infoblox.

TÉMOIGNAGE CLIENT

San Francisco affine la visibilité sur ses opérations réseau afin de renforcer sa posture de sécurité

PRÉSENTATION

San Francisco possède une riche histoire d'innovation, de progrès culturel et d'événements notables.

De la ruée vers l'or du milieu du XIXe siècle au Summer of Love et à l'émergence de l'industrie technologique à l'ère du numérique, San Francisco est depuis longtemps considérée comme un centre économique et d'innovation technologique. Toutefois, ce statut international prestigieux fait également de la ville et de son infrastructure informatique des cibles de choix pour les pirates informatiques et les attaques malveillantes. Nathan Sinclair, responsable des opérations de cyberdéfense pour la ville et le comté de San Francisco, le sait que trop bien. Heureusement, avec l'aide d'Infoblox, N. Sinclair et son équipe ont été en mesure de maintenir un excellent record de temps de fonctionnement ininterrompu et de disponibilité des services pour les plus de 17 000 employés de la ville, les secouristes et les élus, ainsi que pour plus de 800 000 citoyens et des millions de visiteurs qui consultent chaque année les sites web et les services en ligne gérés par la ville.

LE DÉFI :

Protéger la marque San Francisco et maintenir les services publics

Comme pour de nombreuses municipalités ces dernières années, les ransomwares ont été au cœur des efforts de cybersécurité de la ville. Pourtant, contrairement à de nombreuses autres villes des États-Unis qui subissent des pannes dues à des attaques de ransomware et dont la reprise des services en ligne est lente, San Francisco a eu la chance d'éviter les pires effets des cyberattaques. « Avec l'émergence des ransomwares comme une préoccupation majeure en matière de sécurité dans notre secteur, ils ont naturellement attiré l'attention de notre direction informatique », a expliqué N. Sinclair « En fin de compte, cette attention portée à l'ensemble de l'organisation nous a aidés à lancer des initiatives stratégiques pour mieux lutter contre ces attaques ».

Client : *Ville et comté de San Francisco*
Secteur : *Gouvernement*
Lieu : *San Francisco, Californie*

LES INITIATIVES :

- Améliorer la visibilité du réseau pour renforcer la défense contre les attaques de ransomware, de phishing et d'usurpation de sites web.
- Renforcer la capacité de l'équipe à détecter et à contrer l'impact des domaines similaires.
- Assurer une disponibilité réseau ininterrompue pour plus de 17 000 employés, secouristes, élus et résidents de la ville.

LES RÉSULTATS :

- En collectant automatiquement les données de journal de l'infrastructure DDI de la ville, BloxOne Threat Defense fournit des insights instantanés et complets sur les flux de trafic entrants et sortants, éliminant les spots DNS pour une sécurité accrue.
- La threat intelligence en continu permet à l'équipe d'appliquer immédiatement de nouvelles règles de blocage, stoppant ainsi les attaques dans leur élan et prévenant les dommages potentiels.

Nathan et l'équipe de San Francisco ont également dû faire face à des attaques incessantes de phishing et de falsification de sites web. Chaque semaine, ils constatent des dizaines d'attaques de phishing, dont certaines pourraient être des exploits de ransomware, mais qui sont le plus souvent des tentatives grossières pour inciter les destinataires à initier le traitement de transactions frauduleuses. De même, des pirates ont à plusieurs reprises mis en place des sites web frauduleux imitant de près l'aspect et la convivialité des propriétés web authentiques de la ville de San Francisco. La présence en ligne étendue des propriétés web de la ville, y compris de multiples pages dans le domaine principal SF.GOV et les sites connexes, crée une surface d'attaque significative, en particulier en termes d'exposition aux exploits de domaine similaire.

« Nous avons vu de nombreux cas où des pirates ont mis en place des sites web sosies pour faire croire qu'ils étaient une organisation municipale, soit pour collecter des informations personnelles, soit pour payer des amendes routières ou autres », a déclaré N. Sinclair. « Certains sont amateurs et faciles à repérer, mais beaucoup ont l'air remarquablement réels. Nous disposions de certains outils de sécurité capables de détecter et de bloquer ce type d'activités, mais pas au niveau de la couche DNS. C'était un angle mort que BloxOne Threat Defense nous a permis de résoudre et de renforcer notre posture de sécurité ».

LA SOLUTION :

Extension de la mise en œuvre d'Infoblox par la ville avec BloxOne Threat Defense

San Francisco utilise Infoblox NIOS, basé sur des appliances Trinzic, depuis de nombreuses années pour gérer ses opérations DNS, DHCP et IPAM (DDI). Cependant, bien qu'étant un client de longue date, N. Sinclair et son équipe de sécurité ne connaissaient pas très bien les offres d'Infoblox en matière de sécurité. Cela était dû en grande partie aux meilleures pratiques informatiques conventionnelles selon lesquelles les équipes de mise en réseau sont responsables de la gestion de l'infrastructure DDI tandis que les équipes de sécurité sont responsables de la gestion des systèmes de gestion des informations et des événements de sécurité (SIEM), ainsi que des systèmes d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR). Cette approche organisationnelle ne donne à l'équipe de sécurité qu'une visibilité minimale sur ce qui se passe du côté du réseau. Toutefois, dans le monde post-Covid, où le travail à distance et les architectures cloud/hybrides sont devenus monnaie courante, cette répartition des tâches n'était plus viable. La nécessité d'une collaboration plus étroite entre les équipes chargées des réseaux et de la sécurité est devenue évidente.

« Avec la séparation des tâches que nous avions mise en place, ma seule activité réelle avec Infoblox consistait à obtenir des quantités nominales de données de réseau de l'instance NIOS pour les intégrer dans notre pile SIEM/SOAR afin de vérifier la présence de trafic suspect », a expliqué Sinclair. « Mais en consultant l'un des départements de notre organisation cliente, nous avons découvert qu'il avait récemment adopté BloxOne Threat Defense et qu'il nous avait fait une démonstration. Nous avons immédiatement reconnu qu'il s'agissait d'une solution offrant une visibilité complète sur les vulnérabilités du réseau. Ce serait un outil puissant pour bloquer les exploits, stopper les incursions avant qu'elles ne fassent des dégâts et renforcer nos défenses en général. »

BloxOne Threat Defense opère au niveau du DNS pour identifier les menaces que les autres solutions ne voient pas et arrêter les attaques plus tôt dans le cycle de vie de la menace. Grâce à une automatisation omniprésente, à l'apprentissage automatique et à l'intégration de l'écosystème, BloxOne Threat Defense améliore également l'efficacité des opérations de sécurité (SecOps) afin d'optimiser l'efficacité de l'infrastructure de sécurité existante basée sur les fonctionnalités SIEM/SOAR. « Nous avons immédiatement réalisé que, d'un point de vue fonctionnel, BloxOne Threat Defense renforcerait nos capacités de sécurité sur deux fronts », a déclaré M. Sinclair. « Tout d'abord, parce qu'il

- BloxOne Threat Defense assure une sécurité adaptable pour les travailleurs à distance et les endpoints, offrant une tranquillité d'esprit, peu importe l'endroit.

LES SOLUTIONS :

- BloxOne Threat Defense

s'intègre à NIOS, c'est un outil qui permet à mon équipe de faire son travail sans jamais avoir à demander à l'équipe réseau de nous donner accès aux appareils qu'elle gère. Nous voyons toutes ces données, qu'il s'agisse d'appareils de gestion d'adresses IP ou de DNS central. Ensuite, si l'équipe réseau souhaite nous transmettre des règles pour traiter les menaces émergentes, par exemple, nous disposons désormais d'un outil qui nous permet de mettre en œuvre nos propres processus de sécurité. C'est notre outil, il nous appartient. »

LES RÉSULTATS :

Meilleure visibilité, application des règles et protection pour les travailleurs à distance

Nathan et l'équipe de sécurité de San Francisco considèrent que la mise en œuvre de BloxOne Threat Defense apporte des améliorations spectaculaires à la cybersécurité de la ville dans trois domaines principaux :

Visibilité globale – Comme mentionné ci-dessus, BloxOne Threat Defense collecte automatiquement toutes les données de journalisation de l'infrastructure DDI de la ville. Il restitue ensuite instantanément ces données sous forme de graphiques, de diagrammes et de hiérarchies faciles à comprendre, afin de peindre une image complète de ce qui entre et sort exactement des systèmes DNS du réseau. Auparavant, les opérations DNS constituaient un angle mort pour Nathan et son équipe. Ce manque de visibilité constituait une faiblesse majeure en matière de sécurité, car les pirates informatiques malveillants ont concentré leurs attaques sur la couche DNS au cours des dernières années. Jusqu'à 80 % des malwares utilisent aujourd'hui le DNS pour lancer des procédures C2 qui peuvent être utilisées pour voler des données et propager des malwares (recherche de l'unité 42). Le tunneling DNS et les malwares utilisant des algorithmes de génération de domaines sont également largement répandus.

Mise en œuvre des règles de blocage — Avant le déploiement, l'application de nouvelles règles de blocage pour renforcer la sécurité exigeait que Nathan et l'équipe de sécurité collaborent avec plusieurs parties prenantes au sein de l'organisation pour garantir une application uniforme. Aujourd'hui, ils peuvent appliquer de nouvelles règles sans avoir à solliciter une autre équipe. Comme l'a dit Sinclair : « Avec BloxOne Threat Defense, nous disposons de Threat Intelligence provenant d'Infoblox et de partenaires qui alimentent en continu notre pile de sécurité, ce qui nous permet d'agir sur les menaces plus rapidement que jamais. Ces renseignements permettent à BloxOne Threat Defense de nous alerter sur les menaces critiques, de sorte que nous savons quand nous devons bloquer immédiatement les menaces imminentes. Par le passé, nous n'étions pas toujours en mesure d'agir en temps voulu. C'est une avancée majeure pour nous. »

Protections pour les travailleurs à distance — Comme pour la plupart des organisations confrontées à la Covid, la prise en charge des travailleurs à distance a constitué un défi de taille pour l'équipe de SF. « Au début, nous étions désemparés parce que tout ce que nous avions traditionnellement dans notre pile de sécurité était conçu pour protéger nos travailleurs dans les locaux de San Francisco », a déclaré N. Sinclair. « Mais cela nous a aussi permis d'accélérer de nombreux projets. Nous avons rapidement mis en place BloxOne Threat Defense parce que nous devions le faire pour protéger nos utilisateurs. Cette protection est désormais en place partout où nos utilisateurs travaillent, qu'ils soient de retour au bureau ou qu'ils travaillent encore à domicile. »

Nathan et son équipe ont constaté de nombreuses améliorations depuis la mise en œuvre de BloxOne Threat Defense. Une visibilité accrue du réseau, des capacités d'application renforcées et de meilleures protections pour les travailleurs à distance se sont avérées être des avantages précieux. Cependant, le plus grand changement a été la tranquillité d'esprit que BloxOne Threat Defense offre. L'équipe est désormais plus confiante dans sa capacité à détecter et à stopper les menaces critiques plus tôt. « Avec BloxOne, nous disposons d'un contexte beaucoup plus complet et d'une meilleure compréhension de nos données de sécurité. Au lieu d'essayer de comprendre et de corréler les données et de comprendre quelque chose comme : comment les requêtes DNS parviennent-elles à ce site Web ? Auparavant, cela demandait beaucoup de travail. Mais plus maintenant BloxOne nous a débarrassés de cette incertitude. »

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

+1.408.986.4000
www.infoblox.com/fr

Version : 20231120v1