infoblox.

7 PRINCIPAIS RAZÕES PELAS QUAIS DNS MTTRs PARA PROFISSIONAIS DE SEGURANÇA

O DNS não é apenas o resolver de nomes de domínio.

O DNS está se tornando cada vez mais vital como primeira linha de defesa para proteger sua infraestrutura de rede em expansão e reduzir o Tempo Médio de Resposta (MTTR).

VOCÊ ESTÁ ENFRENTANDO DESAFIOS CRÍTICOS DE SEGURANÇA:

Ampliando as possibilidades de ataque

Com o crescimento das necessidades de WFA (trabalhe de qualquer lugar) e da utilização de múltiplas nuvens, há um aumento nas oportunidades para que malware, C2 (Comando e Controle), aparências semelhantes e outras ameaças possam contornar as defesas existentes.

Falta de recursos vitais

A lacuna de habilidades em segurança e o consequente ônus sobre as operações de segurança (SecOps) fazem com que alertas críticos sejam perdidos diariamente ou semanalmente.

Pontos cegos do usuário e do dispositivo

A segurança não tem visão unificada e em tempo real de todos os usuários e dispositivos de rede, incluindo multinuvem e IoT/OT.

Investigação e correção lentas

O atraso no acesso às análises de usuários e dispositivos gera obstáculos nas investigações e estende o tempo de permanência das ameaças, aumentando a exposição do seu negócio a danos adicionais.

US$ 4 MILHÕES

Custo médio de uma violação de dados

270+

Horas em média para identificar e conter ameaças

92%

Os Malwares utilizam o DNS como uma técnica para comando e controle

COMO USAR O DNS PARA DETECÇÃO E RESPOSTA – AJUDAMOS VOCÊ A RESOLVER ESSES DESAFIOS E MUITO MAIS:

1. **Identifique ameaças mais cedo**
   Mapeie consultas DNS para atividades de usuários e dispositivos em tempo real usando IPAM descoberta de aplicativos baseada em DNS.
2. **Pare ataques mais rapidamente**
   Use informações avançadas sobre ameaças para bloquear phishing, ransomware, malware, C2, DGA, exfiltração de dados e outros.
3. **Proteja os sistemas em qualquer lugar**
   Proteja sua rede em expansão de ataques, defendendo-se nas clouds e na borda, incluindo IoT/OT.
4. **Bloquear ameaças emergentes**
   Tenha o poder de detectar ameaças e domínios suspeitos emergentes e bloqueá-los até 3 meses antes.
5. **Identifique lookalikes**
   Use análises de IA/ML em consultas DNS para detectar DGAs, exfiltração de dados e lookalike domain sofisticados com mais rapidez.
6. **Automatize o ROI de segurança**
   Automatize as integrações do ecossistema para compartilhar dados DNS com ferramentas SOC e permitir que SecOps priorize melhor os alertas e minimize os esforços.
7. **Use menos recursos**
   Integre dados de redes e segurança para identificar e bloquear ameaças mais rapidamente, permitindo que as operações de segurança (SecOps) realizem mais com menos recursos.

DNS MTTRs

Saiba mais sobre como a Infoblox Detecção e resposta de DNS
gera enormes benefícios econômicos, melhorando sua segurança proativa e acelerando o tempo de resposta em toda a sua empresa.

Leia o Forrester Total Economic Impact™ Estude hoje