infoblox.

## I 7 PRINCIPALI MOTIVI DELL'IMPORTANZA

# DEL DNS MTTR

## PER I PROFESSIONISTI DELLA SICUREZZA

**Il DNS non è più solo per il networking.**
Il DNS è sempre più vitale come prima linea di difesa per proteggere la tua infrastruttura di rete in espansione e ridurre il Mean Time To Respond (MTTR).

## STAI AFFRONTANDO SFIDE CRITICHE PER LA SICUREZZA:

### Superficie di attacco in espansione
Con la crescita delle esigenze WFA e multi-cloud, aumentano le opportunità per malware, C2, lookalike e altre minacce che aggirano le difese attuali.

### Punti ciechi dell'utente e del dispositivo
La sicurezza non ha una visione unificata e in tempo reale di tutti gli utenti e i dispositivi di rete, inclusi quelli multi-cloud e IoT/OT.

### Mancanza di risorse vitali
Il divario di competenze in materia di sicurezza e il conseguente onere per le SecOps fanno sì che gli avvisi critici vengano persi quotidianamente o settimanalmente.

### Indagine e remediation
L'accesso ritardato alle informazioni forensi sugli utenti e sui dispositivi blocca le indagini e allunga i tempi di permanenza delle minacce, esponendo la tua azienda a maggiori danni.

**$4M**
come costo medio di una violazione dei dati

**270+**
ore in media per identificare e contenere minacce

**92%**
di malware che sfruttano il DNS per il comando e il controllo

## COME DNS DETECTION AND RESPONSE TI AIUTA A RISOLVERE QUESTE E ALTRE SFIDE:

**1 Identifica prima le minacce**
Mappa le query DNS alle attività di utenti e dispositivi in tempo reale utilizzando l'IPAM rilevazione di applicazioni basata su DNS.

**2 Interrompi gli attacchi più rapidamente**
Usa threat intel avanzata per bloccare in anticipo phishing, ransomware, malware, C2, DGA, data exfil e altro.

**3 Proteggi i sistemi ovunque**
Proteggi la tua superficie di attacco in espansione difendendoti nel cloud e all'edge, comprese le parti IoT/OT.

**4 Blocca le minacce emergenti**
Sfrutta la threat hunting globale per rilevare domini sospetti emergenti e bloccarli fino a 3 mesi prima.

**5 Arresta i lookalike**
Usa l'analisi AI/ML sulle query DNS per individuare più rapidamente DGA, data exfil e domini Lookalike sofisticati.

**6 Automatizza il ROI della sicurezza**
Automatizza le integrazioni dell'ecosistema per condividere i dati DNS con gli strumenti SOC e permettere alle SecOps dare maggiore priorità agli avvisi e minimizzare gli sforzi.

**7 Usa meno risorse**
Unisci le informazioni di networking e sicurezza per vedere e bloccare le minacce più rapidamente e consentire alle SecOps di fare di più con meno.

# DNS MTTR

**Scopri di più su come DNS Detection and Response di Infoblox**
porta enormi benefici economici migliorando la tua sicurezza proattiva e accelerando l'MTTR (Mean Time To Response) in tutta l'azienda.

**Leggi lo studio Forrester Total Economic Impact™ oggi**