

Capacités d'analyse forensique de Cisco

Cet ouvrage présente les **capacités d'analyse forensique** des solutions de sécurité **Cisco**, en mettant l'accent sur la stratégie « Avant, Pendant et Après » l'attaque. L'auteur explore des outils **open source** comme Snort et ClamAV, tout en soulignant la supériorité des solutions d'entreprise telles que **Firepower**. Le texte détaille l'utilisation de **Cisco AMP** pour traquer la propagation des fichiers malveillants et identifier le « patient zéro » au sein d'un réseau. Enfin, il explique comment **Cisco Threat Grid** utilise le bac à sable et l'analyse comportementale pour neutraliser les menaces sophistiquées. Cette vue d'ensemble démontre comment ces technologies facilitent le travail des **ingénieurs réseau** lors de la réponse aux incidents.

Explique-moi la stratégie Avant, Pendant et Après de Cisco.

La stratégie **Avant, Pendant et Après (BDA - Before, During, After)** de Cisco est une approche de sécurité axée sur les menaces, inspirée du modèle de la chaîne d'attaque cybernétique (*Cyber Kill Chain*) initialement développé par Lockheed Martin. Cisco a hérité de cette stratégie à la suite de l'acquisition de Sourcefire. Elle structure la défense en trois phases distinctes correspondant au cycle de vie d'une attaque :

1. Avant l'attaque (Before)

L'objectif principal à ce stade est de **prévenir la menace et de réduire la surface d'attaque** afin de bloquer les intrusions avant qu'elles ne se produisent.

- **Principe** : Limiter la communication aux seules entités de confiance et empêcher les systèmes non autorisés d'accéder au réseau.
- **Concepts clés** :

- **Sécurité de la réputation** : Attribuer un score de confiance à un site ou à une source de trafic pour bloquer automatiquement l'accès s'il est jugé malveillant.
- **Contrôle d'accès au réseau (NAC)** : Empêcher tout système inconnu ou non autorisé d'obtenir un accès réseau complet dès sa connexion.
- **Technologies types** : Pare-feu, VPN, contrôles d'accès et filtres de contenu.

2. Pendant l'attaque (During)

Si une menace parvient à franchir le périmètre de sécurité, l'objectif se déplace vers la **détection et la prévention des comportements malveillants en temps réel**.

- **Principe** : Identifier activement l'exploitation d'une faille à l'aide de signatures d'attaque, de profils de comportement ou de la recherche de menaces connues.
- **Concepts clés** :
 - **Optimisation continue** : Les défenses doivent être constamment adaptées pour couvrir les vulnérabilités locales. Cisco intègre par exemple des analyses automatisées des vulnérabilités pour ajuster dynamiquement les capacités de détection des équipements.
- **Technologies types** : Antivirus, antimalwares, systèmes de détection et de prévention d'intrusion (IDS/IPS), ainsi que des solutions de sécurité web et de messagerie.

3. Après l'attaque (After)

Cette phase concerne la **gestion de la sécurité post-compromission** et prend en charge tout ce qui a réussi à contourner les phases précédentes. Elle est indispensable pour valider le bon fonctionnement global de la sécurité.

- **Principe** : Détecter rapidement la compromission, isoler la menace et analyser l'incident pour améliorer les défenses futures.
- **Concepts clés** :
 - **Analyse forensique** : Indispensable pour déterminer l'origine de l'intrusion, identifier le premier système infecté (« patient zéro ») et suivre la propagation des fichiers malveillants sur le réseau.

- **Analyse comportementale rétrospective** : Suivre en continu le comportement des fichiers sur le réseau afin de repérer une activité suspecte (comme un document qui tente de chiffrer le disque dur), même en l'absence de signature connue.
- **Technologies types** : NetFlow (pour l'enregistrement du trafic réseau), pots de miel (*honeypots*), analyse de référence/comportementale et analyse de fichiers.

Exemple concret d'application : L'attaque par rançongiciel (Ransomware)

Pour bien comprendre la synergie entre ces phases, le document détaille comment l'architecture BDA bloque un rançongiciel diffusé via un kit d'exploitation :

1. **Avant** : La solution bloque l'e-mail d'hameçonnage ou empêche la redirection vers le site web malveillant lorsque l'utilisateur clique sur le lien.
2. **Pendant** : Si l'utilisateur accède tout de même au site, le système identifie la tentative d'exploitation d'une vulnérabilité, bloque l'attaque et empêche le téléchargement du ransomware.
3. **Après** : Si la charge utile s'installe malgré tout sur l'hôte, la sécurité détecte que le logiciel tente de chiffrer le disque dur et interrompt immédiatement son exécution.

L'objectif ultime est d'**arrêter l'attaque le plus tôt possible**. Lorsqu'une menace est détectée en phase « Après », le système utilise ces informations (comme les signatures comportementales ou les adresses IP associées) pour mettre automatiquement à jour les règles des phases « Pendant » (mise à jour de l'IPS) et « Avant » (mise sur liste noire des domaines), empêchant ainsi toute infection future.

Comment Cisco AMP identifie le Patient Zéro ?

Cisco AMP (Advanced Malware Protection) identifie le **patient zéro** — c'est-à-dire la première personne ou machine à avoir introduit le fichier malveillant sur le réseau — grâce à une combinaison de technologies d'analyse continue, de traçabilité et de renseignement :

- **La surveillance continue et l'analyse rétrospective :**
Contrairement aux solutions traditionnelles qui se limitent à l'instant de la détection, Cisco AMP surveille et enregistre en permanence l'activité de tous les fichiers circulant sur le réseau. Si un fichier n'est reconnu comme malveillant que tardivement (par exemple, à la suite d'un changement de comportement ou d'une nouvelle analyse), AMP est capable de remonter le temps pour retracer l'intégralité de son parcours historique sur le réseau.
- **L'identification par valeur de hachage unique :** Chaque fichier possède une signature ou empreinte numérique unique (valeur de hachage). Grâce au **marquage rétrospectif**, AMP utilise ce hachage précis pour localiser toutes les instances et versions du fichier sur le réseau, même si l'attaquant ou l'utilisateur a tenté de renommer le fichier.
- **La cartographie de la trajectoire réseau (Network File Trajectory) :** AMP génère une chronologie visuelle de l'apparition de la menace et de sa propagation latérale entre les différents systèmes. En analysant le premier événement de cette trajectoire, l'administrateur accède à une fiche détaillée sur le cas initial. Ce rapport révèle des informations clés, telles que l'identité de l'utilisateur, son adresse IP d'origine, l'heure exacte de l'événement, le protocole applicatif utilisé (comme HTTP) et le navigateur web employé pour télécharger le fichier.

Cette visibilité granulaire permet aux équipes de sécurité de comprendre précisément comment l'infection a débuté, ce qui est indispensable pour corriger la vulnérabilité d'origine et bloquer définitivement le vecteur d'un tel incident.

Quelle est la différence entre AMP for Network et for Endpoint ?

La différence fondamentale entre **AMP for Network** et **AMP for Endpoint** réside dans l'endroit où ils s'exécutent, leur niveau de visibilité et leurs capacités de remédiation :

AMP for Network :

- **Emplacement et visibilité :** Il s'exécute sur une plateforme réseau (telle que Cisco Firepower). Son rôle est d'analyser et de

surveiller les fichiers en transit au moment exact où ils circulent sur le réseau.

- **Limitations de protection** : Puisqu'il fonctionne uniquement au niveau du trafic réseau, il n'a pas d'accès direct aux hôtes (les ordinateurs ou serveurs) qui utilisent et stockent ces fichiers. Par conséquent, si un appareil quitte le réseau de l'entreprise, il n'est plus protégé par cette solution.
- **Limites de remédiation** : Ses actions sont restreintes à ce qu'il peut intercepter en ligne. Il peut bloquer la circulation d'un fichier sur le réseau, mais il ne peut pas supprimer un fichier déjà installé sur un terminal infecté, ni surveiller l'activité interne de l'appareil située au-delà de son pare-feu local.

AMP for Endpoint :

- **Emplacement et visibilité** : Il s'appuie sur un **agent léger** installé directement sur le terminal (l'hôte). Cet agent analyse en continu les fichiers présents sur la machine et offre aux administrateurs de sécurité une visibilité approfondie sur l'ensemble des systèmes, quel que soit leur emplacement géographique dans le monde.
- **Remédiation directe** : Contrairement à la version réseau, si AMP for Endpoint identifie un fichier comme étant malveillant, il a le pouvoir de **le supprimer** physiquement de l'appareil.
- **Collaboration avec le réseau** : Il détecte également les vulnérabilités applicatives présentes sur l'hôte (comme une version obsolète de Java ou d'un autre logiciel) et transmet ces informations à Cisco Firepower. Le pare-feu réseau Firepower peut alors **adapter automatiquement ses capacités de détection IPS** (système de prévention des intrusions) pour bloquer l'exploitation de ces vulnérabilités spécifiques.

En résumé, AMP for Network surveille et bloque les menaces lors de leur transport sur le réseau, tandis qu'AMP for Endpoint protège l'appareil de l'intérieur (qu'il soit connecté au réseau d'entreprise ou non) et collabore avec la sécurité réseau pour boucher les failles de sécurité détectées sur les postes de travail.

Comment Glovebox permet-il d'analyser un fichier ?

La fonctionnalité **Glovebox**, intégrée à la solution de sandbox **Cisco Threat Grid**, permet d'analyser un fichier suspect grâce à une approche interactive et sécurisée :

- **Exécution et interaction en direct** : Glovebox permet aux administrateurs d'**exécuter le fichier douteux et d'interagir directement avec lui** au sein d'un environnement hautement contrôlé et isolé (sandbox). Cela élimine tout risque de contamination du réseau de production tout en permettant d'observer le comportement du fichier en temps réel.
- **Compréhension accélérée de la menace** : Cette méthode interactive aide les analystes à cerner beaucoup plus rapidement la véritable nature d'un fichier (par exemple, pour voir concrètement s'il se comporte comme un rançongiciel) afin de réagir avec une grande précision aux menaces potentielles.
- **Enregistrement et analyse automatisés des données forensiques** : Pendant que l'utilisateur interagit avec le fichier dans la sandbox, le système enregistre automatiquement l'intégralité de son activité. Cela permet de générer un rapport forensique détaillé qui met en lumière :
 - Les **adresses URL** spécifiques auxquelles le fichier malveillant tente d'accéder.
 - La façon dont il **modifie les fichiers système** au cours de son fonctionnement (analyse de son polymorphisme).
 - Les **failles de sécurité** spécifiques qu'il tente d'exploiter pour se propager à d'autres ordinateurs.
 - Des données techniques approfondies sur les **processus créés**, les **modifications de la base de registre**, ainsi que les flux de trafic TCP/IP et DNS générés.

Cette combinaison d'analyse interactive humaine et d'enregistrement automatisé fournit aux enquêteurs forensiques des détails cruciaux pour étayer des allégations de menace, offrant généralement des résultats bien plus rapides et précis qu'une analyse purement manuelle.

Comment Cisco Umbrella bloque-t-il les menaces ?

Cisco Umbrella agit comme une **première ligne de défense** en intervenant directement au niveau des requêtes DNS (Domain Name System). Lorsqu'un utilisateur tente d'accéder à un site, Umbrella intercepte cette recherche d'annuaire avant même que la connexion IP ne soit établie, ce qui permet de bloquer la menace avant qu'elle ne puisse atteindre le système.

Voici concrètement comment la solution bloque les menaces :

1. Le filtrage double (Contenu et Sécurité)

- **Filtrage de contenu** : Permet de définir des politiques d'accès pour bloquer des catégories de sites qui ne sont pas nécessairement dangereuses pour la sécurité, mais jugées inappropriées pour l'organisation (comme les sites de jeux d'argent ou pour adultes).
- **Filtrage de sécurité** : Cible spécifiquement les menaces en analysant les serveurs DNS et leurs associations. Umbrella examine l'entité responsable de l'enregistrement d'un site, les pages web qui génèrent du trafic vers ce site et les destinations des utilisateurs après leur visite. Cela permet de détecter des attaques coordonnées, comme l'utilisation de sites intermédiaires servant de pages de redirection ou d'atterrissage vers du contenu malveillant.

2. L'analyse de réputation basée sur le Big Data

Cisco traite plus de **80 milliards de requêtes DNS par jour**, ce qui lui fournit un volume de données massif.

- **Comparaison globale du trafic** : Umbrella compare l'activité d'un site spécifique avec les tendances mondiales. Par exemple, si une prétendue banque reçoit 95 % de son trafic d'une seule et unique entreprise au lieu d'utilisateurs du monde entier, Umbrella repère l'anomalie.
- **Scores de confiance et listes noires** : Tout comportement suspect fait baisser le niveau de confiance d'un domaine. Une fois qu'un seuil critique est dépassé, le site est automatiquement inscrit sur liste noire et bloqué.
- **Blocage par association** : Si un site malveillant est identifié, Umbrella identifie tous les autres domaines enregistrés par le même acteur ou partageant des liaisons techniques, et les bloque.

de manière proactive avant même qu'ils ne soient utilisés pour lancer une attaque.

3. Une protection omniprésente via API

- **Intégration d'API** : Umbrella peut s'intégrer à d'autres équipements ou logiciels de sécurité (comme un SIEM). Si un autre outil détecte une attaque locale, il peut envoyer l'information à Umbrella pour bloquer instantanément le domaine malveillant au niveau de la passerelle cloud.
- **Couverture hors réseau** : Comme la sécurité est gérée dans le cloud au niveau du DNS, le blocage reste actif pour tous les équipements protégés, y compris les succursales, les ordinateurs portables des collaborateurs en déplacement ou les téléphones mobiles.

Comment Cisco Stealthwatch utilise NetFlow ?

Cisco Stealthwatch utilise le protocole **NetFlow** (qui enregistre le trafic réseau) pour transformer l'ensemble de votre infrastructure en une vaste grille de détection. Cette approche, souvent résumée par l'expression « le réseau comme capteur », permet d'obtenir une visibilité complète sur le trafic physique, virtuel et cloud.

Voici concrètement comment Stealthwatch collecte, analyse et enrichit ces données pour sécuriser votre réseau :

1. La collecte et la centralisation des flux NetFlow

- **Les sources de flux** : Les routeurs, commutateurs, pare-feux et points d'accès sans fil physiques du réseau sont configurés pour générer et envoyer des enregistrements NetFlow vers la solution.
- **Le Collecteur Stealthwatch** : Il s'agit du point d'ancrage centralisé où tous les périphériques réseau envoient leurs flux NetFlow pour traitement.
- **L'UDP Director** : Pour simplifier l'administration dans les grands réseaux, cet outil sert de point de configuration unique. Tous les équipements pointent vers lui, et il se charge de distribuer les flux NetFlow vers les collecteurs appropriés.
- **La conversion du trafic brut** : Dans les zones du réseau où NetFlow n'est pas pris en charge (comme certains réseaux virtuels

est-ouest ou certains environnements cloud), Stealthwatch déploie des **capteurs** ou des agents légers pour capturer le trafic brut et le convertir au format NetFlow.

2. L'analyse comportementale et la détection d'anomalies

Contrairement aux outils réseau classiques qui analysent NetFlow uniquement pour surveiller la bande passante, Stealthwatch l'utilise à des fins de sécurité et d'analyse forensique :

- **Définition d'une base de référence** : Stealthwatch étudie le comportement de chaque périphérique pour comprendre ce qui est « normal » pour lui (fréquence, volume de transfert, heures d'activité).
- **Repérage des menaces furtives** : Si un hôte commence à se comporter de manière anormale — en effectuant des scans de ports, en initiant des déplacements latéraux (comportement typique d'un ver informatique) ou en émettant des signaux inhabituels hors du réseau — il est immédiatement identifié comme une menace prioritaire.
- **Détection des fuites de données (DLP)** : En surveillant les volumes et les méthodes de transfert habituels, le système déclenche une alarme si, par exemple, un employé commence à exporter des volumes de données anormalement élevés à une heure inhabituelle.

3. Le dépassement des limites du NetFlow natif

Le protocole NetFlow comporte des limites intrinsèques que Stealthwatch parvient à surmonter :

- **Ajout des données applicatives** : NetFlow ignore nativement les données de la couche application. Le **capteur Stealthwatch** utilise l'inspection approfondie des paquets (DPI) pour identifier et injecter les détails applicatifs (comme les sites web consultés) directement dans les enregistrements NetFlow.
- **Capture de paquets déclenchée** : NetFlow ne contient que des enregistrements de métadonnées de connexion, pas les paquets réels. Pour remédier à cela lors d'une enquête forensique, Stealthwatch peut déclencher automatiquement une **capture complète de paquets** dès qu'une alerte critique est générée, fournissant ainsi des preuves irréfutables.

Qu'est-ce que Cisco Investigate ?

Cisco Investigate est un **outil d'analyse forensique DNS** directement intégré aux fonctionnalités de la plateforme de sécurité cloud **Cisco Umbrella**.

Cet outil permet aux équipes de sécurité d'effectuer des recherches approfondies pour comprendre l'activité, l'infrastructure et les associations techniques d'un domaine ou d'un site web suspect. Concrètement, Cisco Investigate permet d'interroger un domaine pour visualiser et analyser des informations détaillées telles que :

- Les **enregistrements WHOIS**.
- L'**horodatage** des requêtes.
- Les **scores de sécurité**.
- La **répartition géographique** des accès.
- Toutes les **adresses IP associées** et les **serveurs de noms**.
- Les **cooccurrences** sur d'autres sites web ainsi que les **domaines connexes**.

En recoupant ces relations DNS, l'outil aide à démontrer si un site est lié à d'autres domaines malveillants (comme des serveurs contrôlés par des attaquants hébergeant des chevaux de Troie). Ces informations s'avèrent cruciales pour les enquêteurs afin de reconstituer le fil d'une attaque, d'étayer des allégations de menace ou même de prouver la nature réelle d'un trafic réseau devant un tribunal.

Qu'est-ce que Cisco Tetration ?

Cisco Tetration est une plateforme d'analyse réseau haut de gamme conçue pour offrir une **visibilité en temps réel et ultra-profonde** sur l'ensemble des activités d'un centre de données (*data center*).

Contrairement aux outils de surveillance plus classiques, Tetration se distingue par plusieurs aspects fondamentaux :

1. Une analyse au niveau du paquet (vs NetFlow)

Alors que des solutions comme Cisco Stealthwatch s'appuient sur les métadonnées de flux NetFlow, Tetration va beaucoup plus loin en analysant **chaque paquet et chaque flux réseau à la vitesse de la ligne**, soit un débit phénoménal d'environ **1,5 téraoctet de données par**

seconde. Elle traite cette masse d'informations en quelques minutes grâce à des algorithmes d'apprentissage automatique (*machine learning*).

2. La cartographie complète des dépendances applicatives

La plateforme génère une carte ultra-précise de toutes les applications du centre de données et de leurs interactions. Elle descend jusqu'au **niveau des processus en communication**, enregistrant leur nom de service, leur heure de lancement et d'autres détails granulaires. Cette visibilité est assurée par des serveurs et des capteurs logiciels, et peut être alimentée par des commutateurs réseau compatibles, comme la gamme **Cisco Nexus 9000**.

3. L'application simplifiée du modèle « Zéro Confiance » (Zero Trust)

- **Mise en œuvre automatisée** : Tetration permet de déployer et de maintenir des politiques de sécurité strictes basées sur des **listes blanches « zéro confiance »**, une tâche d'ordinaire extrêmement complexe à réaliser manuellement dans un grand centre de données.
- **Simulation d'impact sans risque** : Pour éviter qu'une nouvelle règle de sécurité ne bloque une application métier légitime en production, Tetration permet de **tester logiquement l'impact des modifications** à l'aide des données historiques, sans aucune perturbation réelle des systèmes.

4. Une machine à remonter le temps pour l'analyse forensique

Pour les enquêteurs numériques, Tetration offre une valeur inestimable : elle **conserve l'intégralité des flux et de l'activité réseau** depuis son déploiement. En cas d'incident, l'administrateur peut littéralement « **rejouer** » l'attaque dans son intégralité. Cela permet de comprendre le déroulement exact de la menace, de voir qui a accédé à quoi, et même de remonter à une ancienne erreur de configuration humaine ayant ouvert la faille initiale.

En somme, c'est l'outil de choix pour les entreprises qui cherchent à sécuriser des environnements complexes, planifier des reprises après sinistre ou migrer des applications critiques en maîtrisant parfaitement leurs risques.

Explique le rôle de Snort dans Cisco

Dans l'écosystème Cisco, **Snort** joue un rôle fondamental à la fois comme outil open source pris en charge par la marque et comme socle technologique de ses solutions de sécurité d'entreprise :

- **Une technologie open source d'origine historique** : Développé en 2001 par Martin Roesch (qui a ensuite fondé la société Sourcefire), Snort est un logiciel gratuit de détection d'intrusion réseau (NIDS) conçu pour Linux et Windows. À la suite de l'acquisition de Sourcefire par Cisco, ce dernier a pris sous son aile cette technologie open source emblématique.
- **Un système de détection et de prévention personnalisable** : Snort fonctionne comme un système de détection et de prévention des intrusions (IDS/IPS) hautement personnalisable. Il surveille le trafic réseau pour identifier et bloquer les comportements malveillants en temps réel, ce qui lui confère un intérêt de premier plan pour l'analyse forensique numérique.
- **Le moteur technologique de Cisco Firepower** : Bien que Snort puisse être utilisé de manière autonome, il sert de fondation à la plateforme de sécurité d'entreprise **Cisco Firepower**. Firepower a été conçu pour automatiser et unifier les capacités de détection d'outils comme Snort. Plutôt que de forcer les administrateurs à configurer manuellement des milliers de signatures d'attaques et à faire interagir plusieurs applications open source de façon complexe, la solution commerciale de Cisco livre un produit clé en main géré par des professionnels.
- **Une détection alimentée par la recherche globale** : Contrairement à l'usage autonome de Snort, son intégration dans les solutions d'entreprise de Cisco lui permet de bénéficier de flux de renseignements exclusifs sur les menaces, notamment ceux développés par l'équipe de recherche sur les menaces mondiales de Cisco, **Talos**.



Explique ClamAV et Razorback

Dans le catalogue des solutions **open source** prises en charge par Cisco (historiquement développées par Sourcefire), **ClamAV** (ClamAV)

et **Razorback** apportent des capacités d'analyse et de protection complémentaires :

1. ClaimAV

- **Rôle principal** : C'est un **moteur antivirus** destiné à détecter les chevaux de Troie, les virus, les logiciels malveillants et diverses autres menaces.
- **Intérêt pour l'analyse forensique** : Il fonctionne comme un outil de sécurité installé directement sur l'hôte. Il est capable de bloquer l'exécution de fichiers suspects et de générer des **données de journalisation (logs) précieuses** pour reconstituer le fil d'un incident.
- **Positionnement** : C'est une excellente alternative de protection pour les organisations qui ne souhaitent pas payer pour un antivirus propriétaire.

2. Razorback

- **Rôle principal** : Il s'agit d'un **framework** qui fournit un traitement avancé des données sur plusieurs niveaux (multiniveaux) ainsi qu'une détection des menaces ciblant le côté client.
- **Structure et valeur forensique** : L'architecture de Razorback est hautement modulaire. Elle s'articule autour d'un **répartiteur** (*dispatcher*) relié à différents modules spécialisés. Chaque module remplit un rôle forensique distinct et essentiel :
 - La collecte, la détection et l'analyse approfondie des données.
 - La production et la restitution de résultats d'analyse.
 - La corrélation d'événements et le renseignement sur les menaces (*threat intelligence*).
 - La distribution des mises à jour de sécurité.

Bien que ces outils soient très performants, le document souligne que leur intégration et leur maintenance manuelle peuvent s'avérer complexes. C'est pourquoi Cisco propose des solutions d'entreprise clés en main (comme la suite Firepower) pour unifier, automatiser et simplifier la gestion de ces technologies de détection.

Qu'est-ce que Daemonlogger?

Daemonlogger est un **enregistreur de paquets rapide**, conçu spécifiquement pour les environnements **NSM** (*Network Security Monitoring*).

Il fait partie de la suite d'outils et de solutions open source initialement développés par la société **Sourcefire** et qui sont aujourd'hui pris en charge par **Cisco**.

Comment fonctionne Joy ?

Selon vos sources, **Joy** est un outil open source pris en charge par Cisco. Son rôle principal est d'agir comme un **outil de capture et d'analyse des données NetFlow et intraflow**.

Malheureusement, les documents actuellement présents dans votre bloc-notes ne fournissent pas d'explications techniques supplémentaires sur son fonctionnement détaillé ou ses protocoles d'analyse.

Qu'est-ce que le framework Moflow ?

Le **framework Moflow** est un outil open source (faisant partie du catalogue hérité de Sourcefire et aujourd'hui soutenu par Cisco) qui fournit des **outils de découverte et de triage des vulnérabilités**.

Compare Stealthwatch et Tetration

Cisco Stealthwatch et **Cisco Tetration** sont deux plateformes de visibilité et d'analyse forensique de premier plan dans le catalogue Cisco, mais elles répondent à des architectures, des environnements et des cas d'usage bien distincts :

1. La source des données et la profondeur d'analyse

- **Stealthwatch** repose sur la technologie **NetFlow** (et ses variantes comme sFlow), qui enregistre les métadonnées des flux réseau. Par défaut, NetFlow ne contient pas les paquets réels. Bien que des capteurs Stealthwatch puissent effectuer une inspection

approfondie des paquets (DPI) pour ajouter des données de la couche application, les données brutes restent consolidées pour l'analyse.

- **Tetration** va beaucoup plus loin en analysant **chaque paquet et chaque flux à la vitesse de la ligne**. La plateforme traite un volume phénoménal de données (environ **1,5 téraoctet par seconde**) en temps réel à l'aide d'algorithmes d'apprentissage automatique.

2. Le niveau de visibilité et l'environnement cible

- **Stealthwatch** est conçu pour l'**ensemble du réseau de l'entreprise** (physique, virtuel et cloud). Il offre une visibilité sur les routeurs, les commutateurs, les pare-feux et le trafic latéral interne ("est-ouest").
- **Tetration** est spécifiquement optimisé pour les **centres de données (data centers)** et les environnements d'applications complexes. Sa visibilité descend jusqu'au **niveau des processus système** au sein des serveurs (nom de service, heure de lancement, etc.), permettant de cartographier l'intégralité des dépendances applicatives.

3. Les cas d'usage principaux et la sécurité

- **Stealthwatch** se concentre sur la **détection des menaces comportementales**. En définissant un comportement de référence ("baseline") pour chaque périphérique, il identifie les anomalies réseau telles que les balayages de ports, la propagation latérale de vers informatiques ou l'exfiltration inhabituelle de données.
- **Tetration** est l'outil de choix pour concevoir et appliquer des **politiques de liste blanche « zéro confiance » (Zero Trust)**. Il permet également de **simuler logiquement l'impact d'une règle de sécurité** sur l'environnement historique avant de la déployer, éliminant ainsi le risque d'interrompre des applications métiers critiques en production.

4. La valeur ajoutée pour l'analyse forensique

- **Stealthwatch** permet d'identifier l'origine d'un incident et de prioriser les enquêtes. Pour compenser l'absence de paquets dans NetFlow, il permet de configurer une **capture de paquets déclenchée** automatiquement par des alertes spécifiques.

- **Tetration** fait office de véritable machine à remonter le temps : il **conserve l'intégralité des flux et de l'activité réseau** depuis son déploiement. En cas d'incident, l'enquêteur peut **rejouer l'attaque dans son intégralité** pour comprendre la progression de la menace, voir qui a accédé à quoi, et identifier précisément quelle erreur de configuration humaine passée a ouvert la faille d'origine.

5. L'infrastructure et le coût

- **Stealthwatch** tire parti de l'infrastructure réseau existante ("le réseau comme capteur") en collectant le NetFlow généré nativement par vos commutateurs et routeurs, ce qui facilite son déploiement.
- **Tetration** représente un **investissement important** en matière de coût et d'infrastructure. Il nécessite le déploiement de serveurs dédiés, de capteurs logiciels applicatifs sur les hôtes, et s'appuie sur des commutateurs haut de gamme comme la gamme Cisco Nexus 9000 pour collecter les données de trafic.

Comment Talos alimente Snort ?

Vos sources n'expliquent pas explicitement le mécanisme par lequel l'équipe Talos alimente Snort en règles ou en signatures de sécurité.

Voici ce que les documents indiquent à ce sujet :

- **Snort** est présenté comme un système open source de détection et de prévention des intrusions (IDS/IPS) personnalisable.
- Les **solutions d'entreprise de Cisco** (qui intègrent et automatisent la technologie de Snort, comme Firepower) proposent des flux de renseignements sur les menaces et de signatures d'attaques basés sur des données réservées aux clients payants.
- **Cisco Talos** est l'équipe de recherche de Cisco qui analyse un nombre massif d'échantillons de menaces à l'échelle mondiale (notamment via Cisco Threat Grid), permettant d'accélérer la détection grâce au renseignement sur les menaces (*threat intelligence*).

C'est quoi Cisco Cloudlock ?

Cisco Cloudlock est une solution acquise par Cisco qui agit comme un **courtier de sécurité d'accès au cloud (CASB - Cloud Access Security Broker)**. Son rôle principal est de protéger les utilisateurs, les données et les applications lorsque les entreprises migrent leurs outils (partage de fichiers comme Dropbox ou Box, outils de supervision comme Salesforce, messagerie comme Gmail) vers le cloud. En effet, lorsque ces données quittent l'infrastructure interne, la visibilité et les contrôles réseaux traditionnels de l'entreprise disparaissent souvent ; Cloudlock vient donc combler ce manque.

Voici ses principales fonctionnalités et cas d'usage selon vos sources :

1. La prévention des pertes de données (DLP)

- **Contrôle des partages** : Cloudlock surveille la façon dont les documents sont partagés et évite qu'un utilisateur interne ne publie par mégarde ou malveillance un document confidentiel sur un service cloud non surveillé.
- **Blocage des données sensibles** : Grâce à sa technologie DLP (*Data Loss Prevention*), la solution peut analyser les fichiers stockés dans le cloud pour repérer des informations hautement sensibles, comme des numéros de carte bancaire. Si un tel fichier est partagé sur Dropbox par exemple, Cloudlock peut **bloquer automatiquement le partage** et signaler l'anomalie.
- **Surveillance des départs** : Il permet également d'identifier des comportements malveillants internes, comme un collaborateur qui téléchargerait massivement des données sensibles (par exemple, des contacts commerciaux) juste avant de quitter l'entreprise.

2. La détection des comptes compromis

- **Connexions géographiquement impossibles** : Cloudlock analyse l'activité et l'origine des connexions. Si votre compte se connecte au cloud depuis deux emplacements géographiquement éloignés dans le monde au même moment, la solution identifie l'anomalie comme une compromission de compte et une fuite potentielle de données.

3. Le contrôle des autorisations d'applications mobiles

- **Évaluation des accès** : Il gère les risques de sécurité liés aux applications mobiles qui demandent l'accès à l'intégralité du

terminal, y compris à des applications contenant des données d'entreprise sensibles comme la messagerie professionnelle.

4. La valeur forensique (Enquêtes numériques)

- **Traçabilité complète** : Pour un enquêteur numérique, Cloudlock est indispensable pour visualiser l'utilisation exacte des services cloud d'une entreprise. Il fournit des rapports précis indiquant **qui a accédé à quelles ressources**. Ces détails temporels et nominatifs constituent des preuves solides et inaltérables à présenter devant un tribunal en cas de litige ou de violation de données.

Pourquoi les attaques par courriel nécessitent-elles une solution dédiée comme Cisco Email Security Appliance (ESA) plutôt qu'un simple pare-feu réseau, et comment s'intègre-t-elle à la sécurité Web ?

Les attaques et le trafic de courrier électronique sont très différents des attaques réseau classiques. Bien que des solutions de sécurité réseau ou web d'entreprise (comme WSA, Firepower ou Meraki) soient efficaces pour bloquer les sources web malveillantes, elles ne suffisent pas face aux spécificités des menaces par courriel.

Pourquoi un simple pare-feu réseau ne suffit pas

Le courrier électronique présente des techniques de contournement uniques qui exigent une solution dédiée comme **Cisco ESA (Email Security Appliance)** :

- **La détection du spam** : Le spam consiste souvent à recevoir du contenu qui est en soi légitime, mais indésirable. Un pare-feu classique, qui cherche des exploits ou des signatures de virus connus, laisse passer ces flux.
- **La modification de format** : Les attaquants modifient la structure des messages pour tromper les filtres génériques. Par exemple, l'insertion d'espaces blancs invisibles pour l'utilisateur suffit à rendre le courriel unique et indétectable pour un système de filtrage de spam classique.
- **L'encodage spécifique** : Les attaquants utilisent fréquemment l'encodage **Base64** pour le transfert de contenu, ce qui permet de masquer le contenu malveillant aux yeux des dispositifs de

sécurité réseau standards qui n'analysent pas en profondeur ces protocoles applicatifs.

Comment Cisco ESA s'intègre à la sécurité Web ?

L'intégration entre la sécurité de la messagerie et la sécurité web est indispensable pour bloquer les scénarios d'attaque hybrides.

En effet, la majorité des cyberattaques combinent ces deux canaux : un attaquant envoie un courriel d'hameçonnage (par exemple, en se faisant passer pour un service postal) contenant un lien externe. L'e-mail en lui-même est relativement sûr car il ne contient que du texte, ce qui lui permet de franchir les défenses de base. Le danger se concrétise lorsque l'utilisateur clique sur le lien, le redirigeant vers un site web malveillant conçu pour exploiter une faille de sécurité web et installer une charge utile.

Pour casser cette chaîne d'attaque, **Cisco ESA s'intègre directement aux solutions de sécurité Web :**

1. L'ESA intercepte et analyse le courriel entrant.
2. Il identifie les liens (URLs) insérés dans le corps du message.
3. Grâce à son intégration web, **l'ESA évalue la réputation et la sécurité de ces liens web avant d'autoriser l'utilisateur à cliquer dessus.**

Cette double vérification constitue une excellente pratique de défense, empêchant les utilisateurs d'être redirigés vers des serveurs d'attaque, même si l'e-mail a été initialement distribué dans leur boîte de réception.

 Nous pourrions explorer comment les e-mails et les rapports d'activité archivés par Cisco ESA peuvent être extraits et filtrés pour servir de preuves juridiques inaltérables lors d'une enquête forensique.

Qu'est-ce que CTA ?

Cisco Cognitive Threat Analytics (CTA) est une fonctionnalité de détection des violations de données basée sur le cloud (SaaS), acquise par Cisco, qui vise à améliorer la réponse aux incidents de sécurité. Voici ce qu'il faut retenir sur son rôle et son fonctionnement :

- **Ce n'est pas un produit autonome** : CTA est une option qui s'active directement sur des serveurs proxys de sécurité web existants, comme la passerelle **Cisco Web Security Appliance (WSA)** ou **Blue Coat ProxySG**.
- **Le ciblage des menaces internes** : Contrairement aux défenses de périmètre classiques (comme Cisco Umbrella ou les filtres de contenu), CTA recherche spécifiquement les menaces déjà installées à l'intérieur du réseau, telles que les **rootkits**, les **botnets** ou les logiciels malveillants diffusant des publicités malveillantes. Elle détecte également l'**exfiltration de données** qui résulte généralement d'une intrusion réseau réussie.
- **La visibilité via le Web** : Même si ces menaces résident sur des machines internes, la plupart utilisent le web pour communiquer avec leurs serveurs de contrôle. CTA estime ainsi que **90 % des menaces internes transitent par Internet**, ce qui signifie qu'elles finiront inévitablement par croiser le chemin d'un proxy.
- **L'analyse comportementale avancée** : Le trafic réseau est surveillé afin de recueillir des informations sur le comportement des utilisateurs et de leurs appareils. En s'appuyant sur l'**apprentissage automatique (machine learning)** et la **détection d'anomalies**, CTA identifie et signale les comportements suspects nécessitant une intervention rapide.
- **L'intégration standardisée** : Pour faciliter l'échange d'informations de sécurité, Cisco CTA est capable de s'intégrer avec d'autres solutions de sécurité en exploitant les protocoles standards **STIX** (Structured Threat Information eXpression) et **TAXII** (Trusted Automated eXchange of Indicator Information).

C'est quoi la différence entre Firepower et Meraki pour la sécurité ?

Cisco Firepower et **Cisco Meraki** sont deux plateformes de sécurité de l'écosystème Cisco qui répondent à des philosophies, des architectures et des besoins opérationnels très différents.

Voici les principales différences de sécurité qui les caractérisent :

1. La philosophie de conception et la gestion

- **Meraki** repose sur une approche hybride qui combine des équipements physiques et une gestion centralisée dans le cloud. **La simplicité est au cœur de son fonctionnement.** Un administrateur peut configurer entièrement un appareil à distance avant même qu'il ne soit livré sur site. L'équipe locale n'a plus qu'à le brancher pour qu'il télécharge automatiquement sa configuration.
- **Firepower** est un pare-feu applicatif d'entreprise classique et complet, conçu pour les environnements exigeant une gestion locale extrêmement poussée et centralisée des menaces.

2. La granularité du contrôle (Pare-feu et IPS)

- **Firepower** offre un contrôle de sécurité extrêmement fin et précis. Il permet aux administrateurs de paramétrer minutieusement les règles de filtrage applicatif, de gérer manuellement des milliers de signatures d'attaques et d'ajuster précisément les défenses.
- **Meraki** propose des fonctionnalités similaires, mais avec des **limitations importantes** pour préserver sa simplicité d'utilisation :
 - Son système de prévention des intrusions (IPS) est une **version allégée** de celui de Firepower.
 - Il est **impossible de paramétrer ou de sélectionner des signatures spécifiques** à activer ou désactiver. L'administrateur doit simplement choisir un niveau de sécurité général, en espérant que les signatures adaptées soient activées par le système.

3. La portée de la protection (AMP)

- Sur un boîtier Meraki, la protection avancée contre les logiciels malveillants (**AMP**) ne peut analyser et détecter que le trafic qui **transite physiquement par l'équipement Meraki**. Firepower propose également cette analyse de flux réseau (AMP for Networks), mais s'intègre nativement de manière beaucoup plus étroite avec des agents terminaux (AMP for Endpoints) pour adapter dynamiquement ses signatures IPS en fonction des vulnérabilités locales détectées sur les hôtes.

4. La valeur forensique (Enquêtes numériques)

- **Meraki** permet d'exporter des rapports de synthèse et des détails d'activité web utiles pour des procédures judiciaires. Toutefois, comme les données sont stockées dans le cloud (modèle hybride),

certaines équipes juridiques pourraient théoriquement questionner la chaîne de traçabilité des preuves (bien que l'infrastructure cloud de Cisco soit hautement sécurisée et reconnue par les tribunaux).

- **Firepower** génère des journaux d'événements locaux complets et un système de classement par impact (niveaux 0 à 4) qui facilitent grandement le tri et l'investigation forensique directe sur le réseau de l'entreprise.

Comment choisir ?

Le choix entre ces deux solutions dépend de la priorité stratégique de votre organisation :

- Privilégiez **Firepower** lorsque **la sécurité absolue et la précision du contrôle sont vos priorités prioritaires**.
- Privilégiez **Meraki** si vos objectifs principaux sont **la simplicité, la facilité de gestion et l'évolutivité**, par exemple pour déployer rapidement et uniformément la sécurité sur des centaines de sites distants.

Comment choisir entre Firepower, WSA et Meraki ?

Le choix entre **Cisco Firepower**, **Cisco WSA** (Web Security Appliance) et **Cisco Meraki** dépend principalement des priorités stratégiques et opérationnelles de votre organisation. Bien que ces trois solutions proposent des fonctionnalités de sécurité qui peuvent sembler similaires, elles répondent à des besoins d'infrastructure très différents :

1. Cisco Firepower : La sécurité absolue et le contrôle précis

- **Quand le choisir** : Lorsque **la sécurité est votre priorité absolue**.
- **Pourquoi** : Firepower est un pare-feu applicatif d'entreprise complet intégrant un système de prévention des intrusions (IPS) extrêmement puissant et des licences de protection avancée contre les logiciels malveillants (AMP). C'est la solution idéale si vous devez inspecter tous les segments de votre réseau et que vous exigez un contrôle granulaire. Contrairement à Meraki, il permet aux experts de paramétrer, d'optimiser et de sélectionner

manuellement des signatures d'attaques spécifiques pour protéger les vulnérabilités propres à votre réseau.

2. Cisco Meraki : La simplicité et le déploiement à grande échelle

- **Quand le choisir** : Si vos objectifs principaux sont la **simplicité de gestion et l'évolutivité**.
- **Pourquoi** : Meraki excelle lorsqu'il s'agit de déployer rapidement et uniformément la sécurité sur des dizaines ou des **centaines de sites distants** (comme des succursales) avec des équipes d'administration réduites. Grâce à son approche hybride cloud et physique, un administrateur peut configurer entièrement un équipement à distance avant même sa livraison. Sur site, l'équipe locale n'a qu'à brancher l'appareil pour qu'il télécharge automatiquement sa configuration. En contrepartie de cette simplicité extrême, le système IPS de Meraki est une **version allégée** de celui de Firepower, sans possibilité de paramétrer ou de choisir individuellement des signatures de sécurité.

3. Cisco WSA : L'optimisation des performances d'accès à Internet

- **Quand le choisir** : Si les **performances de navigation de vos utilisateurs sur Internet sont critiques**.
- **Pourquoi** : Contrairement à Firepower (qui est un pare-feu réseau), Cisco WSA est un **proxy web dédié** qui n'analyse que le trafic Internet sortant (il ne visualise pas le trafic latéral interne). Ses atouts majeurs résident dans l'optimisation de la bande passante grâce à la mise en cache des pages web et à des stratégies de redirection réseau efficaces comme le protocole WCCP. Il intègre également des fonctionnalités de sécurité spécifiques au web souvent absentes des pare-feu applicatifs, telles que la prévention des pertes de données (DLP) et la détection de menaces internes par analyse comportementale cloud (via Cisco Cognitive Threat Analytics).

Comment le modèle Avant, Pendant, Après (BDA) structure-t-il la sécurité ?

La stratégie **Avant, Pendant et Après (BDA)** est l'approche de sécurité de Cisco héritée de l'acquisition de la société Sourcefire. Il s'agit d'une version abrégée du modèle de la chaîne d'attaque cybernétique (*Cyber*

Kill Chain) développé à l'origine par Lockheed Martin, axée principalement sur la gestion des menaces.

Ce modèle structure la sécurité en trois phases temporelles distinctes pour permettre aux défenseurs de stopper une attaque le plus tôt possible :

1. Avant l'attaque (Before) : Prévention et réduction de la surface d'attaque

- **Objectif** : Bloquer les menaces avant qu'elles ne se produisent en limitant les communications aux seules entités de confiance et en empêchant l'exploitation préliminaire des vulnérabilités.
- **Mécanismes clés** :
 - La **sécurité de la réputation** : attribuer un score de confiance à un site ou à une adresse IP en fonction du trafic mondial constaté, afin de bloquer de manière proactive l'accès aux sites potentiellement malveillants.
 - Le **contrôle d'accès au réseau (NAC)** : empêcher tout équipement non autorisé d'obtenir un accès réseau complet dès sa connexion.
- **Exemples de technologies** : Pare-feux, VPN, contrôle d'accès et filtres de contenu.

2. Pendant l'attaque (During) : Détection et prévention en temps réel

- **Objectif** : Repérer et bloquer les comportements malveillants ou l'exploitation active d'une vulnérabilité au moment où l'attaque se produit.
- **Mécanismes clés** :
 - L'analyse basée sur des **signatures d'attaque et de comportement** pour intercepter les menaces connues.
 - L'**optimisation continue** des défenses : Cisco propose notamment une analyse automatisée des vulnérabilités locales pour adapter dynamiquement la détection du réseau.
 - Le recours à des techniques plus avancées comme l'**apprentissage automatique (machine learning)** et l'analyse comportementale.
- **Exemples de technologies** : Antivirus, antimalware, systèmes de détection et de prévention d'intrusion (IDS/IPS), ainsi que les passerelles de sécurité web et de messagerie.

3. Après l'attaque (After) : Réponse, confinement et analyse forensique

- **Objectif** : Gérer la sécurité post-compromission pour toutes les menaces ayant réussi à contourner les contrôles des phases « Avant » et « Pendant ».
- **Mécanismes clés** :
 - La mise en œuvre du **plan de réponse aux incidents** pour confiner la menace (par exemple, bloquer un rançongiciel en cours d'exécution qui tente de chiffrer le disque dur de la victime).
 - La **validation des défenses** : cette phase est indispensable pour savoir précisément ce qui a contourné les filtres existants et corriger les failles.
 - L'**analyse forensique** : étudier le comportement des fichiers suspects et cartographier leur propagation dans le réseau pour remonter jusqu'au patient zéro.
- **Exemples de technologies** : Enregistrement NetFlow, pots de miel (*honeypots*), analyse de référence comportementale et analyse de fichiers.

Une articulation dynamique et circulaire

Pour comprendre la synergie de ce modèle, prenons l'exemple d'une attaque par rançongiciel propagée par un courriel d'hameçonnage :

1. La phase **Avant** tente de bloquer l'e-mail ou la requête DNS initiale lorsque l'utilisateur clique sur le lien malveillant.
2. La phase **Pendant** détecte que le site tente d'exploiter une faille et bloque le téléchargement de la charge utile.
3. La phase **Après** intervient si le malware s'est installé, en détectant son comportement suspect (comme la suppression de sauvegardes ou la modification de la base de registre) pour l'empêcher d'exécuter son processus de chiffrement.

L'amélioration continue : Si une menace n'est détectée qu'au stade « Après », les informations recueillies (valeurs de hachage du fichier, domaines de redirection) sont immédiatement utilisées pour mettre à jour les signatures IPS (phase **Pendant**) et inscrire les domaines malveillants sur liste noire (phase **Avant**), protégeant ainsi le reste de l'organisation contre de futures tentatives.

Comment Cisco ISE bloque-t-il un iPad ?

Cisco ISE (Identity Services Engine) peut bloquer ou limiter l'accès d'un iPad de plusieurs manières, soit de façon autonome lors de sa tentative de connexion, soit de manière dynamique et automatisée en réponse à une menace détectée par un autre outil de sécurité.

Voici comment se déroule ce processus :

1. Le profilage précis de l'appareil

Avant de pouvoir appliquer une règle ou bloquer l'iPad, Cisco ISE doit d'abord l'identifier au sein du réseau. Pour cela, il utilise diverses sondes réseau (telles que DHCP, DNS, HTTP ou RADIUS) :

- À la connexion, l'adresse MAC de l'iPad permet d'abord de l'identifier de manière générale comme un appareil Apple.
- À mesure que d'autres données sont collectées via les sondes DHCP et DNS, Cisco ISE affine sa classification pour l'étiqueter spécifiquement comme un **iPad**.
- Cisco ISE associe ensuite cet appareil à un contexte utilisateur précis (par exemple, pour l'associer à l'iPad de l'utilisateur *jmuniz*).

2. Les méthodes de restriction et de blocage

Une fois l'iPad profilé, Cisco ISE agit comme un système de contrôle d'accès réseau (NAC) et peut modifier instantanément son état de connexion de plusieurs manières :

- **Limiter son accès** : il peut modifier dynamiquement le **VLAN** de l'iPad pour l'isoler ou lui appliquer des **listes de contrôle d'accès (ACL)** restrictives pour bloquer certains flux.
- **Segmenter l'accès** : il peut appliquer des politiques de segmentation via la technologie **TrustSec**.
- **Bloquer complètement l'appareil** : il peut ordonner la **suppression complète de l'iPad du réseau** (déconnexion totale).

3. L'intégration et le blocage automatisé (Remédiation)

L'atout majeur de Cisco ISE réside dans sa capacité à partager ce contexte et à automatiser le blocage en s'intégrant avec des solutions tierces (comme un SIEM comme Splunk ou des outils de sécurité réseau) :

- Si l'iPad de l'utilisateur est connecté et qu'un outil de détection (par exemple, un SIEM) découvre que cet iPad a été infecté par un

logiciel malveillant (comme un ransomware), il envoie une alerte automatique à Cisco ISE.

- Cisco ISE reçoit l'instruction de remédiation et **retire immédiatement l'iPad du réseau**.
- Cette réaction automatisée est essentielle pour contenir la propagation latérale d'une menace, en particulier lors d'incidents survenant à des heures où aucune équipe de sécurité n'est présente pour intervenir manuellement (par exemple, à 3 heures du matin).

(Remarque : Cisco recommande de déployer ces mécanismes de remédiation automatique avec précaution, car une fausse alerte sur un équipement critique pourrait provoquer une interruption de service involontaire.)

Qu'est-ce que Cisco TrustSec ?

Cisco TrustSec est une **option de segmentation dynamique** et de contrôle d'accès réseau gérée par la solution **Cisco Identity Services Engine (ISE)**.

S'appuyant sur la norme de sécurité **802.1x**, cette technologie permet d'appliquer un contrôle d'accès automatisé sur le réseau. Au même titre que les VLAN ou les listes de contrôle d'accès (ACL), les politiques TrustSec sont utilisées pour **attribuer des droits d'accès réseau spécifiques et restreints** à un périphérique ou à un utilisateur en fonction des règles de sécurité préalablement configurées dans Cisco ISE.

Comment fonctionne le profilage d'appareils ?

Le **profilage d'appareils** (ou *profiling*) dans **Cisco ISE** est un processus d'apprentissage continu qui permet d'identifier et de catégoriser précisément chaque équipement connecté au réseau en analysant son comportement et ses échanges.

Voici les étapes clés de son fonctionnement :

1. L'état initial « Inconnu »

Lorsqu'un nouvel appareil se connecte pour la première fois, il n'a pas encore partagé d'informations comportementales. Cisco ISE le place alors par défaut dans la catégorie « **Inconnu** ».

2. L'identification initiale par l'adresse MAC (Couche 2)

Dès la connexion, Cisco ISE extrait l'adresse MAC de l'appareil. Grâce à cette donnée de couche 2, il peut déterminer le constructeur ou la famille générale de l'équipement (par exemple, identifier qu'il s'agit d'un **appareil Apple**). Cependant, cette information reste trop limitée pour connaître le modèle exact de l'appareil.

3. La collecte d'indices via des sondes spécialisées

Pour affiner l'identité de la machine, Cisco ISE écoute le réseau et récolte des données à l'aide de plusieurs **sondes (probes)**. Ces sondes incluent notamment :

- **DHCP** et **DHCPSPAN**
- **DNS**
- **HTTP**
- **SNMP**
- **RADIUS**

4. La classification progressive et détaillée

À mesure que l'appareil communique, ces sondes collectent des informations de protocole et d'application. Cisco ISE analyse ces nouvelles données, continue d'apprendre de ses caractéristiques et **déplace l'équipement vers une catégorie de classification beaucoup plus fine**. C'est ce mécanisme qui lui permet, par exemple, de requalifier un simple "appareil Apple" générique en **iPhone** ou en **iPad** spécifique.

Ce profilage dynamique permet ensuite d'appliquer des règles de sécurité adaptées à la nature et au rôle réel de l'appareil connecté.

Quelle est la différence entre AMP for Network et AMP for Endpoint ?

La différence principale entre **Cisco AMP for Network** (Advanced Malware Protection) et **Cisco AMP for Endpoint** réside dans leur emplacement d'exécution, leur périmètre de protection et leurs capacités de remédiation :

1. Emplacement d'exécution et portée de la surveillance

- **AMP for Network** s'exécute au niveau du réseau, par exemple via un connecteur réseau intégré à une plateforme comme Cisco Firepower. Il surveille et analyse uniquement les fichiers lorsqu'ils transitent sur le réseau.
- **AMP for Endpoint** s'exécute directement sur les hôtes (ordinateurs, serveurs) sous la forme d'un agent logiciel léger. Cet agent analyse en continu l'ensemble des fichiers stockés et présents sur la machine.

2. Mobilité et protection hors réseau

- **AMP for Network** ne protège un équipement que lorsque celui-ci est connecté au réseau de l'entreprise. Si un utilisateur quitte physiquement le réseau, son appareil n'est plus protégé par cette solution.
- **AMP for Endpoint** suit l'appareil partout. Il offre à l'administrateur une visibilité approfondie et continue de tous les fichiers sur l'ensemble des systèmes surveillés, quel que soit leur emplacement géographique dans le monde.

3. Capacités de remédiation (Action face à une menace)

- **AMP for Network** est limité dans ses actions de nettoyage : il peut bloquer le transit ou la propagation d'un fichier malveillant sur le réseau, mais il est incapable de supprimer un fichier déjà installé sur un disque dur ou de détecter l'activité d'un malware se déroulant derrière le pare-feu local du terminal.
- **AMP for Endpoint** dispose de privilèges locaux lui permettant de supprimer directement le fichier identifié comme malveillant sur le système hôte afin de neutraliser l'infection.

4. Analyse des vulnérabilités et synergie

- **AMP for Network** n'a pas visibilité sur les failles de sécurité internes des machines connectées.
- **AMP for Endpoint** scanne en permanence l'hôte à la recherche de vulnérabilités logicielles (comme des versions obsolètes d'Adobe Flash ou d'Oracle Java). Il transmet ces informations à Cisco Firepower, ce qui permet au système de prévention des intrusions (IPS) réseau d'adapter et d'activer automatiquement les signatures de détection pour protéger spécifiquement les vulnérabilités signalées sur vos terminaux.

En résumé, **AMP for Network** agit comme un filtre qui inspecte et bloque les menaces à la volée pendant leur transport, tandis qu'**AMP for Endpoint** est un agent de sécurité résident sur l'hôte, capable d'analyser le comportement local des fichiers, de recenser les vulnérabilités et de supprimer directement les fichiers malveillants.

Comment Cisco Threat Grid identifie-t-il les fichiers suspects ?

Cisco Threat Grid identifie les fichiers suspects en combinant un **sandbox (bac à sable) avancé** et une base massive de **renseignement sur les menaces** (*threat intelligence*).

Voici les mécanismes précis qu'il utilise pour analyser et détecter ces fichiers :

1. Les modes d'acquisition des fichiers

Les fichiers suspects entrent dans le système de deux manières :

- **La surveillance automatique** : Threat Grid analyse automatiquement les fichiers qui transitent par d'autres plateformes de sécurité de Cisco, comme la solution Cisco Firepower.
- **L'envoi manuel** : Les administrateurs peuvent soumettre manuellement tout fichier douteux directement à la plateforme pour évaluation.

2. L'analyse comportementale en sandbox (bac à sable)

Dès qu'un fichier suspect est soumis, il est exécuté au sein d'un environnement virtuel totalement isolé et sécurisé afin d'observer et d'enregistrer ses actions en temps réel. Pendant cette exécution, Threat Grid identifie un ensemble d'indicateurs comportementaux suspects pour évaluer sa dangerosité, notamment :

- **L'activité du registre système** et les détails des processus initiés par le fichier.
- **Le comportement réseau** : les requêtes DNS, les données TCP/IP et l'utilisation de réseaux d'obfuscation ou de communication anonyme comme TOR.
- **La modification de fichiers** : les comportements typiques de rançongiciels (comme la suppression de sauvegardes ou le chiffrement de données) ou les modifications visant à cacher sa nature (polymorphisme).

- **L'exploitation de failles** : l'identification des vulnérabilités logicielles spécifiques dont le fichier tente de se servir pour s'exécuter ou se propager.

3. L'interaction manuelle ou automatique (Glovebox)

Grâce à la fonctionnalité **Glovebox**, les administrateurs réseau peuvent non seulement automatiser l'évaluation, mais également choisir de prendre la main sur l'environnement sandbox afin d'**exécuter le fichier et d'interagir directement avec lui** de façon sécurisée. Cela permet de forcer ou de déclencher manuellement certaines actions du malware pour mieux l'étudier.

4. La preuve visuelle par enregistrement vidéo

Afin d'aider les analystes à comprendre la nature de la menace et de fournir des preuves incontestables de sa malveillance, Threat Grid produit des rapports contenant des **vidéos du fichier en train de s'exécuter** dans la sandbox. On peut ainsi y voir concrètement ce à quoi ressemblerait l'infection sur le poste d'une victime (par exemple, le chiffrement des fichiers ou l'affichage de la demande de rançon).

5. La corrélation avec l'intelligence mondiale (Cisco Talos)

Pour accélérer l'identification, chaque fichier est comparé avec l'immense base de données d'échantillons de menaces mondiales collectée par l'équipe de recherche d'élite **Cisco Talos**. Ce flux de renseignements permet de repérer immédiatement si l'artefact analysé a déjà été observé et documenté ailleurs dans le monde.

Comment Cisco Stealthwatch utilise-t-il NetFlow pour la détection ?

Cisco Stealthwatch repose sur la technologie **NetFlow** (ainsi que ses variantes comme sFlow) pour enregistrer le trafic réseau afin de transformer l'ensemble de l'infrastructure (physique, virtuelle et cloud) en une vaste grille de détection.

Voici précisément comment la solution exploite ces données pour identifier les menaces :

1. La collecte et l'enrichissement des données de flux

- **La réception des flux** : Les équipements réseau de l'entreprise (routeurs, commutateurs, pare-feux, points d'accès) sont configurés pour exporter et envoyer en continu leurs flux NetFlow vers le collecteur de Stealthwatch.

- **La conversion par capteur** : Pour les parties du réseau ou les environnements virtuels ne prenant pas nativement en charge NetFlow, un capteur Stealthwatch (*FlowSensor*) convertit le trafic réseau brut en flux pour garantir une visibilité complète, notamment sur le trafic latéral interne (est-ouest).
- **L'ajout du contexte applicatif** : Les enregistrements NetFlow d'origine ignorant les données applicatives, le capteur de Stealthwatch utilise l'inspection approfondie des paquets (DPI) pour analyser le trafic (qu'il soit en clair ou chiffré) et ajouter des informations sur les protocoles et sites web consultés.

2. L'établissement d'une base de référence (*Baseline*)

Contrairement aux outils NetFlow classiques qui se bornent à analyser la charge ou la congestion du réseau, Stealthwatch évalue en permanence chaque périphérique par rapport à un **comportement de référence considéré comme normal**. Ce profil comportemental prend en compte les volumes de transfert habituels, la fréquence des connexions, les méthodes de transfert et les heures d'activité.

3. La détection d'anomalies et de comportements malveillants

Dès qu'un appareil s'écarte de sa base de référence, Stealthwatch applique des algorithmes comportementaux pour localiser l'activité suspecte et la classer par priorité. Il cible ainsi plusieurs types de menaces :

- **Les scans de ports** : Les systèmes effectuant des balayages réseau pour chercher des cibles émettent une signature comportementale spécifique immédiatement étiquetée comme non autorisée.
- **Les déplacements latéraux** : Une activité réseau inhabituelle entre deux systèmes internes peut révéler la propagation latérale d'un logiciel malveillant (comme un ver informatique).
- **Les communications suspectes vers l'extérieur** : Stealthwatch identifie les signaux de commande et contrôle (C&C/balises) envoyés à l'extérieur du réseau par des machines compromises.
- **La perte de données (DLP)** : Le système déclenche une alarme si un collaborateur (par exemple, un commercial) commence à transférer des volumes de données anormalement élevés, à une heure inhabituelle ou via une méthode non standard.

4. La remédiation aux limites de NetFlow

Par nature, NetFlow n'enregistre que des métadonnées de flux et ne contient pas les paquets réels. Pour surmonter cette limite lors d'une enquête forensique, Stealthwatch peut **déclencher automatiquement une capture de paquets** sur une partie du réseau dès qu'une alerte comportementale pertinente est générée. Les détails de capture de paquets sauvegardés dans les journaux servent alors de preuves valables en cas de litige.

Quel est le rôle de Glovebox dans Threat Grid ?

Dans Cisco Threat Grid, la fonctionnalité **Glovebox** permet aux administrateurs d'analyser plus finement les fichiers suspects grâce aux capacités suivantes :

- **Interagir en direct avec la menace** : Elle offre aux administrateurs la possibilité d'exécuter le fichier suspect et d'interagir directement avec lui au sein d'un environnement de test hautement contrôlé.
- **Accélérer la compréhension** : Cette interaction aide à cerner beaucoup plus rapidement la véritable nature et le comportement réel d'un fichier.
- **Optimiser la réponse aux incidents** : En comprenant mieux le fonctionnement de l'artefact, les équipes de sécurité peuvent réagir avec une précision accrue face aux menaces potentielles.

En résumé, Glovebox transforme une analyse de sandbox purement passive et automatisée en une investigation interactive et dynamique.

 Souhaitez-vous que nous examinions comment les rapports de Threat Grid (incluant les captures vidéo de ces exécutions et l'analyse du registre) enrichissent un dossier de preuve forensique ?

Quel est le rôle de Cisco Threat Grid ?

Cisco Threat Grid a pour rôle principal d'identifier et d'analyser les artefacts malveillants sophistiqués en combinant un **bac à sable (sandbox) avancé** et du **renseignement mondial sur les menaces**. Il s'agit d'un outil essentiel pour évaluer les fichiers suspects, même s'ils ne sont pas encore reconnus comme des menaces par les signatures de sécurité classiques.

Voici ses fonctions et caractéristiques clés :

1. L'analyse comportementale automatisée et approfondie

- **Modes de soumission** : Les fichiers peuvent être envoyés automatiquement à Threat Grid lorsqu'ils transitent par d'autres solutions (comme Cisco Firepower) ou être soumis manuellement par les analystes pour évaluation.
- **Rapports d'activité complets** : Lors de l'exécution isolée d'un fichier suspect, la plateforme enregistre automatiquement son activité sur le registre système, les détails de ses processus, les connexions TCP/IP qu'il tente d'établir, ainsi que ses requêtes DNS.
- **Indicateurs de dangerosité** : Il fournit une liste d'indicateurs de comportement (comme l'utilisation du réseau d'anonymisation TOR ou des actions spécifiques aux rançongiciels, telles que la suppression de sauvegardes) pour expliquer de manière transparente pourquoi un fichier est considéré comme dangereux.

2. L'investigation interactive et visuelle

- **La Glovebox** : Cette fonctionnalité permet aux administrateurs de prendre le contrôle de l'environnement virtuel pour **interagir directement et en toute sécurité avec la menace**, ce qui aide à cerner plus rapidement sa nature.
- **Preuves par enregistrement vidéo** : Threat Grid produit des vidéos montrant le logiciel malveillant en train de s'exécuter dans le bac à sable. L'analyste peut ainsi voir concrètement à quoi ressemble l'infection sur le poste de la victime (par exemple, le chiffrement en direct de l'écran par un rançongiciel), un excellent moyen de sensibiliser les décideurs ou les utilisateurs moins techniques.

3. Une valeur forensique et juridique majeure

- Pour les enquêteurs numériques, l'analyse automatique de Threat Grid fournit des détails cruciaux que l'on n'observe pas toujours

après coup lors d'une simple intervention post-incident (comme le comportement polymorphique d'un fichier ou les URL spécifiques qu'il cherche à contacter).

- Le rapport de Threat Grid associe des valeurs de hachage précises à la menace, ce qui permet de localiser le fichier sur d'autres systèmes réseau et de **fournir des preuves incontestables pour étayer juridiquement des allégations de menace** en justice.

4. Flexibilité de déploiement et intégration massive

- Il s'appuie sur le volume colossal d'échantillons de menaces mondiales analysés par l'équipe d'élite **Cisco Talos** pour accélérer la détection.
- Il s'intègre nativement dans presque tout le catalogue Cisco (AMP, WSA, ESA, Firepower, Meraki MX, Umbrella).
- Il peut être déployé en tant que service cloud ou sous forme d'**appliances dédiées sur site (modèles 5004 et 5504)**, une option particulièrement appréciée par les organisations qui exigent de conserver l'intégralité de leurs fichiers en local.