

Security Event Generation and SOC Data Collection Methods

Ce texte technique présente les méthodes de **génération et de collecte de données** nécessaires au bon fonctionnement d'un centre des opérations de sécurité (SOC). L'auteur souligne l'importance de **dimensionner adéquatement les solutions de stockage** en calculant précisément le nombre d'événements par seconde pour éviter toute perte d'information critique. Un accent particulier est mis sur la **synchronisation temporelle via le protocole NTP**, essentielle pour corrélérer chronologiquement les incidents provenant de sources multiples. Les sources détaillent également la configuration de dispositifs de sécurité, tels que les **pare-feu Cisco ASA et les services FirePOWER**, afin d'exporter leurs journaux vers un système centralisé. Enfin, l'ouvrage propose des critères pour **évaluer et choisir un outil SIEM**, tout en distinguant les capacités d'analyse des technologies SIM et SEM.

Pourquoi la synchronisation NTP est-elle cruciale pour l'analyse des journaux ?

La synchronisation via le protocole **NTP (Network Time Protocol)** est considérée comme un élément indispensable et critique pour l'analyse des journaux au sein d'un centre d'opérations de sécurité (SOC) pour plusieurs raisons fondamentales :

- **Corrélation des événements** : Pour qu'une solution centralisée (comme un SIEM) soit exploitable, les données doivent être catégorisées de manière ordonnée. L'horodatage précis permet de **retracer chronologiquement les événements** et de corrélérer les résultats provenant de différents systèmes. Sans cela, il devient impossible de lier une activité sur un pare-feu à une action correspondante sur un serveur ou un terminal.
- **Validité des alertes et rapports** : Un décalage temporel, même très bref (quelques microsecondes), peut entraîner des problèmes majeurs de journalisation et **invalidier les alertes** générées par le

système. Une heure mal configurée nuit directement à la précision des rapports de sécurité.

- **Précision des investigations** : La synchronisation garantit que tous les périphériques partagent une source de temps faisant autorité. Cela est crucial lors d'une investigation après un incident pour établir une ligne de temps exacte des actions de l'attaquant à travers tout le réseau.
- **Continuité des services** : Outre l'analyse, une synchronisation incorrecte peut perturber certains services réseau qui dépendent de la précision temporelle pour fonctionner correctement.

En résumé, la meilleure pratique consiste à utiliser un serveur NTP pour tous les systèmes afin d'éviter tout « angle mort » ou incohérence dans la surveillance de l'environnement.

Comment configurer l'authentification NTP sur les périphériques Cisco IOS ?

Pour configurer l'authentification NTP sur les périphériques Cisco IOS, vous devez suivre des étapes spécifiques selon que l'appareil agit en tant que serveur ou client. Cette mesure de sécurité est fortement recommandée pour empêcher toute usurpation d'identité et garantir que les horloges ne sont synchronisées qu'avec des sources de confiance. Voici la procédure détaillée basée sur les sources :

1. Configuration sur le serveur NTP

Sur l'appareil configuré comme maître (master), vous devez définir la clé que les clients devront utiliser :

- **Créer une clé d'authentification** : Utilisez la commande `ntp authentication-key [numéro_clé] md5 [votre_clé]`. Par exemple : `ntp authentication-key 1 md5 cisco`.
- **Définir la clé de confiance** : Indiquez au serveur quelle clé il doit approuver avec la commande `ntp trusted-key [numéro_clé]`.

2. Configuration sur le client NTP

Pour qu'un client puisse se synchroniser de manière sécurisée avec le serveur, des étapes supplémentaires sont nécessaires :

- **Définir la même clé d'authentification** : Utilisez la commande `ntp authentication-key [numéro_clé] md5 [votre_clé]`.
- **Spécifier la clé de confiance** : Utilisez la commande `ntp trusted-key [numéro_clé]`.
- **Activer l'authentification** : Saisissez la commande **ntp authenticate**. Cette étape est cruciale car elle ordonne au client de s'authentifier impérativement auprès du serveur avant d'accepter les informations temporelles.
- **Déclarer le serveur** : Configurez l'adresse du serveur avec la commande `ntp server [adresse_IP]`.

Exemple de configuration complète pour un client (Cisco ASA) :

```
(config)# ntp authentication-key 1 md5 cisco
(config)# ntp trusted-key 1
(config)# ntp authenticate
(config)# ntp server 1.1.1.1
```

Une fois la configuration terminée, vous pouvez vérifier le statut de la synchronisation et de l'authentification avec la commande **show ntp associations**.

Quelle est la différence entre les niveaux de strate NTP ?

Dans le protocole NTP, le niveau de **strate (stratum)** sert d'indicateur de distance par rapport à une source de temps de référence. Voici les principales différences et caractéristiques liées à ces niveaux :

- **Définition du saut** : Le numéro de strate représente le **nombre de sauts** (hops) qui séparent un client de la source de temps faisant autorité.
- **Hierarchie et proximité** : Plus le numéro de strate est **bas**, plus l'appareil est proche de la source de temps primaire. Les clients NTP sont conçus pour utiliser prioritairement le serveur ayant le numéro de strate le plus faible afin d'obtenir l'heure la plus précise possible.

- **Sources de Strate 1** : Les serveurs de strate 1 sont synchronisés directement avec une **source faisant autorité**, telle qu'une horloge atomique, une horloge radio ou un système satellite (GPS).
- **Propagation sur le réseau** : Lorsqu'un serveur de strate 1 distribue l'heure à un autre serveur, ce dernier devient un serveur de strate 2. Ce processus continue à chaque nouvel intermédiaire, augmentant le numéro de strate à chaque étape.
- **Configuration pratique** : Dans les environnements réseau, un administrateur peut configurer un équipement (comme un routeur Cisco) pour agir en tant que maître NTP avec un niveau de strate spécifique, par exemple la **strate 3**, pour distribuer l'heure aux autres clients du réseau local.

Il est important de noter que le protocole NTP effectue des vérifications de validité : il ne se synchronisera pas avec un système non synchronisé et comparera plusieurs sources (le minimum recommandé étant de trois) pour détecter d'éventuelles inexactitudes, même si un serveur présente un numéro de strate inférieur.

Qu'est-ce qu'une source de temps faisant autorité ?

Une **source de temps faisant autorité** est la référence primaire et fiable à partir de laquelle un réseau NTP synchronise son heure. Elle représente le sommet de la hiérarchie temporelle.

Selon les sources, voici les caractéristiques principales de ces sources :

- **Types de dispositifs** : Il s'agit généralement d'équipements de haute précision tels qu'une **horloge atomique**, une **horloge radio** ou un système **satellite** (comme le GPS) connecté à un serveur.
- **Référence universelle** : Ces sources sont synchronisées directement avec le **Temps Universel Coordonné (UTC)**.
- **Hiérarchie (Strata)** : Le niveau de **strate** indique la distance (en nombre de sauts) séparant un équipement de cette source faisant autorité. Un serveur directement relié à une telle horloge est considéré comme un serveur de strate 1.
- **Configuration locale** : Dans un environnement Cisco, un administrateur peut désigner un équipement comme une source

officielle pour le reste du réseau local en utilisant la commande `clock calendar-valid`, indiquant ainsi que le système doit être considéré comme une **source de temps officielle**.

- **Alternatives matérielles** : Si l'équipement réseau standard ne peut pas assurer ce rôle de maître, l'utilisation d'un **périphérique matériel dédié** ou d'une horloge atomique externe est recommandée pour garantir la précision.

Il est conseillé de configurer au moins **trois sources** de ce type sur un client afin d'utiliser un algorithme de consensus et de détecter toute inexactitude entre elles.

Quels sont les niveaux de gravité de journalisation ?

De nombreux produits de sécurité réseau utilisent une échelle standardisée comprenant **huit niveaux de gravité** (ou sévérité), numérotés de **0 à 7**. Ces niveaux permettent de classer l'importance des messages de journalisation :

- **0 - Emergencies** : Le système est **inutilisable**.
- **1 - Alert** : Une **action immédiate** est requise.
- **2 - Critical** : Conditions **critiques**.
- **3 - Error** : Conditions d'**erreur**.
- **4 - Warning** : Conditions d'**avertissement**.
- **5 - Notification** : Événements **normaux mais significatifs**.
- **6 - Informational** : Messages d'**information** uniquement.
- **7 - Debugging** : Messages de **débogage** uniquement.

Fonctionnement de la hiérarchie des niveaux

Le choix du niveau de gravité est cumulatif. **Plus le numéro du niveau est élevé, plus le volume de journaux produits est important**, car l'activation d'un niveau spécifique inclut automatiquement tous les niveaux inférieurs (plus graves).

Par exemple, si vous configurez un équipement (comme un pare-feu Cisco ASA) sur le niveau **4 (Warning)**, le système enregistrera les événements de niveau 4, mais aussi tous ceux de niveaux **0 à 3**. En revanche, le niveau **7 (Debugging)** est le plus verbeux, car il capture l'intégralité des messages disponibles, du débogage jusqu'aux urgences système.

Quelles sont les formules pour calculer l'EPS normal et de pointe ?

Pour calculer le nombre d'événements par seconde (EPS), les sources distinguent le calcul pour un trafic normal et celui pour les périodes de pointe, afin de dimensionner correctement les solutions de collecte de données.

1. Formule de l'EPS normal

Pour un trafic de fonctionnement habituel, la formule est la suivante :

EPS = Nombre d'événements système / Période en secondes.

2. Formule de l'EPS de pointe

Le calcul de l'EPS de pointe est plus complexe car il doit anticiper les fluctuations et les incidents de sécurité. Il s'effectue en deux étapes :

- **Calcul de l'EPS de pointe total par jour : EPS de pointe total par jour = EPS normal × Nombre de pics attendus × Durée d'un pic (secondes) × Facteur d'écart.**
- **Conversion en EPS de pointe :** Comme une journée compte 86 400 secondes, on divise le total obtenu par ce chiffre : **EPS de pointe = EPS de pointe total par jour / 86 400.**

Variables clés pour le calcul de pointe

Pour que ces calculs soient précis, il est nécessaire d'estimer ou de mesurer les facteurs suivants :

- **Nombre de pics attendus :** Souvent fixé à trois par défaut (début de journée, retour de déjeuner, fin de journée).
- **Durée d'un pic :** Généralement estimée à une heure (3 600 secondes).
- **Facteur d'écart :** Représente l'augmentation du trafic lors d'un pic (par exemple lors d'une attaque DDoS). Une valeur par défaut se situe entre **deux et cinq fois** l'EPS normal.

Conseil de dimensionnement : Les sources recommandent d'ajouter systématiquement une **marge de sécurité d'au moins 20 %** à vos calculs finaux pour garantir que le système dispose de suffisamment de puissance de traitement et de stockage.

Qu'est-ce que le facteur d'écart dans les calculs d'EPS ?

Dans le cadre du dimensionnement d'une solution de collecte de données, le **facteur d'écart** est une variable utilisée pour calculer l'**EPS de pointe** (Événements Par Seconde) afin d'anticiper les comportements de trafic inhabituels,

Voici ses caractéristiques principales selon les sources :

- **Définition** : Il représente l'**écart moyen par rapport à l'EPS normal** lors d'un pic d'activité.
- **Objectif** : Ce facteur permet de prendre en compte des événements à plus long terme qui génèrent un volume massif de journaux, tels que des **attaques par déni de service distribué (DDoS)** excessives ou une forte **congestion du réseau**.
- **Valeur recommandée** : Bien qu'il puisse varier selon les risques spécifiques à une organisation, une valeur par défaut appropriée se situe généralement entre **deux et cinq fois l'EPS normal**.
- **Rôle dans le calcul** : Il intervient directement dans la formule du calcul de l'EPS de pointe total par jour :
 - $EPS\ de\ pointe\ total\ par\ jour = EPS\ normal \times Nombre\ de\ pics\ attendus \times Durée\ d'un\ pic\ (en\ secondes) \times Facteur\ d'écart.$

L'utilisation de ce facteur est cruciale pour éviter qu'un système ne soit sous-dimensionné, ce qui pourrait provoquer une panne des outils de surveillance du SOC au moment où un incident majeur se produit. Les sources recommandent d'ailleurs d'ajouter une **marge de sécurité supplémentaire d'au moins 20 %** à l'ensemble de ces calculs.

Comment les cyberattaques influencent-elles le facteur d'écart ?

Les cyberattaques influencent directement le **facteur d'écart** en provoquant des augmentations massives et parfois prolongées du volume de journaux générés par seconde (EPS).

Selon les sources, voici comment ces attaques impactent ce facteur :

- **Création de pics à long terme** : Contrairement aux pics de trafic habituels (comme les connexions matinales), une cyberattaque, telle qu'une **attaque par déni de service distribué (DDoS)**

excessive, génère un flux d'événements intense qui peut durer dans le temps.

- **Multiplication du volume d'événements** : Le facteur d'écart est conçu pour absorber ces anomalies. Dans les calculs de dimensionnement, on estime généralement que l'activité générée lors d'un incident de sécurité peut représenter entre **deux et cinq fois l'EPS normal**.
- **Risque de saturation du système** : C'est précisément au moment d'une attaque que le système de collecte de données est le plus sollicité. Si le facteur d'écart n'est pas correctement anticipé, une cyberattaque peut provoquer une **panne des outils de surveillance du SOC**, entraînant une perte de données précieuses au moment où elles sont le plus nécessaires pour la réponse à l'incident.
- **Nécessité d'ajustement selon le risque** : La valeur de ce facteur n'est pas fixe ; elle doit être ajustée en fonction des **menaces potentielles spécifiques** à l'organisation et de son niveau d'exposition aux risques de sécurité.

En résumé, les cyberattaques transforment le facteur d'écart d'une simple variable statistique en un paramètre de **résilience critique**, obligeant les administrateurs à prévoir une capacité de traitement et de stockage bien supérieure à celle requise pour un fonctionnement normal.

Comment les cyberattaques affectent-elles le dimensionnement du stockage ?

Les cyberattaques influencent considérablement le dimensionnement du stockage d'une solution de collecte de données, principalement en provoquant des **augmentations massives et imprévisibles du volume de données** générées par les systèmes de sécurité.

Voici comment ces attaques affectent spécifiquement les besoins en stockage selon les sources :

- **Explosion du nombre d'événements (EPS) :** Le volume d'événements par seconde (EPS) est le facteur déterminant pour le stockage. Lors d'un incident de sécurité majeur ou d'une attaque par déni de service distribué (**DDoS**), le nombre de journaux produits peut être multiplié par **deux à cinq fois** par rapport à un trafic normal. Si le stockage n'est pas dimensionné pour ces pics, le système risque de manquer d'espace au moment le plus critique de l'attaque.
- **Nécessité du facteur d'écart :** Pour éviter le sous-dimensionnement, les calculs de stockage doivent intégrer un « **facteur d'écart** ». Ce paramètre permet d'anticiper les besoins de stockage à long terme liés aux attaques prolongées, garantissant que les données d'événements précieuses ne soient pas perdues par manque d'espace disque.
- **Exigences de conservation post-incident :** Une cyberattaque déclenche souvent des obligations légales ou réglementaires de **conservation des journaux** à des fins d'analyse forensique ou de procédures judiciaires. Ces exigences de rétention prolongent la durée pendant laquelle les données doivent rester stockées, augmentant ainsi les besoins de capacité à long terme.
- **Risque de défaillance du système :** Un sous-dimensionnement du stockage lors d'une attaque peut provoquer une **panne des outils de surveillance du SOC**. Les sources soulignent qu'il est préférable de surdimensionner l'investissement initial en stockage plutôt que de risquer une interruption de service lors d'un incident.
- **Complexité de l'architecture :** La gestion des attaques peut nécessiter des solutions de **stockage local et distant**, ainsi que des mécanismes de **compression des données** pour optimiser l'espace sans perdre la visibilité nécessaire à l'investigation.

En résumé, les sources recommandent d'intégrer systématiquement une **marge de sécurité d'au moins 20 %** au-dessus des estimations de pointe pour garantir que la solution de collecte dispose toujours de l'espace nécessaire pour enregistrer l'activité d'une attaque en cours.

Comment NetFlow aide-t-il à détecter la saturation des systèmes ?

NetFlow aide à détecter la saturation des systèmes en transformant les équipements réseau en capteurs capables de surveiller les comportements du trafic et d'identifier les anomalies de performance.

Voici comment NetFlow contribue spécifiquement à cette détection :

- **Analyse comportementale paramétrée** : NetFlow peut être configuré pour effectuer une analyse comportementale du réseau et alerter le centre d'opérations de sécurité (SOC) en cas de zones critiques, telles que les intrusions ou la **saturation des systèmes**.
- **Détection statistique des anomalies** : Cette méthode, aussi appelée détection comportementale, recherche des tendances anormales dans le trafic réseau. Elle permet d'identifier des **pics de bande passante** ou des variations de trafic à des heures inhabituelles, qui sont des indicateurs directs de saturation ou de surcharge.
- **Alertes sur la surcharge des systèmes critiques** : Une fois qu'une base de référence (baseline) du réseau est établie, les outils NetFlow peuvent générer des alertes spécifiques en cas de **surcharge des systèmes internes critiques** ou de violation des zones de sécurité.
- **Identification de la congestion à long terme** : NetFlow permet de prendre en compte les pics de trafic à plus long terme, comme ceux causés par des attaques par déni de service distribué (DDoS) ou une **congestion du réseau** importante, en analysant l'écart moyen par rapport au trafic normal.
- **Surveillance du débit entre sites** : En surveillant le débit entre différents emplacements physiques ou logiques, NetFlow aide à visualiser si un segment du réseau est proche de ses limites de capacité.

En résumé, NetFlow offre au SOC une visibilité étendue sur tout élément gérant le trafic, permettant de détecter des saturations qui pourraient passer inaperçues si l'on se contentait de surveiller uniquement les points de contrôle de sécurité dédiés.

Comment NetFlow identifie-t-il les intrusions sur le réseau ?

NetFlow identifie les intrusions sur le réseau principalement grâce à une approche de **détection statistique des anomalies**, également appelée **analyse comportementale**. Contrairement aux systèmes basés sur des signatures, NetFlow transforme les équipements réseau en capteurs qui surveillent les tendances du trafic pour repérer des activités suspectes. Voici les mécanismes clés utilisés pour identifier les intrusions :

- **Analyse comportementale et base de référence** : Les outils NetFlow surveillent le comportement du réseau pendant une période donnée (généralement au moins une semaine) pour établir une **base de référence** (*baseline*) de ce qui est considéré comme un trafic normal. Une fois cette base établie, des algorithmes détectent les écarts significatifs qui pourraient indiquer une intrusion.
- **Indicateurs d'anomalies** : Le système génère des alertes lorsqu'il détecte des comportements alarmants tels que :
 - Des **pics de bande passante** soudains.
 - L'utilisation de **ports inhabituels**.
 - Des variations de trafic à des **heures inhabituelles**.
 - Des tentatives de **reconnaissance** ou de balayage de ports (*port scanning*).
- **Surveillance des zones de sécurité** : NetFlow peut être paramétré pour surveiller des segments spécifiques du réseau. Il identifie les intrusions en détectant des **viols de zones de sécurité**, comme lorsqu'un hôte tente d'accéder à un système sensible sans autorisation (ce que certains outils appellent une « violation du verrouillage hôte »).
- **Détection d'attaques sans signature (Zero-day)** : Comme NetFlow se concentre sur le comportement plutôt que sur des schémas d'attaque connus, il est particulièrement efficace pour identifier les **intrusions « Day zéro »** ou les menaces sophistiquées qui n'ont pas encore de signature officielle.
- **Identification de la propagation de logiciels malveillants** : En analysant les flux entre les machines, NetFlow permet de visualiser comment un logiciel malveillant se propage à l'intérieur du réseau après l'intrusion initiale.
- **Communications avec des serveurs de commande (CnC)** : Certains outils couplent les données NetFlow avec des flux de

menaces pour identifier si un appareil interne communique avec des **serveurs de commande et de contrôle** connus, signe flagrant d'un système compromis.

En résumé, NetFlow agit comme un « capteur géant » qui comble les lacunes entre les points de contrôle de sécurité dédiés, permettant de valider les alertes en corrélant les comportements suspects détectés par plusieurs périphériques réseau simultanément.

Comment NetFlow établit-il sa base de référence réseau ?

NetFlow établit sa **base de référence** (*baseline*) en transformant les équipements réseau en « capteurs géants » qui surveillent en continu les tendances comportementales du trafic.

Voici les étapes et caractéristiques clés de ce processus :

- **Période d'observation** : Pour distinguer les comportements normaux des comportements anormaux, la plupart des outils NetFlow nécessitent une période d'apprentissage d'**au moins une semaine de données**.
- **Analyse statistique** : Le système s'appuie sur la **détection statistique des anomalies** (ou analyse comportementale) pour identifier les tendances habituelles du réseau.
- **Utilisation d'algorithmes** : Une fois que le comportement habituel est enregistré, des algorithmes propriétaires convertissent ces données de flux en rapports de performance et de sécurité.
- **Paramétrage de l'environnement** : Pour que la base de référence soit pertinente, il est recommandé de définir au préalable ce qui constitue le **trafic interne** et de spécifier les niveaux de sensibilité des différents segments du réseau.
- **Identification des écarts** : Une fois la base de référence établie, l'outil peut générer des alertes lorsqu'il détecte des variations significatives, telles que :
 - Des **pics de bande passante** imprévus.
 - L'utilisation de **ports inhabituels**.
 - Des flux de trafic à des **heures inhabituelles**.
 - Des violations de zones de sécurité (comme une « violation du verrouillage hôte »).

Cette approche permet à NetFlow de détecter des menaces sophistiquées, notamment des **intrusions « Day zéro »** (sans signature connue), en se basant uniquement sur la déviation par rapport au comportement normal enregistré.

Comment fonctionne la détection statistique des anomalies ?

La **détection statistique des anomalies**, également appelée **détection comportementale**, fonctionne en analysant les tendances du trafic réseau pour identifier des comportements qui s'écartent de la normale. Voici les principes clés de son fonctionnement selon les sources :

- **Établissement d'une base de référence (baseline)** : Pour distinguer le normal de l'anormal, le système doit d'abord « apprendre » le comportement habituel du réseau. La plupart des outils (comme ceux basés sur NetFlow) nécessitent une période d'observation d'**au moins une semaine de données** pour établir cette base de référence.
- **Identification d'indicateurs suspects** : Une fois la base établie, des algorithmes recherchent des anomalies statistiques telles que :
 - Des **pics de bande passante** soudains.
 - L'utilisation de **ports inhabituels**.
 - Des variations de trafic à des **heures inhabituelles**.
- **Détection de menaces inconnues** : Contrairement à la détection par signature qui ne reconnaît que des attaques déjà documentées, la détection statistique peut identifier des **intrusions « Day zéro »** ou des attaques sophistiquées en se basant uniquement sur l'anomalie du comportement.
- **Analyse multi-sources** : En utilisant des technologies comme NetFlow, le SOC peut transformer des équipements réseau standards en capteurs. Cela permet de **valider un événement** en vérifiant si plusieurs périphériques détectent simultanément un comportement anormal similaire.
- **Nécessité de paramétrage** : Pour être efficace et éviter les **fausses alertes**, cette méthode nécessite un paramétrage précis. Il est recommandé de définir clairement ce qui constitue le **trafic**

interne et de spécifier les niveaux de sensibilité pour chaque segment du réseau.

En résumé, cette approche permet de détecter des activités malveillantes après une intrusion (comme la propagation de logiciels malveillants ou la reconnaissance) en surveillant en continu les flux de données plutôt qu'en cherchant des schémas d'attaque fixes.

Comment l'analyse NetFlow complète-t-elle les journaux de pare-feu ?

L'analyse NetFlow complète les journaux de pare-feu en transformant l'ensemble de l'infrastructure réseau en un « **capteur géant** », ce qui permet d'étendre la visibilité bien au-delà des points de contrôle de sécurité traditionnels.

Voici les principales manières dont NetFlow enrichit les données issues des pare-feux :

- **Comblement des angles morts** : Les pare-feu et les systèmes IPS/IDS ont une portée limitée aux points où ils sont déployés. NetFlow permet d'utiliser des équipements réseau standards (commutateurs, routeurs), souvent dépourvus de fonctions de sécurité natives, pour **surveiller le trafic sur tout le réseau**, éliminant ainsi les zones d'ombre.
- **Validation des événements** : L'utilisation de NetFlow aide à **corrélérer et valider les alertes** générées par les produits de sécurité dédiés. La probabilité qu'un incident soit réel est renforcée si plusieurs périphériques réseau détectent un comportement similaire à celui signalé par le pare-feu.
- **Détection d'attaques sans signature (Zero-day)** : Alors que de nombreux pare-feu s'appuient sur des signatures pour bloquer des menaces connues, NetFlow se concentre sur l'**analyse comportementale**. Il peut ainsi identifier des intrusions sophistiquées ou des attaques « Day zéro » en détectant des écarts statistiques par rapport à une base de référence normale.
- **Visibilité sur les mouvements internes** : NetFlow est particulièrement efficace pour détecter des anomalies que les pare-feux pourraient ignorer, comme une **fuite de données non**

autorisée où des données quittent un système critique pour la première fois vers une destination inhabituelle. Il permet de surveiller le trafic « est-ouest » (entre serveurs internes) qui ne transite pas forcément par la passerelle de sécurité principale.

- **Identification des serveurs de commande (CnC) :** En analysant les flux de télémétrie, NetFlow peut identifier si un hôte interne communique avec des **serveurs de commande et de contrôle** connus, même si le trafic semble légitime au niveau du port utilisé (ex : port 80 ou 443).

En résumé, NetFlow apporte une **visibilité contextuelle et comportementale** à l'échelle du réseau qui vient valider, affiner et étendre les alertes locales générées par les pare-feux.

Comment configurer une période d'apprentissage pour la Baseline ?

Pour configurer une période d'apprentissage efficace afin d'établir une base de référence (**Baseline**) comportementale, les sources recommandent de suivre une méthodologie précise axée sur la durée et le paramétrage de l'environnement.

Voici les étapes clés basées sur les sources :

1. Durée de la période d'observation

Pour que les outils d'analyse comportementale (comme ceux basés sur NetFlow) puissent distinguer avec précision les comportements normaux des anomalies, ils nécessitent généralement une période d'apprentissage d'**au moins une semaine de données**.

- *Note relative au dimensionnement :* Si votre objectif est uniquement de mesurer le volume d'événements (EPS) pour dimensionner votre stockage, une période de **24 heures** peut suffire pour identifier les tendances de base entre les périodes normales et de pointe.

2. Paramétrage de l'environnement

La configuration ne se limite pas à laisser l'outil collecter des données ; vous devez l'aider à comprendre le contexte de votre réseau :

- **Définition du trafic interne** : Il est essentiel de configurer l'outil pour qu'il sache ce qui constitue le **trafic interne** par opposition au trafic externe.
- **Segmentation par zones de sécurité** : Vous devez définir des **niveaux de sensibilité** différents pour chaque segment de réseau. Par exemple, vous pouvez créer des zones « sensibles » et « non sensibles » pour permettre à l'outil de générer des alertes spécifiques, comme des violations de verrouillage d'hôte (*host lock violations*), lorsqu'un accès non autorisé est détecté.

3. Ajustement et Tuning

Une fois la base de référence établie après la période initiale, le système utilise des algorithmes pour détecter les écarts statistiques.

- **Optimisation des alertes** : Bien que certains modules (logiciels malveillants, botnets, etc.) nécessitent un **paramétrage minimal** pour être pertinents, un ajustement adéquat est crucial pour éviter les fausses alertes ou une sensibilité insuffisante face à des événements critiques.
- **Recommandations automatiques** : Certains outils avancés, comme Cisco FirePOWER, peuvent proposer des ajustements automatiques ou des listes de recommandations basées sur les vulnérabilités réellement identifiées sur vos périphériques pendant la phase d'observation.

En résumé, la configuration d'une Baseline repose sur une **collecte passive de sept jours complétés** par une **définition active des zones et du trafic de confiance** par l'administrateur.

Quelle est la différence entre NTP et SNTP ?

Selon les sources, le protocole **SNTP** (Simple Network Time Protocol) est une **version limitée du protocole NTP**, spécifiquement conçue pour les clients.

Voici les principales différences identifiées entre ces deux protocoles :

- **Rôles et capacités** : Contrairement au protocole NTP complet, les systèmes utilisant le SNTP sont **exclusivement des clients**. Cela signifie qu'ils peuvent recevoir l'heure de serveurs NTP, mais ne

peuvent pas agir eux-mêmes comme serveurs pour distribuer l'heure à d'autres équipements.

- **Précision** : Le protocole NTP est nettement plus précis. Alors que le **SNTP** fournit généralement une heure précise à **100 millisecondes** près, le **NTP** peut maintenir une précision de l'ordre de **1 milliseconde** sur la plupart des réseaux locaux (LAN) et d'environ 10 millisecondes sur des distances allant jusqu'à 2 000 km.
- **Sécurité et authentification** : Le protocole NTP offre des fonctionnalités de sécurité robustes, notamment un mécanisme d'**authentification chiffrée**. À l'inverse, le SNTP ne permet pas d'authentifier le trafic de manière native, sauf par l'utilisation de listes de contrôle d'accès (ACL) étendues.
- **Complexité de gestion du temps** : Le NTP est capable de prendre en compte des facteurs complexes tels que la latence du réseau, les erreurs d'horloge entre les hôtes et le décalage d'horloge requis, ce qui lui permet de fonctionner sur des réseaux dont la longueur du chemin n'est pas déterminée.

En raison de ces limitations, les sources recommandent d'**utiliser le protocole NTP plutôt que le SNTP** chaque fois que cela est possible afin de garantir une synchronisation optimale et sécurisée.

Comment NetFlow identifie-t-il les intrusions "Day zéro" ?

NetFlow identifie les intrusions « **Day zéro** » (ou jour zéro) en s'appuyant sur une approche de **détection statistique des anomalies**, également appelée **analyse comportementale**, plutôt que sur des signatures d'attaques connues.

Voici les mécanismes précis qui permettent cette identification :

- **Absence de signatures** : Contrairement aux systèmes traditionnels qui ne reconnaissent que les menaces déjà documentées, NetFlow ne cherche pas de schémas d'attaque fixes. Cela lui permet de détecter des menaces sophistiquées qui n'ont pas encore de signature officielle au moment de l'attaque.
- **Établissement d'une base de référence (Baseline)** : Pour identifier une anomalie, les outils NetFlow doivent d'abord «

apprendre » le comportement normal du réseau. Ce processus nécessite généralement **au moins une semaine de données** pour distinguer les tendances habituelles des comportements suspects.

- **Utilisation d'algorithmes propriétaires** : Une fois la base de référence établie, des algorithmes convertissent les données de flux en rapports de sécurité. Ces algorithmes sont conçus pour détecter des **indices ou indicateurs de risque** basés exclusivement sur le comportement du trafic.
- **Indicateurs d'anomalies** : Le système identifie l'intrusion en repérant des déviations statistiques majeures, telles que :
 - Des **pics de bande passante** soudains.
 - L'utilisation de **ports inhabituels**.
 - Des variations de trafic survenant à des **heures inhabituelles**.
- **Surveillance des flux internes** : NetFlow peut identifier une intrusion lorsqu'il détecte une activité inhabituelle après que l'attaquant a pénétré le réseau, comme une **reconnaissance** (analyse de ports par un utilisateur interne), la **propagation d'un logiciel malveillant** ou une fuite de données vers une destination inconnue.

En résumé, en transformant les équipements réseau en capteurs, NetFlow permet de détecter une attaque « Day zéro » simplement parce que le comportement généré par l'intrusion est statistiquement différent du fonctionnement normal enregistré durant la phase d'apprentissage.

Quels sont les avantages d'un SIEM pour le SOC ?

L'utilisation d'une solution de gestion des informations et des événements de sécurité (**SIEM**) offre des avantages déterminants pour l'efficacité d'un centre d'opérations de sécurité (SOC) en combinant les capacités de gestion des informations (**SIM**) et de gestion des événements (**SEM**).

Voici les principaux bénéfices détaillés dans les sources :

- **Visibilité centralisée et rapide** : Le SIEM sert de premier point de contact lors des investigations, offrant au SOC une visibilité

immédiate sur un grand nombre de systèmes. En centralisant la collecte, il permet de suivre l'intégralité des événements et d'éliminer les « angles morts » qui pourraient être exploités lors d'une attaque.

- **Corrélation avancée des données** : L'un des atouts majeurs est sa capacité à **corrélér des données issues de différents produits** ou capteurs. Cela permet de détecter des menaces sophistiquées qui passeraient inaperçues si les journaux étaient analysés de manière isolée. Par exemple, un SIEM peut affiner une alerte provenant d'un système de prévention d'intrusion (IPS) en la comparant aux informations comportementales du reste du réseau.
- **Priorisation et réponse aux incidents** : Grâce aux fonctions SEM, le SIEM consolide de grandes quantités d'événements pour permettre aux administrateurs de **prioriser les alertes critiques** et de réagir de manière appropriée et rapide aux incidents.
- **Indépendance vis-à-vis des fournisseurs** : Contrairement aux outils de gestion spécifiques à un fabricant, le SIEM est conçu pour être **indépendant du fournisseur**, ce qui lui permet d'agréger des données provenant d'infrastructures hétérogènes.
- **Gestion et normalisation des données** : Il assure le traitement de volumes massifs de journaux via la **normalisation et l'agrégation**, rendant les données hétérogènes exploitables et facilement consultables par les analystes.
- **Support aux investigations forensiques et conformité** : Le SIEM facilite l'analyse après incident (**forensic**) grâce à l'archivage, au minage de données et à la génération de rapports historiques. Ces capacités sont également essentielles pour répondre aux exigences de conservation légale et réglementaire des journaux.

En résumé, le SIEM transforme une masse de données brutes en un flux d'informations structurées et corrélées, permettant au SOC de passer d'une surveillance passive à une détection proactive des menaces.

Quelle est la durée de conservation recommandée pour les données ?

Les sources ne spécifient pas une durée de conservation unique ou universelle, mais soulignent que cette durée est une **exigence fondamentale** qui doit être définie par chaque organisation en fonction de ses besoins propres et des contraintes légales.

Voici les points clés concernant la conservation des données de journalisation selon les sources :

- **Un pilier du dimensionnement** : La définition des exigences de conservation est l'une des trois questions essentielles (avec le nombre d'appareils et l'EPS) pour dimensionner correctement une solution de collecte de données. Elle influence directement les besoins de stockage à court et à long terme.
- **Contraintes légales et réglementaires** : La durée de conservation est souvent dictée par la loi ou des normes spécifiques. Par exemple, les organisations soumises à la norme **PCI DSS** (secteur bancaire) ou à la **directive européenne NIS** doivent respecter des obligations précises en matière de protection et de déclaration des journaux.
- **Analyse après incident (Forensic)** : Il est impératif de conserver les fichiers journaux suffisamment longtemps pour pouvoir les utiliser lors de **procédures civiles ou pénales** suite à un incident de sécurité.
- **Planification budgétaire** : Lors de l'évaluation du coût total d'un projet de SIEM, les sources suggèrent de prendre en compte une période de référence, par exemple **5 ans**, pour anticiper les coûts de stockage et de maintenance sur la durée.
- **Capacités techniques** : Lors du choix d'un outil, il convient de vérifier combien de temps les données peuvent rester sur le serveur avant d'être exportées et s'il est facile de réintégrer d'anciennes données pour analyse.

En résumé, bien qu'une période de **5 ans** soit mentionnée comme exemple pour le calcul du coût total de possession (TCO), la durée réelle doit être ajustée selon le niveau de risque et les obligations de conformité de l'entreprise.

Quelles sont les quatre licences disponibles pour Cisco FirePOWER ?

Selon les sources, bien que le texte introduise initialement « trois options de licence différentes », il détaille en réalité **quatre catégories de licences ou d'abonnements** pour les services Cisco FirePOWER :

- **Visibilité et contrôle des applications (AVC)** : Cette licence est **incluse par défaut** dans le système. Elle permet de gérer plus de 3 000 contrôles de couche application et de risque, tout en offrant une visibilité sur les utilisateurs, les sites web et les géolocalisations.
- **Abonnement de filtrage d'URL** : Cette option permet de filtrer plus de **280 millions de domaines** de premier niveau, classés dans plus de 82 catégories selon leur niveau de risque. Elle peut être acquise seule ou au sein de forfaits combinés.
- **Abonnement IPS (Système de prévention des intrusions)** : Cette licence fournit une protection contre les menaces et une **connaissance contextuelle** complète de l'infrastructure, des applications et des utilisateurs pour automatiser la réponse de défense.
- **Abonnement AMP (Advanced Malware Protection)** : Cette licence assure une protection réseau intégrée contre les **logiciels malveillants sophistiqués**. Elle permet notamment l'analyse rétrospective des fichiers pour identifier l'origine d'une infection.

Ces licences peuvent être ajoutées individuellement ou sous forme d'offres groupées (par exemple, une combinaison IPS, AMP et filtrage d'URL). Il est également précisé que la console de gestion **FMC** (FirePOWER Management Center) dispose de sa propre licence de base pour les fonctions de connexion et de configuration standard.

Comment fonctionne l'analyse rétrospective de la licence AMP ?

L'analyse rétrospective, associée à la licence **Cisco AMP (Advanced Malware Protection)**, est une fonctionnalité de sécurité avancée qui

permet de détecter et de traiter des menaces ayant réussi à franchir les premières lignes de défense.

Voici comment elle fonctionne selon les sources :

1. Surveillance continue et évolution du risque

Contrairement à une analyse ponctuelle, la **rétropection des fichiers** consiste en une **analyse continue** des fichiers présents sur le réseau.

Puisque le niveau de menace d'un fichier peut évoluer avec le temps (un fichier jugé "sain" aujourd'hui peut s'avérer malveillant demain), le système surveille constamment son comportement.

2. Traçabilité par hachage SHA-256

Lorsqu'une menace est identifiée a posteriori, le système utilise l'empreinte numérique unique du fichier (**le hachage SHA-256**) pour retracer son parcours exact. Cela permet de :

- **Identifier le point d'entrée** : Retrouver précisément comment le fichier a pénétré le réseau (par exemple, via un téléchargement par navigateur Web).
- **Identifier le "Patient Zéro"** : Déterminer quel utilisateur ou appareil a introduit l'infection initialement.
- **Cartographier l'infection** : Recenser l'intégralité des systèmes du réseau qui hébergent ou ont exécuté ce fichier spécifique.

3. "Remonter le temps" pour la remédiation

Cette approche, qualifiée de **sécurité rétrospective**, permet aux analystes du SOC de remonter le temps pour comprendre l'intégralité du cycle de vie d'une menace. Une fois l'intrusion confirmée :

- **Alertes automatiques** : Le FirePOWER Management Center (FMC) peut générer des alertes spécifiques pour les événements de logiciels malveillants rétrospectifs.
- **Remédiation** : Si la solution **AMP pour les terminaux** est installée, elle peut assurer la **remédiation automatique** des menaces détectées rétrospectivement en mettant les fichiers en quarantaine sur les hôtes infectés.

En résumé, l'analyse rétrospective transforme la protection contre les logiciels malveillants d'un simple filtrage à l'entrée en un système de surveillance permanent capable de corriger les infections après leur apparition.

Comment fonctionne la remédiation automatique avec AMP ?

La **remédiation automatique** avec Cisco AMP repose principalement sur l'interaction entre les différentes versions de la solution, en particulier grâce à **AMP pour les terminaux** (AMP for Endpoints).

Voici comment ce processus fonctionne selon les sources :

- **Action d'AMP pour les terminaux** : Cette version de la solution nécessite l'installation d'un connecteur léger sur les appareils hôtes (ordinateurs portables, tablettes, etc.). Elle est capable d'assurer la **remédiation automatique** des menaces qu'elle détecte elle-même, mais aussi de celles identifiées par **AMP pour les réseaux**.
- **Mise en quarantaine** : Le mécanisme principal de remédiation consiste à **mettre en quarantaine** automatiquement les fichiers identifiés comme malveillants sur les systèmes infectés. Cela permet de neutraliser la menace immédiatement sans intervention manuelle de l'analyste.
- **Synergie avec l'analyse rétrospective** : Lorsqu'un fichier est identifié comme malveillant a posteriori (sécurité rétrospective), le système utilise le hachage **SHA-256** pour identifier tous les systèmes hébergeant ce fichier et peut alors déclencher les mesures de remédiation sur l'ensemble du parc.
- **Automatisation via Cisco ISE** : Les sources mentionnent également une forme de remédiation automatisée plus large via l'intégration avec **Cisco ISE** (Identity Services Engine). Dans ce cas, un outil comme StealthWatch peut demander à ISE de **mettre en quarantaine les appareils** présentant un indice de risque élevé (appareils compromis), ce qui améliore considérablement le temps de réaction aux menaces.

En résumé, la remédiation automatique transforme la détection en une réponse active, permettant de passer de la simple identification d'un logiciel malveillant à sa neutralisation physique par mise en quarantaine immédiate du fichier ou de l'appareil.

Comment installer le connecteur AMP sur un poste hôte ?

D'après les sources fournies, les étapes techniques détaillées (comme une liste de commandes ou une procédure de clic) pour l'installation physique du connecteur sur un système d'exploitation spécifique ne sont pas décrites. Cependant, le document apporte les précisions suivantes sur les modalités de son déploiement :

- **Nature du logiciel** : L'installation d'un **connecteur léger** (*lightweight connector*) est requise sur les appareils hôtes, tels que les ordinateurs portables et les tablettes.
- **Gestion centralisée** : La solution AMP pour les terminaux est **gérée via le cloud** sous la forme d'**ensembles d'agents** pour les terminaux.
- **Visibilité** : Une fois le connecteur en place, il offre une visibilité sur **toutes les applications et tous les processus** de l'appareil.
- **Cas des appareils mobiles** : Pour les terminaux mobiles, la stratégie de gestion nécessite l'installation d'un agent qui implique que le propriétaire de l'appareil **consente à l'administration** de son terminal par le système de sécurité.

Les sources se concentrent principalement sur le fonctionnement de la télémétrie et l'exportation des journaux vers un SIEM, plutôt que sur les guides d'installation logicielle individuelle pour les utilisateurs finaux.

Comment l'intégration avec Cisco ISE améliore-t-elle la réponse aux menaces ?

L'intégration avec **Cisco ISE** (Identity Services Engine) améliore la réponse aux menaces principalement en apportant un contexte précis sur les terminaux et en permettant une **remédiation automatisée**.

Selon les sources, voici comment cette intégration optimise le travail du SOC :

- **Enrichissement du contexte de l'appareil** : ISE permet de dépasser la simple adresse IP en fournissant des informations détaillées sur l'appareil, telles que son **système d'exploitation** et **l'identité de l'utilisateur** associé. Il peut déterminer précisément si un appareil est, par exemple, un iPad ou un iPhone en analysant divers attributs réseau comme ARP, DHCP et DNS.

- **Visibilité accrue** : Ces informations de contexte sont transmises à des outils de surveillance (comme StealthWatch), permettant d'étiqueter les flux réseau avec le type d'appareil et l'adresse MAC de l'hôte surveillé. Cela facilite grandement l'identification du « patient zéro » lors d'une investigation.
- **Mise en quarantaine automatisée** : L'aspect le plus critique pour la réponse aux incidents est la capacité d'ISE à **isoler ou mettre en quarantaine** automatiquement les appareils présentant un indice de risque élevé. Lorsqu'un outil d'analyse détecte qu'un hôte est probablement compromis, il peut demander à ISE de restreindre immédiatement son accès au réseau.
- **Optimisation du temps de réaction** : En automatisant la remédiation, le SOC réduit considérablement le délai entre la détection d'une menace et sa neutralisation physique. Cette réactivité est essentielle pour stopper la propagation d'attaques sophistiquées ou de logiciels malveillants au sein de l'infrastructure.

Comment AMP permet-il l'analyse rétrospective par hachage ?

Cisco AMP (Advanced Malware Protection) permet l'analyse rétrospective en s'appuyant sur une surveillance continue et l'utilisation d'identifiants uniques pour chaque fichier. Voici comment ce processus fonctionne :

- **Surveillance continue** : L'une des fonctionnalités clés d'AMP est la « **rétrospection des fichiers** ». Contrairement à une analyse ponctuelle, AMP effectue une analyse continue des fichiers afin de détecter toute évolution de leur niveau de menace au fil du temps.
- **Utilisation du hachage SHA-256** : Lorsqu'une intrusion est détectée ou qu'un fichier précédemment jugé sain est identifié comme malveillant, le système utilise le **hachage SHA-256** associé à ce fichier. Ce hachage sert d'empreinte numérique unique permettant de tracer précisément le fichier à travers tout le réseau.
- **Sécurité rétrospective** : Cette approche, appelée « sécurité rétrospective », permet aux analystes de « remonter le temps »

pour identifier l'intégralité du cycle de vie d'une menace. Grâce au hachage, le système peut :

- Identifier le **point d'entrée** exact du fichier sur le réseau.
- Recenser tous les **systèmes infectés** (hôtes) qui hébergent actuellement le fichier.
- **Identification du « Patient Zéro »** : En examinant la chronologie de l'attaque, le SOC peut identifier la première personne ayant introduit l'infection sur le réseau (le **patient zéro**) ainsi que la méthode utilisée (par exemple, un téléchargement via un navigateur web).

En résumé, le hachage SHA-256 agit comme un fil d'Ariane qui permet à AMP de transformer une détection tardive en une visibilité complète sur la propagation historique de la menace.

Quelles sont les différences entre les générations de Cisco ASA ?

Les sources distinguent deux générations principales pour la plateforme **Cisco Adaptive Security Appliance (ASA)**, lancée initialement en 2005 pour remplacer les pare-feu PIX et les concentrateurs VPN 3000. Voici les différences majeures entre ces deux générations :

1. Première génération (Série ASA 5500)

- **Architecture modulaire physique** : Cette génération se caractérise par la présence d'un **emplacement physique (slot)** permettant d'insérer différents modules de sécurité matériels.
- **Fonctionnalités** : Ces modules physiques étaient nécessaires pour ajouter des capacités spécifiques telles que la prévention des intrusions (IPS) ou des solutions antimalware.
- **Exemple** : L'ASA 5520 est cité comme un modèle représentatif de cette première génération disposant d'un slot pour module supplémentaire.

2. Deuxième génération (Série ASA 5500-X)

- **Architecture virtualisée** : Contrairement à la première génération, la série 5500-X ne dispose **plus d'emplacements pour modules physiques**.
- **Espace virtualisé interne** : Les fonctionnalités de sécurité supplémentaires (pare-feu applicatif, IPS, protection contre les

logiciels malveillants) s'exécutent désormais dans un **espace virtualisé interne** au processeur.

- **Services FirePOWER** : C'est sur cette génération qu'ont été introduits les services **FirePOWER**, d'abord sous forme d'option logicielle utilisant cet espace virtualisé.
- **Gestion du trafic** : Le flux de trafic entre le logiciel ASA de base et le module de sécurité virtualisé est géré logiquement à l'aide de cartes de stratégie (*policy maps*).

En résumé, le passage à la deuxième génération (série X) a marqué la transition d'une extension de sécurité par **matériel dédié (modules)** vers une extension par **logiciels virtualisés**, simplifiant ainsi la conception physique de l'appareil tout en permettant l'intégration de services plus sophistiqués comme FirePOWER.

Comment configurer un serveur syslog sous Ubuntu pour tester l'EPS ?

Pour configurer un serveur syslog sous Ubuntu afin de mesurer votre EPS (Événements Par Seconde), les sources recommandent d'utiliser l'application **syslog-ng**. Cette méthode permet d'identifier les tendances de journalisation sur une période de **24 heures** afin de capturer les périodes normales et de pointe.

Voici les étapes de configuration détaillées dans les sources :

1. Installation de l'application

Ouvrez un terminal sur votre système Ubuntu (les sources utilisent la version 15.04 par défaut) et saisissez les commandes suivantes pour installer l'outil :

- `sudo apt-get update`
- `sudo apt-get upgrade`
- **`sudo apt-get install syslog-ng`**

Note : Une connexion Internet est nécessaire pour le téléchargement.

2. Édition du fichier de configuration

Utilisez un éditeur de texte tel que **nano** pour modifier le fichier de configuration principal :

```
sysadmin@ubuntu:~$ sudo nano /etc/syslog-ng/syslog-ng.conf
```

3. Paramétrage des règles de collecte

À l'intérieur du fichier, vous devez définir quatre éléments clés pour diriger le trafic (en utilisant par exemple l'IP du serveur 192.168.1.200 et celle d'un pare-feu source 192.168.1.50) :

- **Définir la source** : Spécifiez l'adresse IP du serveur et le port d'écoute (généralement UDP 514) : `source source_example { udp(ip(192.168.1.200) port (514)) ; } ;`
- **Appliquer un filtre** : Pour ne conserver que les messages provenant du périphérique spécifique que vous testez : `filter filter_example { host ("192.168.1.50") ; } ;`
- **Spécifier la destination** : Indiquez le chemin du fichier où les journaux seront stockés : `destination destination_example { file("/var/log/eventdata.log"); } ;`
- **Combiner les règles** : Liez la source, le filtre et la destination dans une instruction log : `log { source ( source_example ) ; filter( filter_example ) ; destination ( destination_example ) ; } ;`

4. Redémarrage du service

Une fois le fichier enregistré, redémarrez le processus pour appliquer les changements :

```
sysadmin@ubuntu:~$ sudo /etc/init.d/syslog-ng restart
```

Une fois le serveur opérationnel, laissez-le collecter des données pendant une journée complète. Vous pourrez ensuite utiliser le volume total d'événements capturés dans le fichier `/var/log/eventdata.log` pour calculer votre EPS normal et de pointe à l'aide des formules de dimensionnement.

Expliquer le calcul de l'EPS de pointe

Le calcul de l'**EPS de pointe** (Événements Par Seconde de pointe) est une étape cruciale pour dimensionner correctement une solution de collecte de données et éviter que le système ne tombe en panne lors d'un incident de sécurité majeur.

Voici les étapes et les formules détaillées pour effectuer ce calcul :

1. Les composantes du calcul

Pour obtenir une valeur réaliste, vous devez d'abord estimer ou mesurer trois facteurs clés :

- **Le nombre de pics attendus** : Il s'agit d'une estimation basée sur l'activité habituelle du réseau. Une valeur par défaut recommandée est de **trois**, correspondant aux connexions du matin, au retour du déjeuner et à la fermeture en fin de journée.
- **La durée d'un pic** : Elle représente la durée estimée de chaque pic d'activité. Une valeur par défaut appropriée est d'**une heure** (soit 3 600 secondes).
- **Le facteur d'écart** : C'est le coefficient multiplicateur par rapport à l'EPS normal lors d'un événement inhabituel (attaque DDoS, congestion, etc.). Il est généralement situé entre **deux et cinq fois l'EPS normal**.

2. Les formules de calcul

Le calcul s'effectue en deux temps :

A. Calcul de l'EPS de pointe total par jour : On multiplie l'activité normale par les facteurs de pointe sur une journée complète.

EPS de pointe total par jour = EPS normal × Nombre de pics attendus × Durée d'un pic (en secondes) × Facteur d'écart

B. Calcul de l'EPS de pointe final : Puisqu'une journée compte 86 400 secondes, on divise le total quotidien pour obtenir la valeur par seconde.

EPS de pointe = EPS de pointe total par jour / 86 400

3. Recommandation de sécurité

Les sources soulignent que, quel que soit le résultat obtenu, il est fortement conseillé d'intégrer une **marge de sécurité d'au moins 20 %**. Cette marge garantit que la solution dispose d'une puissance de traitement et d'un espace de stockage suffisants pour gérer les imprévus sans perte de données précieuses.

En cas de doute sur les chiffres, il est préférable de **surestimer les valeurs** lors de la conception initiale plutôt que de risquer un sous-dimensionnement critique.

Qu'est-ce qu'une violation du verrouillage hôte ?

Une **violation du verrouillage hôte** (*host lock violation*) est une alerte spécifique générée par l'outil de surveillance **StealthWatch** lorsqu'il détecte un **accès non autorisé** vers ou depuis un segment du réseau défini comme une **zone de sécurité sensible**.

Voici les points clés pour comprendre ce concept selon les sources :

- **Segmentation et zones de confiance** : Pour identifier ces violations, l'administrateur doit configurer l'outil NetFlow pour qu'il comprenne l'environnement surveillé en définissant des niveaux de sensibilité différents pour chaque segment de réseau (par exemple, une zone « sensible » et une zone « non sensible »).
- **Détection comportementale** : Cette alerte repose sur l'analyse NetFlow. En surveillant les flux de trafic, le système peut identifier si une adresse IP tente de communiquer avec un système interne critique au mépris des règles de segmentation établies.
- **Sécurité des zones critiques** : L'objectif est de réagir immédiatement dès qu'un hôte tente de franchir les limites d'une zone protégée, ce qui permet au SOC de détecter des intrusions ou des mouvements latéraux suspects au sein du réseau.

En résumé, il s'agit d'un mécanisme de détection comportementale qui transforme les équipements réseau en capteurs capables de signaler toute tentative de violation des zones de sécurité internes.

Comment StealthWatch utilise-t-il NetFlow pour ces violations ?

StealthWatch utilise la télémétrie **NetFlow** pour identifier les **violations du verrouillage hôte** en transformant les équipements réseau standards (commutateurs, routeurs) en un « capteur géant » capable de surveiller l'intégralité du trafic.

Voici comment ce processus fonctionne précisément :

- **Configuration de zones de sécurité** : L'efficacité de StealthWatch repose sur le paramétrage de l'environnement surveillé. L'administrateur doit définir ce qui constitue le **trafic interne** et segmenter le réseau en zones avec différents **niveaux de sensibilité**, par exemple en distinguant une « zone sensible » d'une « zone non sensible ».
- **Analyse par algorithmes propriétaires** : StealthWatch utilise des **algorithmes propriétaires** pour analyser le trafic NetFlow standard. Ces algorithmes recherchent des comportements malveillants, appelés **indices ou indicateurs de risque**, sans se baser sur des signatures d'attaques connues.

- **Détection d'accès non autorisés** : Une « violation du verrouillage hôte » est déclenchée spécifiquement lorsque le système détecte, via les flux NetFlow, un **accès non autorisé** vers ou depuis l'un des segments de réseau définis comme sensibles.
- **Validation et corrélation** : L'utilisation de NetFlow permet également de **valider l'événement**. La probabilité qu'une violation soit réelle est renforcée si plusieurs périphériques réseau détectent simultanément un comportement similaire, offrant ainsi une visibilité plus large qu'un simple point de contrôle de sécurité dédié.

En résumé, StealthWatch agit comme un outil d'analyse comportementale qui interprète les données NetFlow pour faire respecter les politiques de segmentation interne du réseau.

Qu'est-ce que le niveau de strate dans le protocole NTP ?

Le **niveau de strate** (souvent appelé *stratum*) dans le protocole NTP représente la distance hiérarchique entre un équipement et la source de temps primaire faisant autorité.

Voici les caractéristiques principales de ce système de mesure :

- **Indicateur de distance (sauts)** : Le numéro de strate indique précisément le **nombre de sauts NTP** qui séparent un client de la source de temps originelle. Cette source primaire est généralement une horloge atomique ou radio connectée directement à un serveur de temps.
- **Sélection de la source la plus proche** : Les clients NTP utilisent ce numéro pour identifier la source de temps la plus proche de la racine hiérarchique. En règle générale, plus le **numéro de strate est bas**, plus le serveur est considéré comme proche de la source de temps faisant autorité.
- **Hiérarchie et mode maître** : Lors de la configuration d'un périphérique (comme un routeur ou un commutateur Cisco) pour qu'il agisse en tant que serveur NTP maître pour le reste du réseau, l'administrateur doit lui attribuer manuellement un numéro de strate (par exemple, la valeur 3).

- **Limites de la priorité par strate** : Bien qu'un niveau de strate inférieur soit privilégié, le protocole NTP ne se synchronisera pas aveuglément avec une source uniquement sur ce critère. Il compare l'heure transmise par plusieurs systèmes et rejettera une source dont l'heure est incohérente avec les autres, même si son numéro de strate est plus avantageux.

Cette organisation en couches successives permet d'assurer une synchronisation précise et ordonnée à travers l'ensemble du réseau.

Quels ports UDP sont utilisés pour la synchronisation horaire ?

Selon les sources, le protocole principalement utilisé pour la synchronisation horaire est le **NTP** (Network Time Protocol), qui fonctionne sur le protocole **UDP** en utilisant le **port 123** pour la source et la destination.

Voici quelques précisions complémentaires sur les protocoles de temps mentionnés :

- **NTP** : Il utilise ce port pour synchroniser l'heure avec une source faisant autorité (comme une horloge atomique) et la distribuer sur le réseau.
- **SNTP (Simple Network Time Protocol)** : Bien qu'il s'agisse d'une version limitée du NTP réservée aux clients, il s'appuie sur la même infrastructure pour recevoir l'heure des serveurs NTP.
- **Précision** : L'utilisation de ces protocoles sur le port UDP 123 permet d'atteindre une précision de l'ordre de la **milliseconde** sur la plupart des réseaux locaux (LAN) et d'environ 10 millisecondes sur de très longues distances.

Il est essentiel de s'assurer que ce port est ouvert et que la synchronisation est active, car un décalage temporel, même minime, peut invalider les alertes de sécurité et perturber la corrélation des journaux au sein d'un SOC.

Comment calculer précisément l'EPS avec la formule de base ?

Pour calculer précisément l'**EPS** (Événements Par Seconde) à l'aide de la formule de base, vous devez diviser le volume d'activité par le temps écoulé.

Voici la méthodologie et les calculs détaillés selon les sources :

1. La formule de base

Pour un trafic normal, le calcul est le suivant :

EPS = Nombre d'événements système / Période en secondes.

2. Comment obtenir des données précises

Puisqu'il n'existe pas de tableau officiel par fournisseur, la méthode la plus fiable consiste à mesurer l'activité réelle. Les sources recommandent :

- D'installer un **serveur syslog** (comme syslog-ng sur Ubuntu).
- De collecter les journaux pendant une période de **24 heures** afin d'identifier les tendances normales et les périodes de pointe.

3. Le calcul de l'EPS de pointe (Peak EPS)

Une fois l'EPS normal établi, il est crucial de calculer l'EPS de pointe pour éviter une panne du système lors d'un incident. Ce calcul se fait en deux étapes :

A. Calcul du volume de pointe quotidien :

EPS de pointe total par jour = EPS normal × Nombre de pics attendus × Durée d'un pic (en secondes) × Facteur d'écart.

- *Nombre de pics par défaut* : 3 (matin, midi, soir).
- *Durée d'un pic par défaut* : 1 heure (3 600 secondes).
- *Facteur d'écart type* : entre 2 et 5 fois l'EPS normal.

B. Conversion en EPS final : Comme une journée contient 86 400 secondes, on divise le total par ce nombre :

EPS de pointe = EPS de pointe total par jour / 86 400.

4. Marge de sécurité

Pour garantir que votre solution de collecte dispose d'une puissance de traitement suffisante, il est fortement recommandé d'ajouter une **marge d'au moins 20 %** à vos résultats finaux. En cas de doute, il est préférable de surestimer ces chiffres lors de la conception initiale pour prévoir la croissance future du réseau.

Quels sont les niveaux d'impact des alertes d'intrusion FirePOWER ?

Les alertes d'intrusion dans Cisco FirePOWER utilisent des **indicateurs d'impact** pour qualifier la pertinence et la gravité d'un événement par rapport aux cibles présentes sur le réseau.

Voici les cinq niveaux d'impact possibles, tels que détaillés dans les sources :

- ** (0) Inconnu : Ni l'hôte source ni l'hôte de destination ne se trouvent sur un réseau surveillé.
- ** (1) Vulnérable : L'hôte source ou de destination présente une vulnérabilité identifiée et est potentiellement compromis.
- ** (2) Potentiellement vulnérable : L'hôte source ou de destination utilise un protocole d'application serveur.
- ** (3) Actuellement non vulnérable : L'hôte source ou de destination n'a pas le port ouvert ou n'utilise pas le protocole.
- ** (4) Cible inconnue : L'hôte source ou de destination se trouve sur le réseau surveillé, mais n'est pas référencé dans la carte réseau.

Ces indicateurs permettent au centre d'opérations de sécurité (SOC) de générer des notifications spécifiques (par e-mail, syslog ou SNMP) uniquement lorsque certains niveaux d'impact critiques sont atteints, optimisant ainsi le traitement des alertes.

Comment FirePOWER identifie-t-il les hôtes sur le réseau ?

Cisco FirePOWER identifie les hôtes sur le réseau principalement grâce à une fonctionnalité appelée **découverte réseau** (*Network Discovery*), qui permet de créer et de maintenir un profil actualisé de l'infrastructure. Voici les mécanismes et les informations utilisés pour cette identification :

- **Surveillance du trafic** : Le système surveille passivement le flux de données circulant sur le réseau pour déterminer le nombre et les **types d'hôtes** présents.
- **Attributs identifiés** : En analysant le trafic, FirePOWER est capable d'identifier automatiquement les **systèmes**

d'exploitation, les **applications actives** et les **ports ouverts** sur chaque machine. Ces informations permettent de dresser une carte précise des actifs du réseau.

- **Identification des utilisateurs** : En plus des machines, FirePOWER peut identifier les utilisateurs en configurant un **agent utilisateur** (*user agent*) qui surveille les données de connexion et l'activité spécifique des individus.
- **Règles de découverte** : L'administrateur peut affiner ce processus via le FirePOWER Management Center (FMC) en créant des **règles de découverte**. Ces règles permettent de spécifier :
 - Des plages d'adresses réseau ou des zones spécifiques à surveiller.
 - L'exclusion de certains ports.
 - L'inclusion ou l'exclusion explicite des hôtes, des utilisateurs ou des applications dans le processus de découverte.
- **Alertes de détection** : Le système peut générer des notifications (par exemple via syslog) dès qu'un **nouveau périphérique** est détecté, particulièrement sur une portion sensible du réseau.

Cette visibilité est ensuite exploitée par le FMC pour profiler le trafic, évaluer la conformité du réseau et adapter automatiquement les politiques de sécurité (comme l'IPS) en fonction des vulnérabilités réelles des hôtes identifiés.

Comment fonctionne l'agent utilisateur pour suivre les individus ?

L'**agent utilisateur** (User Agent) est une fonctionnalité spécifique de Cisco FirePOWER conçue pour assurer la visibilité et le suivi des individus au sein du réseau.

Voici comment il fonctionne selon les sources :

- **Surveillance des connexions** : L'agent utilisateur est configuré pour surveiller l'activité des utilisateurs, en se concentrant particulièrement sur les **données de connexion** (*login data*).
- **Découverte réseau et profilage** : Il s'intègre au processus de « découverte réseau » de FirePOWER. En plus d'identifier les hôtes

et les applications, il permet d'inclure les **identités réelles** des individus dans le profil actualisé du réseau.

- **Enrichissement des données de journalisation** : Grâce à cet agent, les pare-feux applicatifs peuvent fournir des informations très détaillées au SOC. Par exemple, au lieu de voir simplement une adresse IP, le système peut identifier qu'un **utilisateur spécifique** (nommé) utilise un système d'exploitation précis pour accéder à une application particulière via un navigateur web.
- **Gestion des politiques et conformité** : Les données collectées par l'agent utilisateur permettent de profiler le trafic et de réagir efficacement aux **violations de politiques** en identifiant précisément quel individu est impliqué dans un événement de sécurité.

Dans le cas particulier des **appareils mobiles** (via des solutions MDM), le suivi par agent nécessite généralement l'installation d'un logiciel sur le terminal, ce qui implique que le propriétaire de l'appareil **consente à l'administration** de son terminal par le système de sécurité.

Peut-on automatiser l'envoi des rapports FMC ?

Oui, il est possible d'automatiser l'envoi de certaines informations sous forme de notifications par e-mail, et les sources précisent que les **tableaux de bord du FMC peuvent être exportés sous forme de rapports**.

Voici comment l'automatisation et l'exportation sont abordées dans les sources :

- **Génération automatique d'e-mails** : Le FMC peut être configuré pour générer automatiquement un e-mail (ou une trap SNMP / un message syslog) dès qu'un événement spécifique survient. Les types d'événements couverts sont :
 - Les événements de **logiciels malveillants** (réseau ou rétrospectifs).
 - Les événements de **connexion** déclenchés par des règles de contrôle d'accès préconfigurées.
 - Les événements d'**intrusion**.

- **Configuration des réponses aux alertes** : Pour automatiser ces envois, vous devez d'abord créer une « **réponse à une alerte** » dans le FMC pour définir la destination (l'adresse e-mail) et le mode d'envoi. Une fois créée, cette réponse doit être associée à l'événement déclencheur.
- **Exportation des tableaux de bord** : Le FMC permet de créer des tableaux de bord personnalisés (par exemple sur les menaces IPS ou les performances réseau) qui peuvent ensuite être **exportés sous forme de rapports**.
- **Alertes par indicateur d'impact** : Il est également possible d'automatiser l'envoi de notifications par e-mail basées sur le **niveau d'impact** d'une intrusion (par exemple, ne recevoir un e-mail que si l'impact est de niveau 1 « Vulnérable »).

En résumé, bien que les sources mettent l'accent sur l'envoi automatisé d'alertes par e-mail en réponse à des événements de sécurité, elles confirment que les données consolidées dans les tableaux de bord sont exportables en tant que rapports.

Comment installer l'agent utilisateur FirePOWER sur Active Directory ?

D'après les sources fournies, les **étapes techniques précises** (comme le téléchargement d'un fichier .exe ou la configuration spécifique des permissions sur le serveur Windows) pour installer l'agent utilisateur sur Active Directory ne sont pas détaillées.

Cependant, les sources apportent les précisions suivantes sur le rôle et le fonctionnement de cet agent dans l'écosystème FirePOWER :

- **Rôle de l'agent** : L'agent utilisateur est configuré pour surveiller l'activité des utilisateurs en collectant spécifiquement les **données de connexion** (*login data*).
- **Intégration à la découverte réseau** : Il fait partie du processus de « découverte réseau » de FirePOWER. En haut des règles de découverte dans le **FirePOWER Management Center (FMC)**, l'administrateur a la possibilité de cocher une case pour inclure les « utilisateurs » dans la collecte de données.

- **Visibilité centralisée** : Une fois les données collectées par l'agent, elles sont transmises au FMC, qui devient le point central pour l'affichage des rapports. Cela permet au SOC de voir, par exemple, le nom d'un utilisateur associé à une adresse IP spécifique et à un système d'exploitation.
- **Alternative mentionnée (StealthWatch)** : Pour des besoins similaires de corrélation d'identité, les sources mentionnent que l'outil StealthWatch utilise un serveur nommé **StealthWatch Identity** pour intégrer des annuaires comme **Active Directory** ou LDAP. Cette intégration permet de lier les adresses IP aux identités des utilisateurs.

En résumé, si les sources confirment que l'agent doit être configuré pour extraire les données de connexion afin d'identifier les individus, elles ne décrivent pas la procédure d'installation logicielle proprement dite sur le contrôleur de domaine Active Directory.

Comment FirePOWER évalue-t-il la vulnérabilité d'un hôte (Impact 1) ?

Pour évaluer si un hôte mérite le niveau **Impact 1 (Vulnérable)**, Cisco FirePOWER croise les informations d'une intrusion détectée avec l'état réel de la cible sur le réseau.

Voici les mécanismes précis utilisés pour cette évaluation :

1. La Découverte réseau (Network Discovery)

Avant toute alerte, FirePOWER maintient une **carte réseau** à jour en surveillant passivement le trafic. Il identifie pour chaque hôte :

- Le système d'exploitation.
- Les applications actives.
- Les ports ouverts.

2. L'Analyse des vulnérabilités

Pour qualifier l'impact de niveau 1, le système doit confirmer que l'hôte présente une faiblesse spécifique. Il utilise pour cela deux méthodes :

- **Scanner intégré** : FirePOWER possède son propre scanner de vulnérabilités pour identifier les systèmes potentiellement exploitables.

- **Importation tierce** : Il peut également intégrer les résultats d'analyses provenant de produits tiers spécialisés.

3. Corrélation et Recommandations

Lorsqu'un événement d'intrusion est détecté par une signature IPS, le **FirePOWER Management Center (FMC)** compare cette menace avec le profil de l'hôte :

- **Impact 1 (Vulnérable)** : Si l'attaque correspond à une vulnérabilité effectivement identifiée sur l'hôte (par exemple, un service obsolète tournant sur un port ouvert), l'alerte est classée comme critique car l'hôte est "potentiellement compromis",.
- **Comparaison avec l'Impact 3** : À l'inverse, si l'attaque vise un port qui n'est pas ouvert sur l'hôte cible, le système abaissera le niveau à l'Impact 3 (Actuellement non vulnérable).

Cette évaluation permet au SOC de prioriser ses interventions en se concentrant sur les alertes où l'attaquant a réellement une chance de réussir en raison d'une faille confirmée sur la cible.

Quels systèmes MDM sont mentionnés pour l'agent utilisateur ?

Selon les sources, le système de gestion des terminaux mobiles (MDM) spécifiquement cité comme exemple est **MobileIron**.

Voici les précisions apportées par les sources concernant l'utilisation des agents et des solutions MDM :

- **Stratégie de gestion par agent** : Pour les appareils mobiles, la sécurité peut être assurée par l'installation d'un **agent sur le terminal**. Cette méthode permet de contrôler les applications et d'exécuter des commandes à distance, mais elle nécessite que le propriétaire de l'appareil consente à l'administration de son terminal.
- **Capacités de MobileIron** : Le système **MobileIron Core** est mentionné pour sa capacité à collecter plus de **200 champs de données**, incluant des métriques sur les appareils, les applications, les utilisateurs et leur statut.
- **Exportation des données** : Les données collectées par cet outil peuvent être exportées nativement vers des solutions de reporting

ou d'analyse comme **Splunk**, Tableau, Crystal Reports et QlikView.

Bien que d'autres fournisseurs MDM existent, les sources utilisent principalement MobileIron pour illustrer comment les données d'événements des appareils mobiles peuvent être centralisées et exploitées. Par ailleurs, les sources mentionnent également la gamme **Cisco Meraki** comme une solution d'appliances gérées via le cloud, offrant des fonctionnalités de sécurité mobile similaires.

Comment fonctionne l'inspection dynamique des paquets (avec état) ?

L'**inspection dynamique des paquets** (également appelée inspection **avec état** ou *stateful inspection*) est une technologie de pare-feu qui améliore la sécurité en analysant le contexte des communications plutôt que de filtrer chaque paquet de manière isolée.

Voici son fonctionnement détaillé selon les sources :

1. Suivi des connexions (état)

Contrairement aux premiers pare-feu dits "sans état" qui analysaient chaque paquet entrant ou sortant indépendamment selon des règles statiques, le pare-feu avec état surveille la fiabilité et l'origine de la connexion. Il garde une trace des requêtes envoyées depuis le réseau interne vers l'extérieur.

2. Le mécanisme de vérification

Le principe fondamental repose sur la comparaison systématique du trafic :

- **Analyse du trafic entrant** : Lorsqu'un paquet arrive de l'extérieur, le pare-feu vérifie s'il existe une **requête sortante correspondante** déjà enregistrée.
- **Autorisation ou rejet** :
 - Si le paquet entrant répond à une demande légitime faite précédemment par un utilisateur interne, il est **autorisé**.
 - Si aucune requête sortante correspondante n'est trouvée, le paquet est considéré comme non sollicité et il est **rejeté**.

3. Avantages par rapport au filtrage statique

Cette méthode offre une protection accrue contre certaines cyberattaques :

- **Protection contre l'usurpation d'adresse IP** : Les pare-feu sans état sont vulnérables à l'usurpation car un attaquant peut simuler une adresse de confiance pour contourner les règles. L'inspection dynamique bloque ces tentatives puisque l'attaquant ne peut pas répondre à une requête sortante qu'il n'a pas reçue.
- **Richesse des données** : Les pare-feu avec état, comme la plateforme **Cisco ASA**, permettent de collecter des journaux détaillés pour le SOC, incluant les connexions autorisées/refusées, l'utilisation de la bande passante par utilisateur et l'audit de la traduction d'adresses réseau (NAT/PAT).

Bien que performante, cette technologie a été complétée par les **pare-feu applicatifs** (de nouvelle génération), qui permettent d'aller plus loin en inspectant le contenu même des applications (comme distinguer Facebook de Facebook Games) sur tous les ports et protocoles.

Peut-on utiliser des API pour extraire les données du FMC ?

D'après les sources fournies, il n'est pas explicitement mentionné que le **FirePOWER Management Center (FMC)** dispose d'une API spécifique pour l'extraction des données. Les documents se concentrent sur d'autres méthodes d'exportation pour le FMC.

Voici les précisions apportées par les sources sur l'extraction des données :

- **Méthodes d'exportation du FMC** : Pour transmettre des événements vers une solution de collecte externe (comme un SIEM), le FMC utilise principalement la génération de **messages syslog**, de **traps SNMP** (v1, v2 ou v3) ou l'envoi d'**e-mails**.
- **Centralisation au sein du FMC** : Une fois que les capteurs sont ajoutés au FMC, celui-ci centralise toutes les fonctions de configuration, de gestion, de reporting et d'enregistrement. Les tableaux de bord consolidés peuvent également être **exportés sous forme de rapports**.
- **API mentionnée pour d'autres produits** : Les sources indiquent explicitement qu'une **API d'extraction de journaux** est disponible

pour une autre solution, **Cisco Cloud Web Security (CWS)**, précisant qu'elle comprend plus de 20 attributs.

- **Critères d'évaluation des outils de collecte** : Lors de l'évaluation d'une solution de collecte de données (comme un SIEM), les sources recommandent de vérifier si les formats standards du secteur, incluant les **API**, sont pris en charge pour les fonctionnalités sans agent.

En résumé, bien que les sources encouragent l'utilisation d'API dans l'architecture globale d'un SOC, elles détaillent l'exportation des données du FMC via **syslog, SNMP et e-mail** plutôt que par une API dédiée.

Comment FirePOWER peut-il automatiser la défense IPS ?

Cisco FirePOWER automatise la défense IPS (Système de prévention des intrusions) en s'appuyant sur une connaissance contextuelle du réseau et une corrélation intelligente avec les vulnérabilités détectées. Voici les mécanismes clés permettant cette automatisation selon les sources :

- **Connaissance contextuelle et recommandations** : Grâce à la licence IPS, FirePOWER bénéficie d'une visibilité complète sur les utilisateurs, l'infrastructure et les applications. Cette visibilité permet au FirePOWER Management Center (FMC) de générer des **recommandations automatiques**. Le système adapte ainsi la protection uniquement aux systèmes et protocoles réellement présents sur le réseau, évitant le paramétrage manuel fastidieux.
- **Ajustement automatique (Automatic Tuning)** : Contrairement à d'autres solutions plus limitées, l'offre IPS de FirePOWER est hautement personnalisable et permet un **paramétrage automatique** qui s'adapte en temps réel lorsque de nouvelles vulnérabilités sont identifiées sur les périphériques surveillés.
- **Corrélation avec le scanner de vulnérabilités** : FirePOWER utilise un **scanner de vulnérabilités intégré** (ou importe des données de tiers) pour associer un hôte vulnérable à une signature d'attaque spécifique. Si une menace correspond à une faille confirmée, l'IPS peut **activer automatiquement les**

défenses appropriées pendant que le système attend son correctif.

- **Priorisation par indicateurs d'impact** : Le système qualifie automatiquement la pertinence d'une alerte via des niveaux d'impact. Par exemple, une alerte d'**Impact 1 (Vulnérable)** est générée automatiquement lorsque le système confirme que la cible présente une vulnérabilité identifiée et est potentiellement compromise, permettant au SOC de se concentrer sur les menaces réelles et vérifiées.

En résumé, l'automatisation repose sur la capacité du système à comprendre son environnement pour n'activer que les règles de sécurité pertinentes et à réagir de manière autonome face aux vulnérabilités connues des hôtes.

Comment le FMC génère-t-il des recommandations pour l'IPS ?

Le FirePOWER Management Center (FMC) génère des recommandations pour l'IPS (système de prévention des intrusions) en utilisant une approche contextuelle qui permet d'adapter la défense à la réalité du réseau surveillé.

Voici les mécanismes clés utilisés pour produire ces recommandations :

- **Exploitation de la visibilité réseau** : Le FMC s'appuie sur sa capacité à identifier les périphériques, les utilisateurs et les applications présents sur le réseau pour comprendre précisément l'environnement qu'il doit protéger.
- **Adaptation aux protocoles présents** : Grâce à cette visibilité, l'IPS est capable d'adapter sa protection pour ne cibler que les systèmes et les protocoles qui sont réellement détectés sur le réseau.
- **Scanner de vulnérabilités** : Le FMC utilise son propre **scanner de vulnérabilités intégré** (ou importe des analyses provenant de tiers) pour identifier les failles de sécurité spécifiques affectant les hôtes.
- **Association intelligente** : Le système associe ensuite chaque hôte vulnérable identifié au **fichier de signature IPS** correspondant. Cela permet d'activer les défenses précises

nécessaires pour protéger un système vulnérable en attendant qu'un correctif puisse lui être appliqué.

- **Flexibilité d'application** : Ces ajustements, officiellement appelés « **recommandations FirePOWER** », peuvent être configurés pour s'appliquer de manière totalement automatique ou être présentés sous forme d'une liste de suggestions que l'administrateur peut choisir d'activer manuellement.

En résumé, cette fonctionnalité permet d'automatiser le paramétrage de la sécurité en s'assurant que seules les règles pertinentes pour les vulnérabilités et les protocoles actifs sur le réseau sont activées, ce qui optimise la précision de la détection.

Comment les recommandations FirePOWER optimisent-elles la détection ?

Les **recommandations FirePOWER** optimisent la détection en adaptant automatiquement ou manuellement la protection IPS (Système de prévention des intrusions) à la réalité spécifique de votre réseau.

Voici les mécanismes clés par lesquels cette optimisation s'opère :

- **Adaptation au contexte du réseau** : Le FirePOWER Management Center (FMC) utilise sa visibilité sur les périphériques, les utilisateurs et les applications pour comprendre précisément ce qu'il doit protéger. Cela permet à l'IPS de ne surveiller que les **systèmes et protocoles réellement présents** sur le réseau, évitant ainsi de charger le système avec des règles inutiles.
- **Personnalisation de la défense** : Ces ajustements, appelés « recommandations FirePOWER », peuvent être configurés pour s'appliquer de manière **automatique** ou être présentés sous forme d'une liste que l'administrateur valide manuellement. Cela réduit la complexité du paramétrage granulaire tout en maintenant une haute efficacité.
- **Corrélation avec les vulnérabilités** : Le système exploite un **scanner de vulnérabilités intégré** (ou des données tierces) pour identifier les failles spécifiques des hôtes. Il peut alors associer un système vulnérable au **fichier de signature IPS approprié**.

- **Protection proactive** : Grâce à cette association, les défenses spécifiques sont activées par l'IPS pour protéger les systèmes critiques pendant qu'ils attendent l'application d'un correctif de sécurité (patch).

En résumé, ces recommandations transforment une protection générique en une **défense ciblée et intelligente**, ce qui augmente la précision de la détection tout en optimisant l'utilisation des ressources du matériel de sécurité.

Quelle est la différence entre Impact 1 et Impact 2 ?

Selon les sources, la différence entre l'**Impact 1** et l'**Impact 2** réside dans le degré de certitude concernant la vulnérabilité de la cible face à une attaque détectée par Cisco FirePOWER :

- **Impact 1 (Vulnérable)** : Ce niveau indique que l'hôte (source ou destination) possède une **vulnérabilité spécifique et identifiée** correspondant à l'attaque en cours. Dans ce cas, le système considère que l'hôte est **potentiellement compromis**.
- **Impact 2 (Potentiellement vulnérable)** : Ce niveau est attribué lorsque l'hôte utilise simplement un **protocole d'application serveur** lié à l'alerte. Contrairement à l'Impact 1, il n'y a pas forcément de confirmation qu'une faille précise existe, mais le service est actif et donc théoriquement exposé.

En résumé, l'**Impact 1** confirme une faille de sécurité réelle sur la cible, tandis que l'**Impact 2** signale une exposition basée uniquement sur la présence d'un service ou d'un protocole serveur.

Comment MobileIron exporte ses données vers Splunk ?

L'exportation des données de MobileIron (plus précisément de **MobileIron Core**) vers Splunk s'effectue de manière **native**.

Voici les détails de ce processus fournis par les sources :

- **Richesse des données collectées** : MobileIron Core rassemble plus de **200 champs de données** distincts.

- **Indicateurs transmis** : Ces données comprennent des métriques détaillées sur les **appareils**, les **applications**, les **utilisateurs** ainsi que leur **statut** actuel.
- **Utilisation dans Splunk** : Une fois l'exportation native réalisée, les administrateurs peuvent utiliser ces informations pour analyser, visualiser et exploiter l'ensemble de leur infrastructure mobile directement depuis l'interface de Splunk.

Les sources précisent que cette capacité d'exportation native n'est pas limitée à Splunk, puisque MobileIron peut également transmettre ces mêmes données vers d'autres outils de reporting tiers tels que Tableau, Crystal Reports ou QlikView.

Comment l'inspection avec état protège-t-elle contre l'usurpation IP ?

L'inspection avec état (ou inspection dynamique des paquets) protège contre l'usurpation d'adresse IP en validant que le trafic entrant correspond réellement à une session de communication légitime initiée de l'intérieur.

Voici le mécanisme précis décrit dans les sources :

- **Vulnérabilité des anciens systèmes** : Les premiers pare-feu dits « sans état » (*stateless*) filtraient les paquets de manière statique et isolée, sans se soucier de la fiabilité de la connexion. Un attaquant pouvait donc envoyer des paquets avec une adresse IP simulant celle d'un réseau de confiance pour contourner les règles de sécurité.
- **Suivi du contexte** : Contrairement à ces anciens systèmes, l'inspection dynamique ne se contente pas de regarder les règles de filtrage ; elle mémorise les requêtes envoyées depuis le réseau interne vers l'extérieur.
- **Vérification systématique** : Lorsqu'un paquet arrive de l'extérieur, le pare-feu le compare immédiatement à la **requête sortante correspondante** enregistrée dans sa mémoire.
- **Rejet du trafic non sollicité** : Si un attaquant tente d'usurper une adresse IP pour entrer sur le réseau, le pare-feu constatera qu'**aucune requête sortante n'existe** pour ce flux spécifique. Le

paquet est alors considéré comme non sollicité et est automatiquement **rejeté**, bloquant ainsi la tentative d'accès frauduleuse.

En résumé, l'usurpation IP échoue car l'attaquant ne peut pas simuler l'existence d'une session déjà établie dans la table d'état du pare-feu.

Expliquez le fonctionnement du scanner de vulnérabilités intégré.

Le scanner de vulnérabilités intégré, principalement utilisé au sein du **FirePOWER Management Center (FMC)**, fonctionne comme un outil d'analyse contextuelle qui renforce la précision de la défense réseau.

Voici son fonctionnement détaillé selon les sources :

- **Identification des failles** : Le scanner analyse les hôtes détectés sur le réseau pour identifier les systèmes et les services qui pourraient potentiellement être exploités par un attaquant.
- **Corrélation avec l'IPS** : Sa fonction principale est d'**associer un système vulnérable au fichier de signature IPS (Système de prévention des intrusions) approprié**. En croisant les vulnérabilités détectées avec la base de signatures d'attaques, le système sait exactement quelle protection activer pour quel hôte.
- **Automatisation des recommandations** : Les résultats du scanner permettent au FMC de générer des **recommandations FirePOWER**. Ces ajustements peuvent être automatiques ou présentés sous forme de liste, permettant d'adapter la protection aux seuls protocoles et vulnérabilités réellement présents sur le réseau.
- **Défense proactive (Virtual Patching)** : Ce mécanisme permet d'**activer des défenses spécifiques** pour protéger un hôte vulnérable pendant la période critique où il attend l'application d'un correctif de sécurité officiel.
- **Flexibilité des sources** : Bien que FirePOWER dispose de son propre scanner intégré, il est également capable d'**importer des analyses de vulnérabilités** provenant de produits tiers pour enrichir ses recommandations.

En résumé, ce scanner transforme la détection passive en une réponse active en permettant au système de "comprendre" ce qu'il protège et d'ajuster ses règles de sécurité en conséquence.

Comment FirePOWER fait-il la différence entre les impacts 1 et 3 ?

Cisco FirePOWER fait la distinction entre les impacts 1 et 3 en corrélant une intrusion détectée avec les données de sa **carte réseau** et de son **scanner de vulnérabilités** pour déterminer si l'attaque est réellement pertinente pour la cible.

Voici la différence fondamentale entre ces deux niveaux :

- **Impact 1 (Vulnérable)** : Ce niveau est attribué lorsque le système confirme que l'hôte (source ou destination) présente une **vulnérabilité identifiée** correspondant précisément à l'attaque détectée. Dans ce cas, l'hôte est considéré comme **potentiellement compromis**. Cela se produit généralement lorsqu'une signature IPS correspond à une faille active découverte par le scanner de vulnérabilités intégré de FirePOWER ou importée d'un produit tiers.
- **Impact 3 (Actuellement non vulnérable)** : À l'inverse, l'impact 3 indique que l'hôte visé n'est **pas vulnérable** à cette attaque spécifique car il **n'a pas le port ouvert** ou **n'utilise pas le protocole** visé par la menace. Bien qu'une tentative d'intrusion ait été détectée, elle n'a aucune chance de réussir contre cette cible particulière selon les informations de découverte réseau.

Cette distinction permet aux analystes du SOC de **prioriser les alertes** : une alerte d'impact 1 nécessite une intervention immédiate, tandis qu'une alerte d'impact 3 peut être considérée comme une tentative d'attaque ayant échoué par manque de cible valide