infoblox

ÉTUDE DE CAS

Askari Bank modernise et renforce sa posture de cybersécurité avec Infoblox Threat Defense Advanced

PRÉSENTATION

Askari Bank a ouvert ses portes en avril 1992 et est devenue l'une des principales institutions financières du Pakistan.

Askari propose une gamme complète de services bancaires pour particuliers et entreprises, des services de banque par guichet automatique et mobile, ainsi que des cartes de crédit et de débit, et elle dispose de 537 agences au Pakistan. Depuis sa création, la banque s'est concentrée sur la croissance en améliorant la qualité de ses services, en investissant dans la technologie et les ressources humaines et en tirant parti de son vaste réseau d'agences, qui comprend des services bancaires islamiques et agricoles. La vision d'Askari est de soutenir avec passion le succès de ses clients et de les satisfaire par la qualité de ses services. Un élément clé de cet engagement envers le service est de garantir les plus hauts niveaux de confidentialité et de sécurité aux clients de la banque.

> *"Au cours des différents scénarios testés lors de la preuve de concept, aucune tentative d'infiltration ou d'exfiltration de données réussie n'a abouti. Voir BloxOne Threat Defense bloquer des activités malveillantes dans notre propre environnement nous a donné pleine confiance dans la solution Infoblox."*
>
> **Jawad Khalid Mirza**
> **CISO chez Askari Bank**

LE DÉFI

Renforcer la posture de sécurité pour contrer les menaces émergentes

Comme toutes les institutions financières à travers le monde, la banque pakistanaise Askari Bank est une cible privilégiée des cyberattaques malveillantes. Au fil des années, la banque a déployé plusieurs solutions de cybersécurité, notamment une solution SOAR (Security Orchestration, Automation and Response) et un produit de sécurité DNS Cisco sur lesquels elle mise depuis longtemps. En collaboration avec les consultants de Secure Networks, l'équipe d'Askari a compris que les menaces au niveau de la couche DNS avaient évolué au fil du temps et que l'exploration d'autres options en matière de technologie DNS pourrait contribuer à renforcer la sécurité globale de la banque.

askaribank LIMITED

« Comme nous le savons, le DNS n'a pas été conçu dans une optique de sécurité », a expliqué Jawad Khalid Mirza, responsable de la sécurité informatique chez Askari Bank. « L'architecture ouverte du DNS en a fait une cible de choix pour les pirates. Dans le secteur financier, ces menaces se manifestent le plus souvent par des tentatives d'exfiltration ou d'infiltration de données au sein des entreprises. »

« Les solutions de sécurité classiques sont conçues pour contrer les menaces en bloquant les requêtes DNS», explique Asad Effendi, PDG de Secure Networks, qui a participé à la mise en œuvre du PoC. « Cependant, compte tenu des scénarios d'attaque par malware auxquels nous sommes confrontés aujourd'hui, le simple fait de bloquer le trafic suspect n'est pas toujours la meilleure approche. »

LA SOLUTION

Sécurité DNS avancée avec BloxOne Threat Defense™

Avec une version test de BloxOne Threat Defense installée dans le centre de données d'Askari Bank, l'équipe a simulé une série de scénarios de trafic réseau à l'aide des techniques récentes d'infiltration et d'exfiltration de données caractéristiques des attaques DNS Messenger et à flux rapide. « Au cours des différents scénarios testés lors de la preuve de concept, aucune tentative d'infiltration ni d'exfiltration de données réussie n'a abouti », a déclaré Khalid Mirza. « Voir BloxOne Threat Defense bloquer des activités malveillantes dans notre propre environnement nous a donné pleine confiance dans la solution Infoblox. »

BloxOne Threat Defense opère au niveau du DNS pour détecter 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 étendue et une intégration fluide à l'écosystème, la solution renforce l'efficacité des opérations de sécurité (SecOps) et optimise les performances de l'infrastructure de sécurité existante. Ces capacités ont constitué un argument secondaire important pour l'équipe Askari, qui s'appuie sur sa solution SOAR pour gérer l'ensemble de ses opérations de sécurité. Maintenant que l'équipe d'Askari a pleinement mesuré l'ensemble des capacités et des avantages de BloxOne Threat Defense, la décision a été prise de procéder à une mise en production à l'échelle.

LES RÉSULTATS

Détection plus rapide des menaces, réduction des délais de réponse aux incidents

« BloxOne Threat Defense renforce l'efficacité de l'ensemble de notre infrastructure de sécurité », a expliqué Umair Shakil, responsable du centre des opérations de sécurité de la banque Askari. « Avec la solution Infoblox intégrée à notre plateforme SOAR existante, tous les outils de notre pile de sécurité ont désormais accès à des informations en temps réel sur le réseau et les threat intelligence. Tout fonctionne désormais à l'unisson pour mieux identifier les menaces et y remédier grâce à une automatisation poussée. »

La conception de la sécurité hybride unique de BloxOne Threat Defense utilise la puissance du cloud pour détecter un large éventail de menaces tout en s'intégrant étroitement à l'écosystème sur site. Il offre également une résilience et une redondance non disponibles dans les solutions uniquement cloud. Grâce à une console unique, l'équipe d'Askari peut désormais sécuriser de manière centralisée et automatisée les dispositifs IoT, les applications, les machines virtuelles et les ports de commutation, où qu'ils se trouvent. BloxOne Threat Defense a permis à l'équipe d'Askari de réduire la pression sur les dispositifs de sécurité périmétrique déjà sollicités (tels que les pare-feux, les IPS et les proxys web) en transformant les serveurs DNS, puissants et déjà disponibles, en première ligne de défense. L'équipe prévoit de tirer davantage de valeur de son infrastructure de sécurité grâce au partage d'informations sur les menaces et les attaquants, ainsi que d'améliorer la productivité de ses analystes et administrateurs sécurité.

Client : ***Askari Bank***
Secteur : ***Services financiers***
Pays : ***Pakistan***

LES INITIATIVES :

- Prévenir les techniques d'infiltration et d'exfiltration de données grâce à l'analyse et à l'apprentissage automatique, notamment les exfiltrations de données basées sur le DNS, les attaques DGA, DNS Messenger et à flux rapide
- Détectez et bloquez les exploits, le phishing, les ransomwares et autres malwares modernes
- Identifiez la propagation et les mouvements latéraux des malwares grâce à la surveillance du trafic est-ouest
- Restreignez l'accès des utilisateurs à certaines catégories de contenu Web et suivre leur activité
- Protégez votre marque grâce à la surveillance des domaines similaires pour vos propriétés Internet les plus précieuses
- Contrôlez les risques liés à l'utilisation croissante de DoH : bloquez l'accès aux domaines DoH (DNS sur HTTPS) et redirigez les requêtes DoH vers les DNS de confiance existants

« BloxOne Threat Defense permet à nos analystes SOC de prendre des décisions plus rapides sur la base d'informations contextuelles très précises, ce qui améliore le temps global d'analyse », a déclaré Hasan Imam, ingénieur technique en chef chez Secure Networks. « Le DNS étant devenu un vecteur d'attaque de plus en plus important ces derniers temps, les mesures proactives et le professionnalisme dont fait preuve Askari Bank pour combler cette lacune sont très louables et constituent un exemple fort dans le secteur en matière de sécurité. »

« À mon avis, aucun autre fournisseur de solutions n'offre le niveau de sécurité DNS qu'Infoblox propose avec BloxOne Threat Defense », conclut Khalid Mirza. « En nous associant à Infoblox, Askari Bank bénéficie de la protection nécessaire pour notre infrastructure DNS, ce qui nous permet d'atteindre nos objectifs en matière de services bancaires sécurisés pour nos clients à travers le Pakistan. »

infoblox.

Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

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

+1.408.986.4000
www.infoblox.com