DÉTECTER.
DÉJOUER.
DOMINER.

LES ATTAQUES SOPHISTIQUÉES
ET PROPULSÉES PAR L'IA GRÂCE
À LA PUISSANCE DU DNS

infoblox®

TABLE DES MATIÈRES

LE PROBLÈME D'UNE APPROCHE RÉACTIVE « DÉTECTER ET RÉPONDRE »

Les méthodes classiques deviennent trop lentes, risquées et inefficaces.

L'approche classique de la chaîne de destruction est en train de disparaître. Elle reposait sur une stratégie dite de « patient zéro infection », où une autre organisation servait de première cible, appelée aussi « patient zéro », afin d'observer le comportement du malware, puis d'appliquer ces connaissances à votre propre organisation.

Cependant, ce modèle n'est plus applicable. Les acteurs malveillants d'aujourd'hui conçoivent des malwares spécifiquement adaptés à votre secteur, à votre entreprise, voire à vos employés, ce qui augmente exponentiellement la probabilité que vous soyez le patient zéro.

Le temps moyen d'infiltration d'un acteur malveillant, c'est-à-dire le délai nécessaire à un pirate pour se déplacer latéralement dans un réseau après un accès initial, est désormais de seulement 48 minutes.[1] Cela signifie que les entreprises disposent d'une fenêtre extrêmement courte pour détecter, analyser et neutraliser une attaque avant qu'elle ne se propage davantage dans leur réseau.

TEMPS MOYEN DE PROPAGATION D'UN ACTEUR MALVEILLANT

Compromission initiale

l'acteur malveillant accède au réseau

48 minutes

La durée moyenne nécessaire pour se déplacer latéralement dans le réseau

Impact de l'acteur malveillant

LES ACTEURS MALVEILLANTS TIRENT PARTI D'UN AVANTAGE DÉLOYAL

Malgré les dépenses annuelles des entreprises qui dépassent 200 milliards de dollars en solutions de cybersécurité,[2] des attaques comme les ransomwares continuent de réussir, mettant en lumière des lacunes cruciales dans les approches actuelles.

Alors que les acteurs malveillants utilisent de nouveaux outils pour lancer des attaques plus fréquentes, sophistiquées et furtives, les solutions de sécurité réactives ne suffisent plus. Les malwares générés par l'IA, conçus pour un usage unique, sont désormais si spécifiques que chaque attaque devient un « zero day », sans signature ni comportement connu permettant de la détecter.

COMMENT LES ACTEURS MALVEILLANTS UTILISENT L'IA

La capacité de l'IA à traiter d'immenses volumes de données et à apprendre des schémas permet aux cybercriminels de développer des stratégies d'attaque plus avancées et plus ciblées.

Ingénierie sociale alimentée par l'IA
L'une des méthodes les plus répandues est l'ingénierie sociale alimentée par l'IA, où les pirates créent des e-mails de phishing et des appels vocaux (vishing) très convaincants. Ces messages imitent souvent des interlocuteurs de confiance, trompant ainsi facilement les victimes pour qu'elles révèlent des informations sensibles ou accordent l'accès à des systèmes sécurisés.

Développement de malwares pilotés par l'IA
De plus, l'IA accélère le développement de codes malveillants, réduisant ainsi le temps nécessaire à la création de ransomwares sophistiqués capables d'échapper aux mesures de sécurité classiques. Cette capacité simplifie l'accès au réseau, ce qui permet aux pirates moins expérimentés de lancer des attaques efficaces par ransomware.

Abaissement des barrières à l'entrée pour la cybercriminalité
Enfin, l'IA rend la cybercriminalité plus accessible. Grâce à des outils basés sur l'IA qui automatisent tout, de la création de kits de phishing à la diffusion de malware, même les pirates peu qualifiés peuvent désormais lancer des campagnes crédibles et destructrices. Cette montée de la cybercriminalité « en tant que service », alimentée par l'IA, se traduit par des attaques plus fréquentes, plus variées et plus difficiles à prévoir dans tous les secteurs.

PRINCIPALES TENDANCES DANS LE PAYSAGE DES CYBERATTAQUES

Des outils tels que ChatGPT et FraudGPT permettent à des pirates novices de créer des e-mails de phishing avancés et des malwares ciblés et sophistiqués qui contournent les défenses classiques.

Les attaques par ransomware ont augmenté de 132 % au premier trimestre 2025 par rapport au quatrième trimestre 2024, aidées par l'ingénierie sociale basée sur la duperie par l'IA pour obtenir un accès initial aux réseaux.[3]

Chaque seconde, 11 personnes sont victimes d'attaques de malwares dans le monde. Cela représente 340 millions de victimes par an, un chiffre qui continuera de croître de façon exponentielle.[4]

L'exploitation des vulnérabilités a connu une augmentation de 34 % en raison des menaces basées sur l'IA.[5]

78 % des responsables de la sécurité informatique interrogés ont déclaré que les menaces liées à l'intelligence artificielle ont un impact significatif sur leurs entreprises.[6]

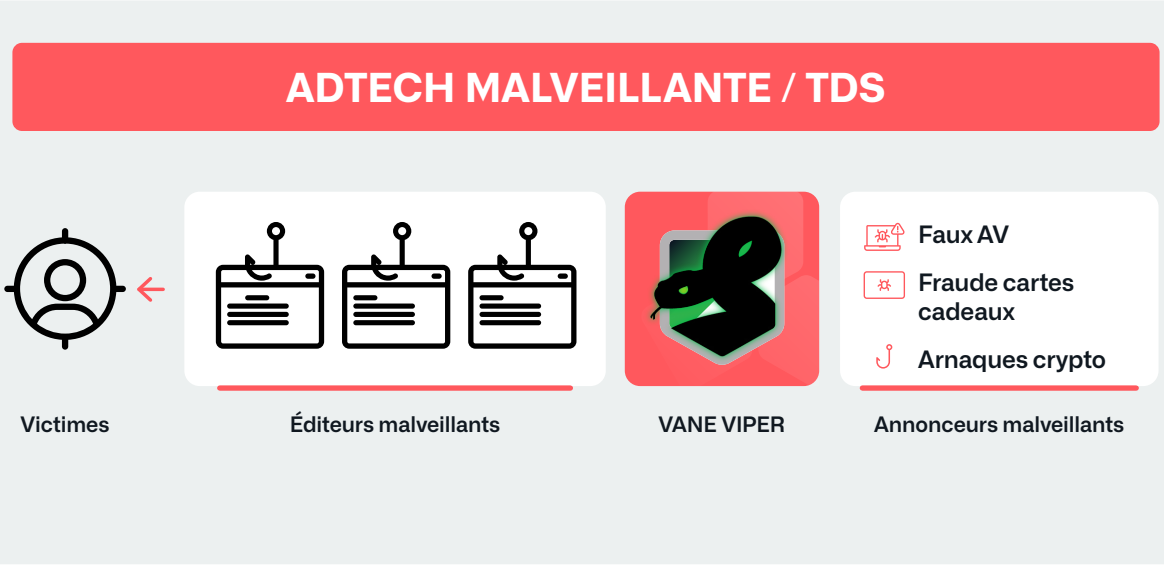
61 % des entreprises ont constaté une augmentation des attaques de deepfake en 2024.[7]

Le nombre de domaines de premier niveau (TLD) a augmenté de manière exponentielle (il y en avait sept il y a 30 ans, aujourd'hui plus de 1 500), ce qui permet aux acteurs de créer facilement des domaines similaires à l'aide de l'IA.[8]

LE RÔLE DES SYSTÈMES DE DISTRIBUTION DU TRAFIC DANS LES ATTAQUES MODERNES

Les systèmes de répartition du trafic (TDS) ont été adoptés par les acteurs malveillants pour renforcer leurs activités nuisibles. Tout comme Google AdSense aide les sites web à générer des revenus en redirigeant les utilisateurs vers des publicités pertinentes, les cybercriminels utilisent des TDS malveillants pour rediriger les utilisateurs vers des sites malveillants, souvent via des sites web piratés ou des publicités trompeuses. Les chaînes de redirection sont conçues pour dissimuler l'infrastructure du pirate, la rendant presque invisible aux outils de sécurité classiques. C'est un système furtif, évolutif et, malheureusement, très rentable pour les acteurs malveillants.

- Les technologies publicitaires malveillantes utilisent les TDS et diffusent principalement des malwares de type infostealer, qui sont au cœur des violations de données d'entreprise.
- Vane Viper, une campagne de faux CAPTCHA à grande échelle qui utilise le TDS pour distribuer Lumma Stealer, possède une infrastructure massive avec plus de 10 000 domaines. Elle a diffusé un million d'impressions publicitaires par jour au quatrième trimestre de l'année civile 2024 via plus de 3 000 sites d'annonceurs.



LA SÉCURISATION PROACTIVE DE VOTRE ENTREPRISE GRÂCE À LA PUISSANCE DU DNS

La sécurité préventive est une approche avancée qui se concentre sur l'anticipation, la prédiction et le blocage des cybermenaces avant qu'elles ne puissent causer des dommages.

Gartner définit la cybersécurité préventive comme suit : « Une approche proactive visant à empêcher, perturber ou dissuader les cyberattaques d'atteindre leurs objectifs. Compte tenu de l'utilisation croissante de l'IA générative par les acteurs malveillants dans les cyberattaques, les technologies de cybersécurité préventives jouent un rôle crucial dans le renforcement de la protection des entreprises contre les malwares alimentés par l'IA, les vulnérabilités zero-day, les ransomwares et autres menaces associées. Ces menaces ne peuvent souvent pas être efficacement atténuées uniquement à l'aide des outils et approches traditionnels de "détection et réponse" ».

Les entreprises peuvent utiliser le DNS pour protéger l'ensemble de leur environnement, infrastructure sur site, charges de travail dans le cloud, utilisateurs à distance et appareils IoT/OT, contre les attaques sophistiquées et modernes.

Une approche avec une protection du DNS est préventive car elle ne repose pas sur le patient zéro. Elle utilise une combinaison de renseignements prédictifs sur les menaces qui bloquent l'infrastructure des acteurs malveillants avant que ceux-ci ne puissent passer à l'action, et d'analyses algorithmiques/ML des requêtes DNS dans les réseaux des clients, afin de fournir une protection avant l'impact.

THREAT INTELLIGENCE PRÉDICTIVE :

Suit les activités préalables à une attaque et identifie l'infrastructure des acteurs malveillants avant qu'elle ne soit exploitée, au lieu de rechercher des variantes de malwares et des domaines individuels.

Exploite la télémétrie DNS et l'apprentissage automatique pour identifier les domaines à haut risque et bloquer les menaces avant qu'elles n'atteignent les réseaux.

Détecte et bloque les TDS, utilisés pour rediriger dynamiquement les utilisateurs vers des sites de phishing, des kits d'exploitation ou des charges utiles de malware.

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

L'Institut national des normes et de la technologie (NIST) a reconnu l'importance du DNS dans la cybersécurité et a inclus des directives de protection du DNS dans son document de référence, le NIST SP 800-81. Le guide souligne le rôle du DNS en tant que couche fondamentale de la cyberdéfense et indique qu'en intégrant une protection DNS aux infrastructures de sécurité existantes, les organisations peuvent améliorer leur capacité à détecter et à bloquer les menaces plus tôt que les systèmes de sécurité classiques.

« Les serveurs DNS peuvent fournir des informations significatives sur les connexions et les flux de données des endpoints et peuvent souvent prévenir les incidents de sécurité plus tôt que d'autres systèmes ».

-**NIST**

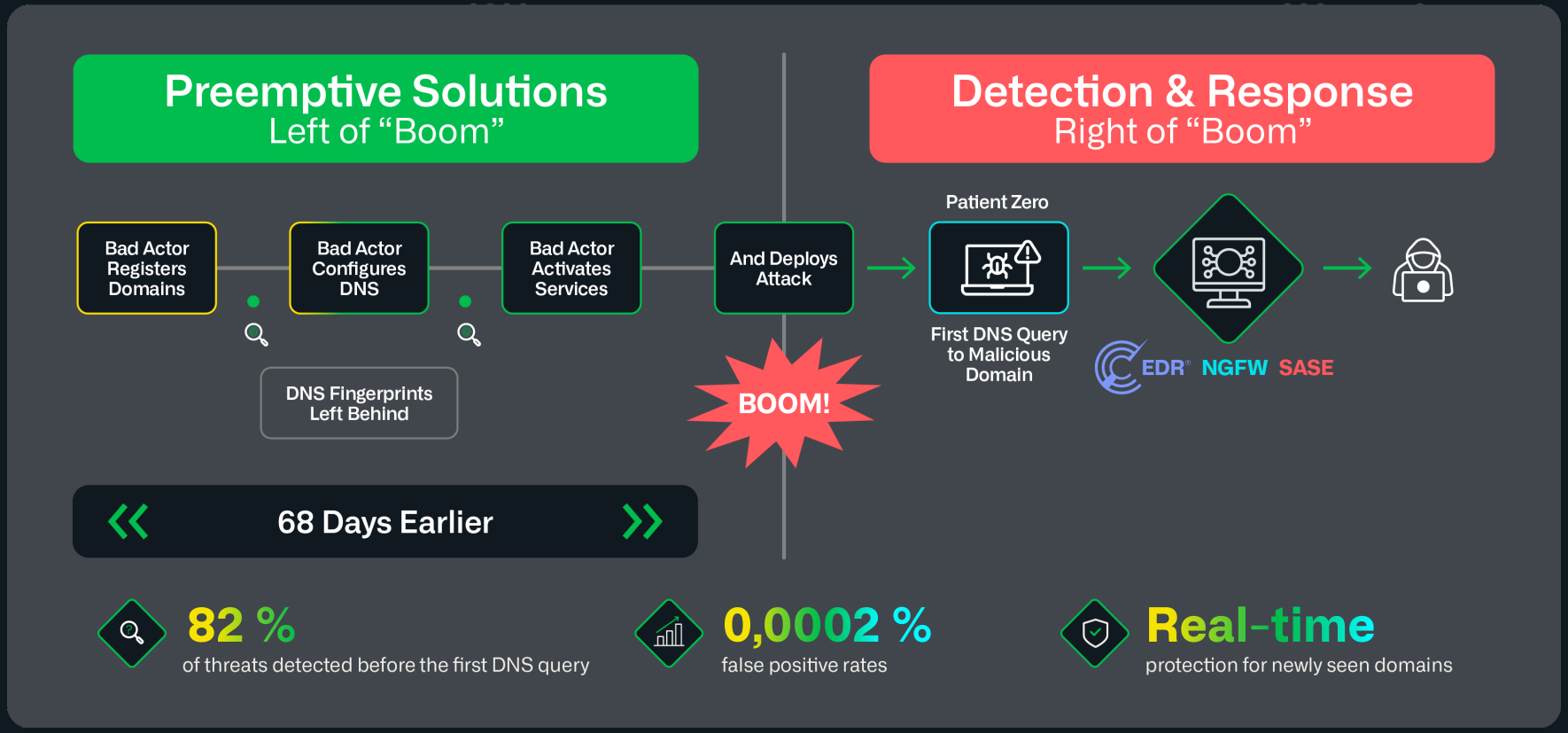
L'offre Protective DNS d'Infoblox, leader du secteur avec Infoblox, Infoblox Threat Defense™, présente de nombreux avantages par rapport aux mesures de sécurité réactives :

- Fournit une protection **avant l'impact** et dès l'intention de communiquer.
- En tant que **résolveur DNS**, c'est-à-dire un serveur ou un logiciel qui convertit les noms de domaine lisibles par l'homme en adresses IP lisibles par les machines, Infoblox **voit chaque connexion DNS** de chaque appareil (y compris les appareils des utilisateurs finaux, IoT/OT), qu'ils soient derrière un pare-feu ou non, qu'il y ait un **agent SASE ou non.**
- Surveille **en temps réel 204 000** clusters d'acteurs malveillants ou groupes d'activités de cyberattaques liées.
- **Bloque 5 fois plus de domaines à haut ou moyen risque** par rapport aux autres outils de sécurité qui recherchent des comportements malveillants connus.
- Bloque en moyenne **68,4 jours plus tôt** que les autres logiciels du secteur.
- **Détecte 82 % des menaces basées sur des domaines** avant la première requête DNS.
- A un **taux de faux positifs de 0,0002 %**.
- Identifie et bloque **l'utilisation non autorisée de l'IA** en fonction de l'activité DNS.
- Contribue à réduire l'exposition aux **enregistrements DNS orphelins** et aux domaines similaires.
- **Réduit la charge de 50 %** sur les autres outils de sécurité, tels que les pare-feux et les systèmes de gestion des informations et des événements de sécurité (SIEM), en **filtrant le trafic malveillant** avant qu'il n'atteigne ces systèmes.
- Attribution facile **des utilisateurs et des appareils** et priorisation des menaces grâce à des informations sur les actifs.

INFOBLOX THREAT DEFENSE

204 000 (et ça continue) de clusters/groupes découverts et surveillés en quasi temps réel.

PLUS DE 100 profils d'acteurs malveillants



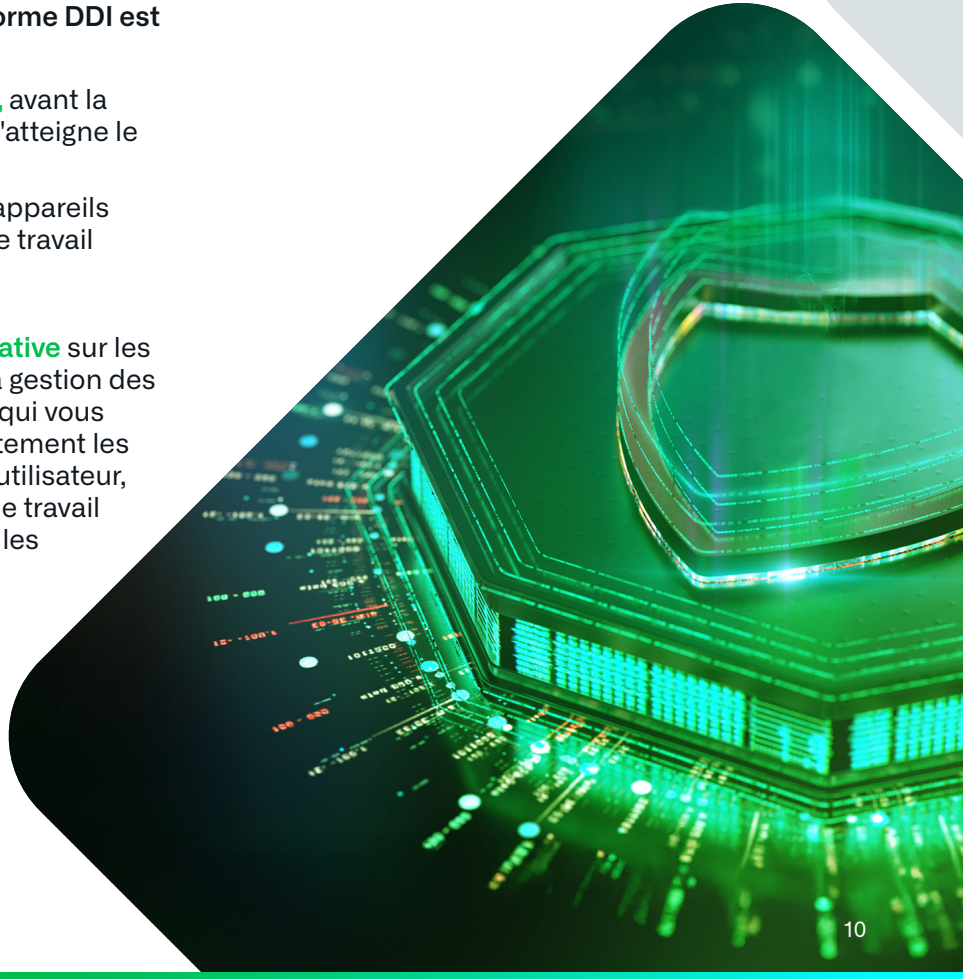
LA PUISSANCE D'UNE PLATEFORME DDI PROTECTRICE

Le DNS protecteur fonctionne mieux là où le DNS est déjà géré : sur une plateforme DDI. Infoblox est le seul fournisseur à offrir une plateforme DDI intégrée et protectrice, ce qui facilite l'activation d'une protection gérée par une seule équipe responsable et redevable de tous les problèmes liés au DNS.

Cela simplifie considérablement les opérations et le dépannage par rapport à l'activation du DNS protecteur dans les pare-feux de nouvelle génération (NGFW) ou les solutions Secure Access Service Edge (SASE). Avec Infoblox comme résolveur DNS, les organisations bénéficient d'une plateforme unifiée qui surveille les données de requête DNS de l'entreprise à la recherche de menaces, évalue les risques lorsqu'un nouveau domaine pénètre dans les résolveurs Infoblox et bloque proactivement en ligne si nécessaire, empêchant ainsi les incidents de se produire.

Autres raisons pour lesquelles l'utilisation de DNS Protecteur sur une plateforme DDI est avantageuse :

- **Bloque à la première étape,** avant la connexion, avant que cela n'atteigne le reste de la pile de sécurité.
- Protège les utilisateurs, les appareils IOT/OT/ICS et les charges de travail dans le cloud grâce à une **meilleure couverture.**
- **Visibilité en temps réel et native** sur les requêtes DNS corrélées à la gestion des adresses IP et au DHCP, ce qui vous permet d'associer immédiatement les activités malveillantes à un utilisateur, un appareil ou une charge de travail spécifique, accélérant ainsi les enquêtes et la remédiation.



AVANTAGES MÉTIER

Réduction du risque de violations de données.

Des économies d'une moyenne de 500 heures d'analyste SOC par mois et de 400 000 $ d'économies de productivité par an.

Un retour sur investissement de 243 % avec une période d'amortissement de moins de six mois.

Réduction de 50 % du nombre d'alertes générées par d'autres outils de sécurité, réduisant ainsi les coûts opérationnels.

LES CAS D'UTILISATION CLIENTS

Les clients d'Infoblox ont mis en œuvre avec succès les solutions Infoblox pour divers cas d'utilisation :

Protection proactive contre les ransomwares

Une chaîne de restaurants à service rapide a décidé d'adopter une approche plus proactive pour améliorer sa posture de sécurité globale en mettant en œuvre un DNS protecteur après plusieurs incidents de ransomwares très médiatisés. Ils souhaitaient également une visibilité totale sur le trafic DNS pour surveiller les menaces.

Prévenir l'exfiltration de données par le biais du DNS

Une grande compagnie d'assurance maladie a comblé les lacunes concernant le DNS Tunneling identifiées lors d'un test d'intrusion interne effectué par leur équipe rouge, qu'ils n'ont pas pu bloquer à l'aide de leurs solutions NGFW et SASE existantes.

Zero Trust

Une entreprise de transport a utilisé une combinaison d'accès à distance et de détection des menaces alimentés par le DNS, ainsi que de solutions pour terminaux, telles que la détection et la réponse aux terminaux (EDR) et la gestion des appareils mobiles (MDM), pour élaborer une stratégie Zero Trust pour les utilisateurs et les appareils afin de protéger « tout le monde, partout, en même temps ».

BRISEZ LA CHAÎNE D'ATTAQUE AVANT QU'ELLE NE COMMENCE. NE SOYEZ PAS LE PATIENT ZÉRO. DEVENEZ UN CYBER-HÉROS.

Pour plus d'informations, veuillez consulter la page Infoblox Threat Defense à l'adresse www.infoblox.com/fr/products/threat-defense.

1. *CrowdStrike 2025 Global Threat Report: Beware the Enterprising Adversary*, Myers, Adam, CrowdStrike Blog, février 27, 2025.
2. *Day 19: Analyzing DNS Logs — Detection Use Cases and How to Spot Malicious Activity*, Infosec Ninja, 7 mai 2025
3. *Massive Surge In Ransomware Attacks—AI And 2FA Bypass In Crosshairs*, Winder, Davey, Forbes, 25 mars 2025.
4. *ITRC Annual Data Breach Report*, Identity Theft Resource Center, janvier 2025.
5. *Verizon 2025 DBIR Report*
6. *Top 40 AI Cybersecurity Statistics*, Fox, Jacob, Cobalt, 10 octobre 2024.
7. *Speedy threat actors improving their lateral movement*, Hurley, Billy, IT Brew, 4 mars 2025.
8. ICANN—In 2012, ICANN (the Internet Corporation for Assigned Names and Numbers) launched a top-level domain expansion program, allowing organizations to apply for custom top-level domains.