Erkennungsmodul in der Konsole für sichere Endgeräte identifizieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Engine identifizieren, die für eine bestimmte Erkennung in der Secure Endpoint-Konsole verantwortlich ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Endpoint-Konsole

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Secure Endpoint Console v5.4.2025030619

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

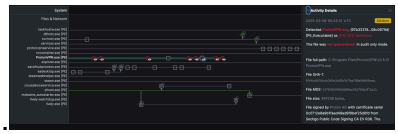
Problem

Die Identifizierung der richtigen Engine, die für eine bestimmte Erkennung verantwortlich ist, ist einer der ersten Schritte, um die Art des Ereignisses zu verstehen und es effektiv auszulösen.

Lösung

1. Navigieren Sie zur Seite Events (Ereignisse) in Ihrer AMP-Konsole, um das Ereignis zu finden, das Sie näher untersuchen möchten.
2. Klicken Sie auf das hervorgehobene Symbol, um Device Trajectory zu öffnen. 

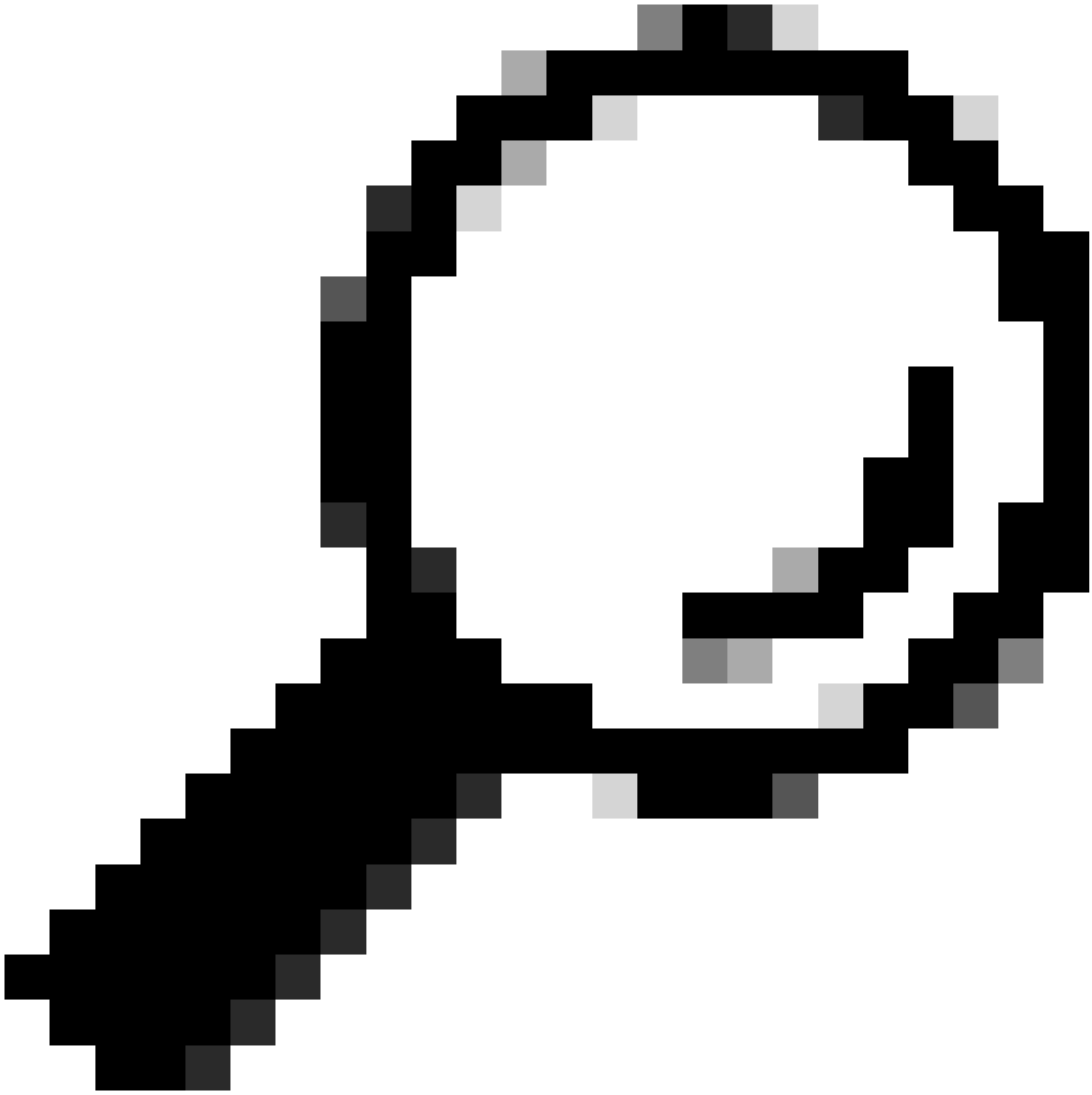
   Device Trajectory-Symbol

3. Die Veranstaltungsdetails finden Sie rechts unter Aktivitätsdetails. 

   Ereignisdetails in Device Trajectory

4. Navigieren Sie nach unten, um den Abschnitt Erkannt von zu finden. 

   Erkannt von Abschnitt



Tipp: Diese Informationen sind wichtig, um die Art der Bedrohung beurteilen und schnell den richtigen Ausschluss für die Konfiguration bestimmen zu können. Darüber hinaus kann die Angabe dieser Details bei der Einreichung eines Falls beim TAC für Untersuchungen mit Fehlalarmen den Prozess beschleunigen.

Wenn Sie den Abschnitt "Erkannt von" nicht anzeigen können oder keine weitere Unterstützung erhalten, wenden Sie sich an das TAC.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.