Fonctionnant avec des détections de protection de malware (AMP), des épidémies, et la réponse fausses avancées d'incident

Contenu

Introduction

Nous tâchons toujours d'améliorer et développer le renseignement sur la menace pour notre technologie avancée de protection de malware (AMP), cependant si votre solution d'AMP ne déclenchait pas une alerte ou déclenchait une alerte incorrectement, vous pouvez prendre quelques mesures d'empêcher de promouvoir l'incidence à votre environnement. Ce document fournit une instruction sur ces actions à entreprendre.

Description

Actions immédiates

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

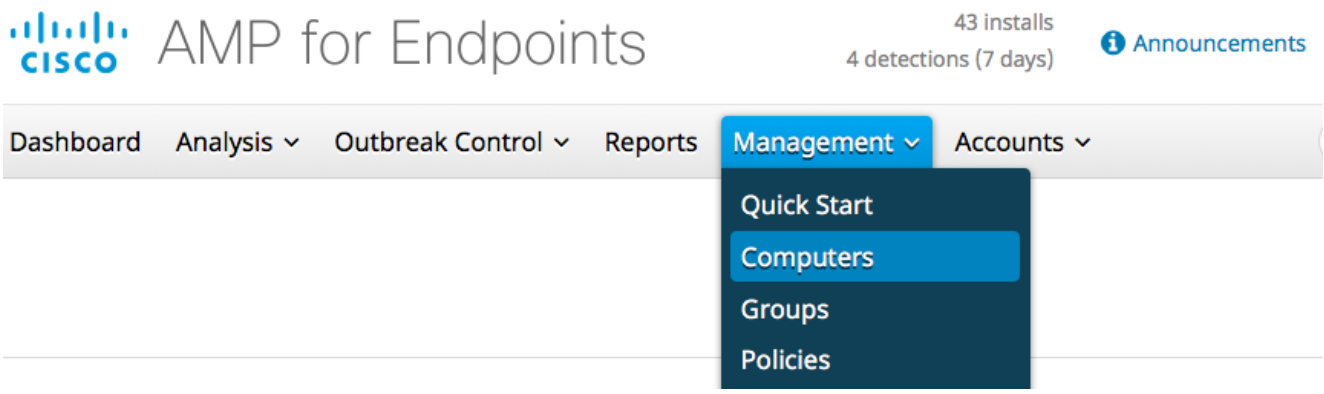
1. Isolez les ordinateurs méfiants du reste du réseau. Ceci a pu inclure arrêter l'ordinateur, ou le déconnecter du réseau physiquement.
2. Notez les informations importantes au sujet de l'infection, comme, du moment où l'ordinateur pourrait être infecté, des activités d'utilisateur sur les ordinateurs méfiants, etc.

Avertissement : N'éliminez pas ou réimagez l'ordinateur. Il élimine les possibilités de trouver le logiciel ou les fichiers offensants pendant l'enquête ou le processus de dépannage légale.

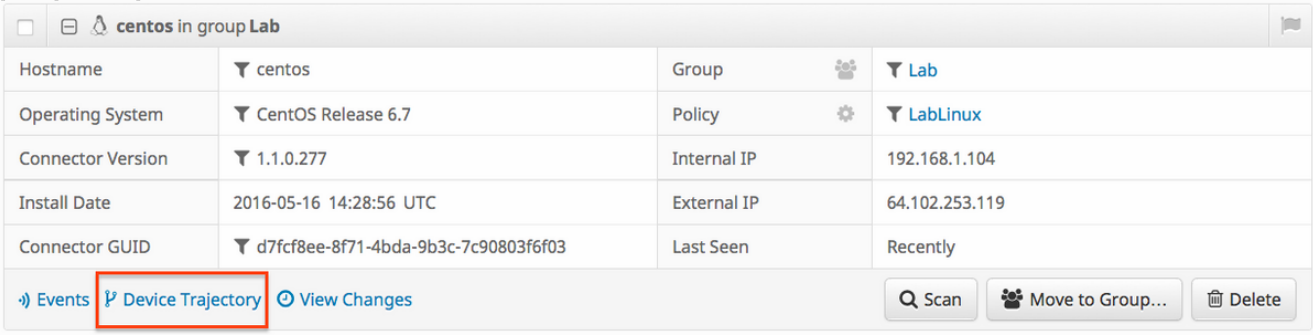
Analyse

1. Employez la caractéristique de **trajectoire de périphérique** pour commencer votre propre enquête. La trajectoire de périphérique est capable d'enregistrer approximativement 9 millions d'événements de fichier les plus récents. L'AMP pour la trajectoire de périphérique de points finaux est très utile pour dépister des fichiers ou des processus que cela a menés à une infection.

Dans le tableau de bord, naviguez vers la **Gestion > les ordinateurs**.



Trouvez l'ordinateur méfiant et développez l'enregistrement pour cet ordinateur. Cliquez sur en fonction l'option de **trajectoire de périphérique**.



2. Si vous trouvez n'importe quel fichier ou informations parasites méfiant, ajoutez-les à vos listes faites sur commande de détection. L'AMP pour des points finaux peut employer une liste faite sur commande de détection pour traiter un fichier ou des informations parasites comme malveillantes. C'est une grande manière de fournir la couverture transitoire pour empêcher davantage d'incidence.

Analyse par Cisco

1. Soumettez tous les échantillons méfiants pour l'analyse dynamique. Vous pouvez manuellement les soumettre de l'**analyse > de l'analyse de fichier** dans le tableau de bord. L'AMP pour des points finaux inclut la fonctionnalité d'analyse dynamique qui génère un état du comportement du fichier de la grille de menace. Ceci a également l'avantage de fournir le fichier à Cisco au cas où l'analyse supplémentaire par notre équipe de recherche serait exigée.

2. Si vous suspectez n'importe quelles détections de *faux positif* ou de *faux négatif* dans votre réseau, nous informons que vous accroissez la fonctionnalité noire faite sur commande de liste ou de liste de blanc pour vos Produits d'AMP. Quand vous entrez en contact avec le centre d'assistance technique Cisco (TAC), fournissez les informations suivantes pour l'analyse :Les informations parasites SHA256 du fichier.Une copie de fichier si possible.Informations sur le fichier tel qu'où il est provenu et pourquoi il doit être dans l'environnement.Expliquez pourquoi vous pensez ceci pour être un faux positif ou un faux négatif.
3. Si vous avez besoin d'assistance atténuant une menace ou exécutant la sélection de votre environnement, vous devrez engager l'équipe des services de réponse d'incident de sécurité

Cisco (CSIRS) qui se spécialisent en créant des plans d'action, en recherchant les ordinateurs infectés, et en accroissant les outils ou les caractéristiques avancés pour atténuer une épidémie active.
Note: Le centre d'assistance technique Cisco (TAC) ne fournit pas à l'assistance ce type d'engagement.L'équipe CSIRS peut enagaged en demandant ce numéro de téléphone : +1-844-831-7715. C'est un service payé commençant à $60,000 à moins que votre organisation ait un arrêtoir pour des services de réponse d'incident de Cisco. Une fois qu'engagé ils fourniront les informations complémentaires au sujet de leurs services et ouvriront une valise pour votre incident. Nous recommandons également la continuation avec votre gestionnaire de compte Cisco de sorte qu'ils puissent fournir des conseils supplémentaires sur le processus.

Articles relatifs

- Collecte de données diagnostiques d'une exécution de connecteur de FireAMP sur Windows
- Types de fichier qui sont balayés par le connecteur de FireAMP