infoblox.

LAS 7 RAZONES PRINCIPALES POR LAS QUE EL DNS IMPORTA A LOS PROFESIONALES DE LA SEGURIDAD

El DNS ya no es solo para redes.
El DNS es cada vez más vital como primera línea de defensa para proteger su infraestructura de red en expansión y reducir su tiempo medio de respuesta (MTTR).

SE ENFRENTA A DESAFÍOS DE SEGURIDAD CRÍTICOS:

Superficie de ataque en expansión
A medida que crecen las necesidades de WFA y multinube, hay más oportunidades de malware, C2, lookalikes y otras amenazas para evitar las defensas actuales.

Puntos ciegos del usuario y del dispositivo
La seguridad no tiene una vista unificada y en tiempo real de todos los usuarios y dispositivos de la red, incluidos la multinube y el IoT/OT.

Falta de recursos vitales
La brecha en las habilidades de seguridad y la carga resultante en SecOps significa que las alertas críticas se pierden a diario o semanalmente.

Investigación y corrección lentas
El retraso en el acceso a los datos forenses de usuarios y dispositivos atasca las investigaciones y prolonga el tiempo de permanencia de las amenazas, exponiendo a su empresa a más daños.

4 MILLONES USD
Coste promedio de una violación de datos

270+
Horas de media para identificar y contener amenazas

92%
de malware aprovecha el DNS para el orden y el control

CÓMO DNS DETECTION AND RESPONSE LE AYUDA A RESOLVER ESTOS DESAFÍOS Y MÁS:

1. **Identifique las amenazas antes**
Asignar consultas DNS al usuario y al dispositivo actividad en tiempo real usando IPAM Descubrimiento de aplicaciones basado en DNS.

2. **Detenga los ataques más rápido**
Utilice información avanzada sobre amenazas para bloquear el phishing, el ransomware, el malware, C2, DGA, extracción de datos y otros antes.

3. **Proteja los sistemas en cualquier lugar**
Proteja su superficie de ataque superficie defendiendo entre nubes y en el edge, incluyendo IoT/OT.

4. **Bloquee las amenazas emergentes**
Aproveche la búsqueda global de amenazas para detectar dominios sospechosos emergentes y bloquearlas hasta 3 meses antes.

5. **Cierre los dominios parecidos**
Utilizar análisis AI/ML en las consultas DNS para detectar más rápidamente DGA, extracción de datos y dominios parecidos sofisticados.

6. **Automatice el retorno de la inversión en seguridad**
Automatice las integraciones del ecosistema para compartir datos DNS con herramientas SOC y permitir que SecOps para priorizar mejor las alertas y minimizar los esfuerzos.

7. **Utilice menos recursos**
Unifique la información de red y seguridad para ver y detener las amenazas antes y permita que SecOps haga más con menos.

Importancia del DNS

Más información sobre cómo Infoblox DNS Detection and Response
genera enormes beneficios económicos al mejorar su seguridad proactivamente y acelera el tiempo medio de respuesta en toda su empresa.

Lea el Impacto económico total de Forrester™ estudiar hoy