ExtraHop

Reveal(x) vs. Darktrace

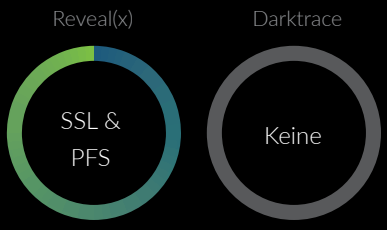
ECHTE INTELLIGENZ. NICHTS KÜNSTLICHES.

DURCHSATZ

EINZIGARTIGE TRANSPARENZ IN JEDER SKALIERUNG

ExtraHop Reveal(x) ist weitaus mehr als ein Tool zur Bedrohungserkennung. Dank umfassender Transparenz, aussagekräftigen Erkenntnissen und sofortigen Antworten in jeder Phase eines Angriffs können Sie verdächtige Geräte unter Quarantäne stellen und mit wenigen Klicks forensische Beweise erfassen, bevor ernster Schaden entsteht.

ExtraHop bietet den 16-fachen Durchsatz in einer einzelnen Appliance und in jeder Skalierung deutlich schnellere Analysen als Darktrace.

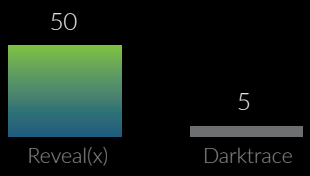


ENTSCHLÜSSELUNG

ENTSCHLÜSSELUNGSFUNKTIONEN

Reveal(x) kann als einziges Sicherheitsanalysetool den Datenverkehr mit Leitungsgeschwindigkeit entschlüsseln, einschließlich aktuellen SSL/TLS-Versionen und sogar bei aktivierter Perfect Forward Secrecy. Darktrace bietet keine Entschlüsselungsfunktionen, sodass der Großteil des Datenverkehrs – inklusive verdächtiger Aktivitäten – sich Ihrer Kontrolle entzieht.

Macht es Ihnen keine Sorgen, wenn 70 % aller modernen Angriffe Ihrem Sicherheitssystem entgehen?



L7-PROTOKOLLDECODIERER

DETAILGENAUIGKEIT UND UMFANG DER DATEN FÜR WERTVOLLE ERKENNTNISSE

Reveal(x) bietet Ihnen anhand von Leitungsdaten vollständige, kontextbezogene Transparenz für alle Ressourcen und Datenlasten von L2 bis L7, einschließlich 50 Unternehmensprotokollen. Darktrace analysiert Paket-Header und beschränkt sich somit zumeist auf L2 bis L4 mit eingeschränkten Kontextinformationen.

Darktrace weiß, dass zwei Systeme miteinander kommunizieren. Reveal(x) weiß auch, worüber.

AUTOMATISIERTE UNTERSUCHUNGEN ZUGUNSTEN SOFORTIGER ANTWORTEN

Die Erkennung von Bedrohungen ist nur der erste Schritt für eine moderne Sicherheitslösung. Der zweite Schritt ist die Überprüfung der potenziellen Bedrohung, damit falsch positive Befunde verworfen werden, bevor ein Alarm ausgelöst wird. Die Bereitstellung forensischer Daten für Untersuchungen und Gegenmaßnahmen in Echtzeit sollte das endgültige Ziel sein, aber Darktrace gibt sich mit der Bedrohungserkennung zufrieden. Reveal(x) erkennt Bedrohungen, automatisiert die Erfassung und Korrelation von Transaktions- und Paketdaten in Echtzeit und ermöglicht dank Integration in SIEM einen optimierten, effizienten Workflow.

SecOps-Teams wünschen sich mehr Effizienz, nicht mehr Alarme.

ABLAUF EINES ANGRIFFS

EXTRAHOP REVEAL(X) SIEHT JEDES DETAIL DES ANGRIFFS. NICHTS BLEIBT IM DUNKELN.

ExtraHop Reveal(x) ist weitaus mehr als ein Tool zur Bedrohungserkennung. Dank umfassender Transparenz, aussagekräftigen Erkenntnissen und sofortigen Antworten in jeder Phase eines Angriffs können Sie verdächtige Geräte unter Quarantäne stellen und mit wenigen Klicks forensische Beweise erfassen, bevor ernster Schaden entsteht.

Reveal(x)		Darktrace
CLIENT VERSUCHT MEHRFACH VERGEBLICH, SICH AN DER DB ANZUMELDEN		Ungewöhnlich hoher SQL-Datenverkehr zwischen DB und seltenem Client
CLIENT MELDET SICH ERFOLGREICH		
CLIENT FORDERT MITTELS „SELECT“ DATEN DER DB AN		
DB BESTÄTIGT ANFRAGE UND BEGINNT DATENÜBERMITTLUNG		KEIN EINBLICK IN DIE NETZWERKAKTIVITÄT
CLIENT SENDET „DROP“-BEFEHL AN DB-AUDIT-TABELLE		
DB BESTÄTIGT DIE ANFRAGE		
CLIENT INITIIERT ÜBERTRAGUNG VIELER DATEN AN EXTERNEN HOST		Ungewöhnlich hohe Menge an übertragenen Daten zwischen Client und seltenem externen Host

DATEN ÜBERTRUMPFEN ALGORITHMEN.

“ Wir haben keine besseren Algorithmen als die Konkurrenz, sondern einfach mehr Daten. ”

PETER NORVIG, DIRECTOR OF ENGINEERING, GOOGLE

Erleben Sie ExtraHop Reveal(x) in Aktion

EXTRAHOP.COM/DEMO

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101, USA
+1 877 3339872 (Tel.)
+1 206 2746393 (Fax)
info@extrahop.com
www.extrahop.com