Beoordeel of betwist IPS Valse Positieven met Paraplu

Inhoud

Inleiding

In dit document wordt beschreven hoe u met Cisco Umbrella Intrusion Prevention Service (IPS) false positives kunt beoordelen of betwisten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

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.

Overzicht

Cisco Umbrella's Intrusion Prevention System detecteert (en blokkeert optioneel) pakketten die worden geacht te zijn geassocieerd met een bekende bedreiging, kwetsbaarheid, maar ook

gewoon wanneer het formaat van het pakket ongebruikelijk is.

Beheerders kiezen welke IPS-handtekeningenlijst wordt gebruikt om bedreigingen te detecteren op basis van deze standaardlijsten:

- Connectiviteit boven beveiliging
- Evenwichtige beveiliging en connectiviteit
- Beveiliging boven connectiviteit
- Maximale detectie

Het is belangrijk om te onthouden dat de gekozen handtekeningenlijst een grote invloed kan hebben op het aantal IPS false positives dat wordt aangetroffen. Van de veiligste modi (zoals Maximale detectie en beveiliging via connectiviteit) wordt verwacht dat ze ongewenste IPS-detecties creëren omdat ze de nadruk leggen op beveiliging. De veiligste modi worden alleen aanbevolen wanneer totale beveiliging vereist is en de beheerder moet anticiperen op de noodzaak om grote aantallen IPS-gebeurtenissen te bewaken en te controleren.

Zie de IPS-documentatie voor meer informatie over de verschillende modi.

IPS-detecties bekijken

Gebruik de Activiteit zoeken op het Umbrella Dashboard om IPS-evenementen te bekijken. Voor elk evenement zijn er twee belangrijke informatie:

- IPS-handtekening-ID/categorie/naam. Zoeken op https://snort.org
- CVE-nummer (indien van toepassing). Zoeken op https://www.cve.org/

Niet alle IPS-detecties wijzen op een bekende exploit/aanval. Veel van de handtekeningen (met name in de Max Detection-modus) geven eenvoudig de aanwezigheid van een bepaald type verkeer of een protocolschending aan. Het is belangrijk om de eerder genoemde informatiebronnen te bekijken, samen met andere details over het evenement (zoals bron / bestemming) om te bepalen of het evenement verder onderzoek van uw beveiligingsteam vereist.

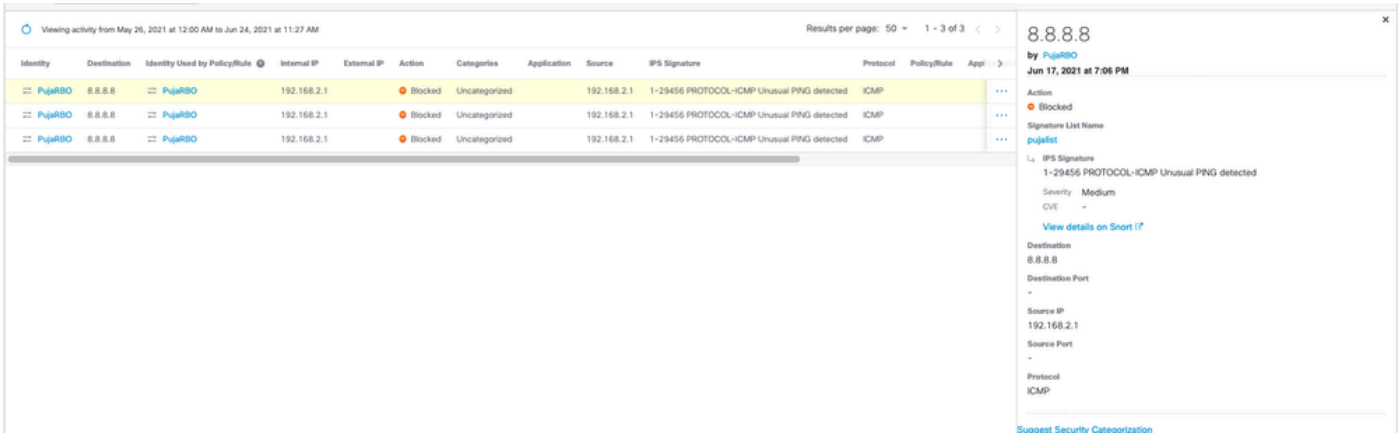
De handtekeningcategorie kan nuttig zijn om extra context te bieden over het type IPS-detectie. Bekijk de rubrieken op snort.org.

Protocolschendingen

In dit voorbeeld is een IPS Event gekoppeld aan deze handtekening: https://www.snort.org/rule_docs/1-29456

De beschrijving van de handtekening is:

"De regel zoekt naar PING-verkeer dat het netwerk binnenkomt en niet het normale formaat van een PING volgt."



4403885889428

In dit geval detecteert de Snort-regel niet noodzakelijkerwijs een bepaalde exploit, maar detecteert in plaats daarvan een misvormd ICMP-pakket dat is geblokkeerd. Op basis van de informatie die beschikbaar is op snort.org en andere details over het evenement (zoals bron/bestemming), kan de beheerder besluiten dat deze gebeurtenis geen verder onderzoek vereist

Compatibiliteit van toepassingen

Sommige legitieme toepassingen zijn niet compatibel met IPS-handtekeningen, met name wanneer de agressievere (Max Detection) modi zijn geconfigureerd. In deze scenario's kan de toepassing worden geblokkeerd om redenen die worden besproken in de sectie Protocolschending. De applicatie kan een protocol op een onverwachte manier gebruiken, of een aangepast protocol gebruiken over een poort die normaal is gereserveerd voor ander verkeer.

Hoewel de toepassing legitiem is, zijn deze detecties vaak geldig en kunnen ze niet altijd door Cisco worden gecorrigeerd.

Als een legitieme toepassing wordt geblokkeerd door IPS, raadt Umbrella aan contact op te nemen met de leverancier van de toepassing met details van het evenement / de handtekening. Toepassingen van derden moeten worden getest op compatibiliteit met de IPS-handtekeningen op snort.org.

Het is momenteel niet mogelijk om een individuele toepassing/bestemming uit te sluiten van IPS-scanning.

IPS-handtekeningen uitschakelen

Als blijkt dat een handtekening compatibiliteitsproblemen veroorzaakt met een toepassing van een derde partij, kan de handtekening tijdelijk of permanent worden uitgeschakeld. Dit mag alleen worden gedaan als u de toepassing vertrouwt en hebt vastgesteld dat de waarde van de toepassing opweegt tegen de beveiligingsvoordelen van de specifieke handtekening.

Voer de stappen uit in de documentatie Een aangepaste handtekeningenlijst toevoegen voor informatie over het maken van een aangepaste handtekeningenlijst. U kunt uw huidige instellingen als sjabloon gebruiken en vervolgens de gewenste regels uitschakelen door ze in te stellen op

Alleen loggen of Negeren.

steunen

Historische gebeurtenissen

Umbrella Support kan geen aanvullende informatie over historische IPS-evenementen verstrekken. IPS Events laat u weten dat het verkeer niet overeenkwam met de IPS-handtekening. De details van de ondertekening zijn openbaar beschikbaar op snort.org. Umbrella slaat geen kopie van onbewerkt verkeer/pakketten op en kan daarom geen verdere context of bevestiging geven over de aard van een IPS-evenement.

IPS-problemen / fout-positieven

Als u een actueel IPS-probleem wilt betwisten (zoals een fout-positief), kunt u contact opnemen met Umbrella Support.

Om deze problemen te onderzoeken, is een pakketopname vereist door Umbrella Support. De ruwe inhoud van pakketten is nodig om te bepalen hoe het verkeer de IPS-detectie heeft geactiveerd. U moet het probleem kunnen repliceren om de pakketopname te genereren.

Voordat u een ticket verhoogt, gebruikt u een tool zoals Wireshark om de pakketopname te genereren bij het repliceren van het probleem. Instructies zijn beschikbaar in onze kennisbank.

Als alternatief kan Umbrella Support helpen bij het genereren van de pakketopname. Ze moeten een tijdstip plannen waarop het probleem met de betreffende gebruiker of toepassing opnieuw kan worden gemaakt.

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.