Résolver les conflits de réseau créés par la présence de plusieurs systèmes pour DNS, DHCP et IPAM
- Consolider les serveurs et augmenter l'efficacité opérationnelle
- Réduire les efforts manuels nécessaires pour gérer le réseau et enquêter sur les menaces

LES RÉSULTATS :

- Consolidation de la gestion DNS en une solution unique et facile à utiliser
- Gestion simplifiée des services réseau essentiels avec une interface web qui ne nécessite aucune formation
- Réduction du temps moyen d'investigation des menaces, de 4 heures à 20 minutes

LES PRODUITS :

- NIOS DDI
- BloxOne Threat Defense

LA SOLUTION

Consolidation des DNS, détection proactive des menaces et visibilité complète

Pour M. Castano, la solution aux problèmes de réseau chroniques qui touchaient la circonscription consistait à regrouper toutes les responsabilités DNS et NTP au sein de la solution qu'ils possédaient déjà et qui était capable de gérer tous leurs besoins en matière de DDI : Infoblox NIOS. « Plutôt que de garder cette configuration trop compliquée avec des enregistrements sur certaines machines Windows et d'autres sur Infoblox que nous essayions de synchroniser, nous avons décidé de transférer le tout vers le Grid NIOS », se souvient-il.

Pour réaliser cette migration, il a fallu transférer des fonctionnalités DDI clés de Microsoft DNS et des contrôleurs de domaine supplémentaires vers Infoblox. M. Castano attribue le bon déroulement de la migration aux services professionnels d'Infoblox, qui ont assisté son équipe. « Leur soutien a été extraordinaire. La transition s'est vraiment bien passée. » Aujourd'hui, toutes les fonctions DDI et NTP de la circonscription sont gérées par le Grid NIOS, qui fonctionne sur deux serveurs NIOS virtuels. À la suite de l'incident de ransomware, OUHSD a cherché une solution qui éliminerait les zones d'ombre ayant permis aux menaces de passer inaperçues, mais qui permettrait aussi à Juan Castano et à son équipe d'être plus proactifs, en détectant et neutralisant les menaces dans les premières instances du cycle d'attaque, avant qu'elles ne soient activées. La circonscription a collaboré avec les services professionnels d'Infoblox pour déployer BloxOne Threat Defense Advanced dans le cadre d'une preuve de valeur. La solution offre une visibilité et un contrôle centralisés pour chaque appareil connecté à l'infrastructure réseau de la circonscription, une détection comportementale des menaces par l'IA et l'apprentissage automatique, ainsi que des fonctionnalités complètes d'investigation et de réponse aux incidents. Dès que la solution a été opérationnelle, elle a commencé à détecter des menaces et des anomalies qui avaient échappé aux outils de détection des menaces et malwares que possédait la circonscription. « Ça nous a ouvert les yeux. Le nombre de détections uniques était étonnamment élevé, déclare M. Castano Il y a énormément de choses que nous ne soupçonnions pas. »

LES RÉSULTATS

Efficacité améliorée, sécurité renforcée

En éliminant le matériel superflu et en consolidant les fonctionnalités DDI avec Infoblox, l'infrastructure réseau de la circonscription est devenue bien plus simple et efficace. M. Castano et ses techniciens réseau disposent désormais d'une plateforme unique pour gérer les réseaux de chaque établissement de la circonscription. « Maintenant que tout est centralisé sur NIOS, je retrouve tous mes réseaux au même endroit, explique Juan Castano. Je peux facilement accéder à chaque réseau, voir les adresses IP réservées, les adresses IP fixes et les baux. »

Outre un environnement rationalisé, NIOS offre à M. Castano et à son équipe informatique une simplicité et une facilité d'utilisation inégalées, en commençant par l'interface web. « Aucune formation n'est nécessaire pour apprendre à l'utiliser. Ça coule de source. Les actions sont faciles à reproduire à chaque fois que nous ajoutons un nouvel établissement ou un nouveau site. Tout fonctionne à la perfection. »

D'après M. Castano, la protection des utilisateurs et des données de la circonscription a également gagné en efficacité grâce à Infoblox. Par exemple, les fonctionnalités de filtrage de BloxOne Threat Defense empêchent automatiquement les élèves et les membres du corps enseignant d'accéder à des domaines malveillants, permettant ainsi à OUHSD d'éviter des événements inquiétants comme celui qui a attiré l'attention de la sécurité intérieure. Cette fonctionnalité exploite l'immense base de données DNS d'Infoblox, ainsi que la threat intelligence à jour, qui signale les problèmes de sécurité que d'autres solutions ne peuvent pas repérer. M. Castano peut donc facilement bloquer les destinations associées au piratage, aux malwares, aux domaines NX et aux adresses IP douteuses, avec un haut degré de précision, et garantit ainsi que le trafic légitime circule sans problème. Grâce à la nature proactive du filtrage d'Infoblox, M. Castano a l'esprit tranquille. « Depuis que nous bénéficions de BloxOne Threat Defense, nous nous sentons beaucoup plus confiants dans notre capacité à protéger chaque utilisateur et chaque appareil de la circonscription contre les cyberattaques et à empêcher les incidents avant qu'ils ne se produisent. »

Aujourd'hui, lorsque des événements de sécurité se produisent, M. Castano peut réagir bien plus rapidement grâce à la visibilité complète des menaces dont il bénéficie grâce à Infoblox. « Ce qui me prenait habituellement quatre heures ne me prend désormais que 20 minutes. » Les informations contextuelles critiques sur l'appareil sont automatiquement recueillies par la solution IPAM et partagées avec des alertes de sécurité. La fonctionnalité Dossier dans BloxOne Threat Defense automatise de nombreuses étapes d'investigation fastidieuses pour aider les analystes à mieux comprendre la menace, les acteurs qui en sont à l'origine, les données WHOIS du site d'hébergement, et plus encore. « C'est bien plus pratique d'avoir toutes les informations recueillies automatiquement et disponibles au même endroit, plutôt que de devoir les chercher manuellement. C'est un gain de temps considérable. »

Pour la cybersécurité ou la gestion du réseau, le temps est essentiel. Grâce à Infoblox, M. Castano et son équipe gagnent encore plus de temps grâce à un environnement unique qui facilite la navigation entre les tâches de réseau et de sécurité. C'est un réel avantage pour les petites et moyennes entreprises comme la leur, où chaque employé n'a d'autre choix que de porter plusieurs casquettes. Par exemple, lorsqu'une activité DNS suspecte se manifeste sur une machine du réseau, M. Castano peut rapidement examiner l'historique DNS de l'appareil à la recherche d'un comportement inadéquat, d'une utilisation suspecte d'une application web ou d'une véritable cybermenace. Les données détaillées des appareils du NIOS fournissent automatiquement le contexte autour de ces événements, y compris des informations précises sur les utilisateurs et les appareils. « Comme tout est bien classé dans le NIOS, je peux rapidement déterminer non seulement le site d'un événement, mais aussi le bâtiment précis au sein de ce site. » Une fois la cybermenace identifiée, l'équipe peut compter sur la réactivité de BloxOne Threat Defense pour isoler automatiquement et corriger un appareil compromis.

L'intégration du réseau et de la sécurité à Infoblox permet non seulement à OUHSD d'améliorer les performances et la protection du réseau, mais elle offre également à M. Castano et à ses associés la liberté d'innover. « Je ne passe pas la plupart de ma journée à vérifier que tout va bien, observe-t-il. Infoblox me permet de me concentrer sur les projets à venir, et ces gains de temps sont essentiels, sans quoi je passerais mon temps à gérer des tâches opérationnelles répétitives. »

Siège social
2390 Mission College Boulevard,
Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version : 20241004v1