Filtrage de réputation de fichiers et analyse de fichiers

Le présent chapitre contient les sections suivantes :

- Survol du filtrage de réputation de fichiers et de l'analyse de fichiers , on page 1
- Configuration des fonctionnalités d'analyse et de réputation de fichiers, on page 6
- Création de rapports et suivi de la réputation et de l'analyse des fichiers , on page 18
- Mesures à prendre lors de changements de verdicts des menaces de fichiers , on page 22
- Résolution des problèmes liés à la réputation et à l'analyse des fichiers , on page 22

Survol du filtrage de réputation de fichiers et de l'analyse de fichiers

Cisco Secure Endpoint assure une protection contre les menaces de type « zero day » et basées sur un fichier cibleen :

- obtenant la réputation des fichiers connus ;
- analysant le comportement de certains fichiers qui ne sont pas encore connus du service de réputation ;
- évaluant en permanence les menaces émergentes au fur et à mesure que de nouvelles informations sont disponibles et en vous informant des fichiers qui sont considérés comme des menaces après leur entrée dans votre réseau.

Cette fonction est disponible pour les téléchargements de fichiers. Fichiers chargés.

Les services de réputation de fichier et d'analyse de fichier proposent des options pour un cloud public ou privé (sur site).

- Le service de réputation de fichier de cloud privé est fourni par l'appliance Cisco Virtual Private Cloud, fonctionnant en mode Cisco Secure Endpoint « proxy » ou « air-gap » (sur site). Consultez Configuration d'un serveur de réputation de fichiers sur site, on page 9.
- Le service d'analyse des fichiers de cloud privé est fourni par une appliance Cisco Cisco Secure Endpoint Malware Analytics sur site. Consultez Configuration d'un serveur d'analyse de fichiers sur site , on page 9.

Mises à jour des verdicts de menaces des fichiers

Les verdicts de menaces peuvent changer à mesure que de nouvelles informations sont disponibles. Un fichier peut initialement être évalué comme inconnu ou sain et l'utilisateur peut ainsi être autorisé à y accéder;. Si le verdict de menace change à mesure que de nouveaux renseignements sont disponibles, vous en serez alerté, et le fichier et son nouveau verdict s'afficheront dans le rapport sur les mises à jour des verdicts Cisco Secure Endpoint . Vous pouvez examiner la du message au point d'entrée comme point de départ pour remédier aux éventuels impacts de la menace.

Les verdicts peuvent également passer de malveillants à sains.

Lorsque l'appliance traite les instances suivantes du même fichier, le verdict mis à jour est immédiatement appliqué.

Des renseignements sur le moment des mises à jour des verdicts sont inclus dans le document sur les critères de fichier mentionné dans Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 4.

Thèmes connexes

- Création de rapports et suivi de la réputation et de l'analyse des fichiers , on page 18
- Mesures à prendre lors de changements de verdicts des menaces de fichiers , on page 22

Survol du traitement de fichiers

Tout d'abord, le site Web à partir duquel le fichier est téléchargé est évalué en fonction du service de réputation Web (WBRS).

Si le score de réputation Web du site se trouve dans la plage configurée pour « Scan » (Analyse), l'appliance analyse simultanément la transaction à la recherche de programmes malveillants et interroge le service en nuage sur la réputation du fichier. (Si le score de réputation du site se situe dans la plage « Block », la transaction est gérée en conséquence et il n'est pas nécessaire de traiter le fichier davantage.) Si un programme malveillant est détecté lors de l'analyse, la transaction est bloquée, quelle que soit la réputation du fichier.

Si l'analyse adaptative est également activée, l'évaluation de la réputation des fichiers et l'analyse des fichiers sont incluses dans l'analyse adaptative.

Les communications entre l'appliance et le service de réputation des fichiers sont chiffrées et protégées contre la falsification.

Après l'évaluation de la réputation d'un fichier :

- Si le fichier est connu du service de réputation de fichiers et qu'il est déterminé comme étant sain, il est remis à l'utilisateur final et .
- Si le service de réputation des fichiers renvoie un verdict malveillant l'appliance applique l'action que vous avez spécifiée à ces fichiers.
- Si le fichier est connu du service de réputation, mais qu'il n'y a pas suffisamment d'informations pour un verdict définitif, le service de de menace en fonction des caractéristiques du fichier telles que l'analyse de l'empreinte de la menace et du comportement. Si ce score atteint ou dépasse le seuil de réputation configuré, l'appliance applique l'action que vous avez configurée dans la politique d'accès de pour les malveillants ou des fichiers à risque élevé.
- Si le service de réputation ne possède aucune information à propos du fichier et que le fichier ne répond pas aux critères d'analyse (voir Fichiers pris en charge pour les services de réputation et d'analyse des

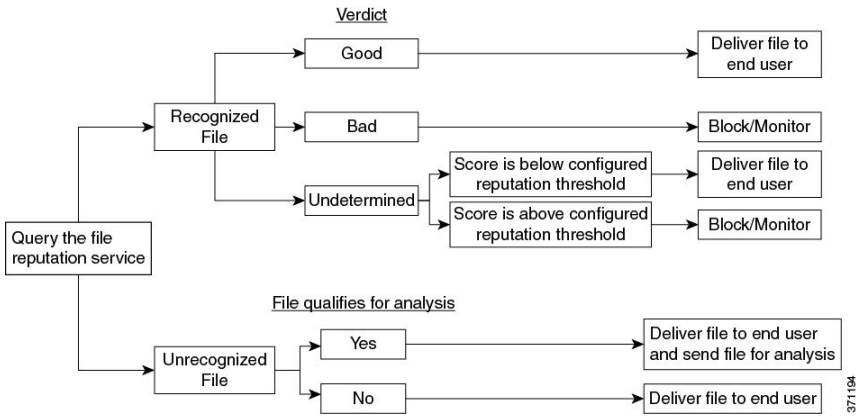
fichiers , on page 4), le fichier est considéré comme non sain et il est mis à la disposition de l'utilisateur final .

- Si vous avez activé le service d'analyse de Fichiers en nuage et que le service de réputation ne possède aucune information à propos du fichier et que le fichier répond aux critères des fichiers pouvant être analysés (voir Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 4), le fichier est considéré comme sain et est facultativement pour analyse.
- Pour les déploiements avec analyse de fichiers sur site, l'évaluation de la réputation et l'analyse de fichier ont lieu simultanément. Si le service de réputation renvoie un verdict, ce verdict est utilisé, car le service de réputation comprend des entrées provenant d'un éventail de sources plus large. Si le fichier est inconnu du service de réputation, le fichier est mis à la disposition de l'utilisateur, mais le résultat de l'analyse de fichier est mis à jour dans le cache local et est utilisé pour évaluer les instances futures du fichier dans .
- Si les informations de verdict de réputation de fichier ne sont pas disponibles parce que la connexion avec le serveur a expiré, le fichier est considéré comme non analysable et les actions configurées sont appliquées.

Fichiers à faible risque

Lorsqu'un fichier est initialement évalué comme inconnu et n'a aucun contenu dynamique, l'appliance l'envoie au moteur de préclassification, où il est désigné comme à faible risque. Ce fichier n'est pas téléchargé pour analyse. En cas d'accès au même fichier avant l'expiration du cache, il est à nouveau évalué comme à faible risque et n'est pas téléchargé pour analyse. Après l'expiration du délai du cache, en cas d'accès au même fichier, il est évalué comme inconnu et à faible risque dans l'ordre. Ce processus est répété pour les fichiers à faible risque. Puisque ces fichiers à faible risque ne sont pas chargés, ils ne feront pas partie des rapports d'analyse de fichiers.

Figure 1: Cisco Secure Endpoint Flux de travail pour les déploiements d'analyse de fichiers dans le nuage



Si le fichier est envoyé pour analyse :

- Si le fichier est envoyé dans le nuage pour analyse : les fichiers sont envoyés sur HTTPS.
- L'analyse prend normalement quelques minutes, mais peut être plus longues.
- Un fichier signalé comme malveillant après l'analyse du fichier peut ne pas être identifié comme malveillant par le service de réputation. La réputation d'un fichier est déterminée par divers facteurs au fil du temps, pas nécessairement par un seul verdict d'analyse de fichier.
- Les résultats des fichiers analysés à l'aide d'une appliance Cisco Secure Endpoint Malware Analytics sur site sont mis en cache localement.

Pour en savoir plus sur les mises à jour des verdicts, consultez Mises à jour des verdicts de menaces des fichiers , on page 2.

Fichiers pris en charge pour les services de réputation et d'analyse des fichiers

Le service de réputation évalue la plupart des types de fichiers. L'identification du type de fichier est déterminée par le contenu du fichier et ne dépend pas de l'extension du nom du fichier.

Certains fichiers de réputation inconnue peuvent être analysés pour connaître les caractéristiques des menaces. Lorsque vous configurez la fonction d'analyse des fichiers, vous choisissez les types de fichiers à analyser. De nouveaux types peuvent être ajoutés dynamiquement; vous recevrez une alerte lorsque la liste des types de fichiers téléchargeables sera modifiée et pourrez sélectionner les types de fichiers ajoutés à charger.

Les détails sur les fichiers pris en charge par les services de réputation et d'analyse ne sont disponibles que pour les clients enregistrés de Cisco. Pour en savoir plus sur les fichiers évalués et analysés, consultez *Critères des fichiers pour les services Advanced Malware Protection des produits Cisco Content Security*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html. Les critères d'évaluation de la réputation d'un fichier et d'envoi des fichiers pour analyse peuvent changer à tout moment.

Pour accéder à ce document, vous devez avoir un compte client Cisco avec un contrat d'assistance. Pour vous inscrire, consultez la page https://tools.cisco.com/RPF/register/register.do.

Votre paramètre pour **DVS Engine Object Scanning Limits** (Limites d'analyse des objets du moteur DVS) dans la page **Security Services > Anti-Malware and Reputation** (Services de sécurité> Antiprogrammes malveillants et réputation) détermine également la taille de fichier maximale pour la réputation et l'analyse des fichiers.

Vous devez configurer des politiques pour bloquer télécharger de fichiers qui ne sont pas adressés par Cisco Secure Endpoint.

Note Un fichier (se trouvant dans un courriel entrant ou sortant) qui a déjà été téléchargé pour analyse, quelle que soit la source, ne sera pas téléchargé à nouveau. Pour afficher les résultats de l'analyse pour un tel fichier, recherchez le SHA-256 dans la page de rapports d'analyse des fichiers.

Thèmes connexes

- Activation et configuration des services de réputation et d'analyse des fichiers , on page 10
- Veiller à recevoir des alertes sur les problèmes Cisco Secure Endpoint , on page 17
- Traitement d'archives ou de fichiers compressés, on page 4

Traitement d'archives ou de fichiers compressés

Si le fichier est compressé ou archivé,

- la réputation du fichier compressé ou d'archive est évaluée.
- Pour certains types de fichiers sélectifs, le fichier compressé ou d'archive est décompressé et la réputation de tous les fichiers extraits est évaluée.

Pour en savoir plus sur les fichiers archivés et compressés qui sont examinés, y compris les formats de fichier, consultez les informations liées à partir de Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 4.

Dans ce scénario,

- Si l'un des fichiers extraits est malveillant, le service File Reputation renvoie le verdict Malicious pour le fichier compressé ou l'archive.
- Si le fichier compressé ou d'archive est malveillant et que tous les fichiers extraits sont sains, le service de réputation des fichiers renvoie un verdict Malicious (Malveillant) pour le fichier compressé ou d'archive.
- Si le verdict de l'un des fichiers extraits est unknown, les fichiers extraits sont éventuellement (s'ils sont configurés et que le type de fichier est pris en charge pour l'analyse de fichier) envoyés pour analyse de fichier.
- Si l'extraction d'un fichier échoue lors de la décompression d'un fichier compressé ou d'une archive, le service File Reputation renvoie le verdict Non analysable pour le fichier compressé ou l'archive. N'oubliez pas que, dans ce scénario, si l'un des fichiers extraits est malveillant, le service de réputation des fichiers renvoie un verdict de malveillance pour le fichier compressé ou l'archive (le verdict de malveillance prévaut sur le verdict Non analysable).
- Un fichier compressé ou d'archive est traité comme non analysable dans les scénarios suivants :
  - Le taux de compactage des données est supérieur à 20.
  - Le fichier d'archive contient plus de cinq niveaux d'imbrication.
  - Le fichier d'archive contient plus de 200 fichiers enfants.
  - La taille du fichier d'archive dépasse 50 Mo.
  - Le fichier d'archive est protégé par un mot de passe ou illisible.

Note La réputation des fichiers extraits avec des types MIME sécurisés, par exemple, texte/brut, n'est pas évaluée.

Confidentialité des informations envoyées dans le nuage

- Seul le SHA qui identifie de manière unique un fichier est envoyé au service de réputation dans le nuage. Le fichier proprement dit n'est pas envoyé.
- Si vous utilisez le service d'analyse de fichier dans le nuage et qu'un fichier est admissible pour l'analyse, le fichier proprement dit est envoyé dans le nuage.
- Les informations sur chaque fichier envoyé dans le nuage pour analyse et ayant un verdict « malveillant » sont ajoutées à la base de données de réputation. Ces renseignements sont utilisés avec d'autres données pour déterminer un score de réputation.

  Les renseignements sur les fichiers analysés par une appliance Cisco Secure Endpoint Malware Analytics sur site ne sont pas partagés avec le service de réputation.

Configuration des fonctionnalités d'analyse et de réputation de fichiers

- Exigences de communication avec les services de réputation et d'analyse de fichiers , on page 6
- Configuration d'un serveur de réputation de fichiers sur site, on page 9
- Configuration d'un serveur d'analyse de fichiers sur site , on page 9
- Activation et configuration des services de réputation et d'analyse des fichiers
- (Services d'analyse des fichiers dans le nuage public uniquement) Configuration des groupes d'appliances , on page 15
- Configuration de l'action du service de réputation et d'analyse des fichiers par politique d'accès , on page 17
- Veiller à recevoir des alertes sur les problèmes Cisco Secure Endpoint , on page 17
- Configuration de rapports centralisés pour les fonctionnalités Cisco Secure Endpoint , on page 18

Exigences de communication avec les services de réputation et d'analyse de fichiers

- Toutes les appliances Secure Web Appliance qui utilisent ces services doivent pouvoir s'y connecter directement par Internet (à l'exception des services d'analyse des fichiers configurés pour utiliser une appliance Cisco Secure Endpoint Malware Analytics sur site).
- Par défaut, la communication avec les services de réputation et d'analyse des fichiers est acheminée par le port de gestion (M1) sur l'appliance. Si votre appliance n'achemine pas de données par le port de gestion, consultez Routage du trafic vers les serveurs d'analyse des fichiers et de réputation de fichier par une interface de données , on page 7.
- Par défaut, la communication avec les services de réputation de fichiers et d'analyse en nuage est acheminée par l'interface associée à la passerelle par défaut. Pour acheminer ce trafic par l'intermédiaire d'une interface différente, créez une voie de routage statique pour chaque adresse dans la section avancée de la page Security Services > File Reputation and Analysis (Services de sécurité > Réputation et analyse des fichiers).
- Les ports de pare-feu suivants doivent être ouverts :

Ports de pare-feu	Description	Protocole	Entrée/Sortie	Hostname (Nom d'hôte)	Interface de l'appliance
32137 (par défaut) ou 443	L'accès aux services Cisco Cloud pour obtenir la réputation de fichier.	TCP	Sortant	Comme configuré dans Security Services > Anti-Malware and Reputation, Advanced section: Advanced Settings for File Reputation (Services de sécurité > Antiprogrammes malveillants et réputation, section Avancé : Paramètre avancé pour la réputation des fichiers), paramètre Cloud Server Pool (Regroupement de serveurs sur le nuage).	Management (Gestion), sauf si une voie de routage statique est configurée pour acheminer ce trafic par un port de données.
443	Accès aux services en nuage pour l'analyse de fichiers.	TCP	Sortant	Comme configuré dans Security Services > Anti-Malware and Reputation, Advanced section: Advanced Settings for File Analysis (Services de sécurité > Antiprogrammes malveillants et réputation, section Avancé : Paramètres avancés pour l'analyse des fichiers).	

- Lorsque vous configurez la fonction de réputation de fichiers, choisissez si vous souhaitez utiliser SSL sur le port 443.

Thèmes connexes

- Activation et configuration des services de réputation et d'analyse des fichiers

Routage du trafic vers les serveurs d'analyse des fichiers et de réputation de fichier par une interface de données

Si l'appliance est configurée pour restreindre le port de gestion aux services de gestion de l'appliance uniquement [sur la page **Network > Interfaces** (Réseau > Interfaces)], configurez plutôt l'appliance pour acheminer le trafic d'analyse des fichiers et de réputation par le port de données.

Ajoutez des voies de routage pour le trafic de données sur la page Network > Routes (Réseau > Voies de routage). Pour connaître la configuration requise et les instructions générales, consultez Configuration des routages de trafic TCP/IP.

Pour la connexion à	Réseaux de destination	Passerelle
Le service de réputation des fichiers	Dans Security Services > Anti-Malware and Reputation (Services de sécurité > Protection contre les programmes malveillants et réputation), section Advanced (Avancé) > section Advanced Settings for File Reputation (Paramètres avancés pour la réputation des fichiers), indiquez le nom (URL) du **serveur de réputation des fichiers** et le nom de **domaine dans le nuage** du regroupement de serveurs en nuage. Si vous choisissez Private Cloud (Cloud privé) pour le serveur de réputation des fichiers, saisissez le nom d'hôte ou l'adresse IP du serveur et indiquez une clé publique valide. Il doit s'agir de la même clé que celle utilisée par l'appliance du cloud privé. Nom d'hôte du regroupement de serveurs en nuage, tel que configuré dans les services de sécurité ; Protection contre les programmes malveillants et réputation, section Avancé : paramètres avancés pour la réputation des fichiers.	Adresse IP de la passerelle pour le port de données
Le service d'analyse de fichiers	• Dans Security Services > Anti-Malware and Reputation (Services de sécurité > Protection contre les programmes malveillants et réputation), section Advanced (Avancé) > section Advanced Settings for File Analysis (Paramètres avancés pour la réputation des fichiers), indiquez le nom (URL) du **serveur d'analyse des fichiers**. Si vous choisissez Private Cloud (Cloud privé) pour le serveur d'analyse des fichiers, saisissez l'URL du serveur et indiquez une autorité de certification valide. • L'ID du client d'analyse des fichiers est l'ID client de cette appliance sur le serveur d'analyse des fichiers (lecture seule). Le nom d'hôte du serveur d'analyse des fichiers, tel que configuré dans les services de sécurité; logiciel contre les programmes malveillants et réputation, section Avancé : Paramètres avancés pour l'analyse des fichiers.	Adresse IP de la passerelle pour le port de données

Thèmes connexes

- Configuration des routages de trafic TCP/IP

Configuration d'un serveur de réputation de fichiers sur site

Si vous prévoyez d'utiliser une appliance Cisco Secure Endpoint Cisco Virtual Private Cloud en tant que serveur d'analyse de fichiers en nuage privé :

- Vous pouvez obtenir la documentation de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud, le guide d'installation et de configuration de FireAMP Private Cloud, à l'adresse http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html

  Utilisez cette documentation pour effectuer les tâches décrites dans cette rubrique.

  Vous pouvez accéder à de la documentation supplémentaire en cliquant sur le lien Help (Aide) sur l'appliance Cisco Secure Endpoint Virtual Private Cloud.
- Installez et configurez l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud en mode « proxy » ou « air-gap » (local).
- Vérifiez que la version logicielle de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud est 2.2, ce qui permet l'intégration avec l' Secure Web Appliance.
- Téléchargez le certificat et les clés Cisco Secure Endpoint Virtual Private Cloud sur cette appliance pour les charger dans cette Secure Web Appliance.

Remarque Après avoir configuré le serveur de réputation de fichier sur site, vous configurerez la connexion à partir de cette Secure Web Appliance. Voir l'étape 6 de Activation et configuration des services de réputation et d'analyse des fichiers , à la page 10

Configuration d'un serveur d'analyse de fichiers sur site

Si vous utilisez une appliance Cisco Secure Endpoint Malware Analytics en tant que serveur d'analyse de fichiers en nuage privé :

- Procurez-vous le Guide d'installation et de configuration de l'appliance Cisco Secure Endpoint Malware Analytics et le Guide d'administration de l'appliance Cisco Secure Endpoint Malware Analytics. La documentation de l'appliance Cisco Secure Endpoint Malware Analytics est disponible sur https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html.

  Utilisez cette documentation pour effectuer les tâches décrites dans cette rubrique.

  De la documentation supplémentaire est accessible à partir du lien Help (Aide) sur l'appliance Cisco Secure Endpoint Malware Analytics.

  Dans le Guide d'administration, recherchez des informations sur tous les points suivants : les intégrations avec d'autres appliances Cisco, CSA, l'API Cisco Sandbox Secure Web Appliance.
- Installez et configurez l'appliance Cisco Secure Endpoint Malware Analytics.
- Au besoin, mettez à jour le logiciel de vos appliances Cisco Secure Endpoint Malware Analytics vers la version 1.2.1, qui prend en charge l'intégration avec Secure Web Appliance.

  Consultez la documentation de Cisco Secure Endpoint Malware Analytics pour obtenir des instructions sur la façon de déterminer le numéro de version et d'effectuer la mise à jour.

- Vérifiez que vos appliances peuvent communiquer entre elles sur votre réseau. Les Secure Web Appliance doivent pouvoir se connecter à l'interface SAINE de l'appliance Cisco Secure Endpoint Malware Analytics.
- Si vous souhaitez déployer un certificat autosigné : générez un certificat SSL autosigné à partir de l'appliance Cisco Secure Endpoint Malware Analytics à utiliser sur votre Secure Web Appliance. Consultez les instructions pour le téléchargement des clés et des certificats SSL dans le guide de l'administrateur de votre appliance Cisco Secure Endpoint Malware Analytics. Assurez-vous de générer un certificat indiquant CN comme nom d'hôte de votre appliance Cisco Secure Endpoint Malware Analytics. Le certificat par défaut de l'appliance Cisco Secure Endpoint Malware Analytics ne fonctionne PAS.
- L'enregistrement de votre Secure Web Appliance sur votre appliance Malware Analytics se produit automatiquement lorsque vous envoyez la configuration pour l'analyse des fichiers, comme décrit dans Activation et configuration des services de réputation et d'analyse des fichiers . Cependant, vous devez activer l'enregistrement comme décrit dans la même procédure.

Note Après avoir configuré le serveur d'analyse de fichiers sur site, vous configurerez la connexion à partir de ce Secure Web Appliance; consultez l'étape 7 de la section Activation et configuration des services de réputation et d'analyse des fichiers .

Activation et configuration des services de réputation et d'analyse des fichiers

Before you begin

- Obtenez des clés de fonctionnalité pour le service de réputation des fichiers et le service d'analyse des fichiers, et les transférer vers cet appliances. Consultez Utilisation des clés de fonctionnalité pour en savoir plus sur l'ajout de clés de fonctionnalité à l'appliance.
- Rencontrez les Exigences de communication avec les services de réputation et d'analyse de fichiers , on page 6.
- Assurez-vous qu'une interface réseau de données est activée sur l'appliance si vous souhaitez utiliser une interface réseau de données pour les services de réputation et d'analyse des fichiers. Voir la section Activation ou modification des interfaces réseau.
- Vérifiez la connectivité aux serveurs de mise à jour configurés (Mises à jour) dans Configuration des paramètres de mise à niveau et de mise à jour de services.
- Si vous souhaitez utiliser une appliance Cisco Cisco Secure Endpoint Virtual Private Cloud comme serveur de réputation des fichiers dans le nuage privé, consultez Configuration d'un serveur de réputation de fichiers sur site, on page 9.
- Si vous utilisez une appliance Cisco Secure Endpoint Malware Analytics en tant que serveur d'analyse de fichiers dans un nuage privé, consultez Configuration d'un serveur d'analyse de fichiers sur site , on page 9.

Étape 1 Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants > Réputation et analyse des fichiers).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Cliquez sur **Enable File Reputation Filtering** (Activer le filtrage de la réputation des fichiers) et éventuellement sur **Enable File Analysis** (Activer l'analyse des fichiers).

- Si l'option **Enable File Reputation Filtering** (Activer le filtrage de réputation des fichiers) est cochée, vous devez configurer la section **File Reputation Server** (Serveur de réputation des fichiers) (à l'**étape 6**), en choisissant l'URL d'un serveur de réputation externe sur un nuage public ou en fournissant les informations de connexion au serveur de réputation sur un nuage privé.
- De même, si l'option **Enable File Analysis** (Activer l'analyse des fichiers) est cochée, vous devez configurer la section **File Analysis Server URL** (URL du serveur d'analyse des fichiers) (à l'**étape 7**), en indiquant l'URL d'un serveur sur un nuage externe ou les informations de connexion au nuage d'analyse privé.

Note De nouveaux types de fichiers peuvent être ajoutés après une mise à niveau et ne sont pas activés par défaut. Si vous avez activé l'analyse des fichiers et que vous souhaitez inclure les nouveaux types de fichiers dans l'analyse, vous devez les activer.

Étape 4 Acceptez le contrat de licence, s'il s'affiche.

Étape 5 Dans la section **File Analysis** (Analyse des fichiers), sélectionnez les types de fichiers requis dans les groupes de fichiers appropriés (par exemple, « documents Microsoft ») afin de les envoyer pour analyse.

Pour en savoir plus sur les types de fichiers pris en charge, consultez le document décrit dans Fichiers pris en charge pour les services de réputation et d'analyse des fichiers , on page 4

Étape 6 Développez le volet **Advanced Settings for File Reputation** (Paramètres avancés pour la réputation des fichiers) et ajustez les options suivantes, si nécessaire :

Option	Description
Cloud Domain (Domaine en nuage)	Nom du domaine à utiliser pour les requêtes de réputation de fichiers.
File Reputation Server (Serveur de réputation des fichiers)	Choisissez : le nom d'hôte du serveur de réputation en nuage public ou le nuage de réputation privé. Si vous choisissez un nuage de réputation privé, indiquez les informations suivantes : • **Server** (Serveur) : nom d'hôte ou adresse IP de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud. • **Public Key** (Clé publique) : indiquez une clé publique valide pour les communications chiffrées entre cette appliance et votre appliance en nuage privé. Il doit s'agir de la même clé que celle utilisée par le serveur en nuage privé : localisez le fichier de clé sur cette appliance, puis cliquez sur **Upload File** (Charger le fichier). **Note** Vous devez avoir déjà téléchargé le fichier de clé du serveur vers cette appliance.
Routing Table (Tableau de routage)	Table de routage (associée à un type d'interface réseau d'appliance, de gestion ou de données) à utiliser pour les services Cisco Secure Endpoint. Si l'appliance est à la fois une interface de gestion et une ou plusieurs interfaces de données activées, vous pouvez sélectionner Management (Gestion) ou Data (Données).

Option	Description
SSL Communication for File Reputation (Communication SSL pour la réputation des fichiers)	Cochez la case **Use SSL (Port 443)** [Utiliser SSL (Port 443)] pour communiquant sur le port 443 au lieu du port par défaut 32137. Consultez le guide de l'utilisateur de l'appliance Cisco Cisco Secure Endpoint Virtual Private Cloud pour obtenir des renseignements sur l'activation de l'accès SSH au serveur. **Note** La communication SSL sur le port 32137 peut vous obliger à ouvrir ce port dans votre pare-feu. Cette option vous permet également de configurer un proxy en amont pour la communication avec le service de réputation des fichiers. Si cette option est cochée, renseignez comme approprié les champs **Server** (Serveur), **Username** (Nom d'utilisateur) et **Passphrase** (Phrase secrète). Si l'option **Use SSL (Port 443)** [Utiliser SSL (Port 443)] est sélectionnée, vous pouvez aussi cocher la case **Relax Certificate Validation** (Assouplir la validation des certificats) pour ignorer la validation de certificat standard si le certificat du serveur proxy de tunnel n'est pas signé par une autorité racine approuvée. Par exemple, sélectionnez cette option si vous utilisez un certificat autosigné sur un serveur proxy de tunnel interne approuvé. **Note** Si vous avez coché l'option **Use SSL (Port 443)** [Utiliser SSL (Port 443)] dans la section SSL Communication for File Reputation (Communication SSL pour la réputation des fichiers) des paramètres avancés pour la réputation des fichiers, vous devez ajouter le certificat de l'autorité de certification du serveur de réputation sur site Cisco Secure Endpoint au magasin de certificats de cette appliance, en utilisant Network > Certificates (Custom Certificate Authorities) [Réseau > Certificats (Autorités de certification personnalisées)] dans l'interface Web. Obtenez ce certificat auprès du serveur [Configuration > SSL > Cloud server > download (Configuration > SSL > Serveur en nuage > télécharger)].
Heartbeat Interval (Intervalle entre les pulsations)	Fréquence, en minutes, à laquelle envoyer un message Ping pour les événements rétrospectifs.
Query Timeout (Délai d'expiration de la requête)	Nombre de secondes écoulées avant l'expiration de la requête de réputation.
File Reputation Client ID (ID du client de réputation des fichiers)	ID de client pour cette appliance sur le serveur de réputation des fichiers (lecture seule).

Note Ne modifiez aucun autre paramètre dans cette section sans l'aide de l'assistance Cisco.

Étape 7 Si vous comptez utiliser le service en nuage pour l'analyse des fichiers, développez le volet Advanced Settings for File Analysis (Paramètres avancés pour l'analyse des fichiers) et réglez les options suivantes au besoin :

Option	Description
File Analysis Server URL (URL du serveur d'analyse des fichiers)	Choisissez : le nom (URL) d'un serveur en nuage externe ou le **Private analysis cloud** (Nuage d'analyse privé). Si vous indiquez un serveur en nuage externe, choisissez le serveur qui est physiquement le plus proche de votre appliance. Les nouveaux serveurs disponibles seront ajoutés à cette liste régulièrement à l'aide des processus de mise à jour standard. Choisissez Private analysis cloud (Nuage d'analyse privé) pour utiliser une appliance Cisco Secure Endpoint Malware Analytics sur site pour l'analyse des fichiers et saisissez les informations suivantes : • **TG Servers** (Serveurs TG) : saisissez l'adresse IPv4 ou le nom d'hôte des appliances Cisco Secure Endpoint Malware Analytics, autonomes ou en grappe. Vous pouvez ajouter au maximum sept appliances Cisco Secure Endpoint Malware Analytics. **Note** Le numéro de série indique l'ordre dans lequel vous ajoutez les appliances Cisco Secure Endpoint Malware Analytics autonomes ou en grappe. Il ne désigne pas la priorité des appliances. **Note** Vous ne pouvez pas ajouter de serveurs autonomes et de serveurs en grappe dans une seule instance. Ils doivent être autonomes ou en grappe. Vous ne pouvez ajouter qu'un seul serveur autonome par instance. En mode grappe, vous pouvez ajouter jusqu'à sept serveurs et tous les serveurs doivent appartenir à la même grappe. Vous ne pouvez pas ajouter plusieurs grappes. • **Certificate Authority** (Autorité de certification) : sélectionnez **Use Cisco Default Certificate Authority** (Utiliser l'autorité de certification par défaut de Cisco) ou **Use Uploaded Certificate Authority** (Utiliser l'autorité de certification chargée). Si vous choisissez **Use Uploaded Certificate Authority** (Utiliser l'autorité de certification chargée) et cliquez sur **Browse** (Parcourir) pour charger un fichier de certificat valide pour les communications chiffrées entre cette appliance et votre appliance de nuage privé. Il doit s'agir du même certificat utilisé par le serveur en nuage privé. **Note** Si vous avez configuré le portail Cisco Secure Endpoint Malware Analytics sur votre appliance pour l'analyse des fichiers, vous pouvez accéder au portail Cisco Secure Endpoint Malware Analytics (par exemple, https://panacea.threatgrid.eu) pour afficher et suivre les fichiers soumis pour l'analyse des fichiers. Pour en savoir plus sur l'accès au portail de Cisco Secure Endpoint Malware Analytics, communiquez avec le centre d'assistance technique de Cisco.

Option	Description
Proxy Settings (Paramètres de proxy)	Cochez la case **Use File Reputation Proxy** (Utiliser le proxy de réputation des fichiers) pour utiliser le même tunnel de proxy de réputation des fichiers que vous avez déjà configuré comme proxy en amont pour l'analyse des fichiers. Si vous souhaitez configurer un autre proxy en amont, décochez la case **Use File Reputation Proxy** (Utiliser le proxy de réputation des fichiers) et saisissez les informations appropriées dans les champs **Server** (Serveur), **Port**, **Username** (Nom d'utilisateur) et **Passphrase** (Phrase secrète).
File Analysis Client ID (ID du client d'analyse de fichier)	ID de client pour cette appliance sur le serveur d'analyse des fichiers (lecture seule).

Étape 8 (Facultatif) Développez le volet Cache Settings (Paramètres de cache) si vous souhaitez configurer la période d'expiration du cache pour les valeurs de disposition de réputation des fichiers.

Étape 9 Développez le volet Threshold Settings (Paramètres de seuil) si vous souhaitez définir la limite supérieure du score d'analyse de fichier acceptable. Le score au-dessus de ce seuil indique que le fichier est infecté. Choisissez l'une des options suivantes :

- Use value from Cloud Service (95) [Utiliser la valeur du service en nuage (95)]
- Enter Custom Value (Saisissez une valeur personnalisée) : par défaut, 95

Note L'option **Threshold Settings** (Paramètres de seuil) est désormais classée comme **File Analysis Threshold** (Seuil d'analyse de fichier) plutôt que comme **Reputation Threshold** (Seuil de réputation).

Étape 10 Envoyez et validez vos modifications.

Étape 11 Si vous utilisez une appliance Cisco Secure Endpoint Malware Analytics sur site, activez le compte pour cette appliance sur l'appliance Cisco Secure Endpoint Malware Analytics.

Des instructions complètes sur l'activation du compte « utilisateur » sont disponibles dans la documentation de Cisco Secure Endpoint Malware Analytics.

a) Notez l'ID du client d'analyse de fichiers qui s'affiche au bas de la section de la page. Cela identifie « l'utilisateur » que vous activerez.
b) Connectez-vous à l'appliance Cisco Secure Endpoint Malware Analytics.
c) Sélectionnez **Welcome... > Manage Users** (Bienvenue... > Gérer les utilisateurs) et accédez aux détails de l'utilisateur.
d) Localisez le compte « utilisateur » en fonction de l'ID de client d'analyse de fichier de vos Secure Web Appliance.
e) Activez ce compte « utilisateur » pour votre appliance.

Important! Modifications nécessaires dans le paramètre d'analyse de fichiers

Si vous prévoyez d'utiliser un nouveau service d'analyse de fichiers public dans le nuage, assurez-vous de lire les instructions suivantes pour maintenir l'isolement du centre de données :

- Les informations sur le regroupement d'appliances existants ne sont pas conservées dans le nouveau serveur d'analyse de fichiers. Vous devez regrouper vos appliances sur le nouveau serveur d'analyse de fichiers.

- Les messages mis en quarantaine dans la quarantaine d'analyse des fichiers sont conservés jusqu'à la période de conservation. Après la période de conservation en quarantaine, les messages sont libérés de la quarantaine d'analyse de fichiers et analysés de nouveau par le moteur Cisco Secure Endpoint . Le fichier est ensuite téléchargé sur le nouveau serveur d'analyse de fichiers pour analyse, mais le message n'est pas de nouveau envoyé en quarantaine d'analyse de fichiers.

Pour plus de détails, consultez la documentation de Cisco Cisco Secure Endpoint Malware Analytics de https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html.

(Services d'analyse des fichiers dans le nuage public uniquement) Configuration des groupes d'appliances

Pour permettre à toutes les appliances de sécurité de contenu de votre organisation d'afficher les détails des résultats de l'analyse des fichiers dans le nuage pour les fichiers envoyés pour analyse à partir de n'importe quelle appliance de votre organisation, vous devez joindre toutes les appliances au même groupe d'appliances.

Note Vous pouvez configurer des groupes d'appliances au niveau de l'ordinateur. Les groupes d'appliances ne peuvent pas être configurés au niveau de la grappe.

Étape 1 Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation > Analyse de réputation et des fichiers).

Étape 2 [S'applique si la licence Smart est désactivée sur votre passerelle de messagerie] Saisissez manuellement l'ID de groupe dans le champ **Appliance ID/Name** (ID/Nom de l'appliance) et cliquez sur **Group Now** (Regrouper maintenant).

Ou

[Applicable si la licence Smart est activée sur votre passerelle de messagerie] Le système enregistre automatiquement l'ID de compte Smart en tant qu'ID de groupe et l'affiche dans le champ **Appliance Group ID/Name** (ID/Nom du groupe d'appliances).

Remarques :

- Une appliance ne peut appartenir qu'à un seul groupe.
- Vous pouvez ajouter un ordinateur à un groupe à tout moment.
- Vous pouvez configurer des groupes d'appliances au niveau de l'ordinateur et de la grappe.
- S'il s'agit de la première appliance ajoutée au groupe, indiquez un identifiant utile pour le groupe. Cet ID est sensible à la casse et ne peut pas contenir d'espaces.
- L'ID de groupe d'appliances que vous fournissez doit être identique sur toutes les appliances qui partageront des données sur les fichiers téléchargés à des fins d'analyse. Cependant, l'ID n'est pas validé sur les appliances suivantes du groupe.
- Si vous mettez à jour l'ID de groupe d'appliances, la modification prend effet immédiatement et ne nécessite pas de validation.
- Vous devez configurer toutes les appliances d'un groupe pour utiliser le même serveur d'analyse de fichiers dans le nuage.
- Si les licences Smart sont activées, les appliances sont regroupées en utilisant l'ID de compte Smart.

Étape 3 Dans la section Appliance Grouping for Cloud Reporting Cloud (Regroupement d'appliances pour la création de rapports en nuage), saisissez l'ID du groupe de rapports d'analyse de fichiers dans le nuage.

- S'il s'agit de la première appliance ajoutée au groupe, indiquez un identifiant utile pour le groupe.
- Cet ID est sensible à la casse et ne peut pas contenir d'espaces.
- L'ID que vous indiquez doit être identique sur toutes les appliances qui partageront des données sur les fichiers téléchargés pour analyse. Cependant, l'ID n'est pas validé sur le groupe d'appliances suivant.
- Si vous saisissez l'ID de groupe incorrectement ou si vous devez le changer pour toute autre raison, vous devez ouvrir un dossier auprès du service d'assistance technique de Cisco.
- Cette modification prend effet immédiatement; elle ne nécessite pas de validation.
- Toutes les appliances du groupe doivent être configurées pour utiliser le même serveur d'analyse de fichiers dans le nuage.
- Une appliance ne peut appartenir qu'à un seul groupe.
- Vous pouvez ajouter un ordinateur à un groupe à tout moment, mais vous ne pouvez le faire qu'une seule fois.

Étape 4 Cliquez sur **Add Appliance to Group** (Ajouter l'appliance au groupe).

Quelles appliances se trouvent dans le groupe d'analyse?

Étape 1 Sélectionnez **Security Services> Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation).

Étape 2 Dans la section Appliance Grouping for File Analysis Cloud Reporting (Groupe d'appliances pour la création de rapports en nuage sur l'analyse des fichiers), cliquez sur **View Appliances in Group** (Afficher les appliances dans le groupe).

Étape 3 Pour afficher l'**ID du client d'analyse de fichiers** d'une appliance particulière, consultez l'emplacement suivant :

Appareil	Emplacement de l'ID du client d'analyse des fichiers
Appliance de sécurité de la messagerie	Section Advanced Settings for File Analysis (Paramètres avancés pour l'analyse des fichiers) sur la page **Security Services > File Reputation and Analysis** (Services de sécurité > Réputation et analyse des fichiers).
Secure Web Appliance	Advanced Settings for File Analysis (Paramètres avancés pour l'analyse des fichiers) sur la page **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation)
Appliance de gestion de la sécurité	Au bas de la page **Management Appliance > Centralized Services > Security Appliances** (Appliance de gestion > Services centralisés > Appliances de sécurité).

Configuration de l'action du service de réputation et d'analyse des fichiers par politique d'accès

Étape 1 Sélectionnez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).

Étape 2 Cliquez sur le lien dans la colonne **Anti-Malware and Reputation** (Protection contre les programmes malveillants et réputation) correspondant à une politique dans le tableau.

Étape 3 Dans la section **Cisco Secure Endpoint Settings** (Paramètres Cisco Secure Endpoint), sélectionnez **Enable File Reputation Filtering and File Analysis** (Activer le filtrage de réputation de fichiers et l'analyse de fichiers).

Si l'analyse de fichiers n'est pas activée globalement, seul le filtrage de réputation de fichier est proposé.

Étape 4 Sélectionnez une action pour **Known Malicious and High-Risk Files** (Fichiers malveillants ou à haut risque connus) : **Monitor** (Superviser) ou **Block** (Bloquer).

La valeur par défaut est Monitor (Superviser).

Étape 5 Envoyez et validez vos modifications.

Veiller à recevoir des alertes sur les problèmes Cisco Secure Endpoint

Vérifiez que l'appliance est configurée pour vous envoyer des alertes relatives à Cisco Secure Endpoint.

Vous recevrez des alertes dans les cas suivants :

Description de l'alerte	Type	Gravité
Vous configurez une connexion à une appliance Cisco Secure Endpoint Malware Analytics sur site (nuage privé) et vous devez activer le compte comme décrit dans la section Activation et configuration des services de réputation et d'analyse des fichiers .	Protection contre les programmes malveillants	Avertissement
Les clés de fonctionnalité expirent	(Comme pour toutes les fonctionnalités)	
Le service de réputation de fichiers ou d'analyse de fichiers est inaccessible.	Protection contre les programmes malveillants	Avertissement
La communication avec les services infonuagiques est établie.	Protection contre les programmes malveillants	Information
		Information
Un verdict de réputation de fichier change.	Protection contre les programmes malveillants	Information
Les types de fichiers pouvant être envoyés pour analyse ont été modifiés. Vous souhaiterez peut-être activer le chargement de nouveaux types de fichiers.	Protection contre les programmes malveillants	Information

Description de l'alerte	Type	Gravité
L'analyse de certains types de fichiers est temporairement indisponible.	Protection contre les programmes malveillants	Avertissement
L'analyse de tous les types de fichiers pris en charge est restaurée après une panne temporaire.	Protection contre les programmes malveillants	Information
Clé de service d'analyse de fichiers non valide. Vous devez contacter le service d'assistance technique de Cisco avec les détails d'ID de l'analyse des fichier pour corriger cette erreur.	Cisco Secure Endpoint	Erreur

Thèmes connexes

- Plusieurs alertes concernant l'échec de la connexion aux serveurs d'analyse ou de réputation des fichiers , on page 23
- Mesures à prendre lors de changements de verdicts des menaces de fichiers , on page 22

Configuration de rapports centralisés pour les fonctionnalités Cisco Secure Endpoint

Si vous souhaitez centraliser les rapports sur une appliance de gestion de la sécurité, consultez les exigences de configuration importantes décrites aux sections Cisco Secure Endpoint de la rubrique relative aux rapports par dans l'aide en ligne ou le guide de l'utilisateur de votre appliance de gestion.

Création de rapports et suivi de la réputation et de l'analyse des fichiers

- Identification des fichiers par algorithme de hachage SHA-256 , on page 18
- Pages de rapport de réputation et d'analyse des fichiers, on page 19
- Affichage des données de filtrage de réputation des fichiers dans d'autres rapports , on page 20
- À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint , on page 21

Identification des fichiers par algorithme de hachage SHA-256

Comme les noms de fichiers peuvent être facilement modifiés, l'appliance génère un identifiant pour chaque fichier à l'aide d'un algorithme de hachage sécurisé (SHA-256). Si une appliance traite le même fichier avec des noms différents, toutes les instances sont reconnues comme ayant le même SHA-256. Si plusieurs appliances traitent le même fichier, toutes les instances du fichier ont le même identifiant SHA-256.

Dans la plupart des rapports, les fichiers sont répertoriés en fonction de leur valeur SHA-256 (dans un format abrégé). Pour identifier les noms de fichiers associés à une instance de programme malveillant dans votre

entreprise, sélectionnez Reporting (Rapports) > Cisco Secure Endpoint et cliquez sur un lien SHA-256 dans le tableau. La page de détails affiche les noms de fichiers associés.

Pages de rapport de réputation et d'analyse des fichiers

Rapport	Description
Cisco Secure Endpoint	Affiche les menaces basées sur les fichiers qui ont été identifiées par le service de réputation des fichiers. Pour les fichiers dont les verdicts ont été modifiés, consultez le rapport sur les mises à jour des verdicts Cisco Secure Endpoint . Ces verdicts ne sont pas reflétés dans le rapport Cisco Secure Endpoint. Si un fichier extrait d'un fichier compressé ou archivé est malveillant, seule la valeur SHA du fichier compressé ou archivé est incluse dans le rapport Cisco Secure Endpoint. La section **Incoming Malware Files by Category** (Fichiers de programmes malveillants entrants par catégorie) indique le pourcentage d'informations SHA du fichier de la liste de blocage reçue de la console Cisco Secure Endpoint qui sont classées comme **Custom Detection** (Détection personnalisée). Le nom de menace du fichier SHA sur la liste de blocage reçue de la console Cisco Secure Endpoint est affiché comme **Simple Custom Detection** (Détection personnalisée simple) dans la section Incoming Malware Threat Files (Fichiers de programmes malveillants entrants) du rapport. Vous pouvez cliquer sur le lien dans la section More Details (Plus de détails) du rapport pour afficher les détails de la trajectoire du fichier au sujet des informations SHA du fichier dans la liste de blocage dans la console Cisco Secure Endpoint. Vous pouvez consulter les détails du verdict de **risque faible** dans la section Incoming Files Handed by Cisco Secure Endpoint (Fichiers entrants gérés par Cisco Secure Endpoint) du rapport.

Rapport	Description
Cisco Secure Endpoint File Analysis (Analyse des fichiers)	Affiche l'heure et le verdict (ou verdict provisoire) pour chaque fichier envoyé pour analyse. L'appliance vérifie les résultats de l'analyse toutes les 30 minutes. Pour afficher plus de 1000 résultats d'analyse des fichiers, exportez les données dans un fichier .csv. Accédez aux résultats détaillés de l'analyse, notamment les caractéristiques des menaces pour chaque fichier. Vous pouvez également rechercher des informations supplémentaires sur une valeur SHA ou cliquer sur le lien au bas de la page des détails de l'analyse des fichiers pour afficher des détails supplémentaires sur le serveur qui a analysé le fichier. **Remarque** Si des fichiers extraits d'un fichier compressé ou archivé sont envoyés pour analyse, seules les valeurs SHA de ces fichiers extraits sont incluses dans le rapport d'analyse des fichiers.
Cisco Secure Endpoint Reputation (Réputation)	Étant donné que Cisco Secure Endpoint est axé sur les menaces ciblées et de type « jour zéro », les verdicts sur les menaces peuvent changer à mesure que les données agrégées fournissent davantage d'informations. Le rapport de réputation Cisco Secure Endpoint répertorie les fichiers traités par cette appliance pour lesquels le verdict a changé depuis la réception du message. Pour plus d'informations sur cette situation, consultez Mises à jour des verdicts de menaces des fichiers , à la page 2. Pour afficher plus de 1000 mises à jour de verdicts, exportez les données dans un fichier .csv. Dans le cas de plusieurs modifications de verdicts pour un seul protocole SHA-256, ce rapport affiche uniquement le dernier verdict, et non l'historique des verdicts. Pour afficher tous les messages affectés par un protocole SHA-256 particulier pendant la plage de temps maximale disponible (quelle que soit la plage de temps sélectionnée pour le rapport), cliquez sur un lien SHA-256.

Affichage des données de filtrage de réputation des fichiers dans d'autres rapports

Les données relatives à la réputation et à l'analyse des fichiers sont disponibles dans d'autres rapports, le cas échéant. La colonne « Blocked by Cisco Secure Endpoint » (Bloqué par/Détecté par) peut être masquée par défaut dans les rapports applicables. Pour afficher d'autres colonnes, cliquez sur le lien Columns (Colonnes) sous le tableau.

Le rapport par emplacement utilisateur comprend un onglet Cisco Secure Endpoint.

À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint

Lorsque vous recherchez des informations sur les menaces liées aux fichiers dans le cadre du suivi Web, gardez à l'esprit les points suivants :

- Pour rechercher des fichiers malveillants trouvés par le service de réputation des fichiers, sélectionnez **Known Malicious and High-Risk Files** (Fichiers malveillants et à haut risque connus) pour l'option **Filter by Malware Category** (Filtrer par catégorie de programmes malveillants) dans la zone Malware Threat (Programmes malveillants) dans la section Advanced (Advanced) du suivi des messages Web.
- Le suivi des Web inclut uniquement des informations sur le traitement de réputation des fichiers et les verdicts de réputation de fichier initiaux renvoyés au moment du traitement d'un message de transaction. Par exemple, si un fichier a initialement été jugé sain, une mise à jour du verdict a révélé que le fichier est malveillant, seul le verdict sain s'affiche dans les résultats du suivi.

  Aucune information n'est fournie pour les pièces jointes propres ou non analysables.

  La mention « Block – AMP » dans les résultats de recherche signifie que la transaction a été bloquée en raison du verdict de réputation du fichier.

  Dans les détails du suivi, le « score de menace AMP » est le score le plus approprié fourni par le service de réputation en nuage quand un verdict clair concernant le fichier ne peut pas être déterminé. Dans cette situation, le score est compris entre 1 et 100. (Ignorez le score de menace AMP si un verdict Cisco Secure Endpoint est rendu ou si le score est de zéro .) L'appliance compare ce score au score du seuil (configuré sur la page Services de sécurité > Anti-Malware and Reputation) pour déterminer l'action à entreprendre. Par défaut, les fichiers renvoyant un score compris entre 60 et 100 sont considérés comme malveillants. Cisco ne recommande pas de modifier la note de seuil par défaut. Le score WBRS correspond à la réputation du site à partir duquel le fichier a été téléchargé; ce score n'est pas lié à la réputation du fichier.
- Les mises à jour de verdicts sont uniquement disponibles dans le rapport sur les mises à jour de verdicts Cisco Secure Endpoint . Les détails du message de d'origine dans le suivi des messages ne sont pas mis à jour avec les changements de verdict. Pour voir les transactions impliquant un fichier particulier, , cliquez sur un SHA-256 dans le rapport sur les mises à jour de verdicts.
- Les renseignements concernant l'analyse de fichier, notamment les résultats de l'analyse et l'envoi ou non d'un fichier pour analyse, sont uniquement accessibles dans le rapport d'analyse des fichiers.

  Des renseignements supplémentaires sur un fichier analysé peuvent être disponibles sur le serveur d'analyse de fichiers en nuage ou sur site. Pour afficher les informations d'analyse de fichier disponibles pour un fichier, sélectionnez le **Reporting > File Analysis** (Rapports > Analyse des fichiers) et saisissez SHA-256 pour rechercher le fichier ou cliquez sur le lien SHA-256 dans les détails du suivi Web. Si le service d'analyse des fichiers a analysé le fichier à partir de n'importe quelle source, vous pouvez voir les détails. Les résultats sont affichés uniquement pour les fichiers qui ont été analysés.

  Si l'appliance a traité une instance ultérieure d'un fichier qui a été envoyé pour analyse, ces instances apparaîtront dans les résultats de recherche du suivi des messages Web.

Mesures à prendre lors de changements de verdicts des menaces de fichiers

Étape 1 Affichez le rapport sur les mises à jour des verdicts de Cisco Secure Endpoint .

Étape 2 Cliquez sur le lien SHA-256 approprié pour afficher les données Web pour toutes les transactions impliquant des le fichier auquel les utilisateurs finaux ont été autorisés à accéder.

Étape 3 À l'aide des données de suivi, identifiez les utilisateurs qui pourraient être en danger, ainsi que des informations telles que les noms de fichiers impliqués dans l'incident et le site Web à partir duquel le fichier a été téléchargé.

Étape 4 Consultez le rapport d'analyse de fichier pour voir si ce SHA-256 a été envoyé pour analyse, afin de comprendre plus en détail la menace qu'implique le fichier.

What to do next

Thèmes connexes

Mises à jour des verdicts de menaces des fichiers , on page 2

Résolution des problèmes liés à la réputation et à l'analyse des fichiers

- Fichiers de journalisation , on page 22
- Plusieurs alertes concernant l'échec de la connexion aux serveurs d'analyse ou de réputation des fichiers , on page 23
- Erreur de clé API (analyse des fichiers sur site) , on page 23
- Les fichiers ne sont pas chargés comme prévu , on page 24
- Les détails de l'analyse des fichiers dans le nuage sont incomplets , on page 24
- Alertes sur les types de fichiers pouvant être envoyés à des fins d'analyse , on page 24

Fichiers de journalisation

Dans les journaux :

- `AMP` et `amp` font référence au service ou au moteur de réputation de fichiers.
- `Retrospective` fait référence aux mises à jour de verdict.
- `VRT` et `sandboxing` font référence au service d'analyse des fichiers.

Les informations sur Cisco Secure Endpoint, y compris l'analyse des fichiers, sont enregistrées dans les journaux d'accès ou dans les journaux du moteurCisco Secure Endpoint . Pour en savoir plus, consultez la rubrique sur la supervision de l'activité du système par le biais des journaux.

Dans le message de journal « Response received for file reputation query » (Réponse reçue à la requête de réputation de fichier), les valeurs possibles pour « upload action » sont les suivantes :

- 1 : SEND. Dans ce cas, vous devez envoyer le fichier pour analyse de fichier.
- 2 : DON'T SEND. Dans ce cas, vous n'envoyez pas le fichier pour analyse de fichier.
- 3 : SEND ONLY METADATA. Dans ce cas, vous envoyez uniquement les métadonnées, et non le fichier entier, à l'analyse de fichier.
- 0 : NO ACTION. Dans ce cas, aucune autre action n'est requise.

Plusieurs alertes concernant l'échec de la connexion aux serveurs d'analyse ou de réputation des fichiers

Problème

Vous recevez plusieurs alertes concernant des échecs de connexion aux services d'analyse ou d'analyse de réputation des fichiers dans le nuage. (Une seule alerte peut indiquer qu'un problème transitoire.)

Solution

- Assurez-vous d'avoir satisfait aux exigences mentionnées dans Exigences de communication avec les services de réputation et d'analyse de fichiers , on page 6.
- Vérifiez les problèmes de réseau qui pourraient empêcher l'appliance de communiquer avec les services en nuage.
- Augmentez la valeur du délai d'expiration de la requête :

  Sélectionnez **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation/Réputation et analyse des fichiers). La valeur du délai d'expiration de la requête se trouve dans la zone des paramètres avancés de la section Cisco Secure Endpoint **Services**.

Erreur de clé API (analyse des fichiers sur site)

Problème

Vous recevez une alerte de clé API lorsque vous tentez d'afficher les détails du rapport d'analyse de fichiers ou l' Secure Web Appliance ne peut pas se connecter au serveur Cisco Secure Endpoint Malware Analytics pour charger les fichiers à analyser.

Solution

Cette erreur peut se produire si vous modifiez le nom d'hôte du serveur Cisco Secure Endpoint Malware Analytics et que vous utilisez un certificat autosigné par le serveur Cisco Secure Endpoint Malware Analytics, ainsi que dans d'autres circonstances éventuellement. Pour résoudre le problème :

- Générez un nouveau certificat à partir de l'appliance Cisco Secure Endpoint Malware Analytics qui porte le nouveau nom d'hôte.
- Chargez le nouveau certificat sur l'appliance Secure Web Appliance.
- Réinitialisez la clé API sur l'appliance Cisco Secure Endpoint Malware Analytics. Pour obtenir des instructions, consultez l'aide en ligne sur l'appliance Cisco Secure Endpoint Malware Analytics.

Thèmes connexes

- Activation et configuration des services de réputation et d'analyse des fichiers

Les fichiers ne sont pas chargés comme prévu

Problème

Les fichiers ne sont pas évalués ou analysés comme prévu. Il n'y a aucune alerte ou erreur manifeste.

Solution

Prenez en compte les éléments suivants :

- Le fichier peut avoir été envoyé pour analyse par une autre appliance et donc déjà être présent sur le serveur d'analyse des fichiers ou dans le cache de l'appliance qui traite le fichier.
- Vérifiez la limite de taille de fichier maximale configurée pour les **limites d'analyse des objets du moteur DVS** sur la page **Security Services > Anti-Malware and Reputation** (Services de sécurité > Protection contre les programmes malveillants et réputation). Cette limite s'applique aux fonctionnalités Cisco Secure Endpoint.

Les détails de l'analyse des fichiers dans le nuage sont incomplets

Problème

Les résultats complets de l'analyse des fichiers dans le nuage public ne sont pas disponibles pour les fichiers chargés à partir d'autres Secure Web Appliance de mon organisation.

Solution

Assurez-vous de regrouper toutes les appliances qui partageront les données de résultats de l'analyse des fichiers. Consultez (Services d'analyse des fichiers dans le nuage public uniquement) Configuration des groupes d'appliances , on page 15. Cette configuration doit être effectuée sur chaque appliance du groupe.

Alertes sur les types de fichiers pouvant être envoyés à des fins d'analyse

Problème

Vous recevez des alertes d'informations sur la gravité sur les types de fichiers qui peuvent être envoyés pour analyse des fichiers.

Solution

Cette alerte est envoyée lorsque les types de fichiers pris en charge changent ou lorsque l'appliance vérifie quels types de fichiers sont pris en charge. Cela peut se produire dans les cas suivants :

- Vous ou un autre administrateur modifiez les types de fichiers sélectionnés pour analyse.
- Les types de fichiers pris en charge changent temporairement en fonction de la disponibilité dans le service en nuage. Dans ce cas, la prise en charge des types de fichiers sélectionnés sur l'appliance sera restaurée dès que possible. Les deux processus sont dynamiques et ne nécessitent aucune action de votre part.
- L'appliance redémarre, par exemple dans le cadre d'une mise à niveau d'AsyncOS.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.