[Externe] - Utilisation d'AMP (Advanced Malware Protection) - Détections erronées, attaques et réponse aux incidents

Table des matières

Introduction

Description

- Actions immédiates
- Analyse
- Analyse par Cisco

Articles associés

Introduction

Nous nous efforçons toujours d'améliorer et d'étendre les informations sur les menaces pour notre technologie AMP (Advanced Malware Protection). Toutefois, si votre solution AMP n'a pas déclenché d'alerte ou a déclenché une alerte par erreur, vous pouvez prendre des mesures pour empêcher tout impact supplémentaire sur votre environnement. Le présent document fournit des lignes directrices sur ces mesures.

Description

Actions immédiates

Si vous pensez que votre solution AMP n'a pas protégé votre réseau contre une menace, prenez immédiatement les mesures suivantes :

1. Isolez les machines suspectes du reste du réseau. Il peut s'agir d'éteindre la machine ou de la déconnecter physiquement du réseau.
2. Notez les informations importantes sur l'infection, telles que l'heure à laquelle la machine peut être infectée, les activités de l'utilisateur sur les machines suspectes, etc.

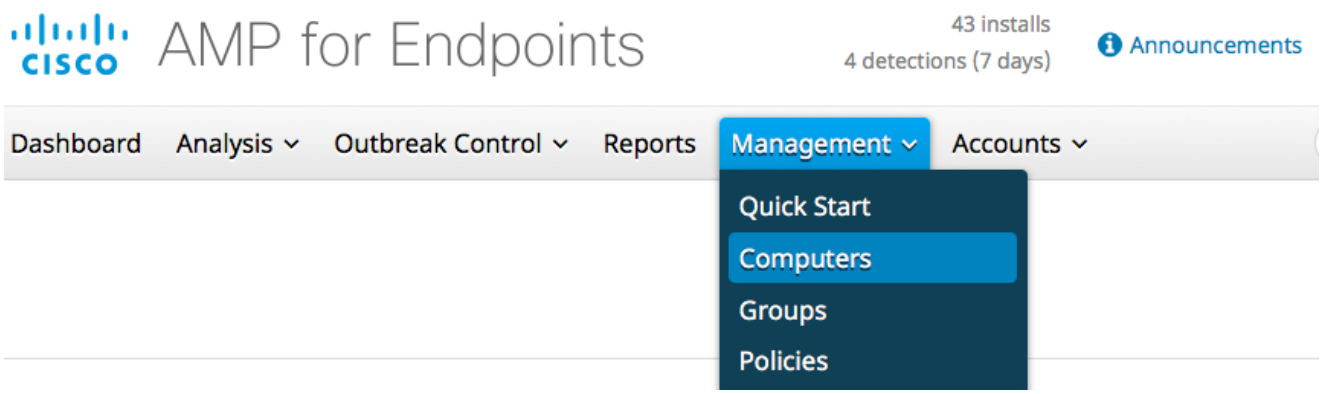
Avertissement : n'effacez pas l'ordinateur et ne le réinstallez pas. Il élimine les risques de trouver le logiciel ou les fichiers incriminés lors d'une enquête judiciaire ou d'une procédure de dépannage.

Analyse

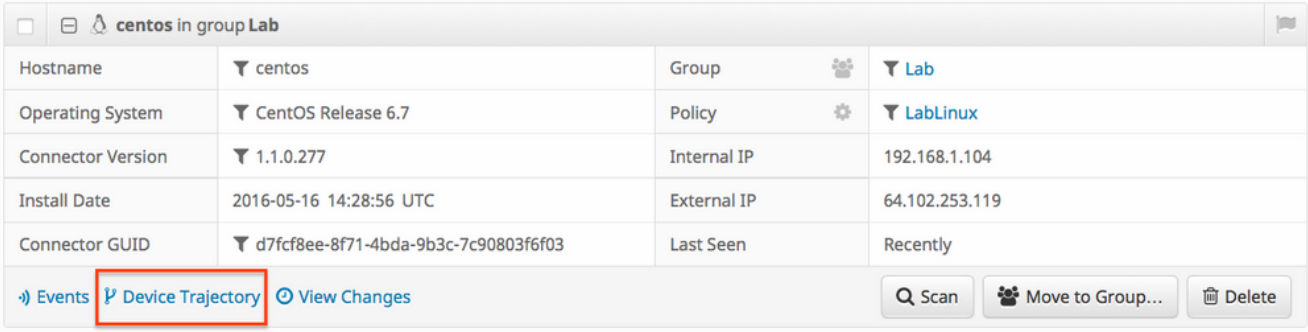
1. Utilisez la fonction Trajectoire du périphérique pour commencer votre propre investigation. Device Trajectory est capable de stocker environ les 9 millions d'événements de fichiers les

plus récents. La trajectoire du périphérique AMP for Endpoints est très utile pour le suivi des fichiers ou des processus ayant entraîné une infection.

Dans le tableau de bord, accédez à Gestion > Ordinateurs.



Recherchez la machine suspecte et développez l'enregistrement de cette machine. Cliquez sur l'option Trajectoire du périphérique.



2. Si vous trouvez un fichier ou un hachage suspect, ajoutez-le à vos listes de détection personnalisées. AMP for Endpoints peut utiliser une liste de détection personnalisée pour traiter un fichier ou un hachage comme malveillant. C'est un excellent moyen de fournir une couverture de type « stop-gap » pour éviter tout impact supplémentaire.

Analyse par Cisco

1. Soumettez tous les échantillons suspects à une analyse dynamique. Vous pouvez les soumettre manuellement à partir de Analyse > Analyse de fichiers dans le tableau de bord. AMP for Endpoints inclut une fonctionnalité d'analyse dynamique qui génère un rapport sur le comportement du fichier à partir de Threat Grid. Cela a également l'avantage de fournir le fichier à Cisco dans le cas où une analyse supplémentaire par notre équipe de recherche est nécessaire.

2. Si vous suspectez des détections de faux positifs ou de faux négatifs sur votre réseau, nous vous conseillons d'utiliser la fonctionnalité de liste noire ou de liste blanche personnalisée pour vos produits AMP. Lorsque vous contactez le centre d'assistance technique Cisco (TAC), fournissez les informations suivantes pour analyse :

- Hachage SHA256 du fichier.
- Une copie du fichier si possible.
- Informations sur le fichier, telles que son origine et la raison pour laquelle il doit se trouver dans l'environnement.
- Expliquez pourquoi vous croyez que c'est un faux positif ou un faux négatif.

3. Si vous avez besoin d'aide pour atténuer une menace ou effectuer un tri de votre environnement, vous devrez faire appel à l'équipe Cisco Talos Incident Response (CTIR), spécialisée dans la création de plans d'action, la recherche de machines infectées et l'utilisation d'outils ou de fonctionnalités avancés pour limiter une épidémie active.

Remarque : Le Centre d'assistance technique Cisco (TAC) ne fournit pas d'assistance pour ce type d'engagement.

Vous pouvez contacter CTIR ici. Il s'agit d'un service payant à partir de 60 000 $, sauf si votre entreprise dispose d'une retenue pour les services de réponse aux incidents de Cisco. Une fois engagés, ils fournissent des informations supplémentaires sur leurs services et ouvrent un dossier pour votre incident. Nous vous recommandons également de contacter votre responsable de compte Cisco afin qu'il vous fournisse des conseils supplémentaires sur le processus.

Articles associés

- Collecte de données de diagnostic à partir d'un connecteur FireAMP sous Windows
- Types de fichiers analysés par le connecteur FireAMP

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.