[Extern] - Werken met Advanced Malware Protection (AMP) voor detectie van fouten, uitbraken en respons bij incidenten

Inhoud

Inleiding

We streven er altijd naar de bedreigingsintelligentie voor onze Advanced Malware Protection (AMP)-technologie te verbeteren en uit te breiden, maar als uw AMP-oplossing niet automatisch een waarschuwing oproept of een waarschuwing afgeeft, kunt u bepaalde acties ondernemen om verdere impact op uw omgeving te voorkomen. Dit document bevat een richtsnoer voor deze actiepunten.

Beschrijving

Onmiddellijke acties

Als u van mening bent dat uw AMP-oplossing uw netwerk niet tegen een bedreiging heeft beschermd, neem dan onmiddellijk de volgende maatregelen:

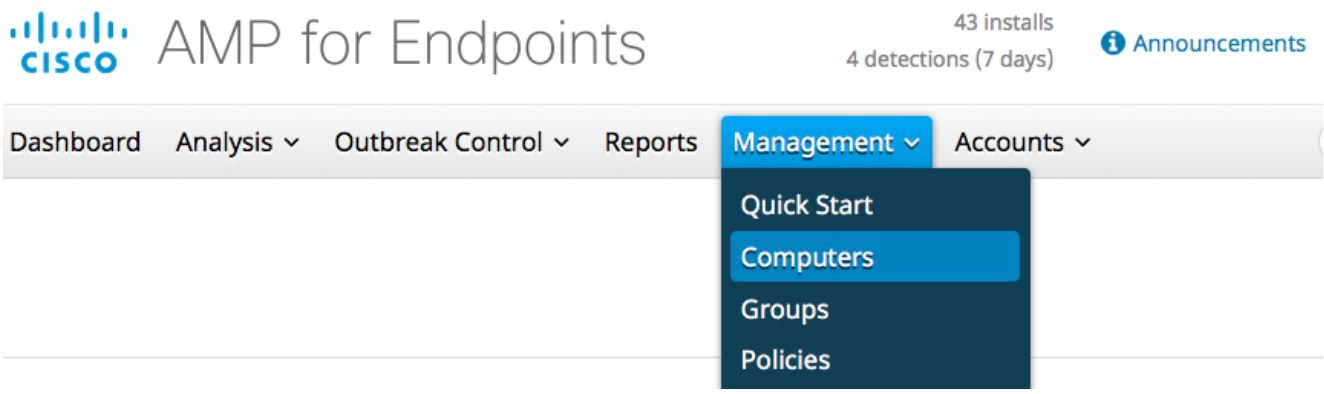
1. Isoleer de verdachte machines van de rest van het netwerk. Dit zou kunnen zijn het apparaat uitzetten of het fysiek loskoppelen van het netwerk.
2. Schrijf de belangrijke informatie over de infectie op, zoals het tijdstip waarop de machine kan worden geïnfecteerd, de gebruikersactiviteiten op de verdachte machines, enz.

   Waarschuwing: haal de machine niet uit of herafbeelding. Het maakt de kans overbodig om de beledigende software of bestanden tijdens het forensisch onderzoek of het oplossen van problemen te vinden.

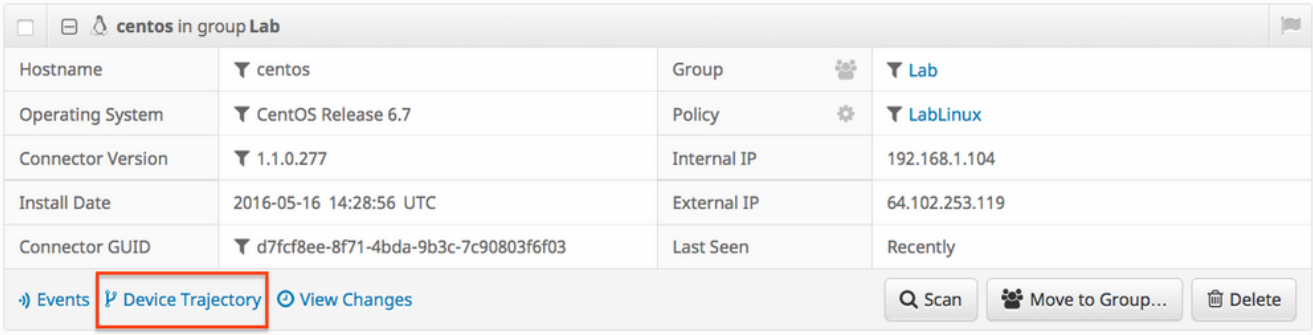
Analyse

1. Gebruik de optie **Apparaattraject** om met uw eigen onderzoek te beginnen. Apparaattraject kan ongeveer de 9 miljoen meest recente bestandsgebeurtenissen opslaan. Het traject van de AMP voor Endpoints is zeer nuttig voor het opsporen van bestanden of processen die tot een infectie hebben geleid.

Schuif in het dashboard naar **Management > Computers**.



Vind de verdachte machine en breid het record voor die machine uit. Klik op de optie **Apparaattraject**.



2. Als u een verdacht bestand of hangend bestand vindt, voegt u dit toe aan de aangepaste detectielijsten. AMP for Endpoints kan een aangepaste detectielijst gebruiken om een bestand of een handig hash als kwaadaardig te behandelen. Dit is een goede manier om te zorgen voor een zo groot mogelijke dekking om verdere impact te voorkomen.

Analyse door Cisco

1. Verwante monsters voor dynamische analyse voorleggen. U kunt deze handmatig indienen bij **Analyse > File Analysis** in het dashboard. AMP voor Endpoints omvat dynamische analysefunctionaliteit die een rapport van het gedrag van het bestand uit Threat Grid genereert. Dit heeft ook het voordeel het bestand aan Cisco te leveren als er extra analyse door ons onderzoeksteam nodig is.

2. Als u een *valse positieve* of *valse negatieve* detectie in uw netwerk vermoedt, adviseren wij u om gebruik te maken van zwarte lijst of witte lijstfunctionaliteit voor uw AMP producten. Wanneer u contact opneemt met Cisco Technical Assistance Center (TAC), geef dan de volgende informatie voor analyse:De SHA256 hash van het bestand.Zo mogelijk een kopie van het bestand.Informatie over het bestand, zoals waar het vandaan komt en waarom het in de omgeving moet zijn.Leg uit waarom dit volgens u een fout-positief of fout-negatief is.
3. Als u hulp nodig hebt bij het beperken van een dreiging of het uitvoeren van een triage van uw omgeving, zult u het Cisco Talos Incident Response-team (CTIR) moeten inschakelen die zich specialiseren in het maken van actieplannen, het onderzoeken van besmette machines en het inzetten van geavanceerde gereedschappen of functies om een actieve uitbraak te verzachten.
   Opmerking: Het Cisco Technical Assistance Center (TAC) biedt geen ondersteuning voor dit type betrokkenheid.U kunt hier contact met het CTIR opnemen. Dit is een betaalde service

die start op $60.000, tenzij uw organisatie een klant heeft voor de service voor incidentele reacties van Cisco. Als zij zich daarna engageren, zullen ze aanvullende informatie over hun diensten verstrekken en een zaak voor uw incident openen. We raden ook aan om uw Cisco-accountmanager te volgen, zodat ze extra instructies voor het proces kunnen geven.

Verwante artikelen

- Verzameling van diagnostische gegevens van een FirePOWER-connector die op Windows actief is
- Bestandstypen die zijn gescand met FirePOWER-connector