ExtraHop

Reveal(x) vs. Darktrace

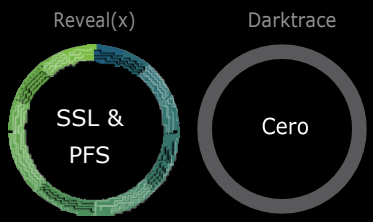
SON LOS DATOS, NO LA MATEMÁTICA

RENDIMIENTO

SEGURIDAD A ESCALA

Reveal (x) recopila y analiza 100 Gbps de datos en tiempo real, proporcionando información rica en contexto dentro de los 15 minutos posteriores a la conexión. Darktrace proporciona 6Gbps de análisis por dispositivo, lo que requiere dieciséis veces más hardware para lograr la misma escala y agrega administración y sobrecarga de correlación.

ExtraHop proporciona **un rendimiento 16 veces mayor en un solo dispositivo**, con un análisis de velocidad de línea más profundo que Darktrace en cualquier escala.

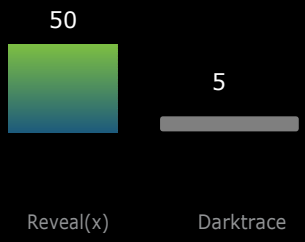


DESCIFRADO

CAPACIDADES DE DESCIFRADO

Reveal (x) es la única solución de análisis de seguridad que puede descifrar el tráfico a la velocidad de línea, incluidas las versiones actuales de SSL / TLS, incluso con la función Perfect Forward Secrecy habilitada. Darktrace no ofrece capacidades de descifrado, dejando la mayoría del tráfico, incluida la actividad maliciosa, completamente opaca.

¿Estás de acuerdo con la visibilidad cero en el 70% de los ataques modernos?

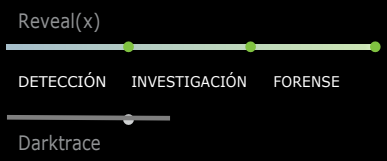


DESCODIFICADORES DE PROTOCOLOS L7

GRANULARIDAD Y AMPLITUD DE DATOS

Reveal(x) utiliza datos de red para proporcionarte una visibilidad contextual completa de todos los activos y contenidos útiles de L2 a L7, incluidos 50 protocolos. Darktrace analiza las cabeceras de paquetes, lo que significa que en su mayoría ven de L2 a L4 con una visión contextual limitada.

Darktrace te dirá que dos dispositivos han comunicado. Reveal(x) te dirá de que han hablado.



FLUJO DE TRABAJO

AUTOMATIZACIÓN DE LA INVESTIGACIÓN

La detección es el primer paso para cualquier solución de seguridad moderna. El segundo paso es confirmar la validez de una amenaza potencial para eliminar falsos positivos antes de enviar una alerta. Proporcionar datos forenses relevantes para la investigación y remediación en tiempo real debe ser el objetivo final, pero Darktrace se detiene en la detección. Reveal(x) detecta amenazas, automatiza la recopilación y correlación de transacciones y paquetes en tiempo real, y se integra con SIEM para proporcionar un flujo de trabajo eficiente y optimizado.

Sec Ops necesita más eficacia y no más alertas.

CRONOGRAMA DE EVENTOS DE UNA BRECHA

REVEAL(X) REVELA TODOS LOS DETALLES DE UN ATAQUE. ILUMINA EL ESPACIO OSCURO.

ExtraHop Reveal(x) va más allá de la detección para proporcionar visibilidad profunda e investigación automatizada en cada paso de un ataque, por lo que puede poner en cuarentena los dispositivos maliciosos antes de que se produzcan daños y obtener pruebas forenses concluyentes con solo hacer pocos clics.

Reveal(x) Darktrace

USUARIO/DISPOSITIVO INTENTA Y FALLA DE HACER LOGIN EN BBDD VARIAS VECES

Cantidad inusual de tráfico SQL entre una bbdd y un usuario/dispositivo raro o desconocido

USUARIO/DISPOSITIVO LOGIN CON ÉXITO A LA BBDD

USUARIO/DISPOSITIVO PIDE DATOS DE LA BBDD CON COMANDO "SELECT"

BBDD RESPONDE CON AFIRMATIVO Y EMPIEZA A DESCARGAR DATOS

CERO VISIBILIDAD DE RED

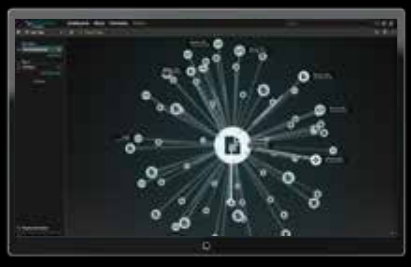
USUARIO/DISPOSITIVO ORDENA "DROP" CONTRA LA TABLE DE AUDITORÍA DE LA BBDD

BBBDD RESPOND ECON AFIRMATIVO

USUARIO/DISPOSITIVO INICIA GRAN TRANSFERENCIA DE DATOS A UN HOST EXTERNO

Transferencia de un volumen atípico entre usuario/dispositivo a un host externo raro o desconocido

> "No tenemos mejores algoritmos que los demás, simplemente tenemos más datos."
>
> **PETER NORVIG**, DIRECTOR OF ENGINEERING, GOOGLE



Experience the Power of ExtraHop Reveal(x)

EX TRA H OP. COM/D EMO

ExtraHop

DotForce, SL,
dotforce.es
info@dotforce.es
+34 914 230 991