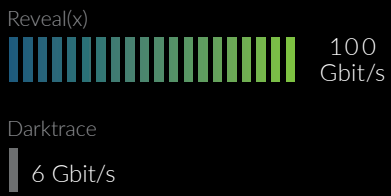
ExtraHop

Reveal(x) face à Darktrace

UNE INTELLIGENCE QUI N'A RIEN D'ARTIFICIEL

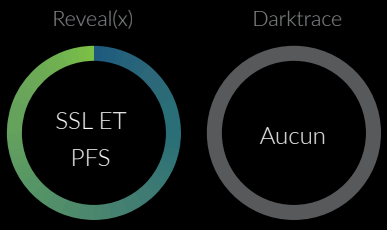


DÉBIT

UNE VISIBILITÉ INÉGALÉE, PARTOUT

Reveal(x) de ExtraHop propose non seulement une fonction de détection, mais aussi une visibilité inégalée, des informations claires et des réponses immédiates à chaque étape d'une attaque. Vous pouvez ainsi mettre en quarantaine les appareils malveillants avant qu'ils ne fassent des dégâts et obtenir des données d'analyse claires en quelques clics.

ExtraHop propose un débit 16 fois supérieur dans une seule appliance, avec une analyse en temps réel plus approfondie que Darktrace, quels que soient les volumes concernés.

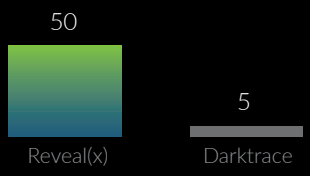


DÉCHIFFREMENT

CAPACITÉS DE DÉCHIFFREMENT

Reveal(x) est la seule solution d'analyse de sécurité en mesure de déchiffrer le trafic en temps réel, versions actuelles de SSL/TLS comprises, même lorsque PFS est activé. Darktrace ne propose aucune fonction de déchiffrement : la majorité du trafic, et de l'activité malveillante, reste donc parfaitement opaque.

Acceptez-vous de ne disposer d'aucune visibilité sur 70 % des attaques modernes ?



DÉCODEURS DES PROTOCOLES DE LA COUCHE L7

DES DONNÉES APPROFONDIES ET COMPLÈTES POUR DES INFORMATIONS CLAIRES

Reveal(x) utilise les données en lignes pour vous donner une visibilité contextuelle complète sur tous les actifs et charges utiles des couches L2 à L7, y compris 50 protocoles d'entreprise. Darktrace analyse les en-têtes des paquets, ce qui limite la visibilité aux couches L2 à L4, et ne propose qu'un contexte restreint.

Darktrace vous indiquera que deux systèmes ont communiqué. Reveal(x) vous révélera la teneur de leur communication.

AUTOMATISATION DES INVESTIGATIONS POUR DES RÉPONSES IMMÉDIATES

La détection constitue la première étape de toute solution de sécurité moderne. La deuxième étape consiste à confirmer la validité d'une menace potentielle afin d'éliminer les faux positifs avant l'envoi d'une alerte. La communication de données d'informatique légale permettant une investigation et une neutralisation en temps réel devrait être l'objectif final de ces solutions, mais Darktrace s'arrête à la détection. Reveal(x) détecte les menaces, automatise la collecte et la mise en corrélation des transactions et des paquets en temps réel, et s'intègre à votre SIEM pour proposer un workflow optimisé et efficace.

Les équipes SecOps ont besoin de plus d'efficacité, pas de plus d'alertes.

CHRONOLOGIE D'UNE VIOLATION

REVEAL(X) DE EXTRAHOP VOIT CHAQUE DÉTAIL D'UNE ATTAQUE. RIEN NE LUI ÉCHAPPE.

Reveal(x) propose non seulement une fonction de détection, mais aussi une visibilité inégalée, des informations claires et des réponses immédiates à chaque étape d'une attaque. Vous pouvez ainsi mettre en quarantaine les appareils malveillants avant qu'ils ne fassent des dégâts et obtenir des données d'analyse claires en quelques clics.

Reveal(x)		Darktrace
LE CLIENT TENTE À PLUSIEURS REPRISES DE SE CONNECTER À LA BD		Volume inhabituel de trafic SQL entre une BD et un client rare
LE CLIENT PARVIENT À SE CONNECTER À LA BD		
LE CLIENT DEMANDE DES INFOS À LA BD AVEC LA COMMANDE SELECT		
LA BD ACCEPTE LA COMMANDE ET COMMENCE L'ENVOI DE DONNÉES		AUCUNE VISIBILITÉ SUR LE RÉSEAU
LE CLIENT ÉMET LA COMMANDE DROP SUR LA TABLE D'AUDIT DE LA BD		
LA BD ACCEPTE LA COMMANDE		
LE CLIENT LANCE UN TRANSFERT DE DONNÉES IMPORTANT VERS UN HÔTE EXTERNE		Transfert de données d'un volume inhabituel entre le client et un hôte externe rare

DES DONNÉES, PAS DES MATHÉMATIQUES

> "Nos algorithmes ne sont pas meilleurs que ceux des autres, nous disposons simplement de plus de données."

PETER NORVIG, RESPONSABLE DE L'INGÉNIERIE, GOOGLE

Découvrez la puissance de Reveal(x) de ExtraHop

EXTRAHOP.COM/DEMO

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (téléphone)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com