

Detectie-engine identificeren in beveiligde endpointconsole

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

Inleiding

In dit document wordt beschreven hoe u de engine kunt identificeren die verantwoordelijk is voor een specifieke detectie in de Secure Endpoint-console.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Endpoint-console

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Endpoint console v5.4.2025030619

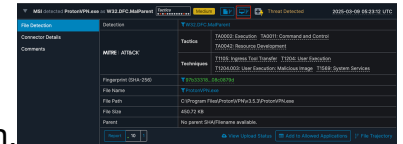
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

Het identificeren van de juiste motor die verantwoordelijk is voor een specifieke detectie is een van de eerste stappen om de aard van de gebeurtenis te begrijpen en deze effectief te testen.

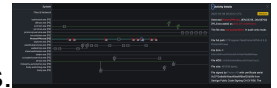
Oplossing

1. Ga naar de pagina Evenementen in uw AMP-console om de gebeurtenis te vinden die u verder wilt onderzoeken.



2. Klik op het gemarkeerde pictogram om Apparaattraject te openen.

Pictogram voor apparaattraject



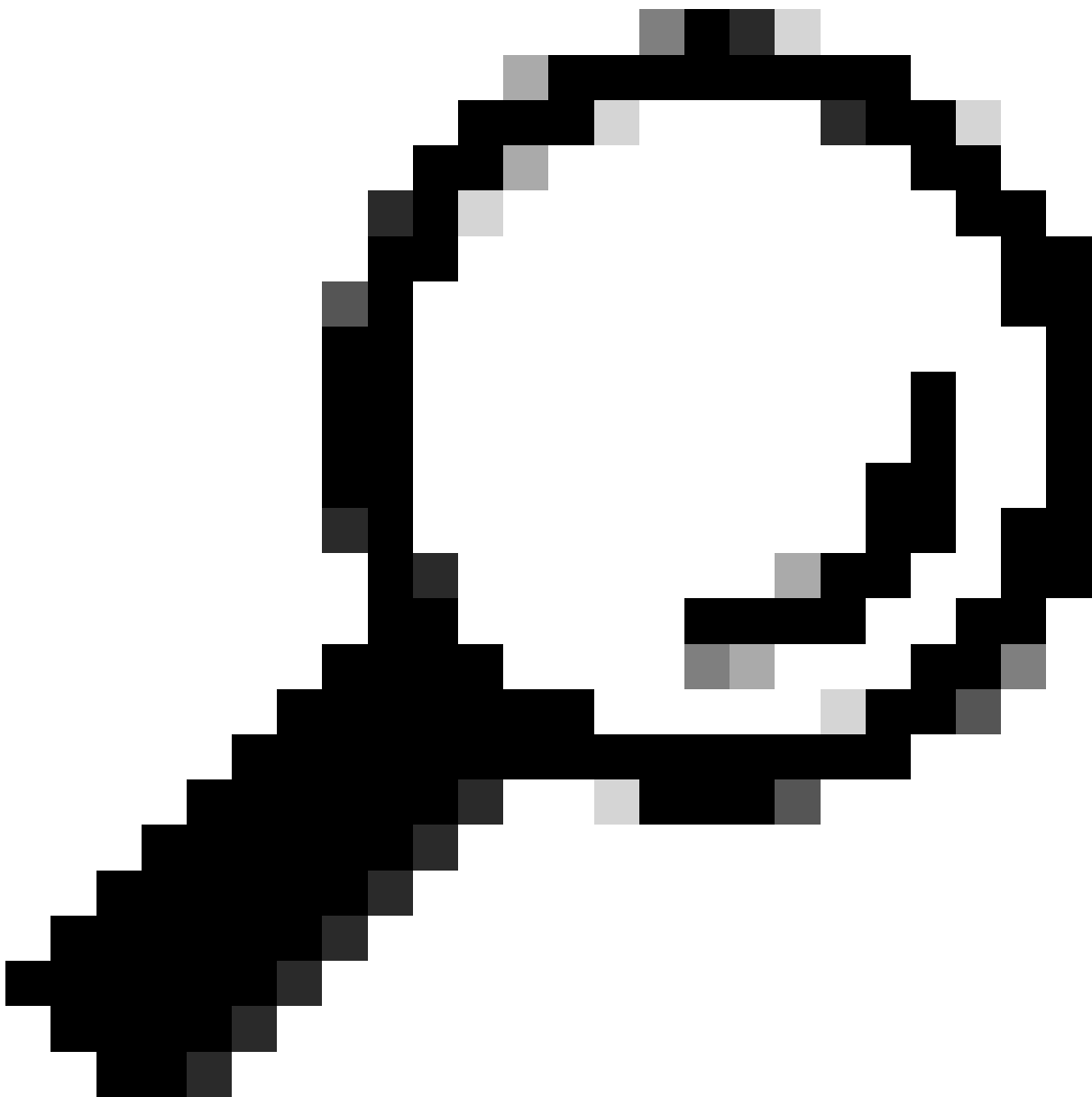
3. U kunt de gebeurtenisgegevens rechts bekijken onder Activiteitsgegevens.

Gebeurtenisgegevens in apparaattraject



4. Blader naar de onderkant om de sectie Gedetecteerd te vinden.

Gedetecteerd per sectie



Tip: Het begrijpen van deze informatie is essentieel om de aard van de bedreiging te beoordelen en snel de aangewezen uitsluiting te bepalen om te vormen. Bovendien kan het verstrekken van deze details wanneer het voorleggen van een zaak aan TAC voor Vals Positief onderzoek helpen het proces versnellen.

Als u het gedeelte Gedetecteerd op niet kunt bekijken of als u verdere assistentie nodig hebt, neemt u contact op met TAC.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.