

L'ABC du DNS, DHCP, et sécurité IPAM

INCLUT DES
TECHNIQUES DE
DÉFENSE
EFFICACES QUE
LES ANALYSTES
DE SÉCURITÉ
PEUVENT
UTILISER



ManageEngine
Log360

Table de matières

Chapitre 1 : Qu'est-ce qu'une DDI?	1
Chapitre 2 : Système de nom de domaine (DNS) - Le résolveur	3
2.1 Qu'est-ce qu'un DNS ?	4
2.2 Comment fonctionne le DNS ?	4
2.3 Menaces pour le DNS	8
2.3.1 Déni de service distribué (DDoS)	8
2.3.2 Empoisonnement du cache DNS	9
2.3.3 Tunnelage du DNS	11
Chapitre 3 : Protocole de configuration dynamique des hôtes - L'assignateur	12
3.1 Qu'est-ce que le DHCP ?	13
3.2 Comment fonctionne le DHCP ?	14
3.3 Menaces pour le DHCP	16
3.3.1 Privation de DHCP	16
3.3.2 Falsification DHCP	17
Chapitre 4 : Gestion des adresses IP (IPAM) - L'administrateur	18
4.1 Qu'est-ce que l'IPAM ?	19
4.2 L'IPAM est-il indispensable ?	19
Chapitre 5 : Défendre la DDI	21
5.1 Mesures pour protéger les infrastructures DNS, DHCP et IPAM d'une organisation	22
5.2 Comment Log360 peut-il vous aider?	23
Références	29

Chapitre 1

Qu'est-ce qu'une DDI ?

Sujets abordés:

- Système de noms de domaine (DNS)
- Protocole de configuration dynamique des hôtes (DHCP)
- Gestion des adresses IP (IPAM)



Le terme DDI a été utilisé pour la première fois par Gartner en 2009, lors de la publication du premier rapport MarketScope.1 Si le terme DDI peut sembler peu familier, vous le reconnaîtrez peut-être comme l'intégration de DNS, DHCP et IPAM.

- ✔ **Le système de noms de domaine (DNS)** est un protocole qui permet de résoudre les noms de sites web en fonction de leur adresse IP correspondante.
- ✔ **Le protocole de configuration dynamique des hôtes (DHCP)** est un protocole de réseau dans lequel un serveur DHCP attribue automatiquement des adresses de protocole Internet (IP) et d'autres paramètres de configuration du réseau aux périphériques du réseau IP.
- ✔ **La gestion des adresses IP (IPAM)** est un système permettant de gérer les espaces d'adresses IP sur un réseau à l'aide du DNS et du DHCP..

DNS, DHCP et IPAM sont des composants essentiels au fonctionnement du réseau d'entreprise. Qu'il s'agisse de diagnostiquer les problèmes de réseau pour réduire les temps d'arrêt, d'identifier les failles dans le réseau ou de prévenir les cyberattaques, la sécurité des DDI est devenue un élément essentiel du livre de jeu de toute organisation en matière de cybersécurité.

Dans cet e-book, nous allons aborder chacun de ces composants en détail.

Chapitre 2

Systeme de noms de domaine (DNS) – Le résolveur

Sujets abordés:

- 2.1 Qu'est-ce que le DNS ?
- 2.2 Comment fonctionne le DNS ?
- 2.3 Menaces pour le DNS
 - 2.3.1 Déni de service distribué (DDoS)
 - 2.3.2 Empoisonnement du cache DNS
 - 2.3.3 Tunnelage DNS



2.1 Qu'est-ce que le DNS?

Tout comme les humains identifient les choses, les lieux et les autres humains par des noms, dans le domaine des réseaux, les ordinateurs et les autres périphériques de réseau s'identifient les uns les autres par leur adresse IP. Cependant, il nous est difficile de nous souvenir de l'adresse IP de chaque site Web que nous consultons. C'est là que le DNS vient à notre secours. On peut l'imaginer comme l'application de contact de votre smartphone qui répertorie les noms des personnes avec leur numéro de téléphone, leur adresse électronique et d'autres détails. Le DNS fournit une liste de tous les sites web avec leurs adresses IP correspondantes. En termes simples, le DNS est un traducteur qui convertit les noms de domaine lisibles par l'homme en adresses IP numériques compréhensibles par la machine.

2.2 Comment fonctionne le DNS?

Vous passez une mauvaise journée et vous connaissez le site web qui va l'égayer : "www.cutedogs.com". Suivons la trace de la façon dont de mignonnes vidéos de chiens se retrouvent sur l'écran de votre ordinateur ou de votre appareil mobile. Voici les étapes à suivre pour convertir un nom de domaine en adresse IP:

ÉTAPE 1

Vous ouvrez votre navigateur Web et tapez "www.cutedogs.com". Tout d'abord, votre navigateur et votre système d'exploitation vont chercher dans leur cache pour récupérer l'adresse IP du site web.

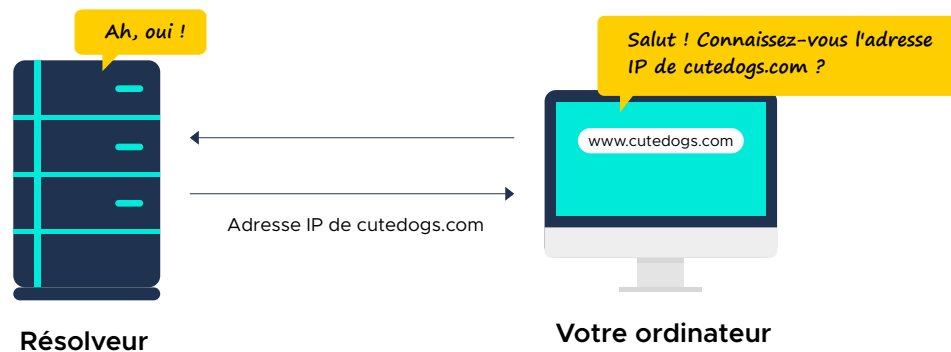


Si l'adresse IP est trouvée dans le cache, le navigateur atteint directement "cutedogs.com" en y faisant référence. L'adresse IP sera trouvée dans le cache si vous avez déjà visité ce site web auparavant, et les détails y sont toujours stockés. Si l'adresse IP n'est pas trouvée dans le cache, l'étape 2 se produit.

ÉTAPE 2

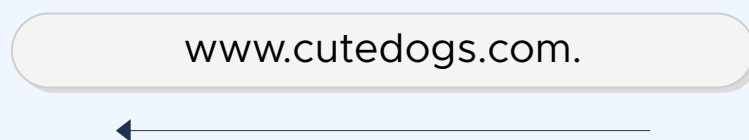
La requête "www.cutedogs.com" est envoyée au serveur du résolveur. Le résolveur vérifie dans sa mémoire cache l'adresse IP de la requête reçue. Si l'adresse IP est trouvée, la valeur est renvoyée à la machine cliente, c'est-à-dire à votre ordinateur.

Définition: Le **résolveur DNS**, également appelé **récurseur DNS**, est un serveur chargé d'effectuer des requêtes supplémentaires pour identifier l'adresse IP du nom de domaine demandé par le client.
Les résolveurs sont situés chez les fournisseurs de services Internet (ISP) ou dans les réseaux institutionnels.



Remarque:

Avant de continuer, vous devez savoir que la résolution des adresses IP se fait de droite vers la gauche. La hiérarchie des domaines descend et devient plus spécifique en allant de droite à gauche. vers la gauche, c'est-à-dire que l'étiquette de gauche est une subdivision de l'étiquette de droite.

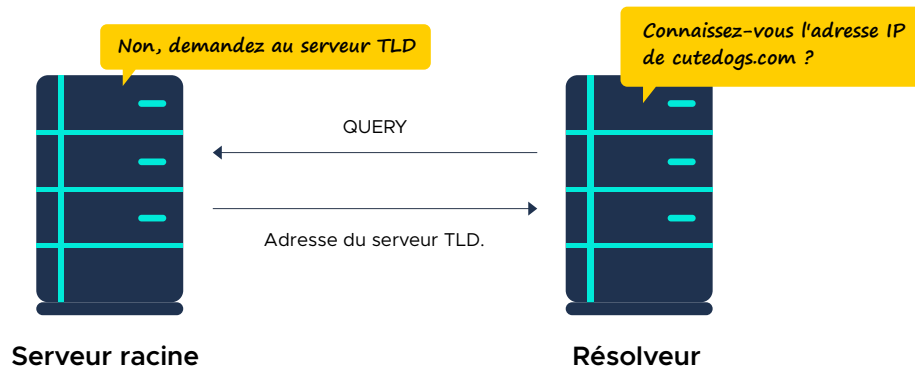


Si l'adresse IP n'est pas trouvée dans le cache du résolveur, la requête est transmise au serveur racine.

ÉTAPE 3

Le serveur racine ne contient pas l'adresse IP de "cutedogs.com", mais redirige le résolveur vers le serveur de domaine de premier niveau, ou serveur TLD, du domaine .com

Définition: Les **serveurs racine** constituent le niveau le plus élevé de la hiérarchie du DNS. Il existe 13 serveurs racine répartis dans le monde entier et gérés par une organisation à but non lucratif appelée Internet Corporation for Assigned Names and Numbers (ICANN).

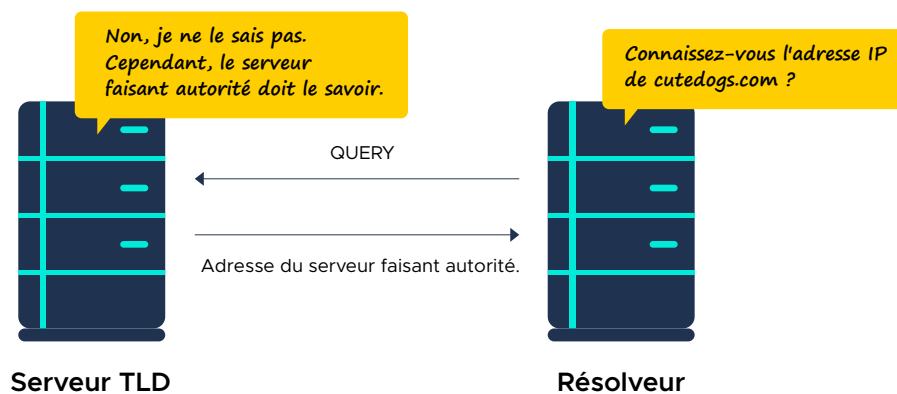


www.cutedogs.com.

STEP 4

Le serveur TLD contient les informations d'adresse pour le domaine de premier niveau ".com" dont "cutedogs.com" fait partie. Le serveur TLD dirige le résolveur vers le serveur de noms faisant autorité pour le domaine cutedogs.com, qui est la destination finale.

Définition: Le serveur **de noms de domaines de premier niveau (TLD)** contient les informations relatives aux adresses des domaines de premier niveau tels que .com, .net, .gov, etc. Les serveurs de noms TLD sont gérés par l'Internet Assigned Numbers Authority (IANA), qui est une branche de l'ICANN.

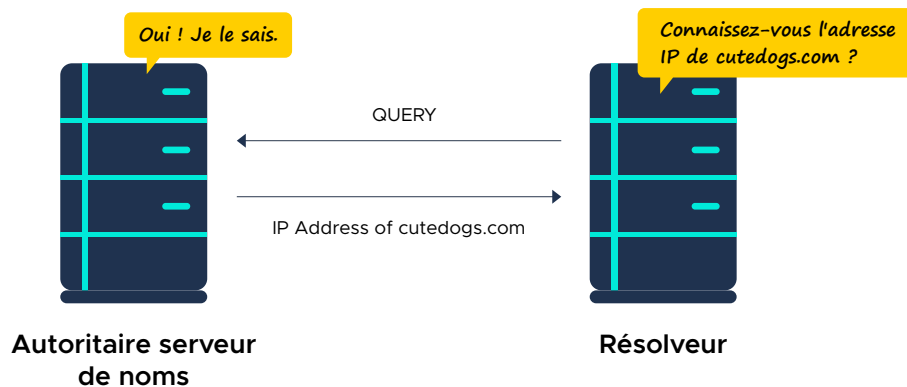


www.cutedogs.com.

ÉTAPE 5

Le serveur de noms faisant autorité détient des informations sur un domaine. Ce serveur fournit au résolveur l'adresse IP de "cutedogs.com".

Définition: Le **serveur de noms** faisant autorité contient des informations sur tout domaine spécifique qu'il dessert, et fournit la réponse réelle à la requête du client, c'est-à-dire l'adresse IP correspondant au nom de domaine demandé.



www.cutedogs.com.

ÉTAPE 6

Le résolveur renvoie l'adresse IP de "cutedogs.com" à votre ordinateur. Grâce à cette information, votre navigateur peut maintenant atteindre "cutedogs.com".



Vous pouvez maintenant regarder des vidéos de chiens mignons et vous sentir plus heureux !

2.3 Menaces pour le DNS

Dans les sections précédentes, nous avons vu en détail le fonctionnement du DNS. Sans le DNS, l'Internet facile d'accès, tel que nous le connaissons aujourd'hui, n'existerait pas. Le DNS est un composant crucial de tout réseau connecté à Internet pour communiquer avec les réseaux externes. La criticité des opérations du DNS, associée au fait qu'il ne peut être complètement verrouillé, en fait une cible privilégiée des cyberattaquants.

Statistique : Selon le rapport mondial sur les menaces DNS d'IDC, 82 % des organisations dans le monde ont été confrontées à une attaque DNS en 2019.2

Nous allons maintenant aborder certains des types d'attaques DNS les plus répandus.

2.3.1 Déni de service distribué (DDoS)

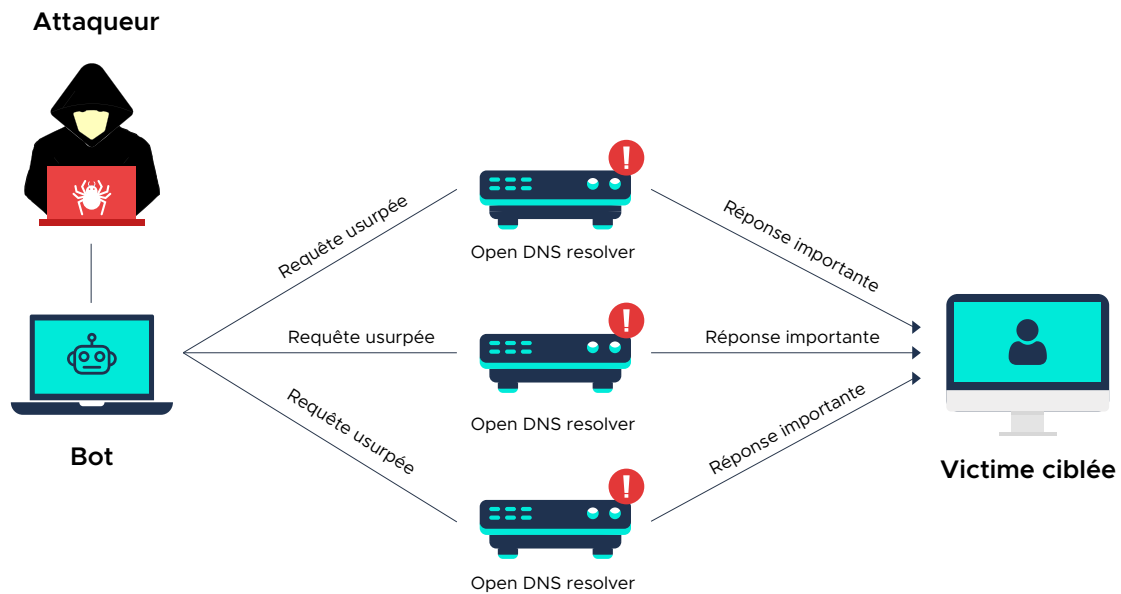
Le DDoS est un type de cyberattaque dans lequel l'attaquant submerge un dispositif ou un réseau avec un trafic massif, le rendant inutilisable pour les utilisateurs prévus. Le DDoS n'est pas une menace spécifique au DNS. Cependant, le DNS est particulièrement vulnérable aux attaques DDoS et il peut constituer un point d'étranglement logique sur un réseau, puisque tous les appareils connectés à votre réseau doivent interagir avec lui pour contacter l'internet.

Attaque par amplification DNS

L'attaque par amplification DNS est un type d'attaque DDoS qui exploite le mode de fonctionnement du DNS. Les attaquants utilisent des résolveurs DNS ouverts et des techniques d'usurpation d'adresse IP pour submerger les victimes avec des charges utiles volumineuses. Les résolveurs DNS ouverts fournissent une résolution récursive des noms pour tout client.

Voici comment se déroule une attaque par amplification DNS:

- ✔ Les attaquants envoient une requête DNS avec une adresse IP usurpée, qui pointe vers l'IP cible, à un résolveur DNS ouvert.
- ✔ Afin d'amplifier la taille de la réponse du résolveur, la requête inclut des arguments tels que "ANY". Alors qu'une requête DNS non malveillante ne demande que l'adresse IP d'un site Web, une requête incluant l'argument "ANY" renvoie des informations sur l'ensemble du domaine (sous-domaines, alias, serveurs de messagerie, etc.), ce qui augmente la taille de la charge utile jusqu'à 50 fois celle de la réponse originale.
- ✔ Une fois que le résolveur reçoit la demande, il envoie la charge utile amplifiée à l'adresse IP usurpée, submergeant le réseau cible, ce qui entraîne une attaque par déni de service.



2.3.2 Empoisonnement du cache DNS

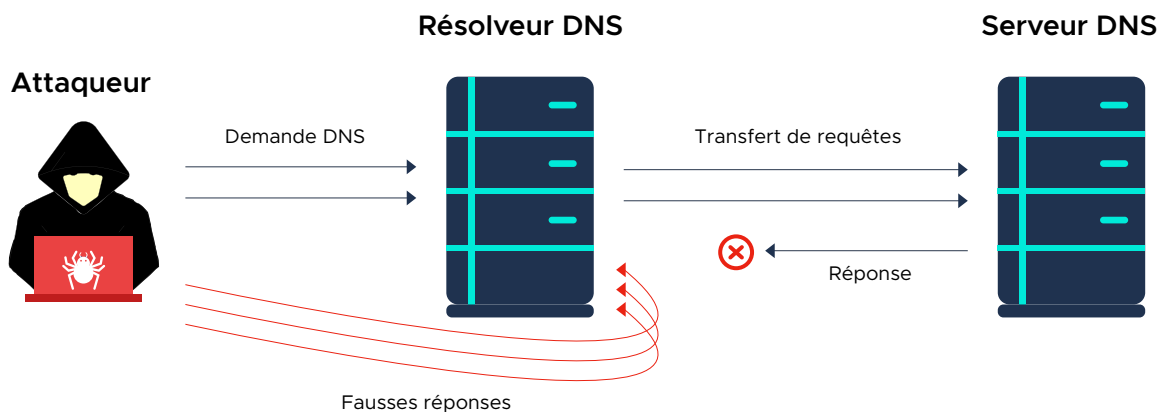
Dans la section 2.2, "Comment fonctionne le DNS ?", nous avons vu que le résolveur DNS vérifie d'abord son propre cache pour trouver l'adresse IP du domaine demandé par un client. Les attaquants peuvent manipuler les résolveurs DNS pour qu'ils mettent en cache de fausses informations. L'enregistrement de fausses informations dans un cache DNS est connu sous le nom de DNS cache poisoning ou DNS spoofing. Le résolveur renvoie alors des adresses IP incorrectes aux clients et les dirige vers des sites Web malveillants.

Voici les étapes de l'attaque par empoisonnement du cache DNS:

- ✔ Les attaquants envoient une requête DNS à un résolveur DNS, qui transmet la requête à un serveur racine, puis à des serveurs de noms TLD et faisant autorité.
- ✔ L'attaquant se fait passer pour le serveur de noms qui fait autorité et bombarde le résolveur de fausses réponses qui ne pointent pas vers le site Web d'origine. Comme le DNS utilise le protocole UDP (User Datagram Protocol), il n'existe aucun mécanisme permettant de vérifier l'identité de l'expéditeur. Le résolveur, ignorant la réponse empoisonnée, stocke la valeur dans son cache.

Définition: Le **protocole UDP (User Datagram Protocol)** est un protocole de communication qui est utilisé dans les connexions tolérant les pertes. Il a une faible latence et permet un transfert de données plus rapide en éliminant le processus d'établissement et de vérification des connexions entre l'émetteur et le récepteur.

- ✔ Désormais, lorsqu'un utilisateur légitime interroge ce résolveur DNS, une fausse réponse qui dirige l'utilisateur vers un site web malveillant est renvoyée du cache.
- ✔ Comme le résolveur DNS n'est généralement pas en mesure de vérifier l'authenticité des données contenues dans son cache, la valeur empoisonnée reste en place jusqu'à ce que le temps de vie (TTL) expire ou que l'entrée soit supprimée manuellement.



Note:

Pour que l'attaque par empoisonnement de cache DNS réussisse, l'attaquant doit connaître ou deviner plusieurs facteurs :

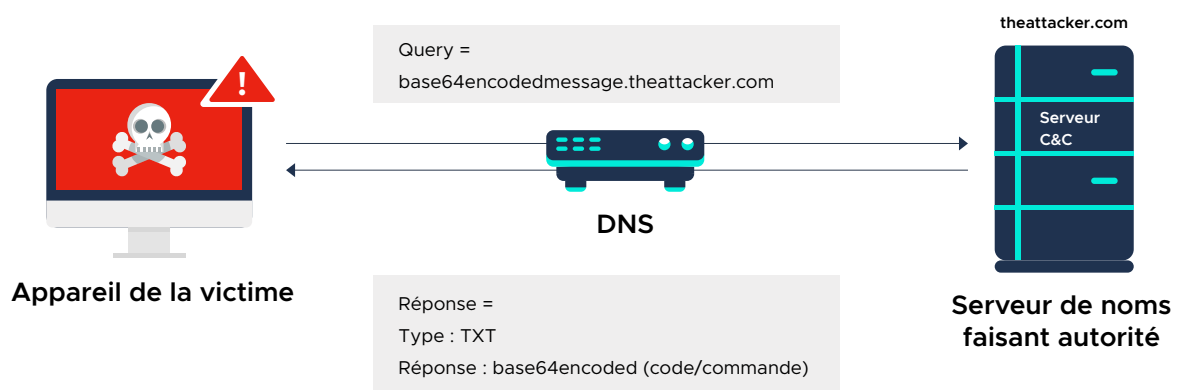
- Les requêtes DNS qui ne sont pas stockées dans le cache du résolveur, afin qu'elles soient transmises au serveur de noms faisant autorité.
- Le serveur de noms faisant autorité vers lequel la requête sera redirigée.
- Le numéro de port utilisé par le résolveur DNS et le numéro d'identification de la demande, afin que la fausse réponse puisse être envoyée au serveur DNS ciblé et son cache empoisonné.

2.3.3 Tunnelage DNS

Similaire au Empoisonnement du cache DNS, le tunnelage DNS abuse également du protocole DNS pour mener des activités malveillantes. Le tunnelage DNS est le processus qui consiste à cacher des données dans les requêtes et les réponses DNS. Le tunnelage DNS est utilisé par les attaquants pour établir une connexion de commande et de contrôle avec un dispositif déjà compromis dans un réseau afin d'exécuter des commandes ou d'exfiltrer des données.

Voici les étapes d'une attaque par tunnelage DNS:

- ✔ Les attaquants enregistrent un domaine (par exemple, theattacker.com) et mettent en place un serveur de commande et de contrôle (C&C) qui fait office de serveur de noms faisant autorité pour "theattacker.com".
- ✔ Le logiciel malveillant sur un appareil compromis envoie un message codé (base64encodedmessage.theattacker.com) sous la forme d'une requête DNS à "theattacker.com", qui est dirigée par le résolveur DNS vers le serveur C&C de "theattacker.com".
- ✔ Le serveur C&C renvoie un enregistrement TXT à l'appareil de la victime. L'enregistrement TXT peut contenir des commandes ou des codes à exécuter par la charge utile malveillante. Le tunnel DNS établi permet d'échanger des informations sans être détecté à travers le périmètre.



Chapitre 3

Protocole de configuration dynamique des hôtes – L'assignateur

Sujets abordés:

- 3.1 Qu'est-ce que le DHCP ?
- 3.2 Comment fonctionne le DHCP ?
- 3.3 Menaces pour le DHCP
 - 3.3.1 Privation de DHCP
 - 3.3.2 Falsification DHCP



3.1 Qu'est-ce que le DHCP?

Nous savons que pour qu'un ordinateur ou un périphérique soit identifié sur un réseau, il lui faut une adresse IP. Les adresses IP peuvent être attribuées aux périphériques de deux manières : statique et dynamique. Dans l'attribution statique d'une adresse IP, l'utilisateur doit saisir manuellement une adresse IP unique et d'autres propriétés du réseau pour chaque périphérique.

Toutefois, cela n'est pas pratique dans les réseaux qui contiennent de nombreux périphériques. C'est là que le protocole DHCP entre en jeu. Le DHCP est un protocole de gestion de réseau qui attribue automatiquement des adresses IP aux périphériques du réseau, ainsi qu'un masque de sous-réseau, une passerelle par défaut et un serveur DNS préféré.

Définition: Le **serveur DHCP** est un serveur réseau qui utilise le protocole DHCP pour automatiser l'attribution d'adresses IP et d'autres paramètres réseau aux clients DHCP.

Le **client DHCP** est tout dispositif connecté à un réseau qui utilise le protocole DHCP pour obtenir des paramètres de réseau à partir d'un serveur DHCP.

En bref, lorsqu'un périphérique est ajouté à un réseau, il envoie une demande d'adresse IP. Le serveur DHCP répond alors avec une adresse IP, et une fois que le nouveau périphérique accepte l'offre, le serveur DHCP la confirme et l'attribue au périphérique. Voyons maintenant en détail le fonctionnement du DHCP.

Remarque:

Il faut veiller à ce que chaque appareil du réseau se voie attribuer une adresse IP locale unique afin d'éviter les conflits d'adresses. Cela revient à dire que deux maisons ne devraient pas avoir la même adresse IP.

Remarque:

Pour l'attribution dynamique d'adresses IP, il y a deux conditions de base:

- Les appareils du réseau doivent exécuter un client DHCP.
- Au moins un serveur DHCP doit être présent sur le réseau. En général, les routeurs ont un serveur DHCP intégré.

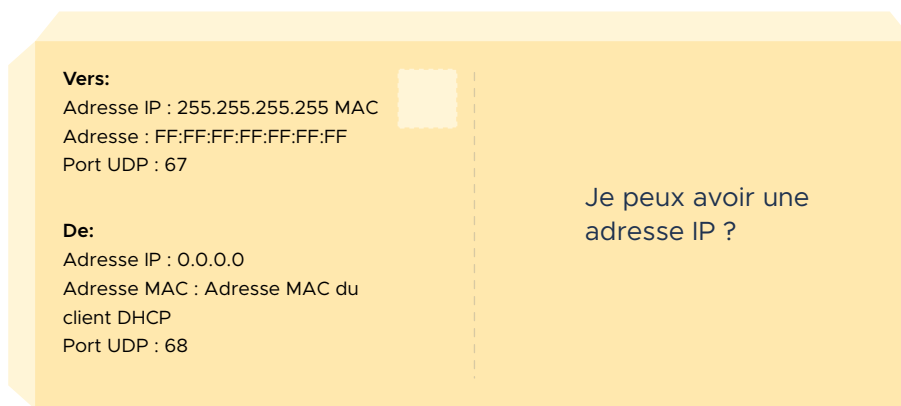
3.2 Comment fonctionne le DHCP?

DHCP suit un processus en quatre étapes appelé DORA (Discovery-Offer-Request-Acknowledgment).

ÉTAPE 1

Découverte DHCP

Le client DHCP diffuse un message de découverte DHCP à tous les périphériques du réseau, car il ne connaît pas l'emplacement du serveur DHCP.



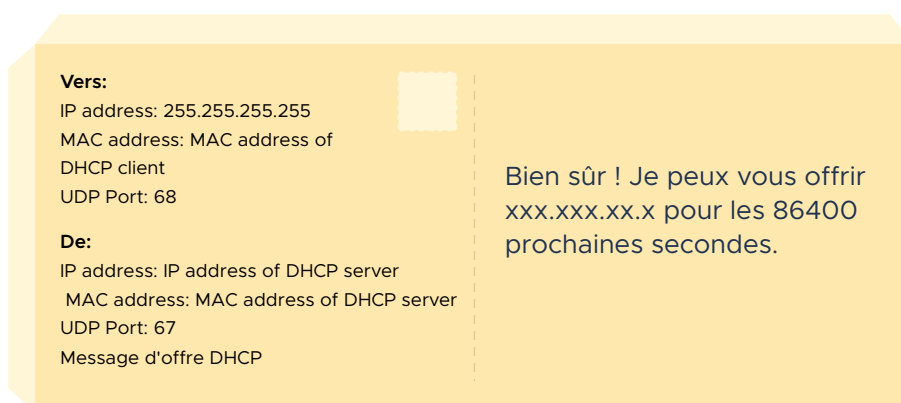
Message de découverte DHCP

- L'adresse IP du récepteur est 255.255.255.255 car il s'agit d'un message de diffusion.
- L'adresse MAC du récepteur est FF:FF:FF:FF:FF:FF puisque l'adresse MAC du serveur DHCP est encore inconnue.
- L'adresse IP de l'expéditeur est 0.0.0.0 car aucune adresse IP ne lui a encore été attribuée.
- Le port UDP 67 est réservé aux serveurs DHCP, et le port 68 est réservé aux clients DHCP.

ÉTAPE 2

Offre DHCP

Le serveur DHCP reçoit le message de découverte et répond par une offre.



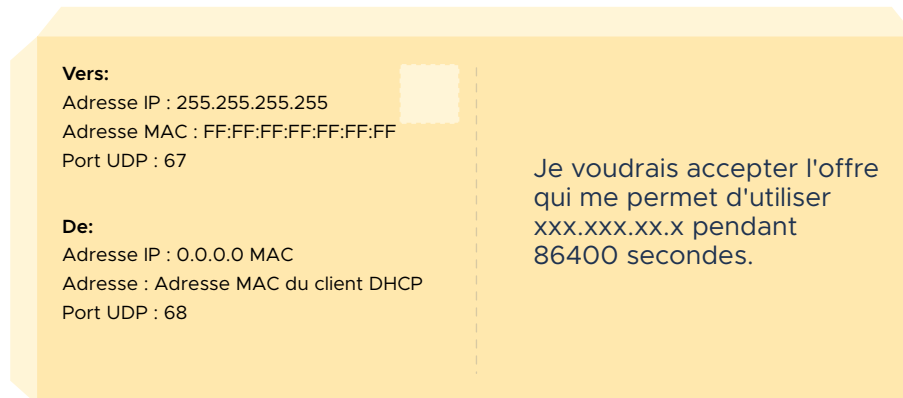
Message d'offre DHCP

- L'adresse IP du récepteur est 255.255.255.255 puisque le client n'a pas encore d'adresse IP.

ÉTAPE 3

Requête DHCP

Entre-temps, le client DHCP a dû recevoir des offres d'au moins un serveur DHCP. Le client envoie un message de demande DHCP dans lequel il spécifie l'adresse IP préférée.



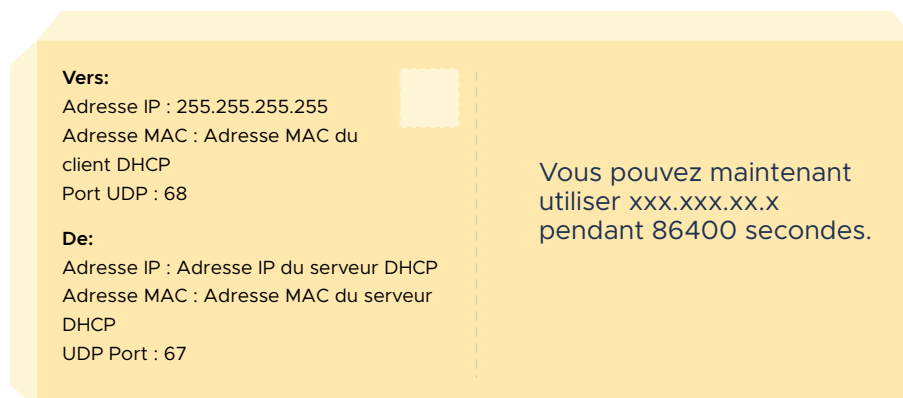
Message de requête DHCP

- L'adresse IP du récepteur est toujours 255.255.255.255 puisqu'il aurait reçu des offres de plus d'un serveur DHCP sur le réseau. Le message est diffusé pour informer les autres serveurs DHCP de libérer à nouveau l'adresse IP offerte dans leurs pools disponibles.

ÉTAPE 4

Accusé de réception DHCP

Par le biais du message d'accusé de réception DHCP, également appelé "ACK", le serveur DHCP confirme au client qu'il peut commencer à utiliser l'adresse IP pendant la période spécifiée et que l'adresse a été réservée.



Accusé de réception DHCP

Une fois ce processus en quatre étapes terminé, le client peut commencer à utiliser la nouvelle adresse IP.

3.3 Menaces pour le DHCP

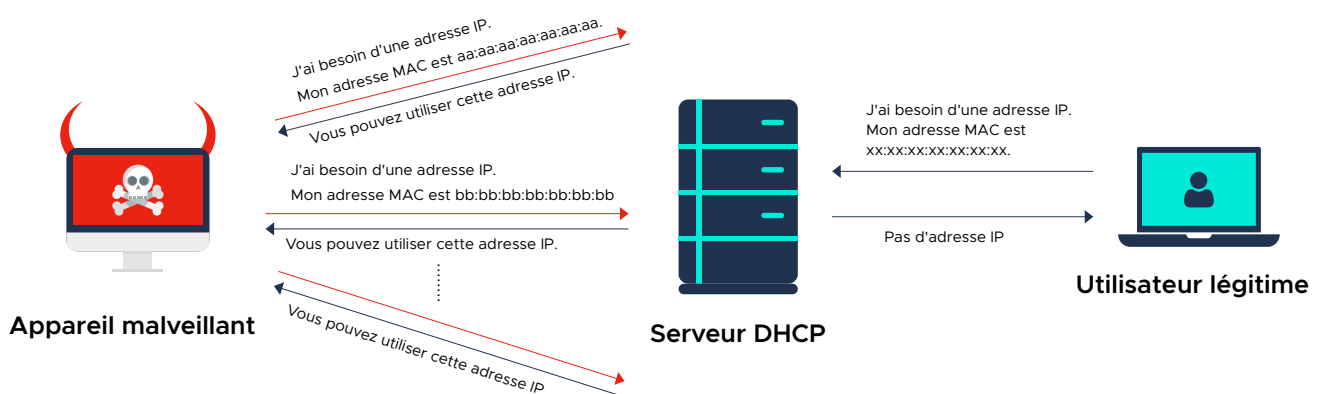
DHCP est l'un des protocoles les plus utilisés pour la configuration des hôtes. Un client DHCP est également connu sous le nom d'hôte. Tout comme le DNS, le protocole DHCP utilise également UDP comme protocole de transport. Le fait que le protocole DHCP n'utilise aucun mécanisme d'authentification pour vérifier l'intégrité des messages échangés entre les clients et les serveurs le rend plus facile à exploiter.

3.3.1 Privation de DHCP

Les serveurs DHCP disposent d'un groupe d'adresses IP qu'ils louent aux hôtes pour une période déterminée. Une attaque par privation de DHCP peut être considérée comme une attaque par déni de service (DoS) sur DHCP. Dans cette attaque, l'attaquant inonde le serveur DHCP d'un grand nombre de demandes. Comme le serveur ne dispose d'aucun mécanisme pour distinguer les demandes légitimes des demandes malveillantes, il peut distribuer des adresses IP à des hôtes malveillants, épuisant ainsi le groupe d'adresses IP et privant de service les utilisateurs légitimes du réseau.

Voici les étapes de l'attaque par privation de DHCP:

- ✔ Un client malveillant obtient un accès non autorisé à un réseau et envoie de nombreux messages DHCP discover en utilisant des adresses MAC falsifiées.
- ✔ Le serveur, à son tour, envoie des offres DHCP, auxquelles le client malveillant répond par des messages de requête DHCP.
- ✔ Le serveur confirme ensuite la requête et envoie un accusé de réception, réservant des adresses IP aux faux clients. Les adresses IP du groupe d'adresses du serveur sont rapidement épuisées et les clients légitimes du réseau ne peuvent pas accéder au serveur.

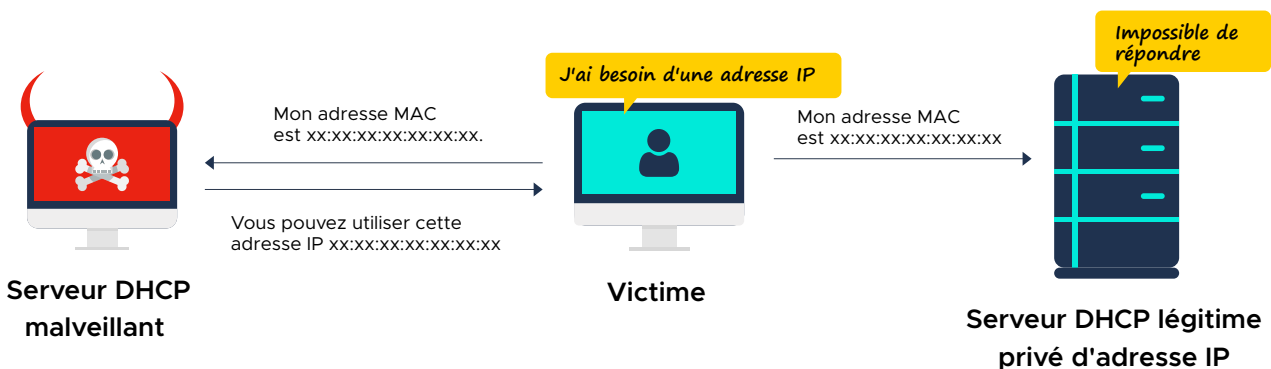


3.3.2 Usurpation d'identité DHCP

Une attaque par usurpation d'identité DHCP est un type d'attaque de type "man-in-the-middle". Une attaque par usurpation DHCP suit généralement une attaque par famine. Dans ce cas, l'attaquant se déguise en serveur DHCP et répond aux clients avec de fausses adresses IP et des configurations réseau erronées, comme le serveur DNS et la passerelle par défaut. L'attaquant peut alors manipuler les paquets de données et intercepter les informations des utilisateurs avant de les transmettre à la véritable passerelle, ou diriger les clients vers de faux serveurs DNS et lancer des attaques de hameçonnage.

Voici les étapes d'une attaque par usurpation d'identité DHCP:

- ✔ Un client diffuse un message DHCP de découverte.
- ✔ Le serveur DHCP est à court d'adresses IP en raison d'une attaque par privation de DNS et est incapable de traiter la demande du client.
- ✔ Un dispositif malveillant se faisant passer pour un serveur DHCP renvoie un message d'offre au client.
- ✔ Le client accepte l'offre, et une adresse IP ainsi que d'autres paramètres de configuration du réseau sont attribués par le faux serveur DHCP. Le client devient alors une victime car le serveur malveillant intercepte toutes les informations de la victime, y compris les mots de passe et autres données sensibles.



Chapitre 4

Gestion des adresses IP (IPAM) – L'administrateur

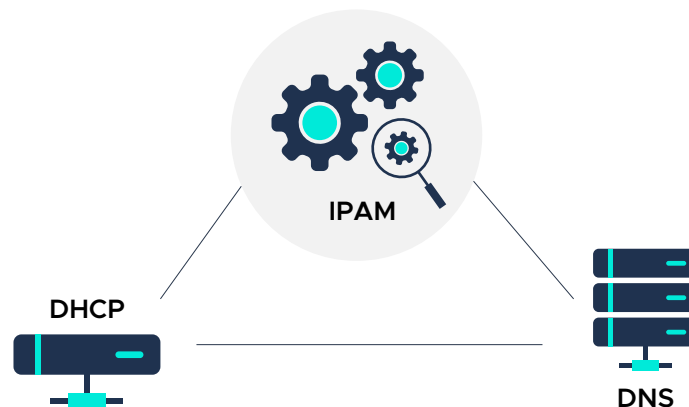
Sujets abordés:

- 4.1 Qu'est-ce que l'IPAM?
- 4.2 L'IPAM est-il indispensable?



4.1 Qu'est-ce que l'IPAM?

La gestion des adresses IP (IPAM) est une méthodologie de planification, de déploiement, de surveillance et de gestion des adresses IP du réseau. L'IPAM implique la gestion de services tels que DHCP et DNS, qui sont impliqués dans l'attribution et la résolution des adresses IP, afin de garantir que l'inventaire des adresses IP attribuables reste à jour et précis.



L'IPAM peut être considéré comme un référentiel de toutes les informations relatives aux adresses IP appartenant à un réseau, telles que :

- Adresses IP disponibles pour l'allocation.
- Statut de chaque adresse IP.
- Nom d'hôte associé à chaque adresse IP.
- Spécifications matérielles associées à chaque adresse IP.
- Détails concernant les sous-réseaux utilisés.

4.2 L'IPAM est-il indispensable?



Il existe un mythe populaire selon lequel, contrairement au DNS et au DHCP, qui sont des composants obligatoires pour que tout appareil connecté au réseau puisse communiquer, une solution IPAM n'est pas vraiment indispensable ; de bonnes vieilles feuilles de calcul peuvent faire l'affaire.

Utiliser des feuilles de calcul pour gérer les espaces d'adresses IP n'est qu'une solution de fortune et non une méthode efficace. Voyons pourquoi.

- ✔ **Explosion des appareils dotés d'une adresse IP** - Dans le monde d'aujourd'hui, les paysages réseau des organisations sont devenus plus complexes et dynamiques en raison de l'utilisation croissante des appareils de l'Internet des objets (IoT) et des politiques de "bring your own device" (BYOD). Le nombre d'appareils compatibles IP connectés à un réseau a augmenté de façon considérable. Dans un tel scénario, il est irréaliste d'utiliser des feuilles de calcul et des documents pour assurer le suivi des informations, telles que les adresses IP, les sous-réseaux, les réseaux locaux virtuels (VLAN) et les appareils connectés.
- ✔ **Conflits dans l'attribution des adresses IP** - La gestion manuelle des adresses IP oblige les administrateurs informatiques à mettre à jour la feuille de calcul chaque fois qu'une nouvelle adresse IP est attribuée, qu'un appareil est déprovisionné ou qu'un changement de statut de l'adresse IP est constaté. Dans les réseaux gérés par plusieurs administrateurs informatiques, des erreurs de synchronisation et des incohérences de données peuvent survenir. La même adresse IP peut être attribuée à différents appareils, créant ainsi une utilisation multiple de l'adresse. Cela rendra tous les appareils indisponibles.
- ✔ **Panne de réseau** - Lorsque les feuilles de calcul ne sont pas mises à jour correctement, le dépannage devient très compliqué, car il faut prendre en compte un certain nombre de facteurs tels que les conflits d'adresses IP, les failles de sécurité et les incompatibilités de ports. Ce processus peut prendre beaucoup de temps et entraîner des pannes de réseau temporaires.

Statistique: Selon une étude menée par l'Institut Ponemon en 2016, le coût moyen des temps d'arrêt du réseau est d'environ **9000 dollars** par minute.³

- ✔ **Point de vue de la conformité et de la sécurité** - Le stockage de toutes les informations dans une simple feuille de calcul est fastidieux, et les administrateurs informatiques constatent souvent qu'il ne fournit que peu, voire pas, d'informations exploitables. En outre, une feuille de calcul ne permet pas de se défendre contre une violation de la sécurité. Au contraire, elle est vulnérable à la manipulation et au sabotage. En outre, certaines réglementations de conformité exigent des journaux et des rapports détaillés sur l'attribution des adresses IP, ce qui devient fastidieux à traiter manuellement.

La formulation et le déploiement d'une stratégie IPAM appropriée n'est pas obligatoire, mais elle est essentielle pour améliorer l'efficacité, la sécurité et la visibilité de votre réseau.

Chapitre 5

Défendre les DDI

Sujets abordés:

- 5.1 Mesures pour protéger les infrastructures DNS, DHCP et IPAM d'une organisation
- 5.2 Comment Log360 peut vous aider ?



5.1 Mesures pour protéger les infrastructures DNS, DHCP et IPAM d'une organisation

Dans les chapitres précédents, nous avons exploré en détail ce qu'est la DDI, et pourquoi vous devriez vous en préoccuper. Il est maintenant temps d'aborder certaines des meilleures pratiques pour tenir les attaques DDI à distance et maintenir votre réseau opérationnel.

- ✔ Mettez périodiquement à jour les mots de passe des comptes DNS. Cela peut empêcher les utilisateurs non autorisés d'accéder aux comptes avec des mots de passe fictifs ou anciens qu'ils conservent encore.
- ✔ Activez l'authentification multifactorielle pour tous les comptes de registre et les comptes d'hébergement DNS.
- ✔ Assurez-vous que le mot de passe et le nom d'utilisateur des périphériques réseau, tels que les routeurs, sont modifiés par rapport aux paramètres d'usine.
- ✔ Les mots de passe ne doivent pas être partagés avec d'autres personnes, stockés ou transmis en texte clair, et réutilisés dans d'autres services.
- ✔ La randomisation est la clé pour éviter l'empoisonnement du cache. Utilisez un port source et un ID de requête aléatoires, ainsi que des lettres majuscules ou minuscules dans les noms de domaine..
- ✔ Assurez-vous que les enregistrements de zone DNS sont signés avec l'extension DNSSEC (Domain Name System Security Extension) et que vos résolveurs DNS effectuent la validation DNSSEC.
- ✔ Configurez les serveurs DNS pour qu'ils n'exécutent que les services nécessaires. Exécutez le résolveur et le serveur de noms faisant autorité sur des serveurs distincts, afin de limiter la taille du vecteur d'attaque.
- ✔ Implémentez le DHCP snooping pour prévenir les attaques par déni de service DHCP et les attaques par spoofing. DHCP snooping est une fonction de sécurité de niveau 2 qui permet aux commutateurs de rejeter le trafic DHCP non autorisé.
- ✔ Activez la journalisation chaque fois que possible afin que toute activité puisse être auditée.
- ✔ Auditez régulièrement les journaux collectés pour identifier les signes d'attaque et prendre des mesures correctives.
- ✔ Utilisez l'analyse en temps réel et la détection des menaces comportementales pour aider à prévenir les attaques à un stade précoce, avant que les dommages ne soient trop importants.

Si la lecture de cette liste non exhaustive des meilleures pratiques de DDI vous a épuisé, ne vous inquiétez pas ! Poursuivez votre lecture pour découvrir comment ManageEngine Log360 peut faire le gros du travail à votre place.

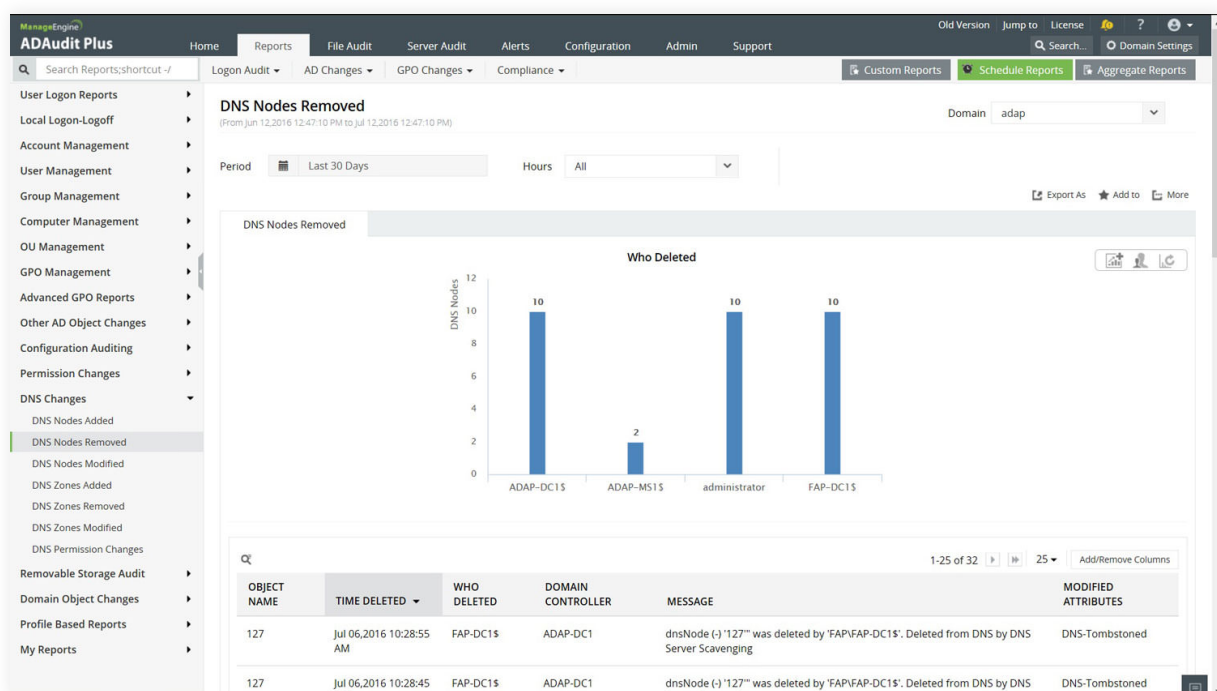
5.2 Comment Log360 peut-il vous aider?

Log360 est une solution complète de gestion des informations et des événements de sécurité (SIEM) qui vous aide à combattre les menaces et les attaques de sécurité, notamment celles décrites dans cet e-book. Grâce à ses fonctions d'analyse approfondie des journaux, d'audit d'Active Directory, d'analyse comportementale basée sur l'apprentissage automatique, corrélation en temps réel, analyse médico-légale et gestion des incidents, Log360 peut vous aider à détecter les attaques en temps réel, ainsi qu'à bloquer et à contenir les cyberattaques.

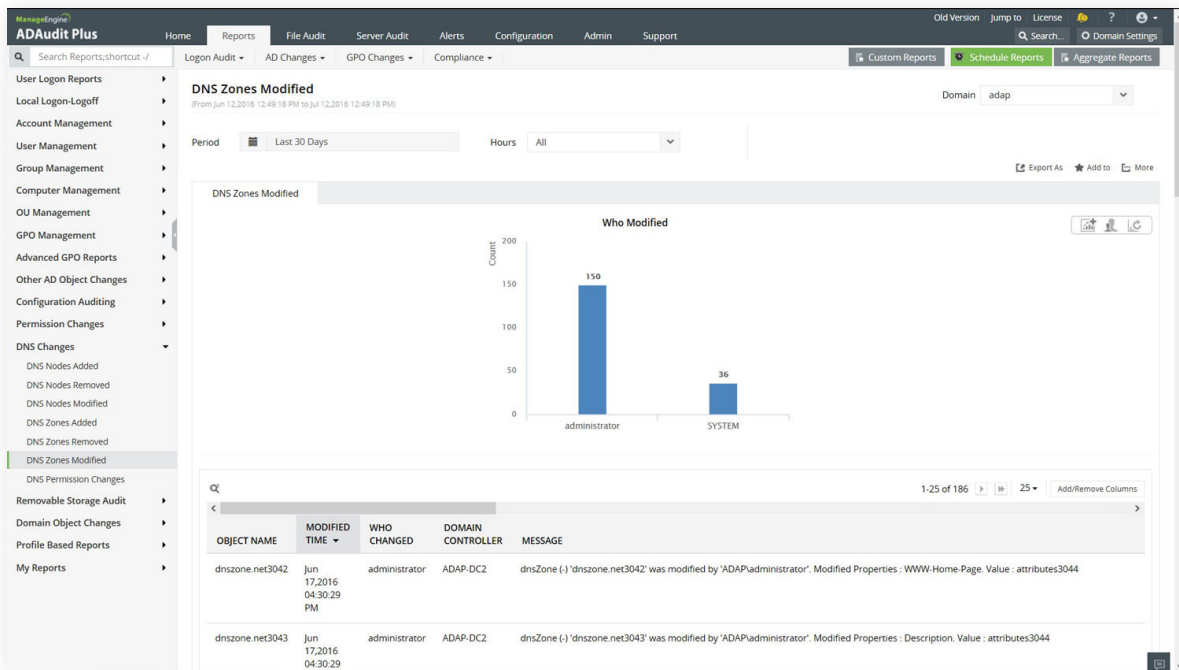
Examinons quelques-unes des fonctionnalités de Log360 qui peuvent vous aider à identifier et à déjouer les attaques DDI.

Audit des DNS

Log360 permet un audit DNS en temps réel et offre une vision claire des modifications apportées au DNS. Il génère également des rapports de sécurité détaillés sur les nœuds DNS et les zones DNS qui ont été modifiés ou supprimés, ainsi que sur les zones DNS ajoutées, avec les modifications cruciales des autorisations DNS.



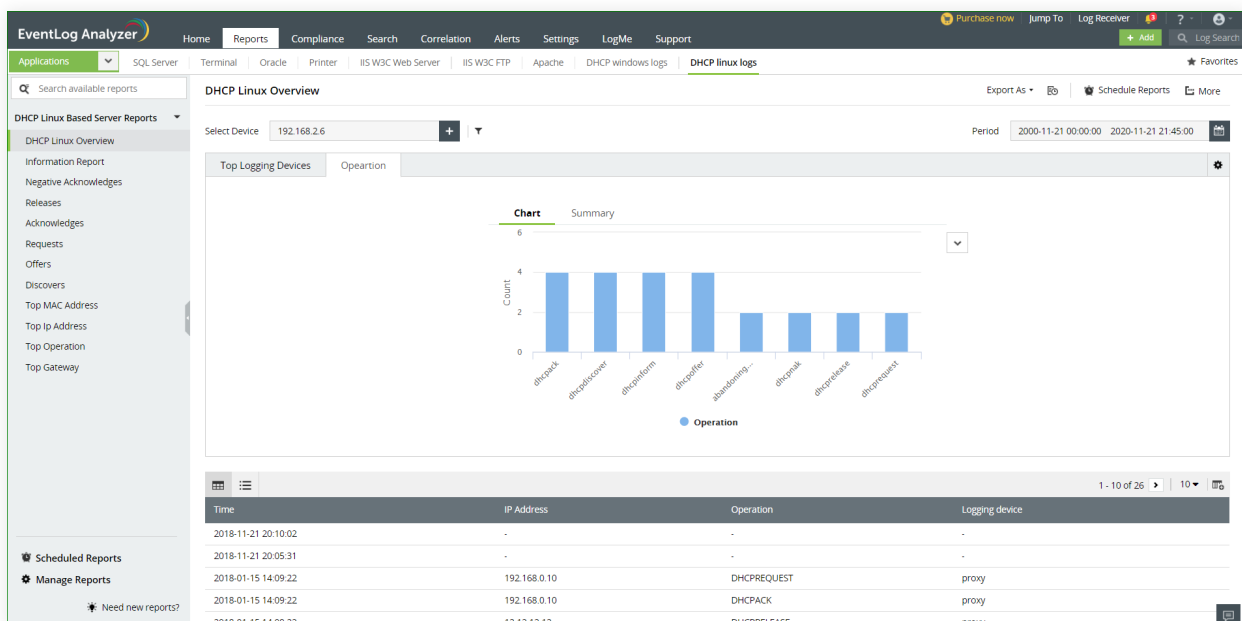
Rapport Log360 indiquant la suppression des codes DNS.



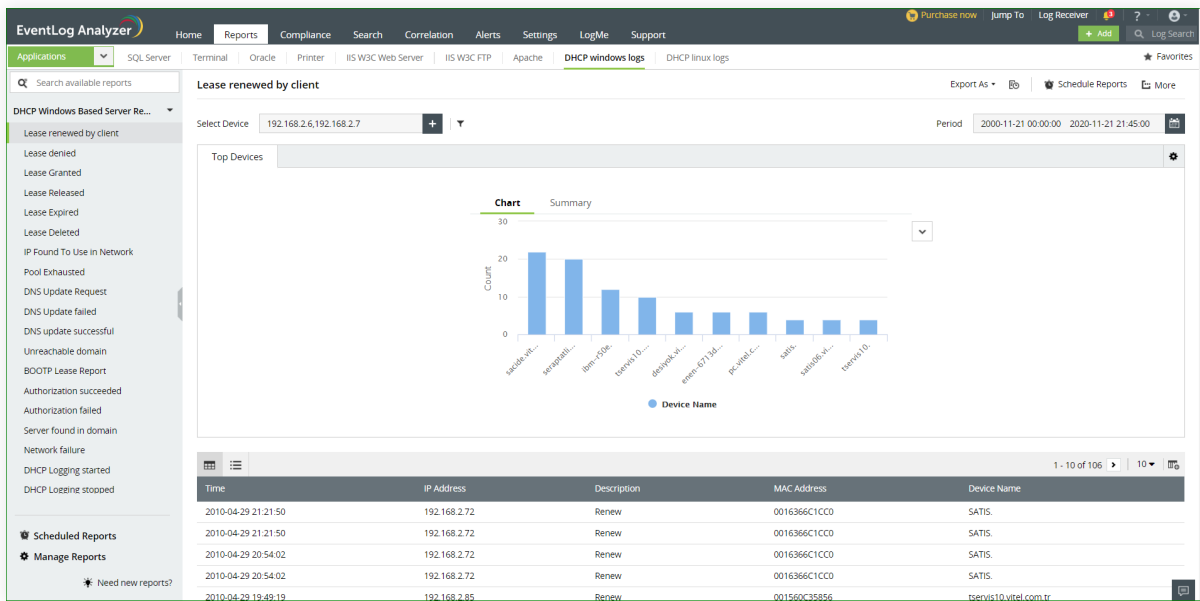
Rapport Log360 indiquant les modifications de la zone DNS ainsi que des informations sur l'auteur et la date de la modification.

L'audit DHCP

En analysant les journaux du serveur DHCP, Log360 est capable de fournir des informations sur les demandes d'adresses IP et les accusés de réception correspondants, les concessions de bail réussies et échouées, et l'épuisement du groupe d'adresses IP du serveur DHCP.



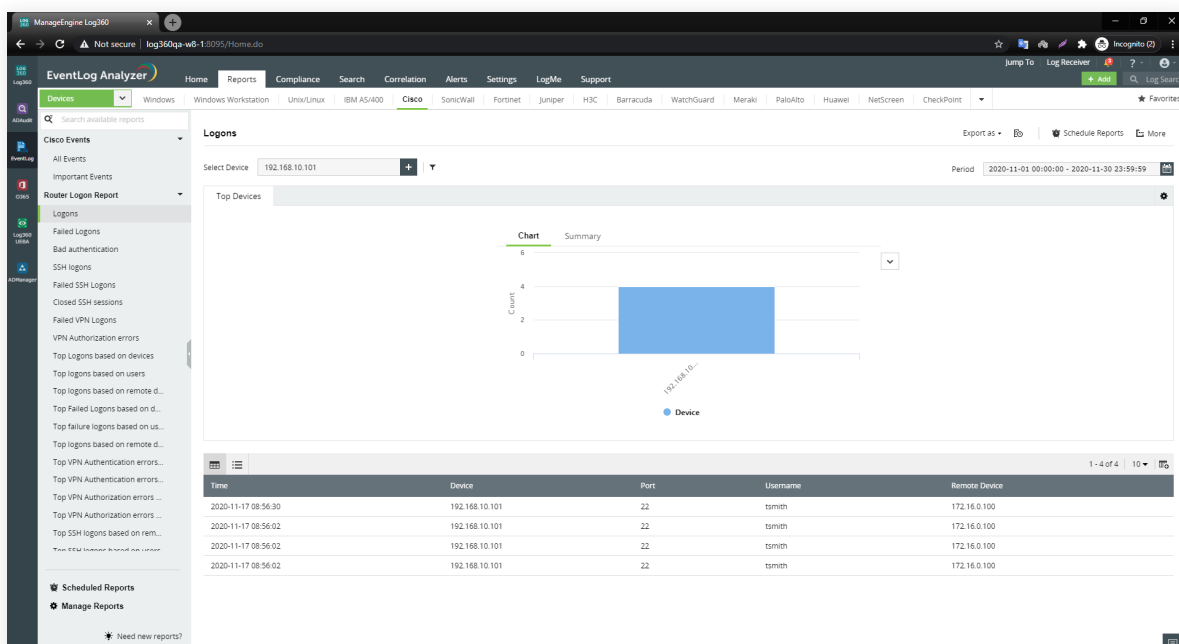
Rapport DHCP Linux Overview résumant tous les événements du journal DHCP.



Rapport listant tous les renouvellements d'adresses IP par les clients.

Audit du routeur

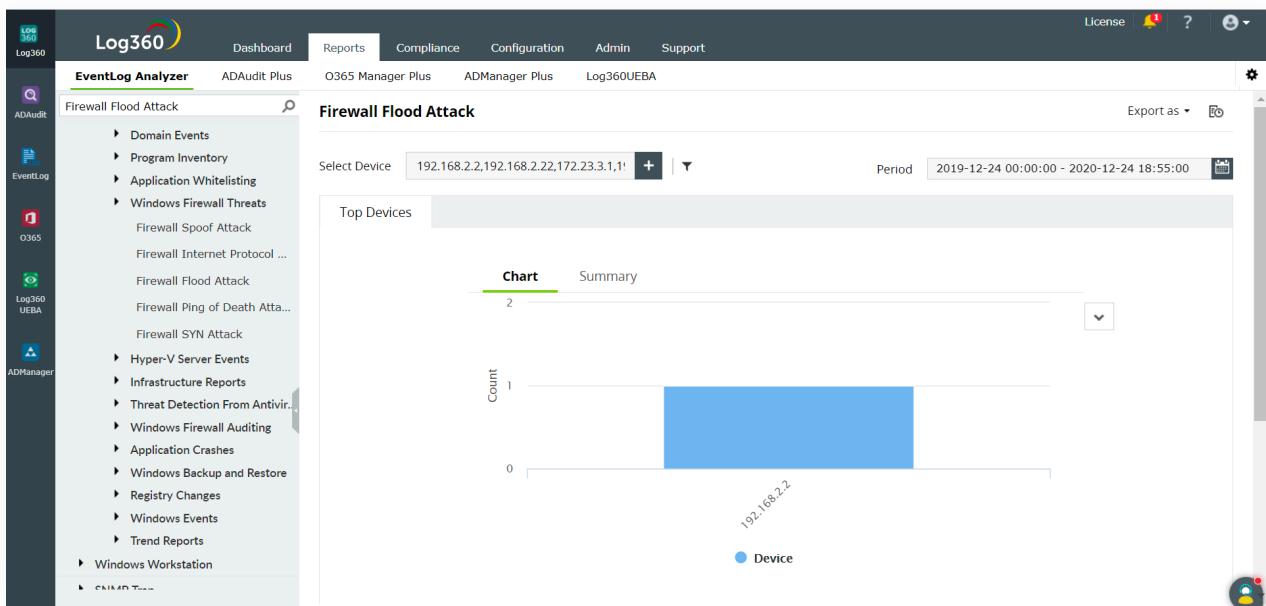
Avec les quantités massives de trafic qui passent régulièrement par les routeurs, la surveillance de l'activité des routeurs peut être un défi. Mais l'audit des routeurs et autres périphériques réseau est un simple exercice avec Log360. Il analyse votre réseau et découvre les routeurs et autres dispositifs syslog qui peuvent être ajoutés pour la surveillance. Grâce aux alertes en temps réel de Log360, vous pouvez détecter instantanément toute activité suspecte, et les rapports prédéfinis sur les journaux des routeurs vous donnent un aperçu de l'activité du réseau.



Rapport décrivant les logins du routeur.

Contrôle du pare-feu

Les pare-feu agissent comme un régulateur du trafic de votre réseau, garantissant que seules les parties de confiance accèdent aux ressources et protégeant vos hôtes des attaques du réseau. En gardant une trace des modifications apportées aux règles, aux configurations et aux paramètres du pare-feu, vous pouvez vous assurer qu'il est correctement configuré pour lutter contre les attaques par inondation, les attaques SYN, les attaques par usurpation, les attaques par demi-scan et les attaques Ping of Death.

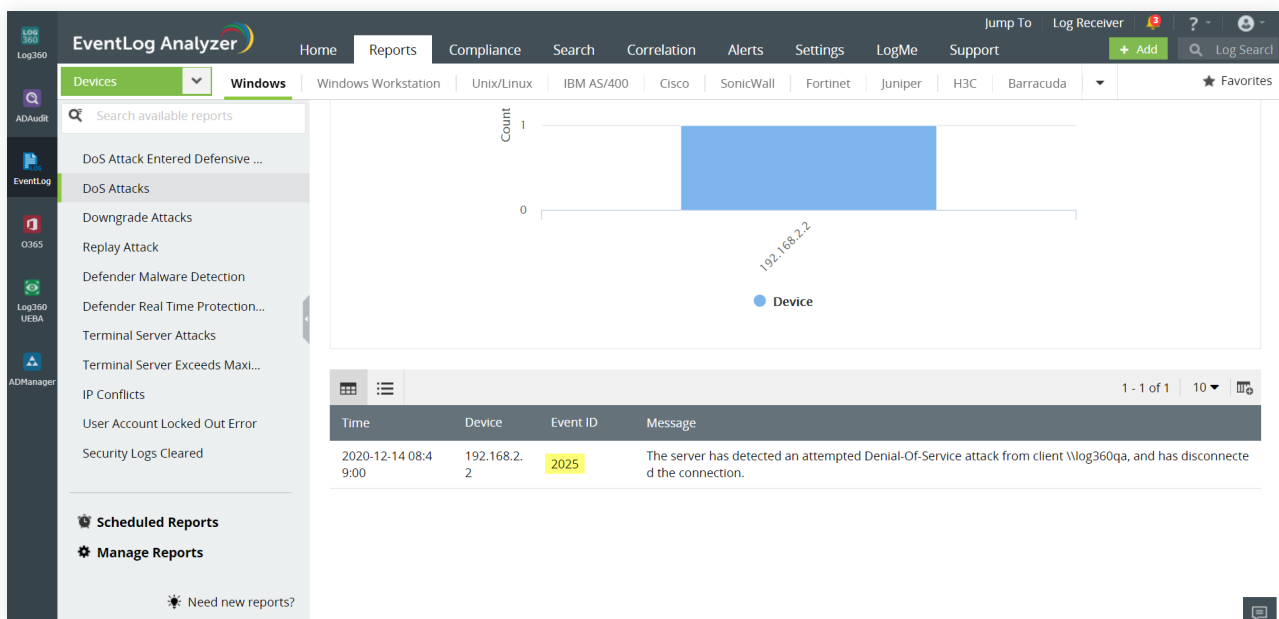


Time	Device	Event ID	Message
2020-12-14 08:50:00	192.168.2.2	15113	SA Server disconnected the following client: 192.168.5.25 because its connection limit was exceeded

Rapport indiquant une attaque par inondation sur un pare-feu

Détection des attaques DoS

Log360 audite les données des journaux de vos dispositifs de sécurité réseau, tels que les pare-feu, les systèmes de détection des intrusions (IDS) et les systèmes de prévention des intrusions (IPS). La solution détecte instantanément les attaques DoS et vous alerte en temps réel. Log360 vous aide également à suivre l'activité des serveurs Web afin de détecter lorsqu'une IP spécifique envoie des demandes de connexion répétées, signe révélateur d'une attaque DoS.

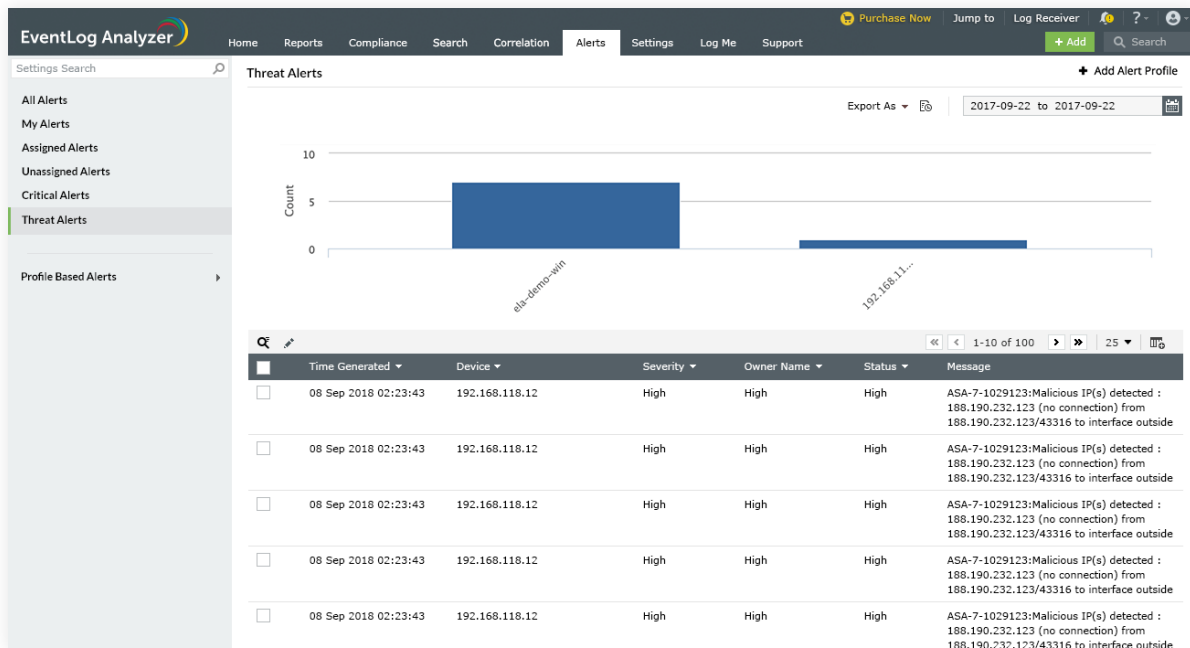


Log360 détecte une tentative de DoS et empêche le déclenchement d'une attaque.

Analyse avancée des menaces

Le module de renseignement sur les menaces de Log360 permet de détecter toute communication avec diverses sources externes malveillantes connues. Il est fourni avec la base de données mondiale de renseignements sur les menaces qui contient plus de 600 millions d'adresses IP malveillantes. Cette base de données est régulièrement mise à jour de manière dynamique et Log360 corrèle instantanément ces données avec les détails du trafic entrant et sortant pour repérer en temps réel le trafic malveillant sur votre réseau. La solution prend également en charge les flux de menaces aux formats STIX, TAXII et OTX.

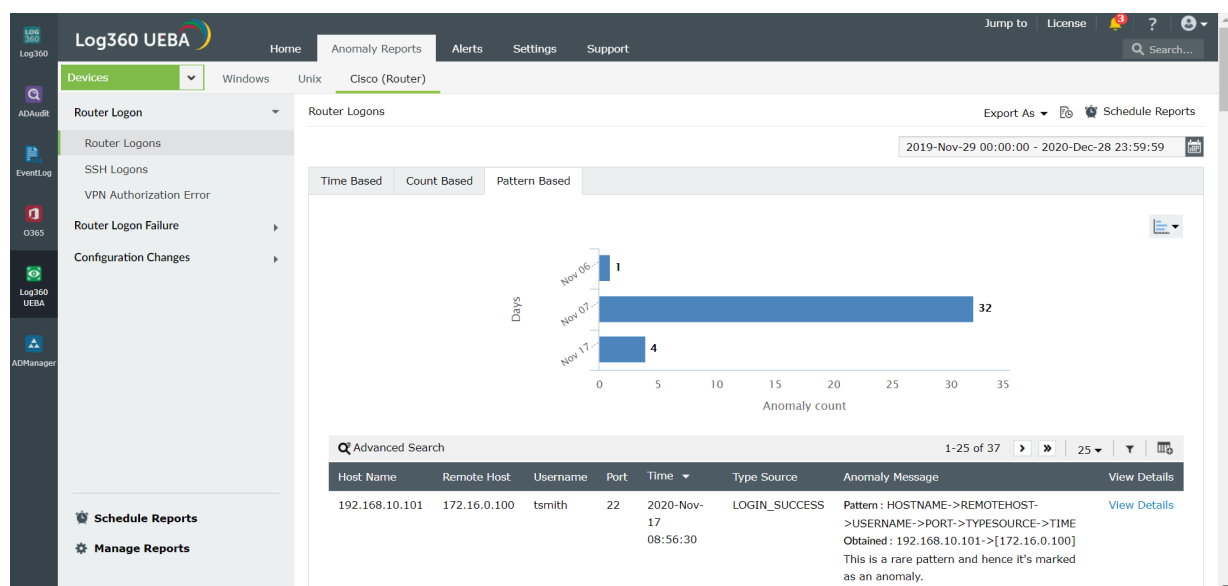
Log360 peut facilement être équipé du module complémentaire Advanced Threat Analytics qui fournit des informations plus approfondies sur les acteurs de la menace, telles que la géolocalisation de l'acteur malveillant, la catégorie de menace, le score de réputation de la source malveillante, etc.



Log360 affichant le trafic provenant d'adresses IP malveillantes.

Analyse du comportement des utilisateurs et des entités (UEBA)

Log360 utilise l'apprentissage automatique pour identifier les modèles de comportement des utilisateurs et des entités dans un réseau, ce qui lui permet de créer un comportement de base. Chaque activité effectuée par les utilisateurs et les entités est ensuite comparée à la ligne de base pour repérer les anomalies qui pourraient indiquer un problème potentiel.



Rapport affichant les connexions suspectes du routeur.

Outre les nombreux rapports évoqués ci-dessus, Log360 propose plus de 400 rapports prêts à l'emploi qui vous aident à suivre toutes les activités des utilisateurs et des entités de votre organisation, et à effectuer des analyses médico-légales en un clin d'œil lorsque le besoin s'en fait sentir. Qu'il s'agisse de vous aider à respecter les règles strictes des mandats de conformité, comme HIPAA, GDPR, etc., ou de vous permettre de créer des alertes personnalisées en fonction des besoins, Log360 est votre solution unique.

Références:

- 1 Rick Rumbarger. "Network complexity: Three trends that are contributing to a 'perfect storm' ". https://www.circleid.com/posts/20100923_network_complexity_three_trends_contributing_to_a_perfect_storm/
- 2 Virendra Soni. "Average cost per DNS attack is now whopping \$1.07 million: Report". <https://www.dailyhostnews.com/average-cost-per-dns-attack-is-1-07-million>
- 3 Ponemon Institute LLC. "Cost of Data Centre Outages". <http://files.server-rack-online.com/2016-Cost-of-Data-Center-Outages.pdf>

ManageEngine Log360

ManageEngine Log360, une solution SIEM complète, aide les entreprises à déjouer les attaques, à surveiller les événements de sécurité et à se conformer aux obligations réglementaires.

La solution comprend un composant de gestion des journaux pour une meilleure visibilité de l'activité du réseau, ainsi qu'un module de gestion des incidents qui permet de détecter, d'analyser, de hiérarchiser et de résoudre rapidement les incidents de sécurité. Log360 est doté d'un module complémentaire innovant d'analyse du comportement des utilisateurs et des entités, basé sur le modèle ML, qui permet d'établir une base de référence pour les comportements normaux des utilisateurs et de détecter les activités anormales des utilisateurs, ainsi que d'une plateforme de renseignement sur les menaces qui apporte des flux de menaces dynamiques pour la surveillance de la sécurité.

Log360 aide les organisations à combattre et à atténuer de manière proactive les attaques de sécurité internes et externes grâce à une gestion efficace des journaux et à un audit AD approfondi.

Pour plus d'informations sur Log360, visitez <https://www.pgsoftware.fr/siem/log360>.

🇺🇸 Obtenez un devis

📄 Télécharger