Configurer et surveiller les événements criminalistiques

L'ensemble de fonctionnalités **criminalistiques** permet de surveiller et d'envoyer des alertes pour d'éventuels incidents de sécurité en capturant les événements criminalistiques en temps réel et en appliquant des règles définies par l'utilisateur. Plus précisément, il permet la :

- Définition de règles pour préciser les événements d'intérêt criminalistique
- Définition des actions de déclencheur pour les événements criminalistiques correspondants
- Recherche d'événements criminalistiques spécifiques
- Visualisation des processus générateurs d'événements et leurs lignages complets

Avertissement Lorsque la fonction d' **criminalistique** est activée, les agents logiciels peuvent avoir besoin de ressources de l'hôte supplémentaires en fonction de la configuration de l'agent. Consultez la section de configuration de l'agent logiciel.

Compatibilité

Les signaux criminalistiques sont rapportés par les agents de visibilité en profondeur sur toutes les plateformes, à l'exception de Solaris. Actuellement, seuls quelques signaux criminalistiques sont pris en charge par AIX. Pour en savoir plus, consultez la section Signaux .criminalistiques

Les renseignements criminalistiques sont fournis par le biais des API du noyau Linux, d'audit et du journal système, les API du noyau Windows, les événements Windows, le système d'audit AIX et autres. En général, les fournisseurs de systèmes d'exploitation garantissent la compatibilité au sein d'une version majeure. Toutefois, il est possible que les API diffèrent légèrement d'une plateforme à l'autre et d'une version mineure à l'autre, car les fournisseurs de systèmes d'exploitation peuvent reporter des fonctionnalités et des correctifs. Par conséquent, certains types d'événements d'criminalistiques peuvent ne pas être disponibles sur certaines plateformes. De plus, l'agent ne tente pas de récupérer ou d'activer les services de système d'exploitation désactivés au démarrage de l'agent.

Par exemple, il existe un certain nombre de signaux criminalistiques qui utilisent le cadre d'audit Linux. Si la criminalistique est activée, un agent de visibilité approfondie insère des règles d'audit Cisco Secure Workload dans le système après le démarrage de l'agent. L'insertion de règle nécessite que le système ait l'utilitaire augenrules installé et le répertoire /etc/audit/rules.d. Si l'une de ces conditions préalables n'est pas remplie, les règles d'audit Cisco Secure Workload ne seront pas insérées. Par conséquent, les signaux criminalistiques, y compris l'accès aux fichiers et la création de sockets bruts, ne seront pas signalés.

Si un utilisateur a activé la fonction criminalistique précédemment et la désactive, l'agent supprime les règles d'audit qui sont insérées par Cisco Secure Workload. Sur Red Hat 7.3 et CentOS 7.3, nous avons observé un bogue du système d'exploitation qui pourrait avoir une incidence sur le processus de suppression de règles. L'agent supprime les règles d'audit en : 1. Suppression du fichier taau.rules dans le dossier */etc/audit/rules.d/* 2. Exécution de *$service auditd restart*. Le système d'exploitation régénère l'ensemble de règles en fonction des fichiers *audit.rules* et **.rules* dans */etc/audit/rules.d/*. Ensuite, auditd chargera les règles dans le système.

Le système d'exploitation ajoute *-D* au début du fichier /etc/audit/rules.d/audit.rules pour effacer toutes les règles avant d'insérer le nouvel ensemble de règles. Cependant, sur les machines Red Hat 7.3 et CentOS 7.3, le fichier */etc/audit/rules.d/audit.rules* peut ne pas comporter *-D*. En effet, le système d'exploitation crée un fichier vide */etc/audit/rules.d/audit.rules* si ce fichier n'existe pas et un fichier de règles par défaut dans le sous-répertoire */usr/watch/doc/audit-* <version> / s'il n'existe pas non plus. Par exemple, */usr/share/doc/audit-2.8.4/rules/10-base-config.rules* est un emplacement possible par défaut pour les règles. Le comportement exact du système d'exploitation peut être observé à partir du script de mise à jour de RPM en exécutant *$rpm-qf-scripts/etc/audit/rules.d*

Sous Linux, certains signaux criminalistiques reposent sur l'observation d'appels systèmes 64 bits. Les appels système Linux 32 bits ne sont pas pris en charge dans la version actuelle.

Signaux criminalistiques

La fonction **Forensics** (Criminalistique) doit être activée pour que les agents logiciels puissent saisir et signaler les événements criminalistiques. La fonction peut être activée dans la configuration de l'agent logiciel. Pour en savoir plus, consultez la section Configuration de l'agent logiciel.

Lorsque la fonction **Forensics** (Criminalistique) est activée, l'agent signale les événements criminalistiques suivants.

Signal	Description
Escalade de privilèges	Les escalades de privilèges, telles que les commandes exécutées avec sudo.
Connexion de l'utilisateur	Événements de connexion de l’utilisateur.
Échec de connexion de l’utilisateur	Les tentatives de connexion de l’utilisateur qui ont échoué
Shellcode	Les exécutions de shell suspectes ressemblant à des tentatives de code shell
Accès au fichier	L'accès aux fichiers sensibles tels que les fichiers de mots de passe.
Compte d'utilisateur	L'ajout ou la suppression de comptes utilisateur
Commande non vue	Les nouvelles commandes que l’agent n’a pas vues. Les utilisateurs peuvent utiliser la note d’anomalie de commande pour ajuster les résultats en fonction de la portée. Consultez la section Commande non vue pour plus de détails.
Bibliothèque non vue	La nouvelle bibliothèque que l'agent n'a pas encore vu fonctionner et qui a été chargée auparavant.
Création d’interface de connexion brute	Les processus créant des sockets bruts. Par exemple, le port knocking (frappe).
Fichier binaire modifié	Les modifications apportées aux valeurs de condensé ou aux heures de modification de fichiers binaires connus.
Bibliothèque modifiée	Les modifications apportées aux valeurs de condensé ou aux heures de modification de bibliothèques connues.
Canaux auxiliaires	Les tentatives d’attaques par canal auxiliaire (Meltdown).
Suivre la connexion de l’utilisateur	Les processus descendants qui bifurquent ou s'exécutent après les événements de connexion.
Suivre le processus	Les événements de processus de suivi signalent les processus qui correspondent aux règles de configuration criminalistique de l’utilisateur en fonction des attributs de processus tels que le chemin binaire, la chaîne de commande, etc.
Anomalie de réseau	Pour les anomalies de trafic réseau du charge de travail, consultez Détection des anomalies de réseau basée sur le PCR pour en savoir plus.

Table 1: Signaux criminalistiques pris en charge sur AIX

Signal	Description
Escalade de privilèges	Les escalades de privilèges, telles que les commandes exécutées avec sudo.
Création d'interface de connexion brute	Les processus créant des sockets bruts. Par exemple, le port knocking (frappe).
Compte d'utilisateur	L'ajout ou la suppression de comptes utilisateur

Escalade de privilèges

Lorsque le processus fait passer son privilège de faible à élevé, ceci est considéré comme une escalade de privilèges. Sous Linux, cela signifie que l'ID utilisateur du processus est passé de non nul à nul. Il existe des cas légitimes tels que la modification du mot de passe d'un utilisateur ordinaire et d'autres programmes binaires à usage spécial tels que Sudo. Cet événement n'est actuellement pas disponible dans Windows. L'escalade de privilèges dans Windows se fait généralement par d'autres mécanismes plutôt que par la modification des privilèges du processus lui-même, c'est-à-dire le niveau d'intégrité. Les escalades de privilèges sur Windows sont couvertes par d'autres types d'événements criminalistiques, tels que des commandes ou des modifications binaires non vues.

Connexion de l'utilisateur

L'utilisateur se connecte aux événements, y compris SSH, RDP et d'autres types de connexions. Chaque fois que cela est possible, les capteurs permettent de savoir qui, quand et comment un utilisateur se connecte. Par exemple, pour SSH sous Linux, les capteurs indiquent le nom d'utilisateur, le type d'authentification (mot de passe, public) et l'adresse IP source.

Échec de connexion de l'utilisateur

Comme pour les événements de connexion de l'utilisateur ci-dessus, les capteurs signalent l'échec des tentatives de connexion avec des informations similaires lorsqu'elles sont disponibles.

Shellcode

Les événements de shellcode ont des interprétations différentes sous Linux et Windows. Sous Linux, les capteurs identifient les processus s'exécutant en tant qu'interface Shell interactive sans session de connexion ni point terminal. (Il n'y a aucune raison réelle pour qu'un shell interactif s'exécute en dehors d'une session de connexion). Dans cette version, la détection des événements de shellcode est limitée, car elle suppose que l'attaque utilisera un shell déjà disponible dans le système. Si une attaque télécharge de nouveaux fichiers binaires, les capteurs signalent ces fichiers binaires soit comme des commandes non vues, soit comme des modifications binaires, s'ils remplacent des fichiers binaires existants. Dans Windows, chaque processus lié à la DLL PowerShell sera étiqueté comme shellcode. Les utilisateurs peuvent créer des règles pour filtrer les dossiers légitimes.

Accès au fichier

Les événements d'accès aux fichiers signalent les accès aux fichiers sensibles, tels que les fichiers de mots de passe. Dans cette version, la liste des fichiers à surveiller ne peut pas être modifiée par les utilisateurs. Sous Linux, le capteur surveille l'accès en écriture au dossier /etc/passwd. Le capteur surveille également les accès en lecture et en écriture au dossier /etc/shadow. Windows ne déclenchera pas cet événement dans cette version.

Compte d'utilisateur

Les événements de comptes d'utilisateurs signalent la création de comptes d'utilisateurs locaux chaque fois que les informations sont disponibles.

Commande non vue

Les événements de commandes non vue signalent des commandes que le capteur n'a pas encore vues. Une commande non vue est définie comme une transition ou une périphérie non vue d'un processus parent à un processus enfant. Par exemple, en supposant qu'un serveur Web (httpd) exécute un script CGI appelé abc.sh, lorsque le capteur le verra pour la première fois, il signale abc.sh comme une commande non vue. Les exécutions ultérieures de abc.sh par le serveur Web n'entraîneront pas d'événements criminalistique, car le capteur l'a déjà vu et signalé. Si un service ou un processus n'exécute jamais de fichier binaire, un événement de commande non vue de ce service ou processus indique une dégradation malveillante possible. Notez que les capteurs sont sans état au redémarrage, donc une commande vue précédemment sera à nouveau signalée après le redémarrage du capteur.

À partir de la version 3.4, pour les grappes de logiciels-services, chaque événement de commande non vue est associé à un score d'anomalie de commande allant de 0.0 à 1.0. Plus la note est faible, plus la transition est anormale. Les transitions de commande, c'est-à-dire les n-uplets (ligne de commande parente, ligne de commande) font l'objet d'une vérification croisée pour détecter les transitions anormales parmi les événements ayant le même n-uplet ci-dessous :

- Les portées les plus étroits auxquels le capteur appartient. Par exemple, l'événement de commande non vue est observé sur la charge de travail W qui appartient aux lignages de portée suivants :: `Portée racine -> A -> B -> C et Portée racine -> D -> E`. Ensuite, la commande est recoupée par rapport à toutes les charges de travail des portées C et E (à noter que C et E peuvent se chevaucher ou non). La note d'anomalie de l'événement est le maximum des notes d'anomalie de l'événement en ce qui concerne ces 2 portées.
- Chemin d'exécution du processus en cours d'exécution.
- Le chemin d'exécution du processus parent.
- Le condensé binaire du processus en cours d'exécution.

Une note de 1.0 signifie que la même transition de commande ayant le même nuplet `(portée la plus étroite, chemin d'exécution, chemin d'exécution parent, condensé binaire)` a été observée. Une note de 0.0 signifie qu'une transition de commande avec un tel chemin d'exécution, le chemin d'exécution parent et le condensé binaire du processus en cours n'a jamais été observée sur des hôtes des mêmes portées. La note d'anomalie peut être utilisé pour supprimer le déclenchement d'alertes de commandes non vues similaires dans la même portée et réduire les faux positifs. Consultez Règles Cisco Secure Workload par défaut pour obtenir un exemple de la façon dont cette note peut être utilisée.

Note Le score d'anomalie est uniquement disponible pour les grappes de logiciels-services à partir de la version 3.4.

Bibliothèque non vue

Les événements de bibliothèque non vue signalent les bibliothèques pour lesquelles le capteur n'a pas vu de processus téléversé auparavant. Une bibliothèque non vue est définie comme une paire non visible de chemin d'exécution binaire et de chemin de bibliothèque. Par exemple, une application téléverse généralement une liste de bibliothèques relativement stable. Un attaquant qui a accès à la machine peut redémarrer l'application et les bibliothèques malveillantes LD_PRELOAD. Lorsque le capteur détecte les bibliothèques malveillantes nouvellement téléversées dans le chemin d'exécution binaire de cette application pour la première fois, il signale des événements de bibliothèque non vue. Les chargements ultérieurs des bibliothèques malveillantes n'entraîneront pas d'événements criminalistique, car le capteur les a déjà vus et signalés. Les cas légitimes comprennent l'application qui téléverse de nouvelles bibliothèques après la mise à niveau ou les applications qui téléversent dynamiquement de nouvelles bibliothèques. Notez que les capteurs peuvent signaler à nouveau une bibliothèque vue précédemment après le redémarrage.

Notez qu'il s'agit d'une fonctionnalité expérimentale et susceptible de changer dans les versions futures.

Création d'interface de connexion brute

Les événements de création d'interface de connexion (socket) brute ne sont pris en charge que sur cette version. Les sockets bruts sont généralement utilisés pour surveiller ou injecter / usurper le trafic. Il y a des utilisations légitimes des sockets bruts, par exemple dans les outils de diagnostic comme tcpdump, ou lors de la création de paquets IP spéciaux comme ping ou aRP. Les utilisations malveillantes incluent les analyses furtives pour éviter la journalisation par machines cible / victime, les programmes malveillants de port d'accès, etc. Les capteurs Cisco Secure Workload créent également des sockets bruts pour collecter des informations relatives au flux. (Par souci de cohérence, les capteurs ne suppriment pas les événements déclenchés par leur propre collecte d'informations de flux).

Fichier binaire modifié

Les événements binaires modifiés signalent les modifications apportées au contenu du fichier et aux attributs des fichiers binaires pour les processus en cours d'exécution. Les capteurs enregistrent les attributs de fichier de chaque processus en cours d'exécution. Si un processus exécute un fichier binaire dans le même chemin, mais avec des attributs de fichier différents (ctime, mtime, taille ou condensé), le capteur signale le processus comme modification de fichier binaire. Les cas légitimes comprennent la mise à niveau de l'application.

Bibliothèque modifiée

Les événements de modification de bibliothèque signalent les modifications apportées au contenu et aux attributs du fichier des bibliothèques pour les processus en cours d'exécution. Les capteurs enregistrent les attributs de fichier des bibliothèques chargées. Si un processus charge une bibliothèque par le même chemin, mais avec des attributs de fichier différents (ctime, mtime, taille ou condensé), le capteur signalera le processus come ayant subi une modification de bibliothèque. Les cas légitimes comprennent la mise à niveau de la bibliothèque.

Notez qu'il s'agit d'une fonctionnalité expérimentale et susceptible de changer dans les versions futures.

Canaux auxiliaires

Les événements des canaux auxiliaires signalent l'exécution de logiciels qui exploitent les vulnérabilités de ces derniers. Cette version fournit une capacité de détection de canal auxiliaire unique sur une plateforme Linux sélectionnée : la fusion (Meltdown). Consultez les détails ci-dessous pour connaître les configurations de machines prises en charge. Il s'agit de fonctionnalités de sécurité avancées qui sont donc désactivées par défaut. Les utilisateurs doivent s'attendre à une augmentation de l'utilisation du processeur lorsque la création de rapports sur les canaux auxiliaires est activée. Le quota de CPU configuré dans l'interface utilisateur sera toujours respecté. Si le sous-processus de collecte criminalistique du capteur détermine que son utilisation du processeur est trop élevée pendant trop longtemps, il s'arrête et le processus du capteur parent le redémarre avec un léger délai. L'activation de cette fonctionnalité sur des noyaux anciens ou non pris en charge pourrait entraîner une instabilité du système. Il est recommandé d'effectuer des tests dans des environnements similaires hors production.

Cette fonctionnalité peut être activée/désactivée à partir de la page de configuration de l'agent dans l'interface utilisateur et dans le profil de configuration de chaque agent.

La fusion (Meltdown) est une attaque de canal auxiliaire qui utilise abusivement les fonctionnalités d'exécution supposée et de mise en cache du processeur (https://meltdownattack.com/). Elle permet à un attaquant de lire les données du domaine privilégié à partir d'un domaine non privilégié, par exemple, la lecture de la mémoire du noyau d'une application de l'espace utilisateur sans privilèges d'anneau 0. La détection de la fusion prend actuellement en charge CentOS 7 et Ubuntu 16.04.

Suivre la connexion de l'utilisateur

Les événements de suivi de connexion d'utilisateur signalent les processus descendants (jusqu'à 4 niveaux) qui sont exécutés après un processus d'événement de connexion d'utilisateur (SSH, RDP, etc.). Les processus signalés dans le cadre de cet événement de suivi de connexion de l'utilisateur le sont à des fins d'audit et n retranscrivent pas nécessairement d'événements de sécurité.

Suivre le processus

Les événements de suivi de processus signalent les processus qui correspondent aux règles de configuration criminalistique de l'utilisateur en fonction des attributs de processus tels que le chemin binaire, la chaîne de commande, etc. Les processus signalés dans le cadre de cet événement de suivi du processus le sont à des fins d'audit et ne comportent pas nécessairement d'événements de sécurité.

Exemple 1 : processus de rapport exécutés par cmd.exe ou powershell.exe

Event Type = Follow Process AND (Process Info - Exec Path contains cmd.exe OR Process Info - Exec Path contains powershell.exe)

Exemple 2 : Indiquer tous les processus créés par winword.exe, excel.exe ou powerpnt.exe.

Event Type = Follow Process with_ancestor (Process Info - Exec Path contains winword.exe OR Process Info - Exec Path contains excel.exe OR Process Info - Exec Path contains powerpnt.exe)

Remarque : Les événements de suivi du processus peuvent être suivis par l'un des signaux de processus suivants :

- Process Info - Exec Path

- Process Info - Command String
- Process Info - Username
- Follow Process - Parent Exec Path
- Follow Process - Parent Command String
- Follow Process - Parent Username

Configuration criminalistique

La fonction criminalistique utilise une configuration basée sur les intents. Les intents spécifient comment appliquer les profils criminalistiques aux filtres d'inventaire. Le profil criminalistique se compose de plusieurs règles criminalistiques. Les profils d'un intent sont appliqués dans l'ordre, de haut en bas.

Règles criminalistiques

Note Le nombre maximal de règles par portée racine est de 100.

Ajout d'une règle criminalistique

Cette section explique comment ajouter de nouvelles règles criminalistiques.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

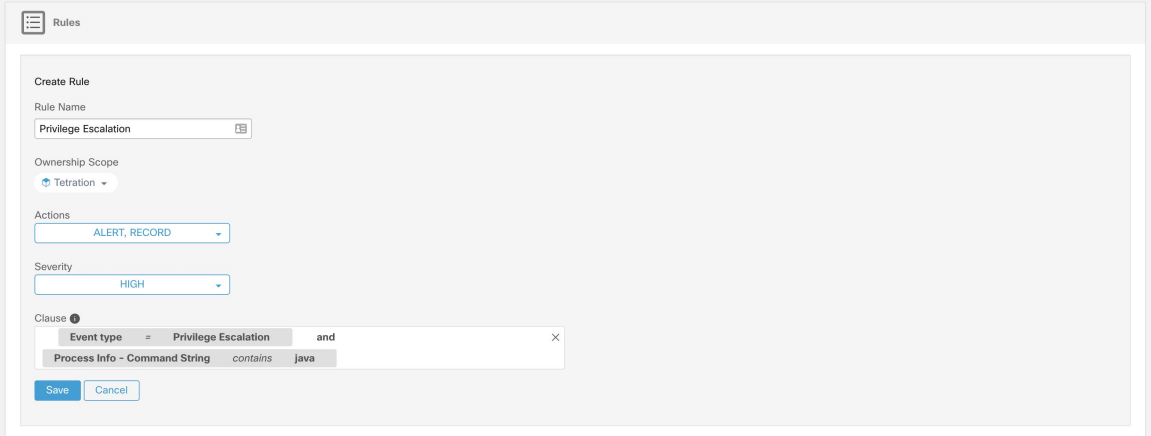
Étape 2 Cliquez sur **Create Rule** (créer une règle).

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom de la règle	Entrez un nom pour la règle. Le nom ne peut pas être vide
Portée de la propriété	Saisissez une portée de propriété pour cette règle.

Champ	Description
Actions	Sélectionnez des actions lorsque cette règle est déclenchée. **Record**(Enregistrement) : signifie que les événements de sécurité correspondants persistent pour une analyse plus approfondie. L'action d'**alerte** signifie la publication des événements de sécurité correspondants dans le système d'alerte Cisco Secure Workload.
Gravité	Sélectionnez le niveau de gravité de cette règle : **LOW**(FAIBLE), **MEDIUM**(MOYEN), **HIGH**(ÉLEVÉ), **CRITICAL**(CRITIQUE) ou **REQUIRES IMMEDIATE ACTION** (NÉCESSITE UNE ACTION IMMÉDIATE)
Article	Saisissez une clause de règle. Une clause doit contenir des signaux d'événement de sécurité provenant d'un événement criminalistique de processus ou d'un événement de charge de travail. Une clause n'est pas valide si elle contient à la fois des signaux de processus et de charge de travail.

Figure 1: Créer une règle



Étape 4 Cliquez sur **Save** (enregistrer).

Composition des règles criminalistiques de base

Une règle criminalistique doit contenir **exactement un** type d'événement criminalistique (par exemple, **Event Type == Unseen Command**). Les clauses facultatives suivantes utilisent les attributs de cet événement (par exemple, **Unseen Command - Parent Uptime**).

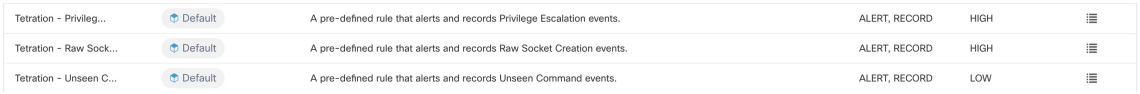
Vous trouverez ci-dessous un exemple d'utilisation du type d'événement **Unseen Command**. Pour obtenir d'autres exemples, consultez les règles par défaut et les règles MITRE.

EventType = Unseen Command et Unseen Command - Parent Uptime (microseconds) >= 60000000.

Règles Cisco Secure Workload par défaut

Les règles Cisco Secure Workload par défaut sont fournies pour aider les utilisateurs à élaborer des règles significatives dans leur environnement. Ces règles sont affichées dans la page de configuration criminalistique et elles ne sont pas modifiables. Les règles sont disponibles dans toutes les portées racine.

Figure 2: Règles par défaut



Les règles criminalistiques Cisco Secure Workload :

1. **Nom** Cisco Secure Workload - Escalade du privilège

   Clause EventType = Privilege Escalation and (**ProcessInfo - ExecPath** *doesn't contain* **sudo and ProcessInfo - ExecPath** *doesn't contain* **ping and Privilege Escalation Is** ⊨ **Type - Suid Binary**)

   Description. Cette règle signale les événements d'escalade de privilèges qui ne sont pas générés par les fichiers binaires setuid. Pour filtrer de manière fiable les fichiers binaires setuid, il est également possible de filtrer **sudo** et **ping** en fonction de « ProcessInfo - ExecPath ». Les utilisateurs Cisco Secure Workload peuvent également filtrer d'autres fichiers binaires setuid en définissant leurs propres règles.

2. **Name** Tetration - Commande non vue

   Clause EventType = Unseen Command and Unseen Command - Parent Uptime (microseconds) >= 60000000 or ProcessInfo - ExecPath *contains* **/bash or ProcessInfo - ExecPath** *contains* **/sh or ProcessInfo - ExecPath** *contains* **/ksh or Parent - ExecPath** *contains* **httpd or Parent - ExecPath** *contains* **apache or Parent - ExecPath** *contains* **nginx or Parent - ExecPath** *contains* **haproxy**

   Description. Cette règle signale les événements de commande non vues qui correspondent à l'un des critères suivants :

   a. Le processus parent est actif pendant plus de **60 000 000** de microsecondes.

   b. Le processus ExecPath contient un certain type d'interpréteur de commandes, par exemple **/bash**, **/sh** et **/ksh**.

   c. Le processus parent ExecPath contient un type d'application serveur, par exemple, **httpd**, **apache**, **nginx** et **haproxy**.

3. **Nom** Tetration - socket brut

   Clause EventType = Raw Socket Creation and (Raw Socket - ExecPath *doesn't contain* **ping and Raw Socket - ExecPath** *doesn't contain* **iptables and Raw Socket - ExecPath** *doesn't contain* **xtables-multi**)

   Description Cette règle signale les événements bruts de création de socket qui ne sont pas générés par **ping** et **iptables**. Les utilisateurs Cisco Secure Workload peuvent également filtrer d'autres fichiers binaires en définissant leurs propres règles.

4. **Name** Tetration - Anomalie de réseau avec commande non vue

   Clause EventType = Network Anomaly and Network Anomaly - Unseen Command Count > 3 and Network Anomaly - Non-seasonal Deviation > 0

   Description Cette règle signale les événements d'anomalie de réseau qui correspondent aux critères suivants :

a. Il y a plus de 3 événements de commande non vue sur la même charge de travail en 15 minutes.

b. L'Attributs de règles est supérieur à 0 (ce qui signifie également qu'il est supérieur ou égal à 6,0, car 6,0 est l'écart minimal signalé pour tous les événements d'anomalie de réseau).

5. **Name** Tetration - Commande anormale non vue

   Clause EventType = Unseen Command and Unseen Command - Anomaly - Score < 0.6

   Description Cette règle signale les événements de commande non vue dont la note d'anomalie est inférieure à 0,6. Cela signifie que seuls les événements fortement anormaux dont les commandes ne ressemblent pas aux commandes observées précédemment sont signalés. Le seuil de 0,6 est déterminé sur la base des expériences de Secure Workload concernant la similarité des commandes à différents seuils. Consultez Commande non vue pour une explication détaillée du résultat.

6. **Nom** Tetration : parent inhabituel de smss

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **smss.exe and (Follow Process - ParentExecPath** *doesn't contain* **smss.exe and Follow Process - ParentExecPath** *doesn't contain* **System)**

   Description Cette règle est spécifique à Windows. Cette règle alerte si smss.exe a un parent qui est différent d'une autre instance de smss.exe ou du processus système.

7. **Nom** Tetration - parent inhabituel de «wininit»

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **wininit.exe and Follow Process - ParentExecPath** *doesn't contain* **smss.exe**

   Description Cette règle est spécifique à Windows. Cette règle alerte si wininit.exe a un parent différent de smss.exe.

8. **Nom** Tetration - parent inhabituel de RuntimeBroker

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **RuntimeBroker.exe and Follow Process - ParentExecPath** *doesn't contain* **svchost.exe**

   Description Cette règle est spécifique à Windows. Cette règle alerte si RuntimeBroker.exe a un parent différent de svchost.exe.

9. **Nom** Tetration - parent inhabituel de services

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **services.exe and Follow Process - ParentExecPath** *doesn't contain* **wininit.exe**

   Description Cette règle est spécifique à Windows. Cette règle alerte si services.exe a un parent différent de winit.exe.

10. **Nom** Tetration - parent inhabituel de lsaio

    Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **lsaio.exe and Follow Process - ParentExecPath** *doesn't contain* **wininit.exe**

    Description Cette règle est spécifique à Windows. Cette règle alerte si lsaio.exe a un parent différent de « wininit.exe ».

11. **Nom** Tetration - Enfant inhabituel de lsass

Clause (EventType = Follow Process and ProcessInfo - ExecPath *doesn't contain* **efsui.exe and ProcessInfo - ExecPath** *doesn't contain* **werfault.exe**) **with ancestor Process Info - ExecPath** *contains* **lsass.exe**

Description Cette règle est spécifique à Windows. Cette règle alerte si lsass.exe a des descendants qui ne sont pas efsui.exe ou Werfault.exe.

Règles MITRE ATT&CK par défaut

Les règles par défaut de la fonction MITRE ATT&CK sont fournies pour envoyer des alertes techniques à partir du cadre de la fonction MITRE ATT&CK (https://attack.mitre.org/). Il y a 24 règles se rapportant au comportement malveillant et la plupart sont mises en correspondance à une technique MITRE particulière. La liste complète des règles se trouve ci-dessous.

1. **Nom** le comportement suspect de MS Office

   Clause (Event type = Follow Process and (Process Info - Exec Path doesn't contain **Windowssplwow64.exe) and (Process Info - Exec Path** *doesn't contain* **chrome.exe) and (Process Info - Exec Path** *doesn't contain* **msip.executionhost.exe) and (Process Info - Exec Path** *doesn't contain* **msip.executionhost32.exe) and (Process Info - Exec Path** *doesn't contain* **msosync.exe) and (Process Info - Exec Path** *doesn't contain* **ofccccaupdate.exe) with ancestor (Process Info - Exec Path** *contains* **winword.exe or Process Info -Exec Path** *contains* **excel.exe or Process Info -Exec Path contains powerpnt.exe)**

   Description Cette règle alerte et enregistre le fait que les processus Microsoft Office (WIN-WORD.exe/EXCEL.exe/POWERPNT.exe) créent des processus enfants. Sur la base de nos recherches, nous avons autorisé quelques processus enfants courants connus pour être créés par ces fichiers binaires MS Office, afin de réduire le nombre de faux positifs.

2. **Nom** T1015 – Fonctions d'accessibilité 1

   Clause Event type = Follow Process (Process Info - Exec Path *contains* **cmd.exe or Process Info -Exec Path** *contains* **powershell.exe or Process Info - Exec Path** *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and (Follow Process - Parent Exec Path** *contains* **winlogon.exe or Follow Process - Parent Exec Path** *contains* **atbroker.exe or Follow Process - Parent Exec Path** *contains* **utilman.exe**)

   Description Cette règle alerte et enregistre les cas où les fichiers binaires des fonctions d'accessibilité (clavier à l'écran, loupe, touches rémanentes, etc). sont utilisés de manière abusive et incitent à ouvrir cmd/powershell/cscript/wscript. L'appel des fichiers binaires d'accessibilité est contrôlé par les processus winlogon, atbroker ou utilman, selon l'endroit où ils sont appelés (à partir de l'écran de connexion ou après la connexion de l'utilisateur). Cette règle intercepte les processus enfants suspects (cmd.exe, powershell.exe, cscript.exe, wscript.exe) des processus d'accessibilité (winlogon.exe, utilman.exe et atbroker.exe). Utilisez-le avec **T1015 – Fonctionnalités d'accessibilité 2** pour détecter également les processus enfants supplémentaires de ces quatre processus enfants suspects**.

3. **Nom** T1015 – Fonctions d'accessibilité 2

   Clause Event type = Follow Process with ancestor ((Process Info - Exec Path *contains* **cmd.exe or Process Info - Exec Path** *contains* **powershell.exe or Process Info - Exec Path** *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and (Follow Process - Parent Exec Path** *contains* **winlogon.exe or Follow Process - Parent Exec Path** *contains* **atbroker.exe or Follow Process - Parent Exec Path** *contains* **utilman.exe))**

   Description Cette règle alerte et enregistre si l'un des exécutables des fonctionnalités d'accessibilité (clavier à l'écran, loupe, touches rémanentes, etc). est corrompu et incite à ouvrir

cmd.exe/powershell.exe/cscript.exe/wscript. exe. L'appel des fichiers binaires d'accessibilité est contrôlé par les processus winlogon, atbroker ou utilman, selon l'endroit où ils sont appelés (à partir de l'écran de connexion ou après la connexion de l'utilisateur). Cette règle capture les processus enfants suspects de ces processus (winlogon, utilman et atbroker). Il faut l'utiliser avec **T1015 – Fonctionnalités d'accessibilité 1** qui alerte les processus enfants suspects des fichiers binaires d'accessibilité.

4. **Nom** T1085 - runll32

   Clause (Event type = Follow Process and Process Info Exec Path *does not contain* **msiexec.exe and Process Info Exec Path** *does not contain* **WindowsSystem32SystemPropertiesRemote.exe with ancestor (Process Info - Exec Path** *contains* **rundll32.exe and Follow Process - Parent Exec Path** *does not contain* **msiexec.exe and not (Process Info -command string** *contains* **Windowssystem32shell32.dll or (Process Info -command string** *contains* **Windowssyswow64shell32.dll or (Process Info -command string** *contains* **WindowsSystem32migrationWinInetPlugin.dll))**

   Description Cette règle alerte et enregistre les cas où rundll32.exe crée des processus enfants. Ce fichier binaire peut être appelé pour exécuter des fichiers binaires/DLL quelconques ou utilisé par control.exe pour installer des éléments malveillants sur le panneau de configuration. Cependant, nous l'avons autorisé si msiexec.exe est le parent ou le descendant de runDLL32.exe. Nous avons également autorisé certaines des commandes courantes runDLL32 qui utilisent des DLL bien connues.

5. **Nom** T1118 – InstallUtil

   Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **hh.exe**

   Description Cette règle alerte et enregistre les cas où InstallUtil.exe crée des processus enfants.

6. **Nom** T1121 - Regsvcs/Remasm

   Clause Event type = Follow Process and (Process Info - Exec path *does not contain* **fondue.exe or Process Info - Exec path** *does not contain* **regasm.exe or Process Info - Exec path** *does not contain* **regsvr32.exe with ancestor (Process Info - Exec Path** *contains* **regasm.exe or Process Info - Exec Path** *contains* **regsvcs.exe)**

   Description Cette règle alerte et enregistre les cas où regsvcs.exe ou regasm.exe créent des processus enfants. Cependant, nous l'avons autorisée si fondue.exe/regasm.exe/regsvr32.exe est généré par regasm.exe ou regsvcs.exe afin de réduire le nombre de faux positifs.

7. **Nom** T1127 – Utilitaires pour développeurs de confiance – msbuild.exe

   Clause (Event type = Unseen Command with ancestor Process Info - Exec Path *contains* **MSBuild.exe) and (Process Info - Exec Path** *does not contain* **Tracker.exe) and (Process Info -Exec Path** *doesn't contain* **csc.exe) and (Process Info - Exec Path** *does not contain* **Microsoft Visual Studio) and (Process Info - Exec Path** *does not contain* **al.exe) and (Process Info - Exec Path** *does not contain* **lc.exe) and (Process Info - Exec Path** *does not contain* **dotnet.exe) and (Process Info - Exec Path** *does not contain* **cvtres.exe) and (Process Info - Exec Path** *does not contain* **conhost.exe) and not (Event type = Unseen Command with ancestor (Process Info - Exec Path** *contains* **Tracker.exe or Process Info - Exec Path** *contains* csc.exe or Process Info - Exec Path *contains* **Microsoft Visual Studio or Process Info - Exec Path** *contains* **al.exe or Process Info - Exec Path** *contains* **lc.exe or Process Info - Exec Path** *contains* **dotnet.exe or Process Info - Exec Path** *contains* **cvtres.exe))**

   Description Cette règle alerte et enregistre les cas où msbuild.exe crée des processus enfants qui n'appartiennent pas à une liste d'autorisation des processus enfants qu'il crée habituellement. Cette règle est actuellement basée sur la commande non vue, par opposition à Suivre le processus, car l'option Suivre le processus ne prend pas encore en charge l'autorisation des sous-arborescences de processus.

La règle actuelle autorise les processus suivants et leurs descendants : Tracker.exe, csc.exe, tout processus du chemin « Microsoft Visual Studio », al.exe, lc.exe, dotnet.exe et cvtres.exe. La règle autorise également conhost.exe. Ces processus peuvent être observés lors de l'utilisation normale de MSBuild.exe (par exemple, lors de la compilation d'un projet à l'aide de Visual Studio). Tous les autres descendants (comportement non habituel) de MSBuild.exe font l'objet d'alertes.

8. **Nom** T1127 – Utilitaires pour développeurs de confiance – rcsi.exe

   Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **rcsi.exe**

   Description Cette règle alerte et enregistre les cas où recsi.exe crée des processus enfants.

9. **Nom** T1127 – Utilitaires pour développeurs de confiance – tracker.exe

   Clause (Event type = Unseen Command with_ancestor Process Info - Exec Path *contains* **tracker.exe) and not (Event type = Unseen Command with_ancestor Process Info - Exec Path** *contains* **MSBuild.exe)**

   Description Cette règle alerte et enregistre les cas où tracker.exe crée des processus enfants et tracker lui-même n'est pas un descendant de MSBuild.exe. Ainsi, les appels légitimes du tracker via Visual Studio sont approuvés, mais les autres appels font l'objet d'alertes. L'une des limites des règles Tracker.exe et MSBuild.exe précédentes est que si un attaquant utilise la technique MSBuild pour créer Tracker, puis fait en sorte que Tracker crée un enfant malveillant, il ne sera pas alerté par l'une ou l'autre des règles puisque Tracker ayant MSBuild comme ancêtre est considéré comme légitime.

10. **Nom** T1128 – DLL de l'assistant Netsh

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **netsh.exe**

    Description Cette règle alerte et enregistre les cas où netsh.exe crée des processus enfants.

11. **Nom** T1136 - Créer un compte

    Clause Event type = User Account

    Description Cette règle alerte et enregistre la création d'un nouvel utilisateur.

12. **Nom** T1138 - Calage des applications

    Clause Event type = Follow Process Info - Exec Path *contains* **sdbinst.exe**

    Description Cette règle alerte et enregistre si sdbinst.exe est appelé.

13. **Name** T1180 - Économiseur d'écran

    Clause Event type = Follow Process AND with ancestor Process Info - Exec Path *contains* **.scr**

    Description Cette règle alerte et enregistre la création d'un processus avec la mention « .scr » dans le chemin d'exécution.

14. **Nom** T1191 – CMSTP

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **cmstp.exe**

    Description Cette règle alerte et enregistre les cas où cmstp.exe crée des processus enfants.

15. **Nom** T1202 – Exécution de commande indirecte – forfiles.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **forfiles.exe**

    Description Cette règle alerte et enregistre les cas où forfiles.exe crée des processus enfants.

16. **Nom** T1202 – Exécution de commande indirecte – pcalua.exe

Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **pcalua.exe**

Description Cette règle alerte et enregistre les cas où pcalua.exe crée des processus enfants.

17. **Nom** T1216 – Exécution de serveur mandataire de script signé – pubprn.vbs

    Clause Event type = Follow Process with ancestor ((Process Info - Exec Path *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and Process Info - Command String** *contains* **.vbs and Process Info - Command String** *contains* **script)**

    Description Cette règle alerte et enregistre les cas où un script vbs est exécuté à l'aide de wscript.exe ou cscript.exe pour créer un nouveau processus, avec un paramètre « script ». Cette technique pourrait être utilisée par un attaquant pour exécuter pubprn.vbs avec un paramètre de script pointant vers un fichier sct malveillant, qui aurait alors pour but l'exécution du code.

18. **Nom** T1218 – Exécution du serveur mandataire binaire signé - msiexec.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **rcsi.exe**

    Description Cette règle alerte et enregistre les cas où msiexec.exe crée des processus enfants.

19. **Nom** T1218 – Exécution serveur mandataire binaire signé - odbcconf.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **odbcconf.exe**

    Description Cette règle alerte et enregistre les cas où odbcconf.exe crée des processus enfants.

20. **Nom** T1218 – Exécution du serveur mandataire binaire signé - Register-CimProvider

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **Register-CimProvider.exe**

    Description Cette règle alerte et enregistre les cas où Register-CimProvider.exe crée des processus enfants.

21. **Nom** T1220 – Traitement de script XSL – msxsl.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **msxsl.exe**

    Description Cette règle alerte et enregistre le cas où msxsl.exe crée des processus enfants.

22. **Nom** T1220 - Traitement de script XSL - wmic

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **wmic.exe and Process Info - Command String** *contains* **.xsl**)

    Description Cette règle alerte et enregistre les cas où un script xsl est utilisé par wmic. Cela peut être utilisé pour lancer des fichiers binaires quelconques.

23. **Nom** T1223 – Fichiers HTML compilés

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **hh.exe**

    Description Cette règle alerte et enregistre les cas où hh.exe crée des processus enfants.

24. **Nom** T1003 – Vidage des informations d'authentification – Lsass

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **procdump.exe and Process Info - Command String** *contains* **lsass**

    Description Cette règle alerte et enregistre les cas où processdump.exe est utilisé pour vider la mémoire des processus lsass.

25. **Nom** T1140 – Désobscurcissement/décodage des fichiers ou des renseignements

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **certutil.exe and (Process Info - Command String** *matches* **.*encode\s.* or Process Info - Command String** *matches* **.*decode\s.***

    Description Cette règle alerte et enregistre les cas où certutil.exe est utilisé pour coder ou décoder un fichier. Cette technique est souvent utilisée par les attaquants pour décoder leur charge utile codée sur l'ordinateur victime.

26. **Name** T1076 - Protocole de bureau à distance (Remote Desktop Protocol)

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **tscon.exe**

    Description Cette règle alerte et enregistre les cas où tscon.exe est exécuté. Les attaquants peuvent utiliser tscon.exe pour détourner des sessions RDP existantes.

27. **Nom** T1197 – Tâches BITS – Powershell

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **powershell.exe and Process Info - Command String** *contains* **Start-BitsTransfer**

    Description Cette règle alerte et enregistre les cas où powershell.exe est utilisé pour exécuter le cmdlet Start-BitsTransfer pour copier ou déplacer des fichiers.

28. **Nom** T1170 – MSHTA

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **mshta.exe**

    Description Cette règle alerte et enregistre les cas où mshta.exe est utilisé pour exécuter des scripts HTA malveillants qui engendrent des processus enfants.

29. **Nom** T1158 - Fichiers et répertoires masqués

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **attrib.exe and Process Info - Command String** *contains* **+h)**

    Description Cette règle alerte et enregistre les cas où attib.exe est utilisé pour définir un fichier/répertoire comme masqué.

30. **Name** T1114 - Collecte des courriels

    Clause Event type = Follow Process (Process Info - Command String *matches* **.*.(ost|pst)(\s|"|').* or Process Info - Command String** *matches* **.*.(ost|pst)$) Process Info - Exec Path** *doesn't contain* **outlook.exe**

    Description Cette règle alerte et enregistre les accès aux fichiers de courriel (.ost et .pst) à partir de tout autre processus qu'outlook.exe.

31. **Nom** T1070 – Retrait de l'indicateur sur l'hôte - Journal des événements

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **wevtutil.exe and Process Info - Command String** *matches* **.*\s(cl|clear-log)\s.***

    Description Cette règle alerte et enregistre les cas où wevtutil.exe est utilisé pour effacer les journaux des événements.

32. **Nom** T1070 – Retrait de l'indicateur sur l'hôte – USN

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **fsutil.exe and Process Info - Command String** *matches* **.*\susn\s.* and Process Info - Command String** *matches* **.*\sdeletejournal.***

Description Cette règle alerte et enregistre les cas où fsutil.exe est utilisé pour supprimer des journaux USN.

33. **Nom** T1053 - Tâche planifiée

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **schtasks.exe and Process Info - Command String** *contains* **create**

    Description Cette règle alerte et enregistre les cas où SCHTASK.exe est utilisé pour créer des tâches planifiées.

34. **Nom** T1003 - Vidage des informations d'authentification - Vaultcmd

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **vaultcmd.exe and Process Info - Command String** *matches* **.*\list.***

    Description Cette règle alerte et enregistre les cas où vaultcmd.exe est utilisé pour accéder au coffre-fort des informations d'authentification Windows.

35. **Nom** T1003 – Vidage des informations d'authentification - Registre

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **reg.exe and ((Process Info - Command String** *contains* **save or Process Info - Command String** *contains* **export) and (Process Info - Command String** *contains* **hklm or Process Info - Command String** *contains* **hkey_local_machine) and (Process Info - Command String** *contains* **sam or Process Info - Command String** *contains* **security or Process Info - Command String** *contains* **system))**

    Description Cette règle alerte et enregistre, les cas où reg.exe est utilisé, pour le vidage de certains éléments du registre.

36. **Nom** T1201 - Découverte de la politique en matière de mots de passe 1

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **change and Process Info - Command String** *contains* **-l**

    Description Cette règle alerte et enregistre les cas où l'utilitaire de modification est utilisé pour répertorier la politique de mot de passe (politique d'âge du mot de passe) sur un ordinateur Linux.

37. **Nom** T1081 – Informations d'authentification dans les fichiers – Linux

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **cat or Process Info - Exec Path** *contains* **grep) and (Process Info - Command String** *contains* **.bash_history or Process Info - Command String** *contains* **.password or Process Info - Command String** *contains* **.passwd)**

    Description Cette règle alerte et enregistre toute tentative de recherche de mots de passe stockés dans les fichiers sur un ordinateur Linux.

38. **Nom** T1081 - Informations d'authentification dans les fichiers - Windows

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **findstr.exe and Process Info - Command String** *contains* **password**

    Description Cette règle alerte et enregistre les tentatives de recherche de mots de passe stockés dans les fichiers sur un ordinateur Windows.

39. **Nom** T1089 – Désactivation des outils de sécurité

    Clause Event type = Follow Process and ((Process Info - Exec Path *contains* **fltmc.exe and Process Info - Command String** *contains* **unload sysmon) or (Process Info - Exec Path** *contains* **sysmon.exe and Process Info - Command String** *contains* **/u))**

Description Cette règle alerte et enregistre les tentatives de déchargement du pilote sysmon à l'aide de fltmc.exe ou de sysmon.exe

Profils criminalistiques

Ajouter un profil

Cette section explique comment ajouter de nouveaux profils criminalistiques.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

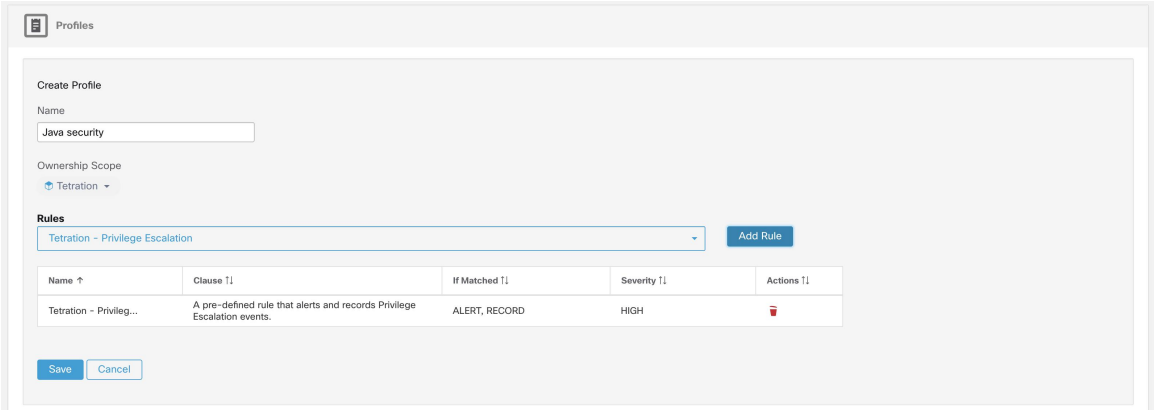
Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

Étape 2 Cliquez sur **Create Profile** (Créer un profil)

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Nom : saisissez un nom pour le profil. Le nom ne peut pas être vide
Portée de la propriété	Saisissez une portée de propriété pour ce profil.
Règles	Ajoutez des règles à ce profil.

Figure 3: Créer un profil



Étape 4 Cliquez sur **Save** (enregistrer).

Modifier un profil

Cette section explique comment un utilisateur modifie des profils criminalistiques.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

Étape 2 Repérez le profil que vous souhaitez modifier et cliquez sur l'icône en forme de **crayon** dans la colonne de droite.

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Mettez à jour le nom du profil. Le nom ne peut pas être vide
Portée de la propriété	Mettez à jour une portée de propriété pour ce profil.
Règles	Ajouter ou supprimer des règles de ce profil.

Étape 4 Cliquez sur **Save** (enregistrer).

Dupliquer un profil

Cette section explique comment un utilisateur clone les profils criminalistiques.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

Étape 2 Recherchez le profil que vous souhaitez cloner et cliquez sur l'icône de **clonage** dans la colonne de droite.

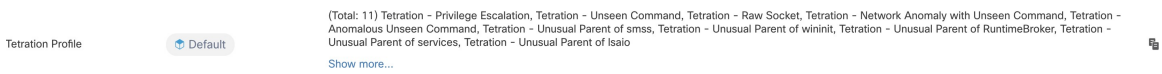
Étape 3 Saisissez le nom du profil cloné.

Étape 4 Cliquez sur **Save** (enregistrer).

Profil par défaut – Profil Cisco Secure Workload

Le profil Cisco Secure Workload contient 11 règles criminalistiques par défaut et peut être ajouté aux intents. Il n'est pas modifiable par l'utilisateur, mais il peut être cloné. Le profil criminalistique par défaut cloné est modifiable.

Figure 4: Profils par défaut



Profil par défaut - Profil MITRE ATT&CK

Le profil MITRE ATT&CK contient 39 règles MITRE ATT&CK et peut être ajouté aux intents. Il n'est pas modifiable par l'utilisateur, mais il peut être cloné. Le profil cloné est modifiable. Le profil MITRE ATT&CK comprend les règles suivantes :

1. Comportement suspect de MS Office
2. T1015 - Fonctionnalités d'accessibilité 1
3. T1015 - Fonctionnalités d'accessibilité 2
4. T1085 - runDLL32
5. T1118 - InstallUtil
6. T1121 - Regsvcs/Regasm
7. T1127 – Utilitaires pour développeurs de confiance – msbuild.exe
8. T1127 – Utilitaires pour développeurs de confiance – rcsi.exe
9. T1127 – Utilitaires pour développeurs de confiance – tracker.exe
10. T1128 – DLL de l'assistant Netsh
11. T1136 - Créer un compte
12. T1138 - Calage d'application
13. T1180 - Économiseur d'écran
14. T1191 - CMSTP
15. T1202 - Exécution indirecte de commandes - forfiles.exe
16. T1202 - Exécution indirecte de commandes - pcalua.exe
17. T1216 - Exécution de script de serveur mandataire signé - publicationprn.vbs
18. T1218 - Exécution serveur mandataire binaire signé - msiexec.exe
19. T1218 - Exécution serveur mandataire binaire signé - odbcconf.exe
20. T1218 - Exécution serveur mandataire binaire signé - Register-CimProvider
21. T1220 – Traitement des scripts XSL - msxsl.exe
22. T1220 – Traitement des scripts XSL – wmic
23. T1223 - Fichiers HTML compilés
24. T1003 - Vidage des informations d'authentification - Lsass
25. T1140 - Désobscurcissement/décodage de fichiers ou de renseignements
26. T1076 - Protocole de bureau à distance

27. T1197 - Opérations BITS – Powershell
28. T1170 – MSHTA
29. T1158 - Fichiers et répertoires masqués
30. T1114 - Collecte des courriels
31. T1070 – Retrait d'indicateur sur l'hôte - Journal des événements
32. T1070 – Retrait d'indicateur sur l'hôte – USN
33. T1053 - Tâche planifiée
34. T1003 - Vidage des informations d'authentification - Vaultcmd
35. T1003 - Vidage des informations d'authentification - Registre
36. T1201 - Découverte de la politique 1
37. T1081 - Renseignements d'authentification dans les fichiers - Linux
38. T1081 - Renseignements d'authentification dans des fichiers - Windows
39. T1089 - Désactivation des outils de sécurité

Journal des modifications : Criminalistique

Les **administrateurs du site** et les utilisateurs qui ont la capacité `SCOPE_OWNER` (PROPRIÉTAIRE DE PORTÉE) sur la portée racine peuvent afficher les journaux des modifications pour chaque règle, profil et intent criminalistique en cliquant sur l'icône, comme illustré ci-dessous.

Figure 5: Journal des modifications

Ces utilisateurs peuvent également afficher une liste des règles, des profils et des intents supprimés en cliquant sur le lien **View Deleted Rules/Profiles/Intents** (Afficher les règles, les profils et les intents supprimés) sous le tableau correspondant.

Pour en savoir plus sur le **journal des modifications**, consultez le Journal des modifications. Les propriétaires de la portée racine peuvent uniquement afficher les entrées du journal des modifications pour les entités appartenant à leur portée.

Visualisation criminalistique

Accès à la page Criminalistique

Cette section explique comment accéder à la page criminalistique.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Cliquez sur le lien **Security** (sécurité) dans le panneau de gauche.

Étape 2 Cliquez sur l'élément **criminalistique**. La page Criminalistique s'affiche.

Figure 6: Criminalistique de sécurité

Navigation parmi les événements criminalistiques

Cette section explique comment parcourir les événements criminalistiques correspondants.

Avant de commencer

Vous devez vous connecter en tant **qu'administrateur de site**, **service d'assistance à la clientèle** ou **propriétaire de la portée** dans le système et accéder à la page Criminalistique.

Procedure

Étape 1 Choisissez une plage spécifique dans le **sélecteur de plage temporelle** en haut de la page.

Étape 2 Sélectionnez **Severity** (gravité).

Étape 3 Dans **Filters**(filtres), saisissez les filtres des événements criminalistiques correspondants et cliquez sur **Filter Forensic Events**(filtrer les événements criminalistiques).

Étape 4 Le tableau des événements criminalistiques correspondants est mis à jour en fonction de la plage temporelle, de la gravité et des filtres sélectionnés.

Note Les événements criminalistiques sont visibles au niveau de la portée racine et ne le seront pas si l'on passe à des portées inférieures/enfants.

Inspection d'un événement criminalistique

Cette section explique comment inspecter les événements criminalistiques.

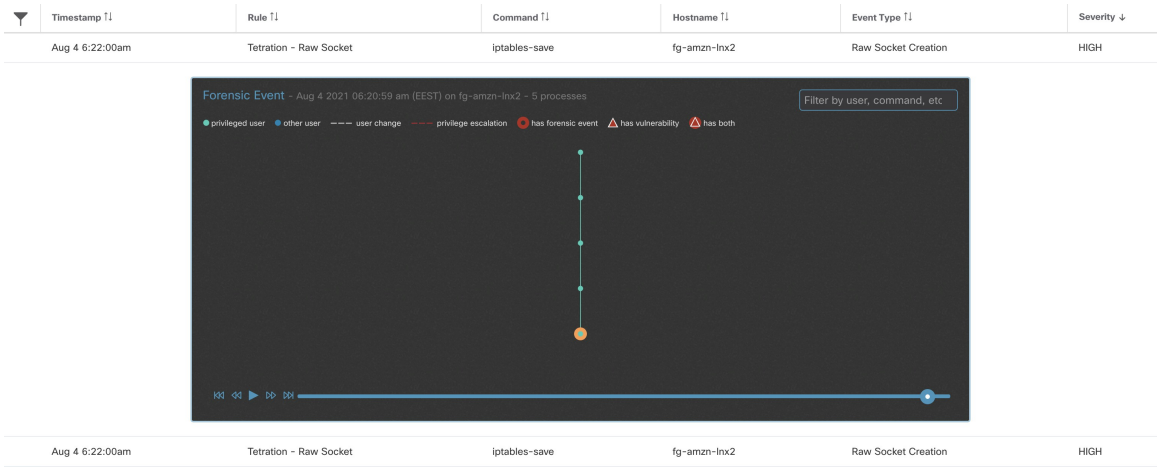
Avant de commencer

Vous devez vous connecter en tant **qu'administrateur de site**, **de service d'assistance à la clientèle** ou de **propriétaire de portée (portée racine)** au système.

Procedure

Étape 1 Cliquez sur l'événement à inspecter. Le volet **Détails du processus** s'affiche.

Figure 7: Tableau des événements criminalistiques



Étape 2 Dans l'arborescence, cliquez sur le processus à inspecter pour plus de détails.

Figure 8: Détails du processus criminalistique

Champs affichés dans les événements criminalistiques

Chaque événement criminalistique comporte plusieurs champs qui fournissent des données utiles. Il existe quelques champs communs à tous les différents types d'événements criminalistiques et quelques champs propres à un événement criminalistique particulier.

Vous trouverez ci-dessous une liste des champs qui font partie de l'interface utilisateur. Le premier tableau décrit les champs communs à tous les événements criminalistiques, suivi d'un tableau décrivant les informations sur le processus qui sont affichées avec chaque alerte, puis des tableaux contenant des champs uniques par événement criminalistique. Certains des champs peuvent être présents dans plusieurs tableaux, en raison de la façon dont les données sont stockées et exportées.

Champs communs

Champ	Description
Bin attr ctime	Modification de l'heure sous Linux / Création de l'heure du fichier binaire dans Windows
Bin attr hash	Condensé SHA256 du fichier binaire
Bin attr mtime	Heure modifiée du binaire
Bin attr name	Nom du fichier binaire sur le système de fichiers
Bin attr size	Taille du fichier binaire sur le système de fichiers
Bin exec path	Chemin complet du fichier binaire
Cmdline	Ligne de commande complète du processus à exécuter
Event time usec	Heure (en microsecondes) pendant laquelle cet événement est observé

Renseignements relatifs au processus

Champ	Description
Identifiant de processus	ID de processus du processus
ID du processus parent	ID de processus du parent du processus
Utilisateur	Utilisateur qui a exécuté le processus
Chemin d'exécution	Chemin complet du fichier binaire qui correspond au processus.
Heure de début	Heure à laquelle le processus a été lancé
Commande complète	Ligne de commande complète du processus à exécuter

Escalade de privilèges

Champ	Description
Parent cmdline	Ligne de commande complète du parent du processus
Parent exe	Chemin complet du parent du processus
Parent Uptime (microseconds)	Temps depuis l'exécution du parent du processus
Parent Username	Utilisateur qui a exécuté le parent du processus
Types bitmap suid binary	Indique si le bit SUID est défini sur binaire

Connexion de l'utilisateur

Champ	Description
Auth type password	Indique l’authentification par mot de passe
Auth type pubkey	Indique l’authentification par clé
Type login ssh	Indique qu’un utilisateur est connecté par SSH
Type login win batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Type login win cached	Indique la connexion avec des informations d’authentification en cache (type 11, CachedIntetractive)
Type login win interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Type login win network cleartext	Indique une connexion par SSH (type 8)
Type login win network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Type login win new cred	Indique l’utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Type login win remote interactive	Indique une connexion à distance (type 10, par exemple RDP)
Type login win service	Indique qu’un service a été démarré par SCM (type 5)
Type login win unlock	Indique que l'ordinateur a été déverrouillé (type 7)
Src IP	Adresse IP source à partir de laquelle l’événement de connexion a été généré
Src Port	Port source à partir duquel l’événement de connexion a été généré
Nom d’utilisateur	Nom d’utilisateur associé à l’événement de connexion

Échec de connexion de l’utilisateur

Champ	Description
Auth type password	Indique l’authentification par mot de passe
Auth type pubkey	Indique l’authentification par clé
Type login ssh	Indique qu’un utilisateur est connecté par SSH

Champ	Description
Type login win batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Type login win cached	Indique la connexion avec des informations d'authentification en cache (type 11, CachedIntetractive)
Type login win interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Type login win network cleartext	Indique une connexion par SSH (type 8)
Type login win network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Type login win new cred	Indique l'utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Type login win remote interactive	Indique une connexion à distance (type 10, par exemple RDP)
Type login win service	Indique qu'un service a été démarré par SCM (type 5)
Type login win unlock	Indique que l'ordinateur a été déverrouillé (type 7)
Src IP	Adresse IP source à partir de laquelle l'événement de connexion a été généré
Src Port	Port source à partir duquel l'événement de connexion a été généré
Nom d'utilisateur	Nom d'utilisateur associé à l'événement de connexion

Shellcode

Champ	Description
Sources de signaux bitmap cmd as sh no tty	Indique qu'un processus Shell n'est associé à aucun point terminal.
Powershell bitmap des sources de signal	Indique que le processus a chargé la dll powershell (System.Management.Automation)

Accès au fichier

Champ	Description
Fichier	Chemin complet du fichier consulté

Champ	Description
Lecture permanente	Indique que le fichier avait l'autorisation de lecture
Lecture écriture permanente	Indique que le fichier avait des autorisations de lecture et d'écriture
Écriture permanente	Indique que le fichier avait l'autorisation en écriture

Compte d'utilisateur

Champ	Description
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur qui a été créé
Ops acct add	Indique qu'un nouveau compte a été ajouté

Commande non vue

Champ	Description
Anomalie - Note	Note (0 à 1,0) indiquant la fréquence à laquelle la ligne de commande a été vue précédemment; une note plus basse signifie que la commande est plus anormale.
Anomalie - Similitude - Élevé	Vrai si le score d'anomalie est supérieur à 0,8 et est inférieur à 1
Anomalie - Similitude - Moyenne	Vrai si le score d'anomalie est supérieur à 0,6 et est inférieur ou égal à 0,8
Anomalie - Similitude - Faible	Vrai si le score d'anomalie est supérieur à 0 et est inférieur ou égal à 0,6
Anomalie - Similitude - Observé	Vrai si le score d'anomalie est de 1, c'est-à-dire que la même commande a déjà été vue
Anomalie - Similitude - Unique	Vrai si le score d'anomalie est de 0, c'est-à-dire que la commande n'a jamais été vue auparavant
Parent cmdline	Ligne de commande complète du processus parent
Parent exepath	Chemin binaire du processus parent
Temps de disponibilité du parent	Temps écoulé depuis l'exécution du processus parent
Parent username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent
Temps de disponibilité du capteur	Disponibilité du capteur

Bibliothèque non vue

Champ	Description
Chemin de la bibliothèque	Le chemin d'accès complet du fichier de bibliothèque qui n'était pas associé au processus auparavant

Création d'interface de connexion brute

Champ	Description
Chemin d'accès exe	Chemin complet du processus qui a créé le connecteur brut

Bibliothèque modifiée

Champ	Description
Le nom de la bibliothèque modifié	Le chemin d'accès complet de la bibliothèque qui a été modifiée

Canaux auxiliaires

Champ	Description
Fusion de bitmap des sources de signal	Indique l'utilisation de l'exploit « meltdown » (Fusion)

Suivre la connexion de l'utilisateur

Champ	Description
Nom d'utilisateur	Nom de l'utilisateur qui a exécuté le processus

Suivre le processus

Champ	Description
Parent cmdline	Ligne de commande complète du processus parent
Parent exepath	Chemin binaire du processus parent
Parent uptime usec	Temps écoulé depuis l'exécution du processus parent
Parent username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent

Champ	Description
Time since last changed usec	Temps écoulé entre l'heure de début du processus et son heure de changement de fichier binaire (mtime)
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur qui a exécuté le processus

Anomalie de réseau

Pour en apprendre davantage, consultez la page Règles de criminalistique pour les événements d'anomalie de réseau (détection des anomalies de réseau) pour obtenir la liste des attributs associés aux événements d'anomalies de réseau.

Analyse criminalistique : zones de recherche

Les tableaux ci-dessous décrivent les champs de recherche de la barre de recherche de la page Forensics Analysis (Analyse criminalistique).

Champs divers

Champ	Description
Nom de la règle criminalistique	Événements marqués par une règle criminalistique particulière
Nom d'hôte	Événements provenant d'un nom d'hôte particulier
ID du capteur	Événements provenant d'un capteur particulier
Gravité	Événements d'une gravité particulière

Termes de recherche dans les analyses criminalistiques

Champs communs

Ces champs sont communs à différents types d'événements. Ils ont le préfixe « Nom de l'événement – Événement ». Par exemple, « Binary Changed – Binary Attribute – CTime (epoch nanoseconds) »

Champ	Description
Binary Attribute - CTime (epoch nanoseconds)	Modification de l'heure sous Linux / Création de l'heure du fichier binaire dans Windows
Binary Attribute - Hash	Condensé SHA256 du fichier binaire

Champ	Description
Binary Attribute - MTime (epoch nanoseconds)	Heure modifiée du binaire
Binary Attribute - Filename	Nom du fichier binaire sur le système de fichiers
Binary Attribute - Size (bytes)	Taille du fichier binaire sur le système de fichiers
Event Binary Path	Chemin complet du fichier binaire
Ligne de commande	Ligne de commande complète du processus à exécuter

Fichier binaire modifié

Il n'y a aucun autre terme de recherche que ceux décrits dans le tableau « Champs communs ».

Accès au fichier

Les termes de recherche pour l'accès au fichier ont le préfixe « Accès au fichier – » par exemple « Accès au fichier – Nom de fichier ».

Champ	Description
Nom de fichier	Chemin complet du fichier consulté
Is = Permission - Read	Indique que le fichier avait l'autorisation de lecture
Is = Permission - ReadWrite	Indique que le fichier avait des autorisations de lecture et d'écriture
Is = Permission - Write	Indique que le fichier avait l'autorisation en écriture

Suivre le processus

Les termes de recherche de suivi de processus ont le préfixe « Follow Process – » (Suivez le processus) par exemple « Follow Process - Parent Command Lin ».

Champ	Description
Parent Command Line	Ligne de commande complète du processus parent
Parent Exec Path	Chemin binaire du processus parent
Parent Uptime (microseconds)	Temps écoulé depuis l'exécution du processus parent
Parent Username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent
Heure de début du processus depuis la dernière modification de fichier (microsecondes)	Temps qui s'écoule entre le début du processus et la dernière modification de fichier (correspondante)
Nom d'utilisateur	Noms d'utilisateur associés au processus suivi

Suivre la connexion de l'utilisateur

Les termes de recherche du suivi de la connexion de l'utilisateur ont le préfixe « Follow User Logon - » par exemple « Follow User Logon - Username » (suivre la connexion de l'utilisateur - nom d'utilisateur).

Champ	Description
Nom d'utilisateur	Nom d'utilisateur associé à un processus

Ldap

Les termes de recherche Ldap ont le préfixe « Ldap - », par exemple « Ldap - Department »

Champ	Description
Service	Service utilisateur AMS Ldap associé au nom d'utilisateur du processus (si disponible)
Description	Description d'utilisateur AMS Ldap associée au nom d'utilisateur du processus (si disponible)
Nom d'utilisateur	Nom d'utilisateur AMS Ldap associé au processus (si disponible)

Bibliothèque modifiée

Les termes de recherche Library Changed (modification de bibliothèque) ont le préfixe « Library Changed – » ou « Library Changed – Service »

Champ	Description
Nom de fichier Lib	Le chemin d'accès complet de la bibliothèque qui a été modifiée

Escalade de privilèges

Les termes de recherche d'escalade de privilèges sont précédés du préfixe « Privilege Escalation – », par exemple « Privilege Escalation - Parent Command line (ligne de commande parente) ».

Champ	Description
Parent Command Line	Ligne de commande complète du parent du processus
Parent Exec Path	Chemin complet du parent du processus
Parent Uptime (microseconds)	Temps depuis l'exécution du parent du processus
Parent Username	Utilisateur qui a exécuté le parent du processus
Type - Suid Binary	Indique si le bit SUID est défini sur binaire

Renseignements relatifs au processus

Les termes de recherche des informations de processus ont le préfixe « Process Info - », par exemple « Process Info - binaryHash ».

Champ	Description
Condensé binaire	Condensé du fichier binaire associé au processus
Chaîne de commande marquée d'un jeton	Ligne de commande marquée d'un jeton du processus
Chaîne de commande	Ligne de commande complète du processus
Chemin d'accès exécutable	Chemin complet du fichier binaire qui correspond au processus

Connecteur brut

Les termes de recherche du connecteur brut comportent le préfixe « Raw Socket - ». Par exemple, « Raw Socket - Exec Path »

Champ	Description
Chemin d'accès exécutable	Chemin complet du processus qui a créé le connecteur brut

Shellcode

Les termes de recherche de code Shell ont le préfixe « Shellcode - ». Par exemple, « Shellcode - Source - Non issue de la connexion »

Champ	Description
Source – Non issue de la connexion	Indique qu'un processus Shell n'est associé à aucun point terminal.
Source – Powershell	Indique que le processus a chargé la dll powershell (System.Management.Automation)

Canaux auxiliaires

Les termes de recherche des Canaux auxiliaires ont le préfixe « Shellcode - ». Par exemple, « Shellcode - Source - Fusion »

Champ	Description
Source - Fusion	Indique l'utilisation de l'exploit « meltdown » (Fusion)

Commande non vue

Les termes de recherche de commandes non vues sont précédés du préfixe « Unseen Command – » (Commande inconnue) – Anomalie – Similitude – Élevée).

Champ	Description
Anomalie - Note	Note (0 à 1,0) indiquant la fréquence à laquelle la ligne de commande a été vue précédemment; une note plus basse signifie que la commande est plus anormale.
Anomalie - Similitude - Élevé	Vrai si le score d'anomalie est supérieur à 0,8 et est inférieur à 1
Anomalie - Similitude - Moyenne	Vrai si le score d'anomalie est supérieur à 0,6 et est inférieur ou égal à 0,8
Anomalie - Similitude - Faible	Vrai si le score d'anomalie est supérieur à 0 et est inférieur ou égal à 0,6
Anomalie - Similitude - Observé	Vrai si le score d'anomalie est de 1, c'est-à-dire que la même commande a déjà été vue
Anomalie - Similitude - Unique	Vrai si le score d'anomalie est de 0, c'est-à-dire que la commande n'a jamais été vue auparavant
Parent Cmdline	Ligne de commande complète du processus parent
Parent Exepath	Chemin binaire du processus parent
Temps de disponibilité du parent	Temps écoulé depuis l'exécution du processus parent
Parent Username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent
Temps de disponibilité du capteur	Disponibilité du capteur
Anomalie - Dernières commandes similaires	Cinq dernières commandes similaires à la commande de l'événement observées précédemment

Bibliothèque non vue

Les termes de recherche de bibliothèque non vue ont le préfixe « Unseen Library – » par exemple « Unseen Library – Lib Filename »

Champ	Description
Nom de fichier Lib	Le chemin d'accès complet du fichier de bibliothèque qui n'était pas associé au processus auparavant

Compte d'utilisateur

Les termes de recherche des comptes d'utilisateurs ont le préfixe « User Account – » par exemple « User Account – Account Name » (Nom du compte).

Champ	Description
Nom du compte	Nom d'utilisateur de l'utilisateur qui a été créé
Operation - Add Account	Indique qu'un nouveau compte a été ajouté

Connexion de l'utilisateur

Les termes de recherche de connexion d'utilisateur ont le préfixe « User Logon – » par exemple « User Logon - Auth Type - Password » (mot de passe).

Champ	Description
Auth Type - Password	Indique l'authentification par mot de passe
Auth type - Pubkey	Indique l'authentification par clé
Login Type - Login Via SSH	Indique qu'un utilisateur est connecté par SSH
Login Type - Windows Login Batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Login Type - Windows Login Cached	Indique la connexion avec des informations d'authentification en cache (type 11, CachedIntetractive)
Login Type - Windows Login Interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Login Type - Windows Network Cleartext	Indique une connexion par SSH (type 8)
Login Type - Windows Network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Login Type - Windows Login New Credential	Indique l'utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Login Type - Windows Login Remote Interactive	Indique une connexion à distance (type 10, par exemple RDP)
Login Type - Windows Login Service	Indique qu'un service a été démarré par SCM (type 5)
Login Type - Windows Login Unlock	Indique que l'ordinateur a été déverrouillé (type 7)
IP de la source	Adresse IP source à partir de laquelle l'événement de connexion a été généré
Source Port (port source)	Port source à partir duquel l'événement de connexion a été généré

Champ	Description
Nom d'utilisateur	Nom d'utilisateur associé à l'événement de connexion

Échec de connexion de l'utilisateur

Les termes de la recherche User Logon Failed sont précédés du préfixe « User Logon Failed - ».Par exemple, « User Logon Failed - Auth Type - Password »

Champ	Description
Auth Type - Password	Indique l'authentification par mot de passe
Auth type - Pubkey	Indique l'authentification par clé
Login Type - Login Via SSH	Indique qu'un utilisateur est connecté par SSH
Login Type - Windows Login Batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Login Type - Windows Login Cached	Indique la connexion avec des informations d'authentification en cache (type 11, CachedIntetractive)
Login Type - Windows Login Interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Login Type - Windows Network Cleartext	Indique une connexion par SSH (type 8)
Login Type - Windows Network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Login Type - Windows Login New Credential	Indique l'utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Login Type - Windows Login Remote Interactive	Indique une connexion à distance (type 10, par exemple RDP)
Login Type - Windows Login Service	Indique qu'un service a été démarré par SCM (type 5)
Login Type - Windows Login Unlock	Indique que l'ordinateur a été déverrouillé (type 7)
IP de la source	Adresse IP source à partir de laquelle l'événement de connexion a été généré
Source Port (port source)	Port source à partir duquel l'événement de connexion a été généré
Nom d'utilisateur	Nom d'utilisateur associé à l'événement de connexion

Alertes criminalistiques

Les événements criminalistiques peuvent être trouvés dans le système d'alerte Cisco Secure Workload si leurs règles de correspondance contiennent une action d' **alerte**.

Accès aux alertes criminalistiques

Cette section explique comment accéder aux alertes criminalistiques.

Avant de commencer

- Connectez-vous au système en tant **qu'administrateur de site**, **service d'assistance à la clientèle** ou **propriétaire de la portée**.
- Activez les alertes pour la source d'alerte **criminalistique**.

Procedure

Étape 1 Dans le volet de navigation, sélectionnez **Configure Alerts** (Configurer les alertes).

Étape 2 La page d'alertes s'affiche.

Vérification des détails de l'alerte

Avant de commencer

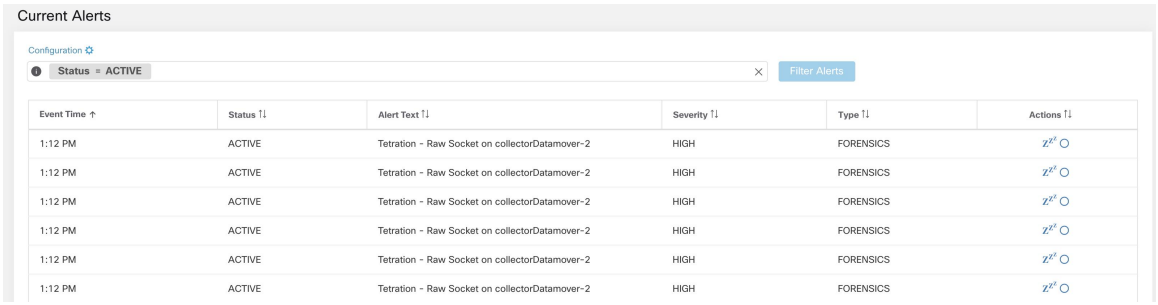
Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Dans la page d'alertes, cliquez sur l'alerte à vérifier.

Étape 2 Cliquez sur profile/rule (Profil/Nom) pour afficher les détails de la règle ou du profil criminalistique correspondant. Si le profil/la règle correspondant(e) est mis(e) à jour après l'émission d'alertes, un indicateur d'avertissement s'affiche.

Figure 9: Page d'alerte criminalistique



En outre, vous pouvez répéter ou inclure/exclure une alerte. Reportez-vous à la section Alertes actuelles pour en savoir plus.

Intégration externe

Des alertes criminalistiques peuvent être envoyées à des outils de surveillance externes tels que syslog. L'alerte criminalistique est envoyée au format JSON. Les définitions des champs JSON sont indiquées dans la section « Champs affichés dans les événements criminalistiques » ci-dessus.

Vous trouverez ci-dessous un exemple de sortie JSON Kafka :


```
  {
    "severity": "HIGH",
    "tenant_id": 0,
    "alert_time": 1595573847156,
    "alert_text": "Tetration - Anomalous Unseen Command on collectorDatamover-1",
    "key_id":
"d89f926cddc7577553eb8954e492528433b2d08e:5efcfdf5497d4f474f1707c2:5efcfdf6497d4f474f1707d6:20196:CMD_NOT_SEEN",

    "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='forensics', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/db10d21631eebefc3b8d3aeaba5a0b1b45f4259e85b591763d7eaee9161ca076",

    "root_scope_id": "5efcfdf5497d4f474f1707c2",
    "type": "FORENSICS",
    "event_time": 1595573795135,
    "alert_details": "{\"Sensor
Id\":\"d89f926cddc7577553eb8954e492528433b2d08e\",\"Hostname\":\"collectorDatamover-1\",\"Process
 Id\":20196,\"scope_id\":\"5efcfdf5497d4f474f1707c2\",\"forensic\":{\"Unseen
Command\":\"true\",\"Unseen Command - Sensor Uptime (microseconds)\":\"34441125356\",\"Unseen
 Command - Parent Uptime (microseconds)\":\"35968418683\",\"Unseen Command - Parent
Username\":\"root\",\"Unseen Command - Parent Command Line\":\"svlogd -tt
/local/logs/tetration/efe/ \",\"Unseen Command - Parent Exec Path\":\"/sbin/svlogd\",\"Unseen
 Command - Anomaly - Score\":\"0\",\"Unseen Command - Anomaly - Similarity -
Unique\":\"true\",\"Process Info - Command String\":\"gzip \",\"Process Info - Exec
Path\":\"/bin/gzip\"},\"profile\":{\"id\":\"5efcfdf6497d4f474f1707e4\",\"name\":\"Tetration

Profile\",\"created_at\":1593683390,\"updated_at\":1593683390,\"root_app_scope_id\":\"5efcfdf5497d4f474f1707c2\"},\"rule\":{\"id\":\"5efcfdf6497d4f474f1707d6\",\"name\":\"Tetration
 - Anomalous Unseen
Command\",\"clause_chips\":\"[{\\\"type\\\":\\\"filter\\\",\\\"facet\\\":{\\\"field\\\":\\\"event_type\\\",\\\"title\\\":\\\"Event

type\\\",\\\"type\\\":\\\"STRING\\\"},\\\"operator\\\":{\\\"label\\\":\\\"\\u003d\\\",\\\"type\\\":\\\"eq\\\"},\\\"displayValue\\\":\\\"Unseen
 Command\\\",\\\"value\\\":\\\"Unseen
Command\\\"},{\\\"type\\\":\\\"filter\\\",\\\"facet\\\":{\\\"field\\\":\\\"forensic_event__cmd_not_seen_data__cmdline_anomaly_info__score\\\",\\\"title\\\":\\\"Unseen
```

```
 Command - Anomaly -
Score\\\",\\\"type\\\":\\\"NUMBER\\\"},\\\"operator\\\":{\\\"label\\\":\\\"\u003c\\\",\\\"type\\\":\\\"lt\\\"},\\\"displayValue\\\":\\\"0.6\\\",\\\"value\\\":\\\"0.6\\\"}]\",\"created_at\":1593638390,\"updated_at\":1595539498,\"root_app_scope_id\":\"5efcfdf5497d4f474f1707c2\"}}"

  }
```

La valeur dans alert_détails est elle-même une chaîne JSON échappée dont le contenu pour l'alerte ci-dessus est visible ci-dessous :

```
  {
    "Sensor Id": "d89f926cddc7577553eb8954e492528433b2d08e",
    "Hostname": "collectorDatamover-1",
    "Process Id": 20196,
    "scope_id": "5efcfdf5497d4f474f1707c2",
    "forensic": {
      "Unseen Command": "true",
      "Unseen Command - Sensor Uptime (microseconds)": "34441125356",
      "Unseen Command - Parent Uptime (microseconds)": "35968418683",
      "Unseen Command - Parent Username": "root",
      "Unseen Command - Parent Command Line": "svlogd -tt /local/logs/tetration/efe/ ",
      "Unseen Command - Parent Exec Path": "/sbin/svlogd",
      "Unseen Command - Anomaly - Score": "0",
      "Unseen Command - Anomaly - Similarity - Unique": "true",
      "Process Info - Command String": "gzip ",
      "Process Info - Exec Path": "/bin/gzip"
    },
    "profile": {
      "id": "5efcfdf6497d4f474f1707e4",
      "name": "Tetration Profile",
      "created_at": 1593638390,
      "updated_at": 1593638390,
      "root_app_scope_id": "5efcfdf5497d4f474f1707c2"
    },
    "rule": {
      "id": "5efcfdf6497d4f474f1707d6",
      "name": "Tetration - Anomalous Unseen Command",
      "clause_chips":
"[{\"type\":\"filter\",\"facet\":{\"field\":\"event_type\",\"title\":\"Event
type\",\"type\":\"STRING\"},\"operator\":{\"label\":\"=\",\"type\":\"eq\"},\"displayValue\":\"Unseen
 Command\",\"value\":\"Unseen
Command\"},{\"type\":\"filter\",\"facet\":{\"field\":\"forensic_event__cmd_not_seen_data__cmdline_anomaly_info__score\",\"title\":\"Unseen
 Command - Anomaly -
Score\",\"type\":\"NUMBER\"},\"operator\":{\"label\":\"<\",\"type\":\"lt\"},\"displayValue\":\"0.6\",\"value\":\"0.6\"}]",

      "created_at": 1593638390,
      "updated_at": 1595539498,
      "root_app_scope_id": "5efcfdf5497d4f474f1707c2"
    }
 }
```

Les détails des événements criminalistiques sont inclus dans le champ criminalistique. Pour obtenir la liste des attributs des événements criminalistiques, consultez Champs affichés dans les événements criminalistiques. Ces attributs sont également affichés dans les détails de l'alerte dans l'interface utilisateur.

Note de criminalistique

Où voir la note criminalistique

Tableau de bord de sécurité

Figure 10: Section de la note criminalistique dans le tableau de bord de la sécurité

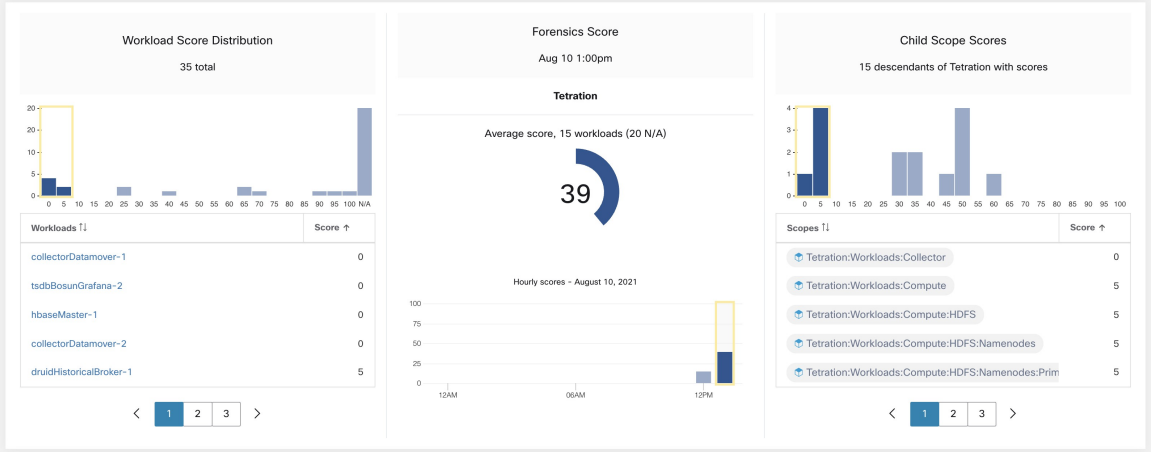
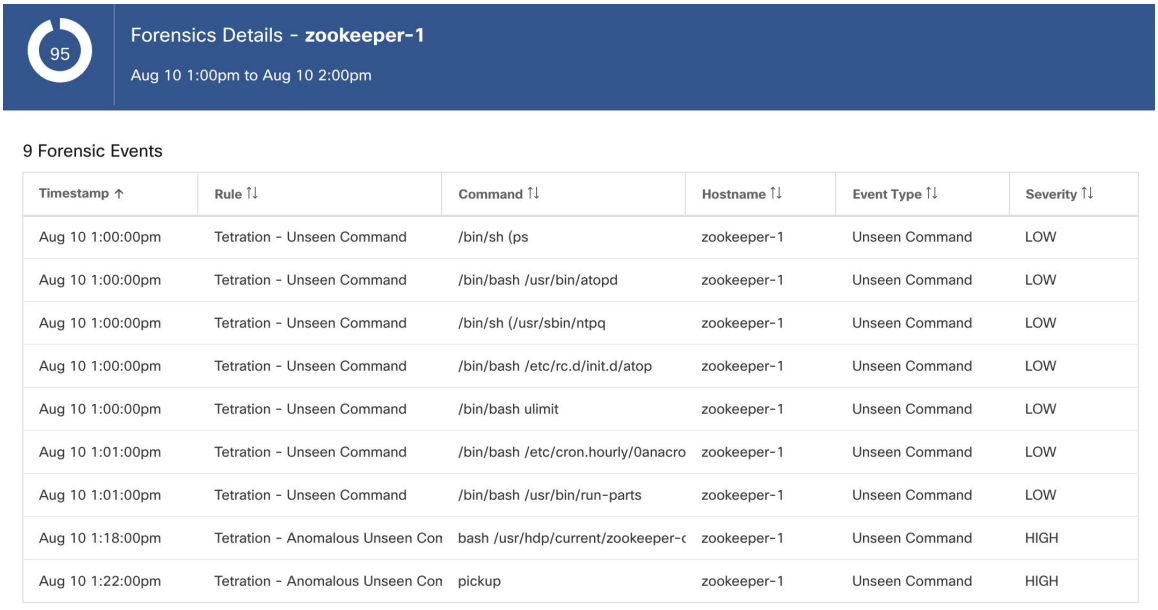


Figure 11: Section des détails de la note criminalistique dans le tableau de bord de la sécurité



Timestamp	Rule	Command	Hostname	Event Type	Severity
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/sh (ps	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash /usr/bin/atopd	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/sh (/usr/sbin/ntpq	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash /etc/rc.d/init.d/atop	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash ulimit	zookeeper-1	Unseen Command	LOW
Aug 10 1:01:00pm	Tetration - Unseen Command	/bin/bash /etc/cron.hourly/0anacro	zookeeper-1	Unseen Command	LOW
Aug 10 1:01:00pm	Tetration - Unseen Command	/bin/bash /usr/bin/run-parts	zookeeper-1	Unseen Command	LOW
Aug 10 1:18:00pm	Tetration - Anomalous Unseen Con	bash /usr/hdp/current/zookeeper-c	zookeeper-1	Unseen Command	HIGH
Aug 10 1:22:00pm	Tetration - Anomalous Unseen Con	pickup	zookeeper-1	Unseen Command	HIGH

Comment la note de criminalistique est-elle calculée?

Pour chaque charge de travail, nous calculons une note criminalistique. La note criminalistique d'une charge de travail est calculée à partir des événements criminalistiques observés sur cette charge de travail en fonction

des profils activés pour cette portée. Une note de 100 signifie qu'aucun événement criminalistique n'a été observé par les règles configurées dans les profils activés, et une note de 0 signifie qu'un événement criminalistique a été détecté qui nécessite une action immédiate. La note criminalistique d'une portée est la note moyenne de charge de travail dans cette portée. La note criminalistique pour une heure donnée est le minimum de tous les résultats de cette heure.

- Un événement criminalistique ayant le niveau de gravité REQUIRES IMMEDIATE ACTION (NÉCESSITE UNE ACTION IMMÉDIATE) réduit la note de l'ensemble de la portée à zéro.
- Un événement criminalistique avec le niveau de gravité CRITICAL (CRITIQUE) réduit la note de la charge de travail avec une pondération de 10.
- Un événement criminalistique avec le niveau de gravité HIGH (ÉLEVÉ) réduit la note de la charge de travail avec une pondération de 5.
- Un événement criminalistique avec la gravité MEDIUM (MOYENNE) réduit la note de la charge de travail avec une pondération de 3.
- Un événement criminalistique ayant la gravité LOW (FAIBLE) ne contribue pas à la note criminalistique. Cela est recommandé pour les nouvelles règles lorsque la qualité du signal est toujours en cours d'optimisation et est susceptible d'être bruitée.

Par exemple, une charge de travail comporte 3 événements criminalistiques qui correspondent respectivement à 2 règles de gravité *CRITIQUE* , 1 règle de gravité *ÉLEVÉE* et 1 règle de gravité *FAIBLE*. La note criminalistique pour cette charge de travail est : 100 – 1 * 10 – 1 * 5 – 1 * 0 = 85.

Les notes criminalistiques sont S.O. pour les charges de travail dans lesquelles la fonction criminalistique n'est pas activée.

Comment améliorer la note criminalistique

Vous pouvez régler votre note criminalistique en ajustant les règles criminalistiques activées. En créant des règles moins parasitées, vous obtiendrez une note plus précise. La prise en compte et la prévention d'événements criminalistiques légitimes (les événements qui sont la preuve d'une intrusion ou d'une autre activité malveillante) sont un autre bon moyen d'améliorer votre score criminalistique.

Mises en garde

- Les détails de la note criminalistique affichent tous les événements criminalistiques au cours de cette heure. Cela signifie que les détails de la note criminalistique peuvent afficher des événements légaux autres que ceux utilisés pour le calcul de cette dernière.
- La note criminalistique est actuellement disponible pour les capteurs de visibilité approfondie et d'application.

Détection des anomalies de réseau basée sur le PCR

La fonction d'anomalie de réseau détecte des quantités anormalement importantes de données qui entrent ou sortent des charges de travail selon le concept de rapport producteur-consommateur (PCR). Le PCR est défini comme suit :

```
Egress app byte count - Ingress app byte count
  PCR = ------------------------------------------
        Egress app byte count + Ingress app byte count
```

La valeur de PCR se trouve dans la plage [-1.0, 1.0], où :

- PCR = 1.0 signifie que la charge de travail envoie uniquement des données.
- PCR = -1,0 signifie que la charge de travail reçoit uniquement des données.
- PCR = 0.0 signifie que la charge de travail a équilibré les quantités de données entrantes et sortantes.

Comme pour les autres fonctionnalités criminalistiques, vous pouvez utiliser la configuration basée sur les intents pour configurer les événements d'anomalies de réseau que vous souhaitez enregistrer ou sur lesquels vous souhaiter alerter. Les événements d'anomalies de réseau détectées des charges de travail sont exportés toutes les 5 minutes et comparés aux règles configurées 5 minutes plus tard. Par conséquent, les nouveaux événements d'anomalie de réseau ne sont observés sur l'interface utilisateur que toutes les 5 minutes avec un retard pouvant aller jusqu'à 10 minutes à partir du moment de survenance de l'événement.

Note Dans les versions 3.2 et 3.1 du logiciel Cisco Secure Workload, la détection des anomalies de réseau était appelée détection de fuites de données.

Règles de criminalistique pour les événements d'anomalie de réseau

Consultez Configuration criminalistique sur la façon d'ajouter des règles criminalistiques.

Attributs de règles

Cette section explique les détails des attributs pour définir une règle liée à une anomalie de réseau. La règle d'anomalie de réseau la plus simple est :

```
Event Type = Network Anomaly
```

Autres attributs dans l'événement Anomalie de réseau pour affiner les règles pour vos centres de données :

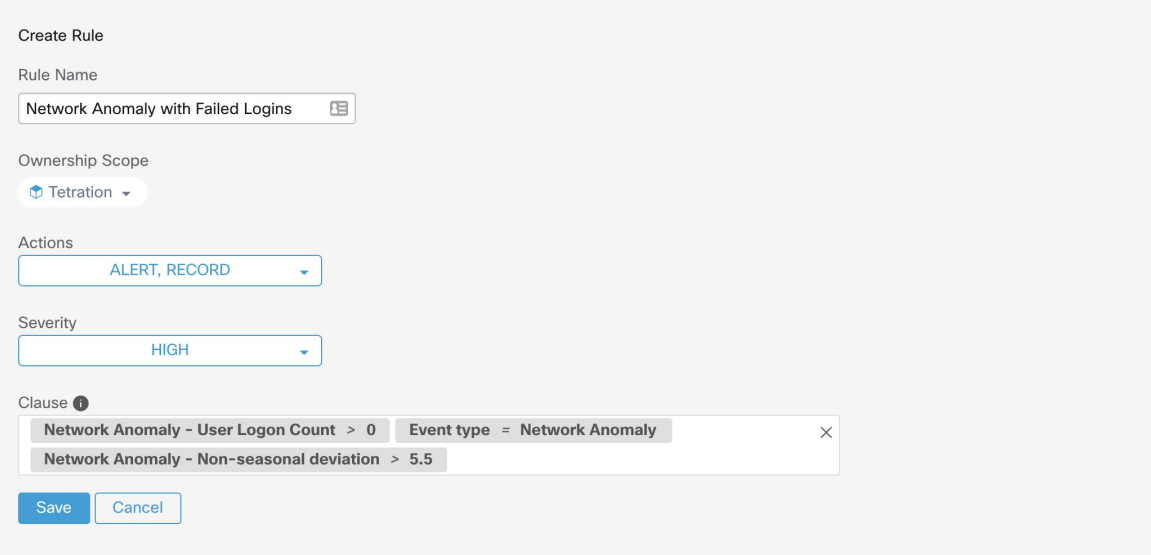
Table 2: Attributs de règle dans l'événement Anomalie de réseau

Attribut	Description
Nom de l'hôte	Le nom d'hôte du travail qui émet cet événement.
Horodatage (origine, millisecondes)	Horodatage (en millisecondes) de l'événement.
Écart PCR	L'écart du PCR (Rapport Fournisseur-Consommateur) par rapport à la moyenne au moment de l'événement en tant que multiple de l'écart type historique.
Écart non saisonnier	Il s'agit de l'écart PCR après suppression du modèle de saisonnalité (par exemple, par tâches cron). La valeur de l'écart non saisonnier est toujours supérieure ou égale à 6.
PCR	Le rapport fournisseurs-consommateurs.

Attribut	Description
EIR	Le rapport d'entrée de sortie, qui est le rapport entre le nombre total d'octets d'application de sortie et le nombre d'octets d'application d'entrée.
Nombre d'octets d'application de sortie	Le nombre d’octets d’application de sortie, qui correspond au nombre total d’octets du contenu des paquets (à l’exclusion des en-têtes) sortant de la charge de travail.
Nombre d'octets d'application d'entrée	Le nombre d'octets d'application entrants, qui est le nombre total d'octets du contenu des paquets (à l'exclusion des en-têtes) circulant dans la charge de travail.
Protocole	Le protocole pour lequel la série chronologique du PCR est calculée. Actuellement, les protocoles pris en charge sont TCP, UDP et Aggregate. La fonction Aggregate PCR est calculée en fonction de la somme totale des nombres d’octets TCP, UDP et ICMP.
Nombre de connexion d’utilisateurs	Le nombre d'événements de connexion d’utilisateur sur la charge de travail au cours des 15 dernières minutes environ. Il s'agit du nombre d'événements de connexion de l'utilisateur, qu'il existe ou non des règles correspondantes. Pour connaître les détails des événements de connexion de l'utilisateur, vous devez définir des règles pour enregistrer les événements pour les charges de travail qui vous intéressent et les afficher sur la page Analyse criminalistique.
Nombre d'échecs de connexion de l’utilisateur	Le nombre d’échecs de connexion des utilisateurs sur le charges de travail au cours des 15 dernières minutes environ. Il s'agit du nombre d'événements d'échec de la connexion de l'utilisateur, qu'il existe ou non des règles correspondantes. Pour connaître les détails des événements d'échec de connexion de l'utilisateur, vous devez définir des règles pour enregistrer les événements pour les charges de travail qui vous intéressent et les afficher sur la page Analyse criminalistique.
Nombre de commandes non vues	Le nombre d’événements de commande non vues sur la charge de travail au cours des 15 dernières minutes environ. Il s'agit du nombre d'événements de commandes non vues, qu'il existe ou non des règles correspondantes. Pour connaître les détails des événements de commandes non vues, vous devez définir des règles pour enregistrer les événements pour les charges de travail qui vous intéressent et les afficher sur la page Analyse criminalistique.

Attribut	Description
Date, heure (UTC) - année	L'année de l'événement.
Date, heure (UTC) - Mois	Le mois de l'heure de l'événement (1, 2, etc. . .).
Date, heure (UTC) - Jour	Le jour du mois de l'heure de l'événement (1, 2, etc. . .).
Date, heure (UTC) - Heure	L'heure du jour de l'événement (1, 2, . . . , 24).
Date, heure (UTC) - Minutes	Minute d'une heure de l'événement (1, 2,. . . , 60).
Date, heure (UTC) - Seconde	La seconde de la minute de l'heure de l'événement (1, 2,. . . , 60).
Date, heure (UTC) - Jour de la semaine	Le jour de la semaine correspondant à l'heure de l'événement (0 à 7 pour lundi au dimanche).

Figure 12: Définition de règles criminalistiques pour les événements d'anomalie de réseau



Vous trouverez ci-dessous des exemples de règles :

Listing 7.10.1.1.1 : Détecte les anomalies de réseau pour UDP uniquement.

```
Event Type = Network Anomaly AND Network Anomaly Is = Protocol - UDP
```

Listing 7.10.1.1.2 : Détecte les écarts importants après la suppression du modèle saisonnier (s'il est détecté), avec un seuil sur le nombre d'octets d'application de sortie pour un sous-ensemble de charges de travail dont les noms contiennent *sensibleDataServer*.

```
Event Type = Network Anomaly AND Network Anomaly - Non-seasonal Deviation > 10.0)
AND Network Anomaly - Egress App Byte Count > 1000000
AND Network Anomaly - Host Name CONTAINS sensitiveDataServer
```

Listing 7.10.1.1.3 : Détecte les événements d'anomalie de réseau sur les charges de travail avec des événements de commande non vues, à l'exception des événements d'anomalie de réseau qui se produisent de 7 h 30 UTC à 7 h 35 UTC tous les jours.

```
    Event Type = Network Anomaly AND Network Anomaly - Unseen Command Count > 0
    AND ( Network Anomaly - Date Time (UTC) - Hour != 7
    OR Network Anomaly - Date Time (UTC) - Minute < 30 OR Network Anomaly - Date Time (UTC)
 - Minute > 35 )
```

Actions découlant d'une règle

Action	Description
ENREGISTRER	Les événements correspondants contribuent à la note d'anomalie de réseau et peuvent être trouvés à l'aide du tableau de bord de sécurité ou de la page Workload Profile (de profil de charge de travail) ou de l'onglet Network Anomaly (anomalie du réseau).
ALERTE	Les événements correspondants s'affichent sur la page Alerts (Alertes) et dans les Alert Publishers (Serveurs de publication d'alertes) choisis.

La section suivante décrit plus en détail où trouver les événements d'anomalie de réseau détectés dans l'interface utilisateur.

Où voir les événements d'anomalies de réseau

Note Les événements d'anomalies de réseau ne sont actuellement *pas* affichés sur la page d'analyse criminalistique. Vous pouvez trouver les événements d'anomalies de réseau dans les pages suivantes.

- **Tableau de bord de sécurité :** les événements d'anomalies de réseau qui correspondent aux règles avec l'action **RECORD** (ENREGISTRER) se trouvent dans la section de la note d'anomalies de réseau dans le tableau de bord de la sécurité. S'il y a des charges de travail avec des notes différentes (inférieures à 100), en cliquant sur le nom de la charge de travail, vous pouvez afficher les séries chronologiques du PCR et les événements d'anomalies de réseau sur cette charge de travail. Sur le côté droit de chaque ligne du tableau des événements d'anomalie de réseau, vous pouvez voir des liens d'action qui peuvent vous aider à rechercher des flux et d'autres événements criminalistiques intervenus au moment de l'événement d'anomalie de réseau correspondant. Consultez la section Latence des anomalies de réseau pour connaître le retard connu du signalement dans la note d'anomalies de réseau.

Figure 13: Note d'anomalie de réseau dans le tableau de bord de la sécurité

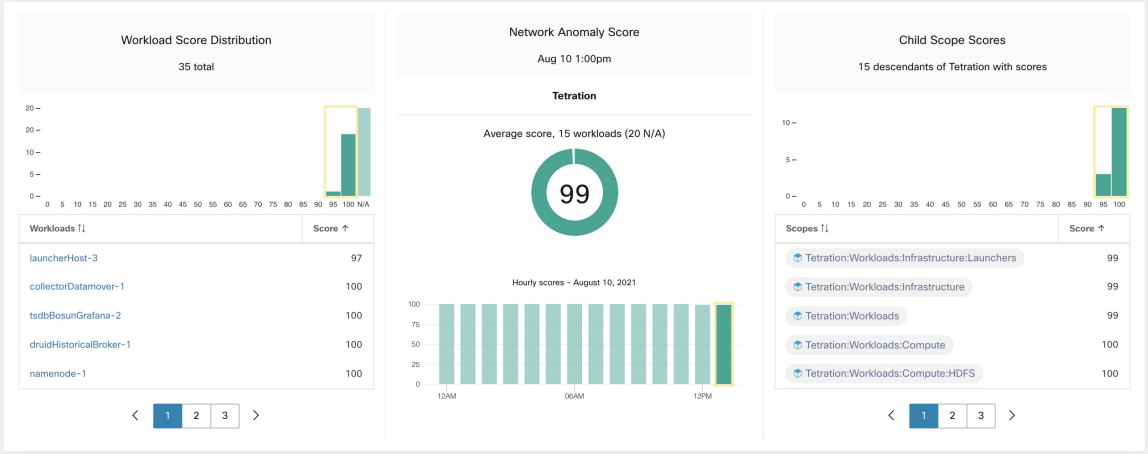
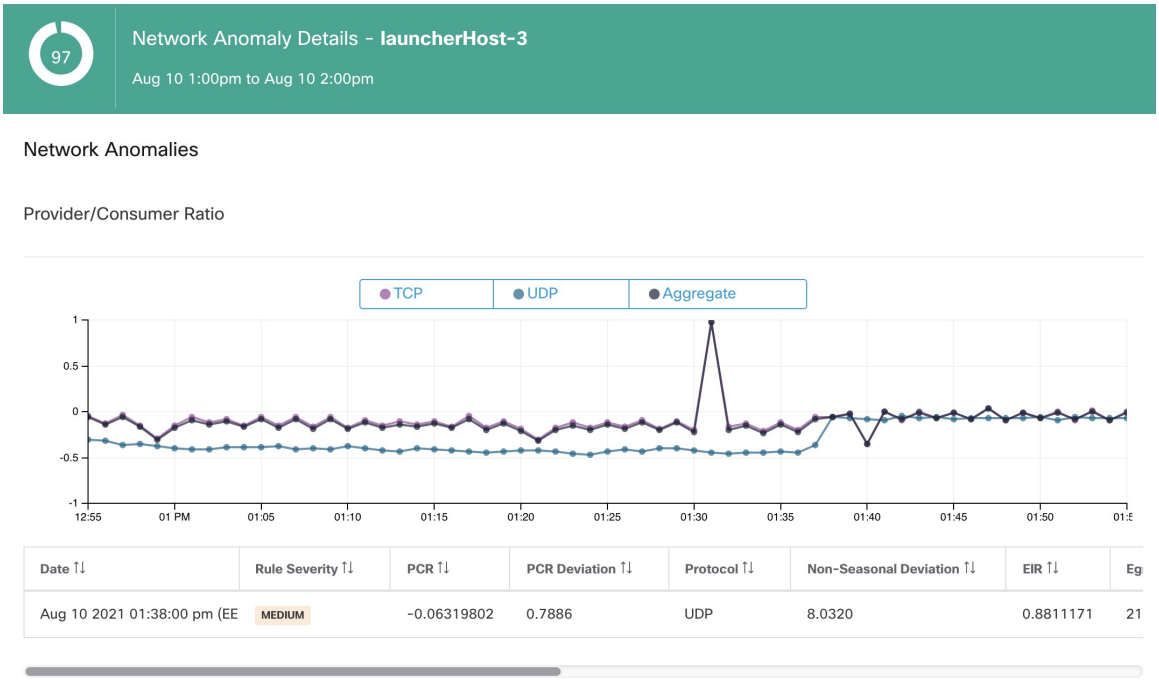
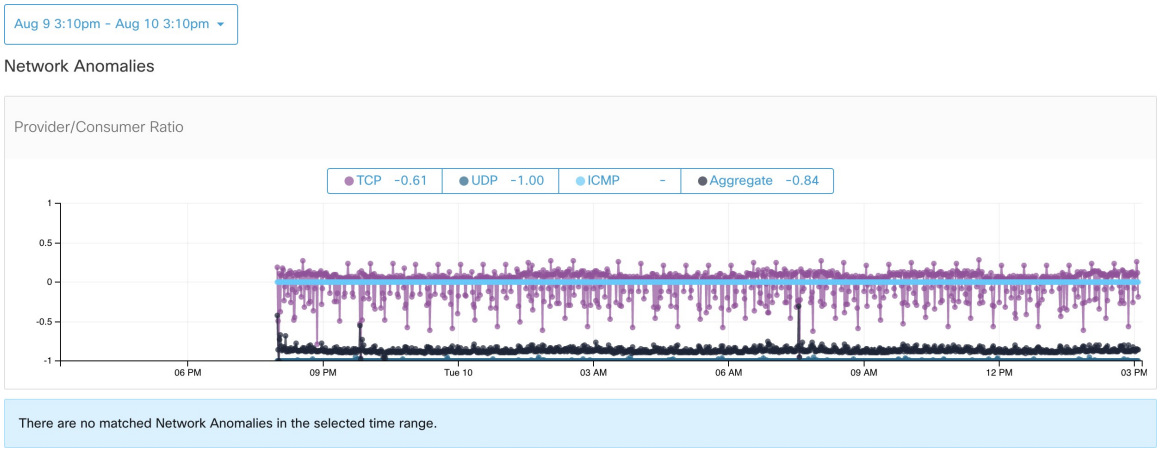


Figure 14: Note d'anomalie de réseau dans le tableau de bord de la sécurité, par charge de travail



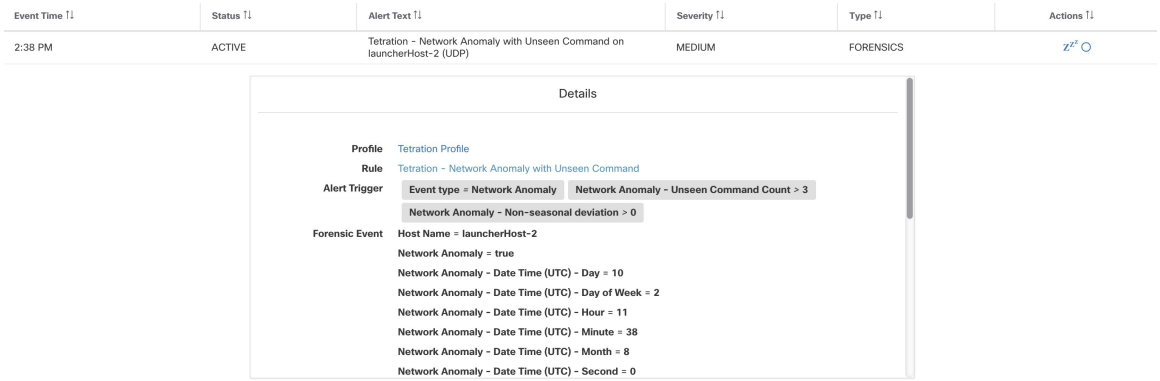
- Page Profil de charge de travail/onglet Anomalie de réseau **:** sur cette page, vous pouvez voir le graphique de la série chronologique PCR et les événements d'anomalie de réseau qui correspondent aux règles de l'action **RECORD** (ENREGISTRER). Ce que vous pouvez voir sur cette page est similaire à ce que vous trouvez en cliquant sur le nom de la charge de travail dans le tableau de bord de la sécurité.

Figure 15: Onglet Anomalie de réseau dans la page du Profil de charge de travail



- **Alertes :** Si la règle d'anomalie de réseau est configurée avec l'action **ALERT** ALERTE), les événements correspondants sont affichés dans la page Alertes et sont également disponibles sur le serveur de publication d'alertes.

Figure 16: Alerte d'anomalie de réseau



Notes de gravité des règles et d'anomalies de réseau

Le calcul de la note d'anomalie de réseau est similaire à celui de la note criminalistique. Pour chaque charge de travail, nous calculons un niveau d'anomalie de réseau. Le score d'anomalie de réseau d'une charge de travail est dérivé des événements d'anomalie de réseau observés sur cette charge de travail en fonction des profils activés pour cette portée. Une note de 100 signifie qu'aucun événement d'anomalie de réseau n'a été observé par le biais des règles configurées dans les profils activés. Une note de 0 signifie qu'une anomalie de réseau a été détectée et nécessite une action immédiate.

- Un événement d'anomalie de réseau avec le niveau de gravité REQUIRES IMMEDIATE ACTION (NÉCESSITE UNE ACTION IMMÉDIATE) réduit la note pour l'ensemble de la portée à 0.
- Un événement d'anomalie de réseau avec le niveau de gravité CRITICAL (CRITIQUE) réduit la note de la charge de travail avec un impact de 10.
- Un événement d'anomalie de réseau avec un niveau de gravité HIGH (ÉLEVÉ) réduit la note de la charge de travail avec un impact de 5.

- Un événement d'anomalie de réseau avec le niveau de gravité MEDIUM (MOYEN) réduit la note de la charge de travail avec un impact de 3.
- Un événement d'anomalie de réseau avec la gravité LOW (FAIBLE) ne contribue pas à la note d'anomalie de réseau. Cela est recommandé pour les nouvelles règles lorsque la qualité du signal est toujours en cours d'optimisation et est susceptible d'être bruitée.

Pour chaque charge de travail, la note totale d'impact est agrégée toutes les 5 minutes pour calculer la note de cette charge de travail au cours de ces 5 minutes.

Pour les charges de travail sans types de capteurs activés pour les anomalies de réseau, les notes d'anomalie de réseau sont S.O.

Rétention des données PCR et des événements d'anomalies de réseau

Les données de PCR et les événements d'anomalie de réseau sont conservés pendant 7 jours.

Latence des anomalies de réseau

Les notes d'anomalie de réseau signalées dans le tableau de bord de sécurité ont des retards de 5 minutes. Par exemple, la note d'une charge de travail pour l'heure 10 h à 10 h 59 est basée sur les événements d'anomalie de réseau qui se produisent entre 9 h 55 et 10 h 54

Mises en garde

- Les anciens événements de fuite de données demeurent des événements de fuite de données au lieu d'événements d'anomalie de réseau.
- La détection des anomalies de réseau par protocole est une nouvelle fonctionnalité dans la version 3.3 et le protocole n'est pas défini dans les anciens événements de fuite de données.

Process hash anomaly detection

As the name suggested, this feature detects process hash anomaly by assessing the consistency of process binary hashes across the system. The motivation of this feature is as follows. Imagine that you have a farm of Apache web servers that are cloned from the same setup configuration (e.g., those servers are deployed from the same automation scripts). Then you would expect that the hashes of httpd binaries on all servers are the same. If there is a mismatch, it is an anomaly and might worth a further investigation.

Formally, we define *process group* as the set of processes across workloads in the same rootscope that have the same combination of executable binary path, OS version, and package info (if applicable)1.

Note Package info is included since 3.4 release; in the previous releases, the process group is defined based on the combination of executable binary path and OS version only.

In the example above, suppose that all Apache web servers are running httpd 2.4.43 on CentOS 7.7 and in the same rootscope, then the corresponding process group is the set of processes (across all servers) that have

the same combination: binary path of `/usr/sbin/ httpd` & OS version of `CentOS-7.7` & package version of `httpd-2.4.43`. It is expected that the hashes of all binaries in the same process group are the same, and an anomaly will appear if any mismatch is detected.

Besides detecting anomalous process hashes, this feature also detects process hashes that appear in a Flagged list uploaded by user. The motivation is that you may have a list of known malware hashes, and would like to know if a process associated with any of those hashes is run.

To reduce false alarms, we use the National Software Reference Library's Reference Data Set (RDS) provided by NIST (we also call it NIST RDS dataset) as a Benign list; a benign hash is considered "safe" (see Analyse des rapports d'informations sur les menaces on how to enable NIST RDS dataset). You can also upload your own hash Benign list.

In addition to the NIST RDS dataset, we also curate **Secure Workload Hash Verdict** service. When this service is enabled, if any known malware hash shows up, it will be detected as malicious hash. On the other hand, if the hash is known and legit, then it is also marked as benign in the anomaly analysis. Due to the extremely large dataset and fast updates that covers all known and legit process hashes that can be used to either approve or red flag processes running on a workload, Cisco Secure Workload Hash Verdict is only available via Cisco Secure Workload Cloud. Please refer to Automatic Threat Intelligence Updates to ensure Cisco Secure Workload Hash Verdict service is accessible from your appliance.

Output of this feature is a security score called **process hash score**. This score is calculated and output hourly. Like all other security scores, a higher process hash score is better. In particular, for a process hash:

- Hash score of 0 means that the hash is flagged or malicious
- Hash score of 100 means that the hash is either benign, or consistent across workloads (no mismatch)
- Hash score from 1 to 99 means that the hash is considered anomalous (i.e., there is some mismatch)

The process hash score of an workload is the minimum process hash score of all hashes observed in that workload, with 0 meaning there is a flagged or malicious process hash in the system, and 100 meaning there is no hash anomaly observed in the system.

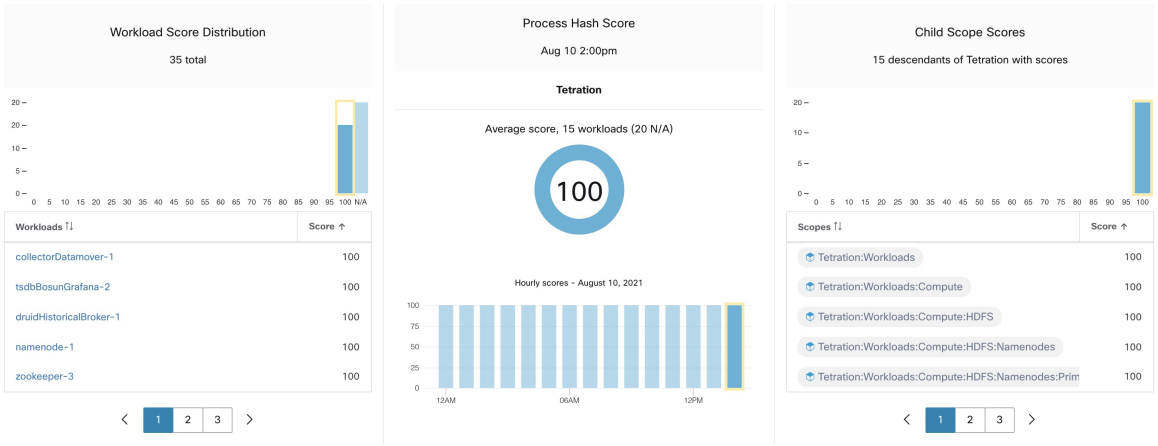
Comment activer la fonctionnalité de condensé de processus

La fonction de condensé de processus est activée par défaut sur les agents de visibilité approfondie et les agents d'application; aucune configuration criminalistique n'est nécessaire. Si de tels agents sont présents dans votre système, vous devriez commencer à voir les résultats dans les 2 heures suivant le démarrage du système.

Où voir la note de condensé de processus

- **Tableau de bord de sécurité**

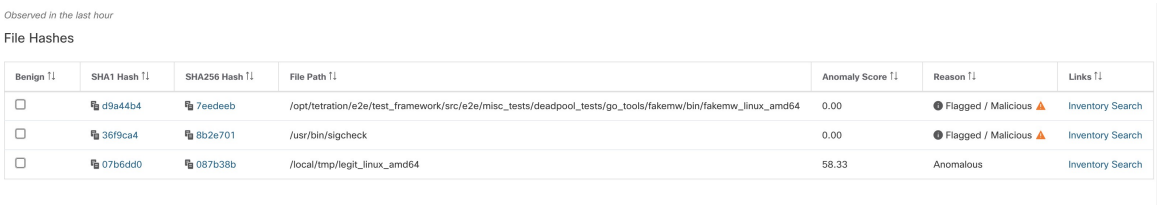
Figure 17: Traiter la section de la note de condensé dans le Tableau de bord de sécurité



Traiter la section de la note de condensé dans le Tableau de bord de sécurité

- **Page du profil de la charge de travail** / Onglet Condensé du fichier :

Figure 18: Onglet Condensé du fichier dans la page de Profil de charge de travail



Onglet Condensé du fichier dans la Page Profil de la charge de travail

Comment la note de condensé de processus est calculée

Pour chaque condensé de processus, nous calculons une note comme suit :

1. Si le condensé est signalé ou malveillant, `note = 0`
2. Sinon, si le condensé est inoffensif, `note = 100`
3. Sinon, si le condensé est en anomalie, la `note` est comprise dans la plage `[1, 99]`, plus elle est élevée, mieux c'est.
4. Sinon, `note = 100`

La logique de calcul de la note dans (3) est la suivante : nous calculons d'abord la note minimale du condensé (qui est égale à un moins le ratio de population de ce condensé dans la population de charge de travail sous la même portée), puis nous l'inscrivons dans l'intervalle `[0,0, 1,0]` à l'aide d'une fonction d'information `-log2(x)`. Si la note minimale du condensé est supérieure à 0,5, nous inscrivons à nouveau la note dans l'intervalle `[1,0, 99,0]`. Prenons l'exemple de la batterie de serveurs Web Apache ci-dessus et considérons le condensé de `httpd`. Voici quelques scénarios :

- Supposons que `httpd` ait deux valeurs de condensé (`h1` et `h2`) sur 1 000 serveurs de la batterie : `h1` sur 1, `h2` sur les 999 autres serveurs. Dans ce cas :

- `population_ratio(h1) = 0,001, population_ratio(h2) = 0,999`. Ensuite :
- `minority_score(h1) = 0,999,minority_score (h2) = 0,001`. Ensuite :
- `note (h1) = -log2 (0,999) * 98 +1 = 1,14;`
- Puisque `minority_score(h2) < 0,5, h2` n'est pas considéré comme une anomalie, alors `score(h2) = 100`.

- Supposons que `httpd` ait deux valeurs de condensé (`h1` et `h2`) sur 10 serveurs de la batterie : `h1` sur 1 serveur, `h2` sur les 9 autres serveurs. Dans ce cas :
  - `population_ratio(h1) = 0,1 = population_ratio(h2) = 0,9`. Ensuite :
  - `minority_score(h1) = 0,9, minority_score(h2)= 0,1`. Ensuite :
  - `note(h1) = -log2 (0,9) * 98 +1 = 15,90;`
  - Puisque `minority_score(h2) < 0,5, h2` n'est pas considéré comme une anomalie, alors `score(h2) = 100`.

- Supposons que `httpd` comporte deux valeurs de condensé (`h1` et `h2`) sur deux serveurs de la batterie : `h1` sur un serveur, `h2` sur l'autre. Dans ce cas :
  - `population_ratio(h1) = population_ratio(h2) = 0,5`. Ensuite :
  - `minority_score(h1) = minority_score(h2) = 0,5`. Ensuite :
  - `score(h1) = score(h2) = -log2(0,5) * 98 + 1 = 99,0`. Il s'agit du score le plus élevé pour un condensé qui est considéré comme une anomalie.

- Supposons que `httpd` n'ait qu'une seule valeur de condensé (`h1`) sur tous les serveurs. Dans ce cas, `minority_score(h1) = 0,0 < 0,5;` par conséquent, il n'est pas considéré comme une anomalie et son `score(h1) = 100`.

Enfin, la note de condensé de processus d'une charge de travail est la note de condensé de processus minimale de tous les condensés observés dans cette charge de travail.

Vous pouvez trouver ici des renseignements supplémentaires sur la fonction d'information `-log2(x)`.

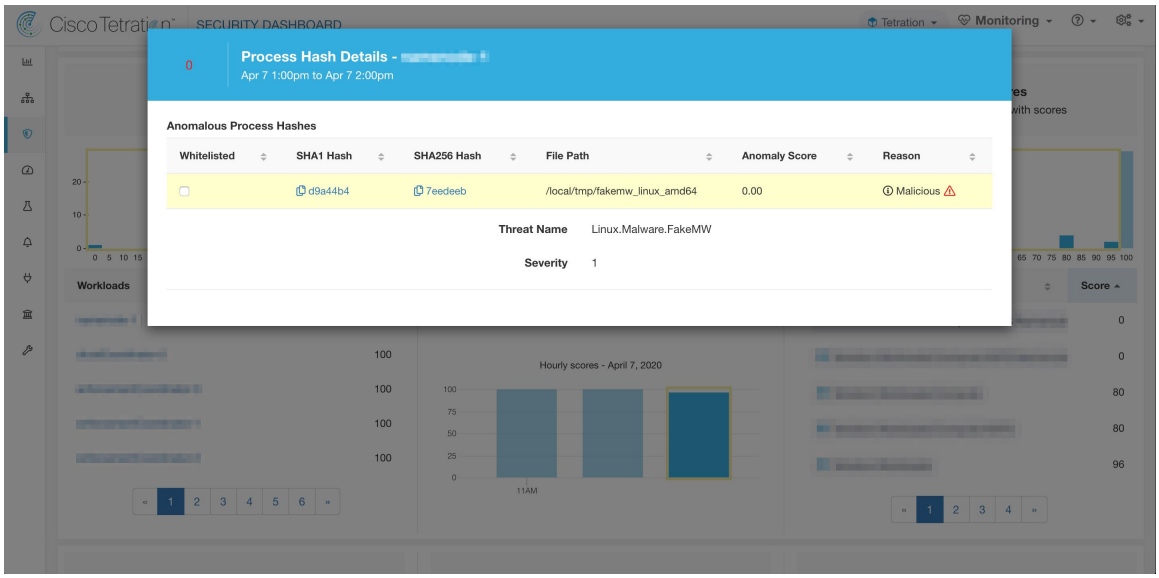
Comment améliorer la note de condensé de processus

Une note de condensé de processus de 0 pour une charge de travail signifie qu'un condensé de processus signalé ou malveillant est apparu dans cette charge de travail; le fait d'empêcher ce processus de s'exécuter à nouveau améliore le résultat. Une note de condensé de processus positive inférieure à 100 signifie qu'il y a une anomalie de condensé de processus dans votre système; ce n'est pas malveillant mais mérite une enquête plus approfondie. Après une enquête approfondie, s'il est conclu que le condensé est sûr, l'ajouter à votre liste « Bénigne » améliorera également le résultat. L'utilisateur peut marquer les condensés anormaux comme « bénins » en cochant la case « Bénin » dans la page File Hashs/Process Hash Details (Détails des condensés de fichiers/processus) ou en téléversant une liste bénigne via OpenAPI.

Détails sur la menace

Comme mentionné précédemment, si Cisco Secure Workload, le service Hash Verdict (Verdict de condensé) est activé, tout condensé de logiciel malveillant connu, lorsqu'il apparaît, est signalé comme malveillant. Dans ce cas, des informations supplémentaires sur les menaces du condensé malveillant (recueillies sur notre plateforme de renseignements sur les menaces) sont fournies. Actuellement, les données supplémentaires sur les menaces comprennent le *nom* et *la gravité* de la menace. Le nom est le nom de la menace, tandis que la gravité est une valeur comprise entre 1 et 5 pour indiquer sa gravité, où 1 signifie la menace la moins grave et 5 la plus grave.

Figure 19: L'utilisateur peut cliquer sur la ligne contenant le code de condensé malveillant pour afficher les détails des renseignements sur les menaces



Mises en garde

- La tâche d'analyse du condensé des processus est exécutée une fois par heure, mais il peut s'écouler jusqu'à deux heures avant que les notes/résultats attendus ne s'affichent dans le tableau de bord de la sécurité, en fonction de l'action. Voici des exemples :
  - Si vous chargez votre liste de condensés marqués et qu'un condensé de processus figurant dans cette liste apparaît, il peut s'écouler jusqu'à une heure avant que la note ne soit reflétée dans le tableau de bord de la sécurité.
  - Si vous supprimez un condensé de votre liste marquée, il peut s'écouler jusqu'à deux heures avant qu'il soit effacé et que le résultat soit reflété dans le tableau de bord de sécurité.
- Conservation :
  - Les résultats détaillés de l'analyse de condensé de processus sont conservés pendant au moins 7 jours.
- L'onglet File Hashs (Condensés de fichiers) dans la page Workload Profile (Profil de charge de travail) affiche uniquement les détails du condensé de processus analysés au cours de la dernière heure.

- Les versions précédentes des agents de visibilité approfondie et d'application, et les points d'accès AnyConnect signalaient uniquement les valeurs de condensé SHA256. Par conséquent, la correspondance avec la liste marquée/bénigne du condensé SHA1 n'est pas prise en charge pour ces agents.
- La note de condensé de processus est calculée en fonction d'une portée racine particulière. Si une charge de travail appartient à plusieurs portées racine, la note de condensé de processus de cette charge de travail est la note minimale de toutes les portées racine auxquelles elle appartient.
- Pour réduire davantage les fausses alertes lors de l'analyse des anomalies de condensé de processus, nous marquons également tous les fichiers binaires Cisco Secure Workloadcomme bénins en fonction de leurs chemins d'accès à leurs fichiers. Ce mécanisme se produit uniquement lorsque ces condensés n'apparaissent dans aucune liste de condensé définie par l'utilisateur ou ne sont pas signalés par le service Hash Verdict Cisco Secure Workload.

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.