ANALYSE NETWERKVERKEER

INZICHT IN UW NETWERKVERKEER

Een analyse op het verkeer van de firewall en/of het netwerk is het proces van het monitoren en analyseren van inkomend en uitgaand netwerkverkeer om potentiële beveiligingsrisico's en aanvallen te identificeren. We helpen bij het opsporen van afwijkend gedrag, kwetsbaarheden en bedreigingen, zodat gerichte maatregelen kunnen worden genomen om de beveiliging te verbeteren.

WAAROM EEN ANALYSE OP HET NETWERKVERKEER?

Een analyse van het netwerkverkeer op de firewall is cruciaal omdat de firewall fungeert als de eerste verdedigingslinie tegen cyberdreigingen. Het biedt inzicht in wat er het netwerk binnenkomt en verlaat, waardoor verdachte activiteiten, ongeautoriseerde toegangspogingen en kwetsbaarheden tijdig worden opgespoord. Door deze analyse kunnen organisaties gerichte maatregelen nemen om beveiligingslekken te dichten, ongewenst verkeer te blokkeren en de algemene netwerkbeveiliging te versterken.

Daarnaast helpt het bij het identificeren van inefficiënties in regels en draagt het bij aan compliance met wet- en regelgeving. Het zorgt zo voor een veiliger en efficiënter netwerk.

WAT DOEN WE?

BIJ HET UITVOEREN VAN EEN ANALYSE VAN HET NETWERKVERKEER NEMEN WE DE VOLGENDE STAPPEN:

Verzamelen van netwerkdata
We plaatsen apparatuur bij de firewall om gedetailleerd netwerkverkeer vast te leggen, inclusief inkomend en uitgaand verkeer, en zorgen ervoor dat alle relevante logs beschikbaar zijn voor analyse. Indien gewenst plaatsen we ook apparatuur binnen het netwerk om over verschillende segmenten te kunnen meten.

Bepalen van baseline
We stellen een normale verkeersbaseline vast om te begrijpen wat typisch is voor het netwerkverkeer, zodat afwijkingen snel geïdentificeerd kunnen worden.

Analyse van verkeer
We analyseren het verzamelde netwerkverkeer, op zoek naar verdachte of ongeautoriseerde toegangspogingen en ongebruikelijke verbindingen.

Identificeren van risico's
We beoordelen de bevindingen om potentiële risico's, kwetsbaarheden en misconfiguraties te identificeren die de netwerkbeveiliging kunnen compromitteren.

Rapporteren en aanbevelen
We rapporteren onze bevindingen en doen aanbevelingen voor het verbeteren van de configuraties en het netwerkverkeerbeheer.

DE DRIE GROOTSTE VOORDELEN VAN EEN NETWERKVERKEER ANALYSE

Vroegtijdige detectie van bedreigingen
Identificeert verdachte activiteiten en ongeautoriseerd verkeer.

Optimalisatie van firewallregels
Helpt bij het opsporen van inefficiënte of onjuiste configuraties, wat leidt tot een betere netwerkprestaties en beveiliging.

Versterking van netwerkbeveiliging
Biedt inzicht in kwetsbaarheden, waardoor gerichte maatregelen genomen kunnen worden om het netwerk beter te beschermen.