[Extern] - Arbeiten mit AMP (Advanced Malware Protection) - Fehlerkennung, Outbreaks und Reaktion auf Vorfälle

Inhalt

Einführung

Wir bemühen uns stets, die Bedrohungsinformationen für unsere AMP-Technologie (Advanced Malware Protection) zu verbessern und zu erweitern. Wenn Ihre AMP-Lösung jedoch keine Warnmeldung auslöst oder eine falsche Warnmeldung auslöst, können Sie einige Maßnahmen ergreifen, um weitere Auswirkungen auf Ihre Umgebung zu verhindern. Dieses Dokument enthält eine Richtlinie zu diesen Aktionspunkten.

Beschreibung

Sofortige Maßnahmen

Wenn Sie der Meinung sind, dass Ihr Netzwerk durch Ihre AMP-Lösung nicht vor einer Bedrohung geschützt wurde, führen Sie die folgenden Schritte sofort aus:

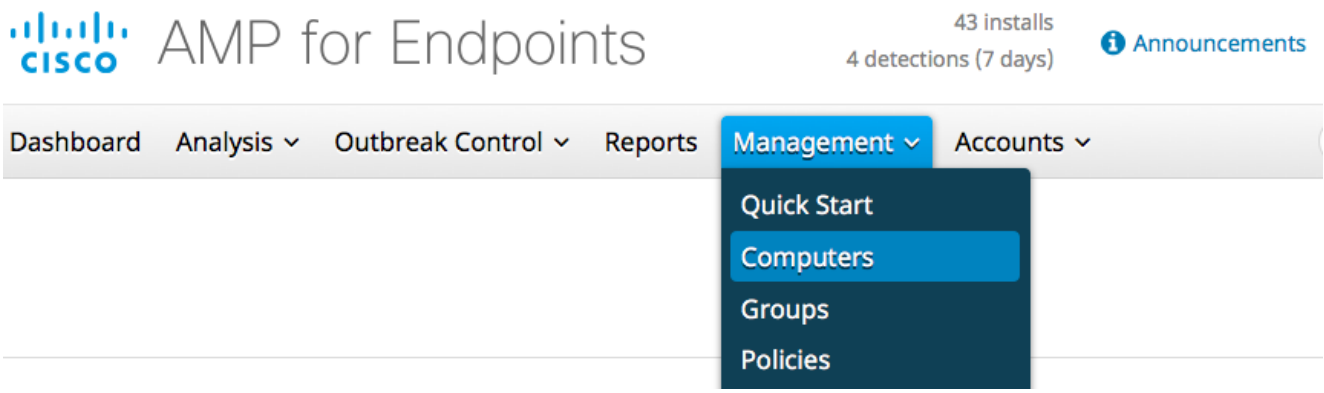
1. Isolieren Sie die verdächtigen Systeme vom Rest des Netzwerks. Dies kann das Ausschalten oder physische Trennen des Geräts vom Netzwerk umfassen.
2. Notieren Sie sich wichtige Informationen über die Infektion, z. B. den Zeitpunkt, zu dem der Computer infiziert werden könnte, die Benutzeraktivitäten auf den verdächtigen Computern usw.

   Warnung: Löschen Sie den Computer nicht, und erstellen Sie kein neues Bild. Sie verhindert, dass schädliche Software oder Dateien während der forensischen Untersuchung oder Fehlerbehebung gefunden werden.

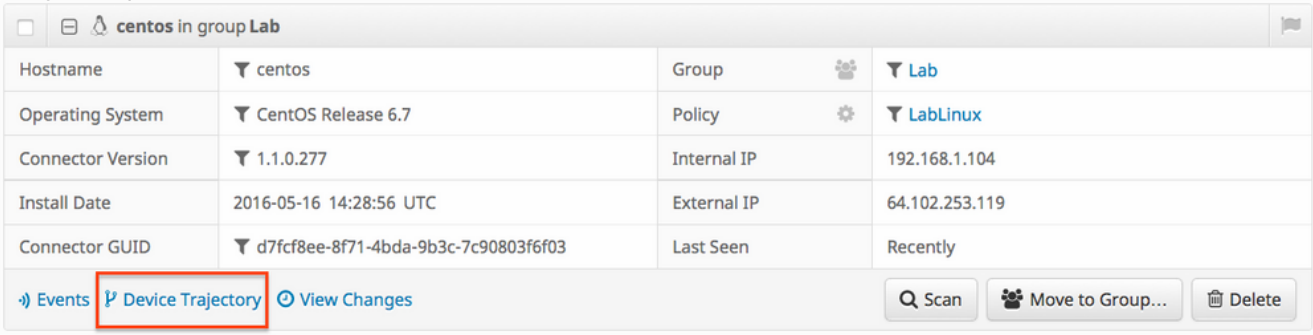
Analyse

1. Verwenden Sie die Funktion **Device Trajectory**, um Ihre eigene Untersuchung einzuleiten. Device Trajectory kann ungefähr die 9 Millionen aktuellsten Dateiereignisse speichern. Die AMP für Endgeräte-Device Trajectory ist sehr hilfreich, um Dateien oder Prozesse zu verfolgen, die zu einer Infektion führten.

Navigieren Sie im Dashboard zu **Verwaltung > Computer**.



Finden Sie den verdächtigen Computer und erweitern Sie den Datensatz für diesen Computer. Klicken Sie auf die Option **Device Trajectory**.



2. Wenn Sie verdächtige Dateien oder Hashs finden, fügen Sie diese Ihrer benutzerdefinierten Erkennungsliste hinzu. AMP für Endgeräte kann eine benutzerdefinierte Erkennungsliste verwenden, um eine Datei oder einen Hash als schädlich zu behandeln. Dies ist ein hervorragender Weg, um Lücken zu schließen und weitere Auswirkungen zu verhindern.

Analyse durch Cisco

1. Senden Sie verdächtige Stichproben zur dynamischen Analyse. Sie können sie manuell über **Analyse > Dateianalyse** im Dashboard senden. AMP für Endgeräte enthält Funktionen für dynamische Analysen, die einen Bericht über das Verhalten der Datei von Threat Grid generieren. Dies hat auch den Vorteil, dass die Datei Cisco zur Verfügung gestellt wird, falls weitere Analysen durch unser Forschungsteam erforderlich sind.

2. Wenn Sie *falsch positive* oder *falsch negative* Erkennungen in Ihrem Netzwerk vermuten, empfehlen wir Ihnen, benutzerdefinierte Blacklist- oder Whitelist-Funktionen für Ihre AMP-Produkte zu verwenden. Wenn Sie sich an das Cisco Technical Assistance Center (TAC) wenden, geben Sie die folgenden Informationen für die Analyse an:Der SHA256-Hash der Datei.Eine Kopie der Datei, wenn möglich.Informationen über die Datei, wie z. B. woher sie stammt und warum sie in der Umgebung sein muss.Erklären Sie, warum dies Ihrer Meinung nach falsch positiv oder falsch negativ ist.
3. Wenn Sie Hilfe bei der Eindämmung von Bedrohungen oder bei der Durchführung einer Triage Ihrer Umgebung benötigen, müssen Sie das Cisco Talos Incident Response (CTIR)-Team einbeziehen, das sich auf die Erstellung von Aktionsplänen, die Recherche infizierter Systeme und die Nutzung fortschrittlicher Tools oder Funktionen zur Eindämmung eines

aktiven Outbreaks spezialisiert hat.
Hinweis: Das Cisco Technical Assistance Center (TAC) leistet bei dieser Art von Zusammenarbeit keine Unterstützung.CTIR kann hier kontaktiert werden. Hierbei handelt es sich um einen kostenpflichtigen Service ab 60.000 US-Dollar, es sei denn, Ihr Unternehmen verfügt über eine Rückstellung für Incident Response Services von Cisco. Nach der Kontaktaufnahme stellen sie zusätzliche Informationen zu ihren Services bereit und eröffnen ein Ticket für Ihren Incident. Wir empfehlen Ihnen auch, sich mit Ihrem Cisco Account Manager in Verbindung zu setzen, um ihm zusätzliche Unterstützung beim Prozess zu bieten.

Verwandte Artikel

- Erfassen von Diagnosedaten eines unter Windows laufenden FireAMP-Connectors
- Von FireAMP Connector gescannte Dateitypen