Un document de réflexion rédigé
par Forrester Consulting commandité
par Infoblox

Juillet 2020

Accélérez la résolution des menaces grâce au DNS

Utilisez le DNS comme contrôle de sécurité de premier niveau pour détecter, bloquer et examiner les attaques

FORRESTER®

Table des matières

Projet réalisé sous la direction de :
Sarah Brinks,
Consultant senior spécialiste des impacts sur le marché

Contribution aux recherches :
Groupe de recherche Forrester sur la sécurité et les risques

A PROPOS DE FORRESTER CONSULTING

Forrester Consulting fournit des services de conseil fondés sur des études de marché aux cadres dirigeants afin de faciliter leur réussite au sein de leur entreprise. Qu'il s'agisse de sessions brèves à vocation stratégique ou de projets personnalisés, les services de Forrester Consulting vous mettent en relation directe avec des analystes de recherche qui appliquent leurs connaissances d'expert aux défis spécifiques de votre entreprise. Pour plus d'informations, visitez forrester.com/consulting.

FORRESTER®

Les enquêtes sur les menaces sont trop longues.

74 % des équipes d'opérations de sécurité passent plus de 4 heures à enquêter sur un incident de menace.

Davantage d'automatisation est nécessaire.

58 % des responsables S&R utilisent un mélange de processus manuels et automatisés de réponse aux incidents, et seulement 31 % sont presque entièrement automatisés.

Synthèse

On peut lire dans la presse que les données clients sont plus précieuses dans l'économie actuelle que le pétrole.[1] Si l'on souscrit à cette idée, la protection des données clients doit être une priorité pour toutes les entreprises. Cela signifie que tous les chemins d'accès aux données clients doivent être sécurisés, quel que soit l'endroit où ces données sont stockées. Le système de noms de domaine (DNS) est un service réseau fondamental, essentiel non seulement à la connectivité mais également à la sécurité, car il peut fournir une porte dérobée pour des fuites de données. Son importance en tant que contrôle de sécurité de premier niveau ne doit donc pas être négligée, en particulier en temps de crise et de changement, comme l'afflux récent de travailleurs à domicile / à distance.

En janvier 2020, Infoblox a demandé à Forrester Consulting d'évaluer l'utilisation du DNS dans la détection des attaques malveillantes et la prévention des pertes de données. Forrester a mené une enquête en ligne auprès de 203 personnes représentatives parmi des experts travaillant pour des entreprises à la pointe des meilleures pratiques en sécurité, afin de constituer un bon exemple pour tous ceux désireux d'améliorer leur propre stratégie de sécurité. Nous avons interrogé des responsables américains en matière de sécurité et de risque (S&R) issus d'entreprises dont le chiffre d'affaires annuel est supérieur ou égal à 1 milliard de dollars, dans le secteur public, la vente au détail, l'éducation, la santé et les services financiers. La moitié des répondants ont le titre de directeur de la sécurité des informations (CISO). Ces experts en S&R utilisent DNS comme un composant essentiel de leur stratégie de sécurité.

Les responsables S&R s'appuient sur le DNS pour trois priorités essentielles : 1) détecter et bloquer les menaces le plus tôt possible dans la chaîne de cyber-attaque ; 2) enquêter sur les menaces et y répondre ; et 3) identifier rapidement les périphériques compromis.

RÉSULTATS CLÉS

- **Le DNS est un point de départ essentiel pour les enquêtes sur les menaces.** Les requêtes et réponses DNS sont l'une des trois principales sources de données utilisées par les équipes de sécurité pour la recherche et l'enquête sur les menaces. Les enquêteurs s'appuient sur le DNS car il détecte les activités malveillantes plus tôt dans la chaîne de cyber-attaque que les autres outils de sécurité. Il offre également aux responsables S&R une visibilité précieuse sur les périphériques émettant des requêtes vers des destinations malveillantes. Cette visibilité leur permet de mettre fin à ces connexions et de protéger l'ensemble de leur infrastructure.
- **Le DNS comble les lacunes laissées par d'autres outils de sécurité.** Il n'existe pas d'outil de sécurité parfait qui résoudra tous vos problèmes, mais il est important d'avoir des outils pour combler les lacunes laissées par d'autres outils. Les responsables S&R interrogés ont déclaré que le principal avantage de l'utilisation du DNS interne en tant que point de contrôle de sécurité pour arrêter les attaques malveillantes était de pouvoir détecter des menaces qui autrement ne seraient pas interceptées par d'autres outils comme le tunneling DNS / l'exfiltration des données, les algorithmes de génération de domaine (DGA) et les attaques par domaine similaire.
- **La majorité des responsables S&R souhaitent améliorer le retour sur investissement en matière de sécurité.** Cinquante-six pour cent des responsables S&R ont indiqué que l'amélioration du retour sur investissement en matière de sécurité était le service le plus utile pour leur entreprise. Alors que la dernière décennie a vu des investissements croissants dans les outils de sécurité, les responsables S&R souhaitent désormais voir quel retour sur investissement ils peuvent obtenir avec les investissements existants avant d'approuver un budget pour davantage d'outils et de technologies.

FORRESTER®

Le DNS est essentiel pour répondre aux principales priorités de sécurité

Les responsables S&R sont conscients que le maintien de la confiance des clients est essentiel à leur activité et que perdre ou compromettre leurs données est la façon la plus rapide de perdre cette confiance. Les responsables S&R réellement dévoués utilisent tous les outils à leur disposition pour détecter et bloquer les menaces, enquêter sur leur apparition et y répondre, et identifier rapidement les périphériques compromis. En interrogeant 203 responsables S&R, nous avons examiné chaque priorité :

DETECTION

- **L'identification des périphériques compromis commence par le DNS.** Il y a plus de risques dans l'environnement réseau actuel que par le passé. Avec l'émergence de la pandémie COVID-19, puis la reprise générale des activités pour toutes les entreprises, des lacunes dans les stratégies de sécurité apparaissent. De plus en plus d'employés travaillent à domicile avec leurs propres périphériques, c'est-à-dire en connectant des appareils de l'Internet des objets (IoT) sans les mesures de sécurité appropriées, etc. Les équipes de sécurité doivent être en mesure d'identifier et de répondre rapidement aux périphériques s'ils deviennent compromis. Les réseaux, périphériques et accès Internet non sécurisés compromettent les données des clients. Les requêtes DNS et les données de réponse sont l'un des trois principaux outils utilisés par les entreprises pour identifier rapidement les périphériques compromis. Les deux outils principaux sont la gestion des adresses IP (IPAM) (67 %) et les journaux des périphériques réseau (62 %).
- **Le défi de l'exfiltration des données se poursuit.** Arrêter l'exfiltration des données n'a jamais été simple. Dans les cas extrêmes, les menaces internes peuvent exfiltrer les données via DNS, bien que les attaquants soient beaucoup plus susceptibles de transférer les données volées via HTTP/HTTPS ou FTP. Dans ce dernier cas, l'organisation cible a de la chance si la demande DNS qui précède l'exfiltration figure sur une liste d'indicateurs de compromis (IOC) publiée.
- **Les responsables S&R bénéficient d'une vision approfondie sur les attaques avec des enquêtes DNS.** Lorsqu'une attaque/infection se produit, les enquêteurs ont besoin d'outils qui offrent une vue globale de l'étendue et de la gravité de la menace. Les enquêtes sur les domaines/adresses DNS sont l'un des deux principaux outils utilisés par les enquêteurs pour déterminer qui, dans leur organisation, a été infecté après une attaque/infection. En fait, les analyses DNS et de programmes malveillants sont tous deux signalés comme les principaux outils utilisés pour identifier les données et systèmes auxquels l'attaquant a obtenu un accès. Le DNS est également utile aux enquêteurs pour déterminer la quantité d'informations auxquelles l'attaquant a obtenu un accès.[2]

Le DNS est un point de contrôle des menaces essentiel.

69 % des responsables S&R utilisent le DNS comme point de contrôle pour se défendre contre les attaques.

BLOCAGE DES MENACES

- **Le DNS est un des trois plus importants points de contrôle de sécurité pour se défendre contre les attaques.** Les filtres/pare-feux DNS ont été classés juste derrière les passerelles/proxy Web sécurisés et les systèmes de détection/prévention des intrusions que les équipes de sécurité utilisent pour se défendre contre les attaques. En fait, 66 % des responsables S&R ont déclaré que le DNS leur permet de détecter l'activité des programmes malveillants plus tôt dans la chaîne d'élimination, réduisant ainsi la charge pesant sur leurs défenses périmétriques.
- **Trois responsables S&R sur quatre utilisent des solutions de prévention des pertes de données (DLP) pour protéger les données.** Plus des trois quarts des personnes interrogées utilisent des solutions de prévention des pertes de données pour protéger leurs données clients. Les 24 % restants des responsables S&R utilisent d'autres solutions comme les pare-feux de nouvelle génération, les passerelles Web sécurisées et les agents de sécurité d'accès au cloud (CASB) pour protéger leurs données.

ENQUETE SUR LES MENACES ET REPONSE

Quatre-vingt-dix pour cent des responsables S&R de notre étude ont déclaré considérer ou avoir considéré le DNS comme un point de départ pour leurs enquêtes sur les menaces. Le DNS joue un rôle essentiel dans l'accélération des taux de réponse aux incidents sur tous les périphériques de l'entreprise sur le réseau principal, dans les filiales et les sites de travailleurs mobiles, ainsi que dans l'IoT. Une approche à l'échelle de l'entreprise pour le partage des renseignements sur les menaces est considérée comme essentielle pour plus d'un tiers des responsables S&R, tandis que 45 % d'entre eux confirment que cela profiterait à leur entreprise.

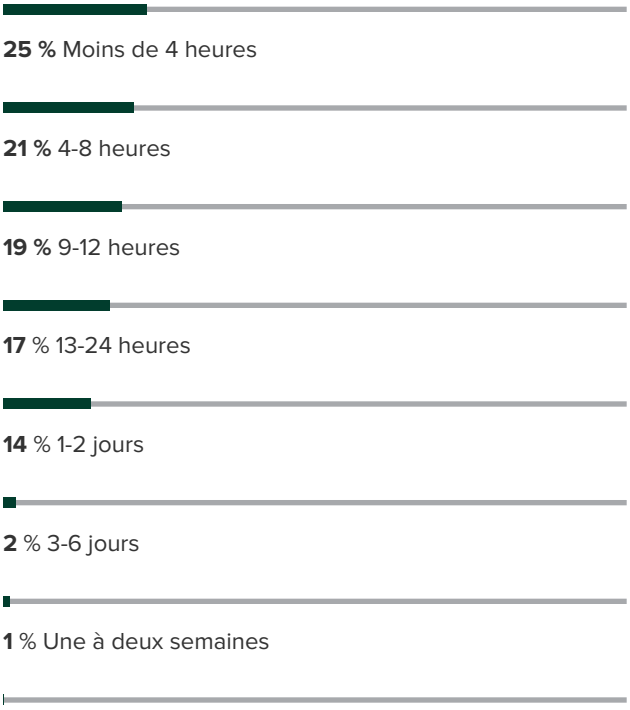
- **Même les responsables S&R ne peuvent gérer qu'une à deux enquêtes par jour.** Presque la moitié (46 %) des responsables S&R de notre étude ont constaté qu'il faut en moyenne entre 1 et 8 heures pour enquêter sur une menace. Cela correspond environ à une ou deux enquêtes complètes par jour en moyenne. Des temps de réponse plus rapides nécessitent des intégrations et un partage automatique des données entre des outils qui sont tous deux pris en charge par un personnel qualifié et formé et soutenus par des processus précis (voir Figure 1).
- **L'automatisation est essentielle pour améliorer les taux de réponse aux incidents.** Près de 60 % des responsables S&R seniors utilisent un mélange de processus manuels et automatisés de réponse aux incidents. Seuls 31 % des responsables S&R interrogés ont déclaré que leurs processus de réponse aux incidents étaient presque entièrement automatisés. Ces responsables sont conscients que toute partie du processus qui peut être automatisée devrait l'être, dans le but d'améliorer la rapidité et la précision des réponses aux incidents. L'utilisation d'outils d'orchestration, d'automatisation et de réponse de sécurité (SOAR) constitue la méthode d'automatisation du processus de réponse aux incidents de la plupart des personnes interrogées ; d'autres sélectionnent spécifiquement des outils qui incluent l'automatisation ou utilisent des scripts développés en interne. Les scripts développés en interne sont utilisés le plus souvent dans le secteur public. Des milliers de scripts ont été écrits au fil du temps pour traiter diverses parties du processus de réponse aux menaces, qui peuvent devenir un fardeau à maintenir au fil du temps.

Le DNS permet d'effectuer des enquêtes plus efficaces.

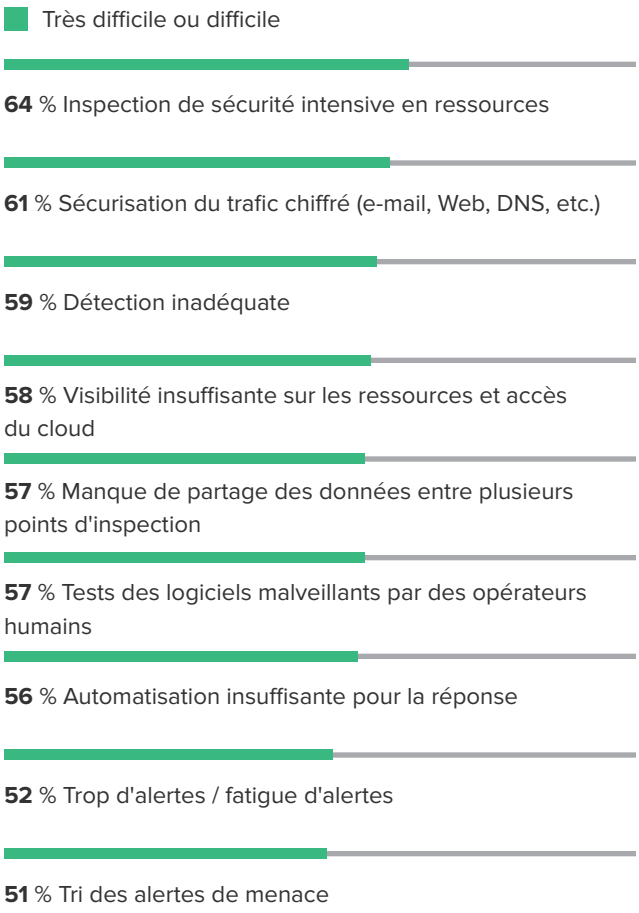
Les responsables S&R utilisent les données DNS tout au long des enquêtes pour corréler les journaux réseau, déterminer l'exposition et examiner les ressources sortantes.

Figure 1

« En moyenne, combien de temps environ votre équipe d'opérations de sécurité met-elle à enquêter sur une menace ? »



« Dans quelle mesure chacun des facteurs suivants est-il difficile pour la prévention des menaces et les enquêtes sur les menaces de votre organisation ? »



Participants : 203 décisionnaires américains en matière de sécurité
Source : étude commanditée menée par Forrester Consulting pour le compte d'Infoblox, avril 2020

› **Le DNS est une source de données d'enquête de premier plan.** Quarante-trois pour cent des responsables S&R comptent sur les requêtes et les réponses DNS pour effectuer des enquêtes sur les menaces. Cela signifie que le DNS est l'une des trois principales sources de données sur lesquelles se reposent les enquêteurs (à 43 %), derrière les journaux réseau (57 %) et les données de gestion des événements et des informations de sécurité (SIEM) (44 %) (voir Figure 2). Le DNS est un élément clé de la stratégie de sécurité des responsables S&R en protégeant les entreprises contre les menaces que d'autres outils de sécurité auraient pu manquer et en permettant aux enquêteurs de savoir quels périphériques ont demandé des connexions à des destinations malveillantes.

Figure 2

« Parmi les sources de données suivantes, sur lesquelles vos équipes de sécurité comptent-elles pour mener une enquête/une recherche de menaces ? »

Participants : 203 décisionnaires américains en matière de sécurité
Source : étude commanditée menée par Forrester Consulting pour le compte d'Infoblox, avril 2020

FORRESTER®

Les équipes S&R doivent être polyvalentes

Selon l'enquête de Forrester Analytics « Global Business Technographics® Security Survey, 2019 », 43 % des personnes interrogées aux Etats-Unis ont été victimes d'une ou de plusieurs violations qui ont compromis des données sensibles au cours des 12 derniers mois.[3] Vingt-deux pour cent des entreprises attaquées ont déclaré que l'attaque était effectuée via DNS. Le volume élevé de menaces provenant de sources et d'attaquants nombreux implique que les responsables S&R doivent faire face à de nombreux défis :

- **Les équipes S&R sont submergées par des facteurs pendant les enquêtes.** Faute d'un accès immédiat et sans entrave à toutes les ressources d'études sur les incidents, les enquêteurs ont souvent le sentiment d'avoir une détection inadéquate. Ils ont besoin d'une visibilité claire et d'un accès aux clouds privés et publics. En outre, le trafic crypté par e-mail, sur le Web et bientôt sur DNS pose des problèmes aux enquêteurs sur les menaces.
- **La fatigue s'installe et l'automatisation est à la traîne.** Le volume d'alertes que les enquêteurs sur menaces traitent chaque semaine, voire chaque jour, peut être intimidant. Cinquante-deux pour cent des responsables S&R ont déclaré qu'un trop grand nombre d'alertes ou une fatigue sur les alertes constitue un problème. A cela s'ajoute le fait que le tri des alertes de menace est une difficulté pour 51 % des personnes interrogées. Comment gérer cette fatigue ? L'automatisation est la réponse directe, mais même parmi les principaux responsables S&R que nous avons interrogés, 56 % ont déclaré qu'ils ne disposent pas d'une automatisation suffisante pour répondre aux menaces.
- **Détection et blocage des mauvaises destinations et des sites malveillants pour les travailleurs mobiles en cas de crise.** Lorsque la pandémie de COVID-19 a commencé à frapper les Etats-Unis de manière significative en mars 2020, la main-d'œuvre nord-américaine s'est massivement tournée vers le travail à domicile / mobile. Des employés qui n'avaient jamais eu à travailler à domicile ont soudain dû trouver un moyen de travailler à domicile tout en protégeant les données sensibles des clients. Notre enquête a été menée principalement à la fin du mois de mars, alors que la pandémie commençait seulement aux Etats-Unis. Même alors, les responsables S&R pensaient qu'ils étaient moins efficaces pour détecter et bloquer les menaces sur leurs sites de travailleurs mobiles (voir Figure 3). Les responsables S&R ont été mis à l'épreuve en 2020 puisqu'ils ont dû apprendre à sécuriser les périphériques et les réseaux des travailleurs mobiles à un volume plus élevé qu'ils ne l'avaient jamais fait auparavant. Pour ces responsables S&R, pouvoir agir rapidement et de manière décisive apporte le succès sur le long terme.

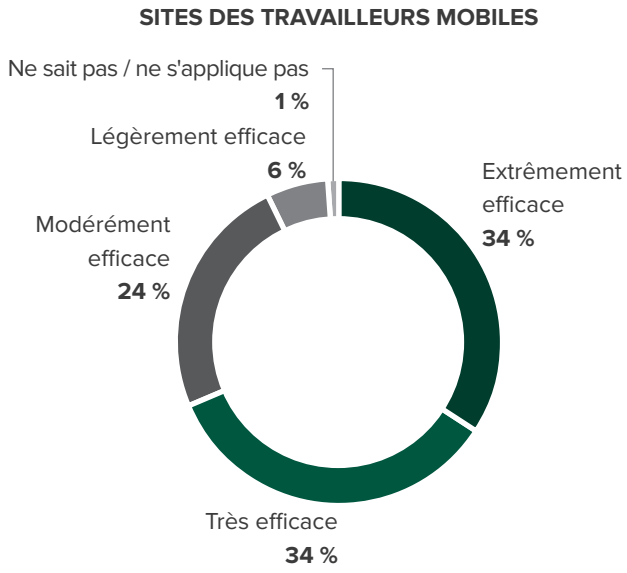
Selon l'enquête « Global Business Technographics Infrastructure Survey, 2019 » de Forrester Analytics, les entreprises peuvent posséder plus de 500 000 tablettes et plus de 2 millions d'ordinateurs portables, créant ainsi de nombreux points potentiels d'infection et d'attaque.

Le DNS est essentiel pour détecter les menaces.

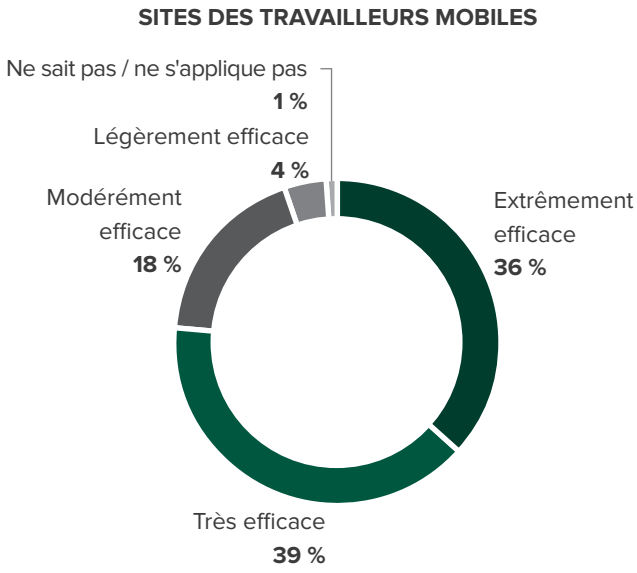
66 % des responsables S&R ont déclaré que le DNS est capable de détecter les menaces que leurs autres outils de sécurité ne peuvent pas détecter.

Figure 3

« Dans quelle mesure êtes-vous efficace pour détecter l'accès aux mauvaises destinations et aux sites malveillants aux emplacements suivants ? »



« Dans quelle mesure êtes-vous efficace pour bloquer l'accès aux mauvaises destinations et aux sites malveillants aux emplacements suivants ? »

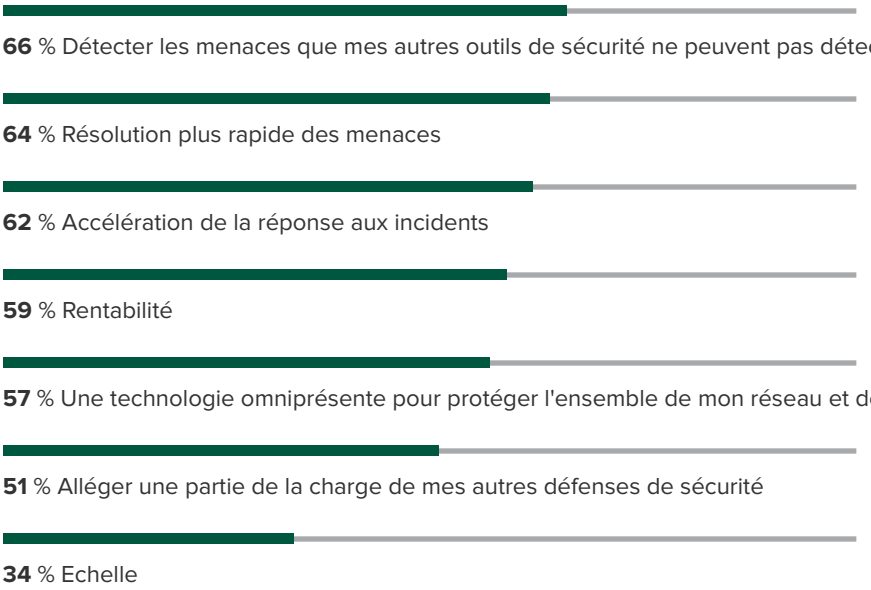


Participants : 203 décisionnaires américains en matière de sécurité
Source : étude commanditée menée par Forrester Consulting pour le compte d'Infoblox, avril 2020
Remarque : la somme des pourcentages peut être différente de 100, car les chiffres sont arrondis.

- **L'utilisation du DNS interne comme point de contrôle de sécurité permet de résoudre des problèmes de sécurité essentiels.** Soixante-six pour cent des responsables S&R ont déclaré que le DNS est capable de détecter des menaces que leurs autres outils de sécurité ne peuvent pas détecter. Le DNS aide également à accélérer les temps de réponse aux incidents, ce qui accélère la résolution des menaces. Le DNS aide la technologie de leurre d'une organisation, qui peut piéger des attaquants lorsqu'ils pénètrent pour la première fois ; cette même technologie peut être exploitée pour rediriger les hôtes vers des zones d'inspection spéciales lorsqu'ils demandent des ressources de réputation inconnue. Plus d'un tiers des entreprises déclarent que l'utilisation du DNS interne comme point de contrôle de sécurité peut les aider à arrêter les attaques malveillantes à grande échelle (voir Figure 4).
- **Les responsables S&R doivent relever des défis spécifiques au COVID-19.** Les entreprises ont été contraintes à mener une expérience sans précédent de travail à distance qui ne semble pas devoir se terminer. Jusqu'à ce qu'un vaccin soit disponible, il y aura toujours une partie de la main-d'œuvre à distance.[4] En plus du volume beaucoup plus élevé de travailleurs mobiles, les responsables S&R doivent également relever des défis supplémentaires posés par le COVID-19. Avec la réduction du personnel sur site, de nombreux responsables S&R ont dû trouver des solutions d'automatisation pour combler les lacunes en personnel et surveiller en permanence l'accès et l'utilisation du cloud. De nombreuses entreprises ne disposent pas des outils/logiciels nécessaires pour permettre à leur personnel mobile de travailler pleinement. D'autres entreprises, en particulier celles situées en milieu rural, manquent de bande passante Internet pour répondre à leurs besoins. Les cyberpirates développent leurs attaques de hameçonnage et d'ingénierie sociale, et tirent parti des vulnérabilités des outils de collaboration. Ne baissez pas la garde ![5]

Figure 4

« Quels sont les avantages que vous pouvez attendre de l'utilisation du DNS interne comme point de contrôle de sécurité pour arrêter les attaques malveillantes ? »

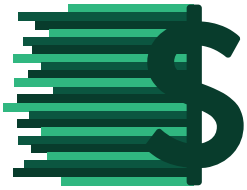


Participants : 203 décisionnaires américains en matière de sécurité
Source : étude commanditée menée par Forrester Consulting pour le compte d'Infoblox, avril 2020

Répondre aux besoins en retour sur investissement et en contexte de menace

Les responsables S&R doivent s'efforcer de définir les projets qui génèrent le plus de valeur pour leur entreprise. Ils ont également souvent du mal à justifier les budgets existants. En tirant parti des partenaires capables de mesurer les performances et de fournir un contexte aux menaces, les responsables peuvent mieux justifier leurs budgets et investir dans des outils et technologies de pointe. Cette étude a mis en évidence certains points :

- **Même les meilleurs responsables S&R recherchent des services supplémentaires.** Nous avons ciblé des responsables S&R de plus haut niveau pour cette étude, mais même ces experts dans des entreprises qui généralement mènent la voie sur les meilleures pratiques en matière de sécurité reconnaissent qu'ils peuvent continuer à s'améliorer. Les responsables S&R recherchent vivement un service qui améliorera leur retour sur investissement en matière de sécurité. En réalisant des économies sur leurs enquêtes, ils peuvent investir davantage dans l'innovation, une meilleure technologie et le recrutement / la formation du personnel. En outre, ils recherchent des services de surveillance continue qui répondent à leurs défis de visibilité. Ils souhaitent également pouvoir automatiser les tâches de sécurité courantes et répétitives, ce qui se traduira par une réduction des coûts. Et si l'on considère l'avenir, l'automatisation ne peut qu'être une aubaine pour la sécurisation d'une main-d'œuvre qui commence tout juste à s'installer dans le travail à distance, de façon permanente ou semi-permanente.

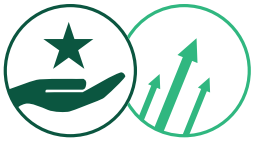


Le retour sur investissement est le plus important.

56 % des responsables S&R ont indiqué que l'amélioration du retour sur investissement en matière de sécurité était le service le plus utile pour leur entreprise.

FORRESTER®

- **Les responsables S&R recherchent un contexte plus détaillé pour les identificateurs de menace.** Les responsables S&R de notre étude étaient clairs, ils ont classé les renseignements sur les menaces comme la ressource la plus importante pour améliorer les capacités de sécurité globales de leur organisation (voir Figure 5). L'un des éléments clés de l'amélioration de ces capacités est une meilleure compréhension des identificateurs de menace spécifiques. Les responsables attendent de leurs prestataires qu'ils comprennent le contexte à la fois des menaces uniques qui pèsent sur leur environnement et de la complexité de leur activité. En sachant ce qu'il faut rechercher, les enquêteurs peuvent fournir des réponses plus efficaces aux violations, trier plus rapidement les menaces et mieux collaborer avec les équipes. Les informations contextuelles des alertes peuvent faire la différence entre des résolutions de menace immédiates et prolongées.
- **Les travailleurs mobiles ont besoin de meilleurs renseignements sur les menaces.** Pendant la pandémie du coronavirus, de nombreuses entreprises demandent ou imposent à leurs employés de travailler à domicile. Des millions d'employés qui se connectaient sur des postes de travail sur des réseaux d'entreprise se connectent désormais depuis leur domicile ou ailleurs sur des réseaux publics. L'authentification renforcée et le VPN, qui auparavant ne concernaient qu'un sous-ensemble d'employés à un moment donné, deviennent maintenant le point d'entrée pour l'ensemble des travailleurs.[6] On s'attend à ce que de nombreux employés restent chez eux pour la majeure partie de l'année 2020 et que certains ne reviennent jamais travailler au bureau. Les grandes entreprises offrent aux employés une flexibilité accrue pour travailler à distance. Cependant, notre étude a révélé qu'il est plus difficile même pour les responsables S&R les plus qualifiés de détecter et bloquer les mauvaises destinations et les sites malveillants pour les travailleurs mobiles. Les responsables doivent agir rapidement pour exploiter DNS comme un dispositif de renseignements de base sur les menaces, afin d'accélérer la réponse aux incidents, de découvrir et de gérer l'inventaire et d'optimiser leurs piles de sécurité pour une résolution plus rapide des menaces.

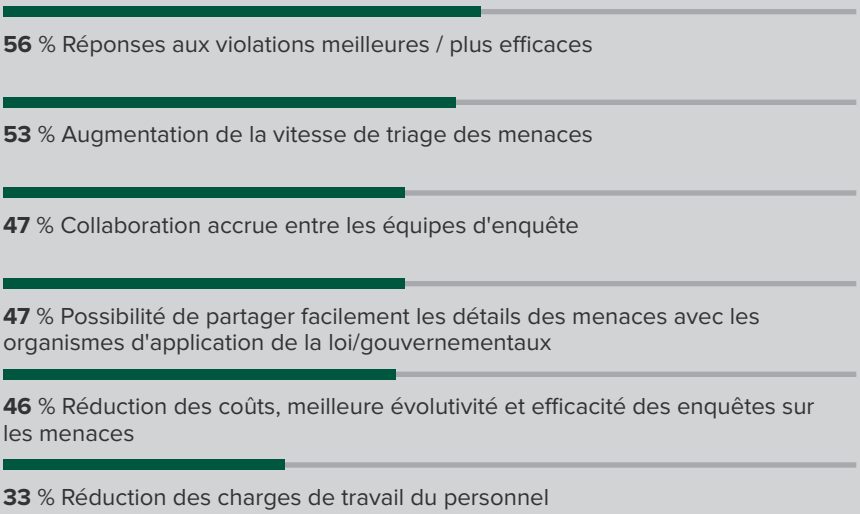


Le contexte facilite une réponse efficace.

La moitié des responsables S&R considèrent que plus de contexte / un meilleur contexte améliore l'efficacité en matière de triage, de réponse aux violations et de collaboration.

Figure 5

« Quels sont les avantages que vous pouvez attendre du fait de disposer d'avoir plus de contexte / un meilleur contexte sur des identificateurs de menace spécifiques ? »



Participants : 203 décisionnaires américains en matière de sécurité
Source : étude commanditée menée par Forrester Consulting pour le compte d'Infoblox, avril 2020

FORRESTER®

Principales recommandations

L'enquête approfondie menée par Forrester auprès de 203 responsables américains de la sécurité et des risques sur l'utilisation du DNS comme point de contrôle de sécurité fondamental a généré plusieurs recommandations importantes :

Partager les renseignements sur les menaces dans toute l'entreprise. La majorité des entreprises interrogées par Forrester estiment qu'une approche à l'échelle de l'entreprise en matière de partage de renseignements sur les menaces est un avantage essentiel pour leur entreprise. Les professionnels de la sécurité et des risques doivent distribuer les renseignements sur les menaces utilisés par leurs principales équipes d'analyse de sécurité et d'investigation dans toute l'entreprise afin d'optimiser la valeur de ces renseignements au moment opportun, lorsque cela peut être le plus efficace.

Continuer à accélérer les fonctions de réponse aux incidents. En 2018 et 2019, un nombre record de vulnérabilités critiques et élevées ont été enregistrées. Aujourd'hui, une équipe de gestion de la sécurité voit une nouvelle vulnérabilité élevée ou critique apparaitre, en moyenne, toutes les 9 heures[7]. En même temps, les attaquants automatisent l'exploitation des vulnérabilités récemment publiées, élargissant la surface de la menace mondiale et s'implantant dans les organisations de manière opportuniste. La pression pour répondre aux incidents et aux vulnérabilités qui les provoquent pousse les entreprises à prendre le chemin le plus rapide vers la vérité. Et pour beaucoup, le DNS est cette route.

Prendre le contrôle de la gestion de la découverte des ressources. La gestion moderne des ressources est l'un des problèmes les plus difficiles à résoudre, en partie en raison de la facilité avec laquelle de nouveaux périphériques peuvent être connectés aux réseaux d'entreprise par les employés, les équipes distantes et les partenaires. La découverte des ressources reste un défi. Les solutions DNS intégrées, DHCP et IPAM, peuvent vous aider, car elles constituent le seul type de point de contrôle avec lequel il est garanti que chaque périphérique peut interagir. Utilisez les données IPAM pour identifier rapidement les périphériques compromis. La gestion du cycle de vie des ressources, de l'intégration à la mise au rebut, devient une discipline à part entière.

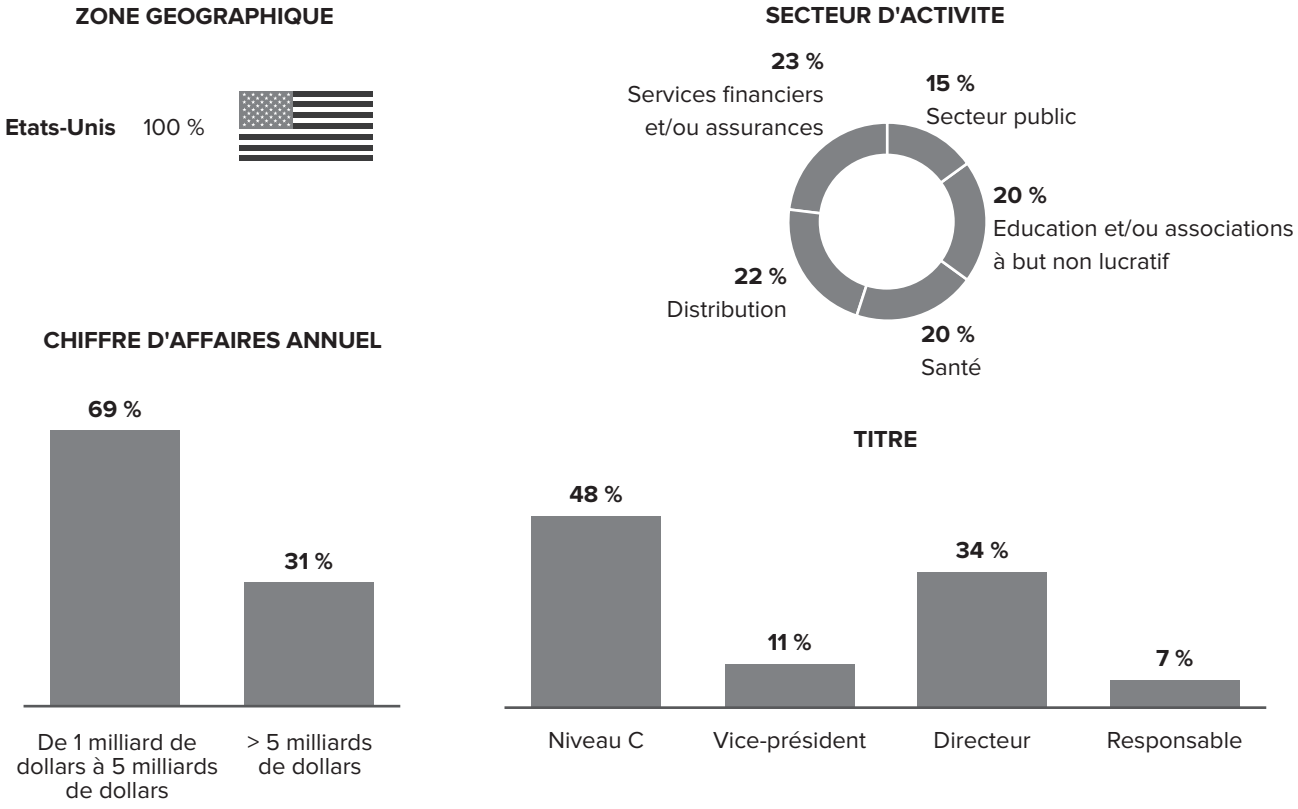
Etendre tactiquement l'infrastructure de sécurité existante. L'architecture de la pile de sécurité est en train de changer, avec une tendance à fournir presque tous les composants de sécurité, et même tous dans certains cas, depuis le cloud. La concurrence pour la meilleure recette de pile de sécurité est âpre, mais cinq ans ou plus pourraient passer avant qu'une solution dominante n'émerge. Les entreprises prudentes peuvent prolonger la durée de vie de leur infrastructure de sécurité existante grâce à des optimisations. Les renseignements sur les menaces via le DNS peuvent jouer ici un rôle majeur, dans la mesure où la classification « danger connu » permet aux entreprises d'effectuer des déterminations aisées plus rapidement et de transférer uniquement les inspections les plus difficiles vers la pile complète, où le sandboxing et l'analyse humaine ont le dernier mot.

Continuer à défendre, en profondeur. Internet est désormais chiffré ; les fournisseurs d'analyses et de visibilité réseau (NAV) déclarent de manière informelle à Forrester qu'ils voient entre 72 % et 95 % de trafic chiffré dans les réseaux d'entreprise. Pour de nombreuses entreprises, seules les métadonnées telles que les demandes DNS restent visibles pour l'analyse en temps réel. Les professions de la sécurité et des risques continueront à adopter les techniques éprouvées et réelles de pare-feu et de filtrage DNS comme première ligne de défense contre les programmes malveillants, le phishing et les ransomware. Les attaquants le savent et ont mis en place des algorithmes pour générer des noms de domaine pseudo-aléatoires pour les opérations C2, ce qui a conduit à une course aux armements que seule l'IA sera en mesure de combattre en temps réel.

Annexe A : méthodologie

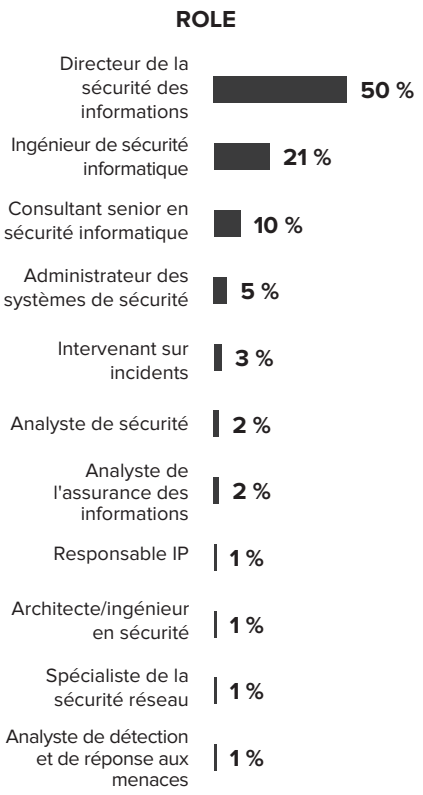
Dans cette étude, Forrester a mené une enquête en ligne auprès de 203 décisionnaires américains en matière de sécurité, travaillant dans les secteurs de services financiers, la santé, l'éducation, la vente au détail et le secteur public, afin d'évaluer la manière dont ils utilisaient le DNS dans leurs enquêtes sur les menaces. Les personnes interrogées ont reçu une légère rémunération en remerciement pour le temps consacré à l'enquête. L'étude a débuté en avril 2020 et s'est achevée en avril 2020.

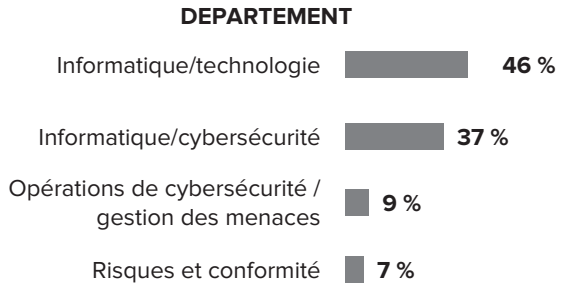
Annexe B : données démographiques



Participants : 203 décisionnaires américains en matière de sécurité
Source : étude commanditée menée par Forrester Consulting pour le compte d'Infoblox, avril 2020
Remarque : la somme des pourcentages peut être différente de 100, car les chiffres sont arrondis.

FORRESTER®





RESPONSABILITE

	Stratégie d'évaluation de la sécurité et des risques	Stratégie de renseignements sur les menaces
Principale	79 %	79 %
Responsabilité partagée	17 %	18 %
Fournir une entrée et exécuter	3 %	3 %

Participants : 203 décisionnaires américains en matière de sécurité
Source : étude commanditée menée par Forrester Consulting pour le compte d'Infoblox, avril 2020
Remarque : la somme des pourcentages peut être différente de 100, car les chiffres sont arrondis.

Annexe C

NOTES DE FIN

[1] Source : Dan Gallagher, « Data Really Is the New Oil », The Wallstreet Journal, 9 mars 2019.

[2] Source : Forrester Analytics Global Business Technographics Infrastructure Survey, 2019.

[3] Source : Forrester Analytics Global Business Technographics Security Survey, 2019.

[4] Source : « Collection: Learn To Support A Remote Workforce Permanently », Forrester (https://www.forrester.com/fn/37Kn3Q4mpMBdAxFZhMFbf1).

[5] Source : « Address The Security And Privacy Challenges Of Working From Home », Forrester (https://www.forrester.com/fn/21NX5awklkxYASgFFz0Ejx).

[6] Source : Sean Ryan, « A Spike In Home Workers Raises MFA Resilience Questions », Forrester Blogs, 17 mars 2020, https://go.forrester.com/blogs/a-spike-in-home-workers-raises-mfa-resilience-questions/.

[7] Source : National Institute of Standards and Technology, CVSS Severity Distribution Over Time (https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time).

FORRESTER®