Managed Access Feed og Managed Threat Feed

Managed Access Feed og Managed Threat Feed er dynamiske lister som kan brukes til å blokkere (blacklist) eller tillate (whitelist) trafikk til og fra deres organisasjon. Managed **Threat Feed** er basert på en strøm av kontinuerlige indikatorer (IP-adresser, URLs og domener) som er relatert til mulige eller eksisterende trusler for en organisasjons sikkerhet. **Managed Threat Feed** brukes til å blokkere trafikk til og fra kjente dårlige kilder.

Managed Access Feed består av en gruppe IP-adresser, URLer og domener som brukes til å tillate (whitelist) trafikk til og fra klarerte store Internett-tjenester som Microsoft Azure og Amazon Web Services, noe som passert perfekt i en Zero Trust modell.

INTELLISEC

Managed Threat Feed

Med tjenesten **Manged Treat Feed** vil deres organisasjon få tilgang til store mengder indikatorer (IP-adresser, URLer og domener) som brukes av kjente trusselaktører eller trusselkampanjer. Deres organisasjon vil bli holdt oppdatert på det siste innen trusseletterretning frembrakt av sikkerhetseksperter og kunstig intelligens (AI) fra hele verden.

For deg som kunde vil tjenesten bestå av følgende elementer:

Kontinuerlig sikkerhet
Indikatorene vil automatisk oppdateres ved bruk av trusseletterretnings-databaser, hvor disse inneholder alt som er blitt oppdaget de siste 24 timene. Dette fjerner all manuell interaksjon når det gjelder å legge til eller fjerne IP-adresser fra blokkerte IP-adresser og i brannmur regelsett. Managed Threat Feed bruker datakilder som innhenter trusselinformasjon fra flere store sikkerhetstilbydere fra hele verden.

APT fokusert
Listen som benyttes har spesielt søkelys på Advanced Persistent Threats (ATP), som vanligvis er en trusselaktør som en stat eller statsponset gruppe, med konkrete mål som å stjele, spionere eller sabotere. I tillegg er det også lister som omhandler Tor exit-nodes, noe som ofte er brukt i typiske Cyber-angrep.

Forenklet levering
Managed Threat Feed listene er gjort tilgjengelig som vanlig .txt filer, som kan lastes ned fra Intellisec.io. På denne måten kan deres organisasjon benytte listen på et bredt utvalg av sikkerhetsprodukter, som brannmur, Intrusion Detection og/eller Prevention Systems som har støtte for nedlasting av eksterne dynamiske lister. For enkelhets skyld tilbyr Intellisec «how-to» konfigurasjonsguider for et stort antall sikkerhetsprodukter.

Ved kjøp av tjenesten Maganged Firewall vil Managed Threat Feed automatisk bli oppdatert via denne tjenesten.

Managed Access Feed

Managed Access Feed forenkler prosessen ved å tillate trafikk til og fra de store Internett-tjenestene som Microsoft Office 365, Microsoft Azure og Amazon Web Services. Disse tjenestene benytter seg ofte av store serier med IP-adresser og domener, noe som kan gjøre dette uoversiktlig. Managed Access Feed kan for eksempel brukes til å håndtere inngående og utgående trafikk til slike tjenester.

Zero Trust policy
Managed Access Feed tjenesten passer perfekt i en Zero Trust orientert modell, hvor man ønsker å tillate trafikk (whitelist) som kommer og går i ditt nettverk. Ved å bruke API'er fra de ulike tjenesteleverandørene vil Managed Access Feed holde oversikt over alle IP-adresser og domener som til enhver tid blir brukt av de ulike tjenesteleverandørene. På denne måten kan deres organisasjon opprettholde ZeroTrust prinsipper uten at man manuelt må følge med på alle IP-adresser og domener som disse tjenestene benytter.

Forenklet levering
Managed Access Feed listene er gjort tilgjengelig som vanlig .txt filer, som kan lastes ned fra Intellisec.io. På denne måten kan listen benyttes på et bredt utvalg av sikkerhetsprodukter, som brannmur, Intrusion Detection og/eller Prevention Systems som har støtte for nedlasting av eksterne dynamiske lister. For enkelhets skyld tilbyr Intellisec «how-to» konfigurasjonsguider for et stort antall sikkerhetsprodukter

Ved kjøp av tjenesten Maganged Firewall vil Managed Access Feed automatisk bli oppdatert via denne tjenesten.