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

Contenu

Introduction

Nous nous efforçons toujours d'améliorer et d'étendre l'intelligence des menaces pour notre technologie AMP (Advanced Malware Protection). Toutefois, si votre solution AMP n'a pas déclenché d'alerte ou déclenché une alerte par erreur, vous pouvez prendre certaines mesures pour éviter tout autre impact 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, effectuez immédiatement les actions suivantes :

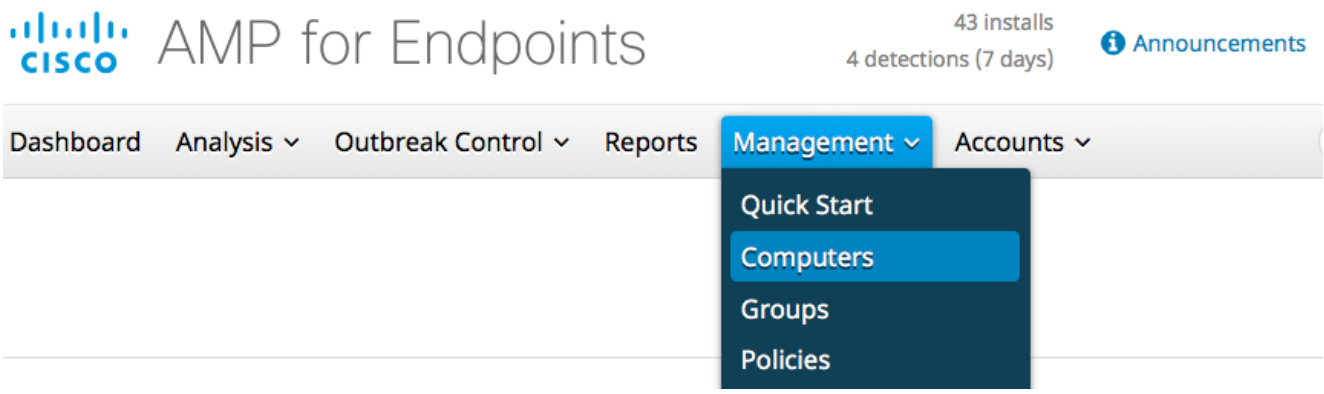
1. Isolez les machines suspectes du reste du réseau. Cela peut inclure la mise hors tension de la machine ou sa déconnexion physique du réseau.
2. Notez les informations importantes sur l'infection, telles que l'heure à laquelle la machine pourrait être infectée, les activités de l'utilisateur sur les machines suspectes, etc.

   Avertissement : Ne pas effacer ou réinstaller la machine. Il élimine les chances de trouver le ou les logiciels incriminés au cours d'une enquête judiciaire ou d'un processus de dépannage.

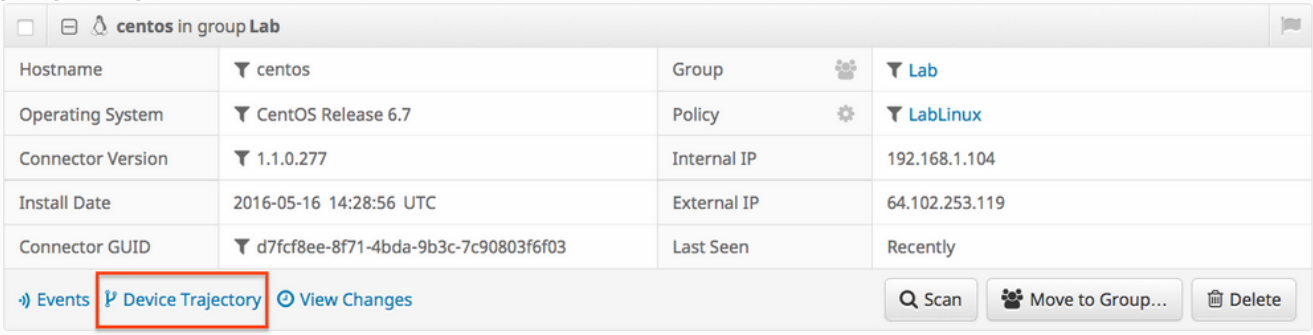
Analyse

1. Utilisez la fonction **Trajectoire du périphérique** pour commencer votre propre enquête. La trajectoire de périphérique peut stocker environ les 9 millions d'événements de fichiers les plus récents. La trajectoire du périphérique AMP for Endpoints est très utile pour suivre les fichiers ou les processus qui ont conduit à une infection.

Dans le tableau de bord, accédez à **Management > Computers**.



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. Il s'agit d'un excellent moyen d'assurer une couverture de l'intervalle de temps à autre afin d'éviter tout impact supplémentaire.

Analyse par Cisco

1. Soumettez tout échantillon suspect pour analyse dynamique. Vous pouvez les soumettre manuellement à partir de **Analysis > File Analysis** 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 présente également l'avantage de fournir le fichier à Cisco au cas où une analyse supplémentaire par notre équipe de recherche serait nécessaire.

2. Si vous soupçonnez des détections *de faux positifs* ou de *faux négatifs* dans 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 pourquoi il doit être 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 pour effectuer un triage de votre environnement, vous devrez faire appel à l'équipe Cisco Talos Incident Response (CTIR), qui se spécialise 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.

Note: Le centre d'assistance technique Cisco (TAC) ne fournit pas d'assistance pour ce type d'engagement.On peut contacter le CTIR ici. Il s'agit d'un service payant à partir de 60 000 $, à moins que votre entreprise ne dispose d'une réserve 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 puisse fournir des conseils supplémentaires sur le processus.

Articles connexes

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