Kaspersky Network Security-feeds met dreigings-gegevens

kaspersky bring on the future

Alleen endpoint-bescherming is niet voldoende.

Bescherming opnetwerkniveau is ook noodzakelijk.

Dit is waarom:

- Bescherming tegen verschillende soorten aanvallen moet bestaan uit meerdere lagen
- Niet alle hosts in je omgeving hebben endpointbescherming, bijvoorbeeld bedrijfskritieke servers en hosts in een industrieel netwerk
- Sommige 'beschermde' hosts zijn mogelijk niet bijgewerkt met handtekeningen/hashes/detectieregels

Kaspersky Network Security-feeds met dreigingsgegevens

Bijna elk bedrijf heeft tegenwoordig een Next-Generation Firewall (NGFW). Firewall is een van de meest effectieve moderne netwerkbeveiligingscontroles en verhoogt het beschermingsniveau van bedrijfsnetwerken tegen cyberaanvallen.

Het merendeel van NGFW's is niet alleen in staat om interne kennis over cyberdreigingen te gebruiken, maar biedt ook functies waarmee je dynamische lijsten van IoC's (indicators of compromise) kunt gebruiken van externe bronnen. Zo kun je cyberdreigingen in realtime blokkeren

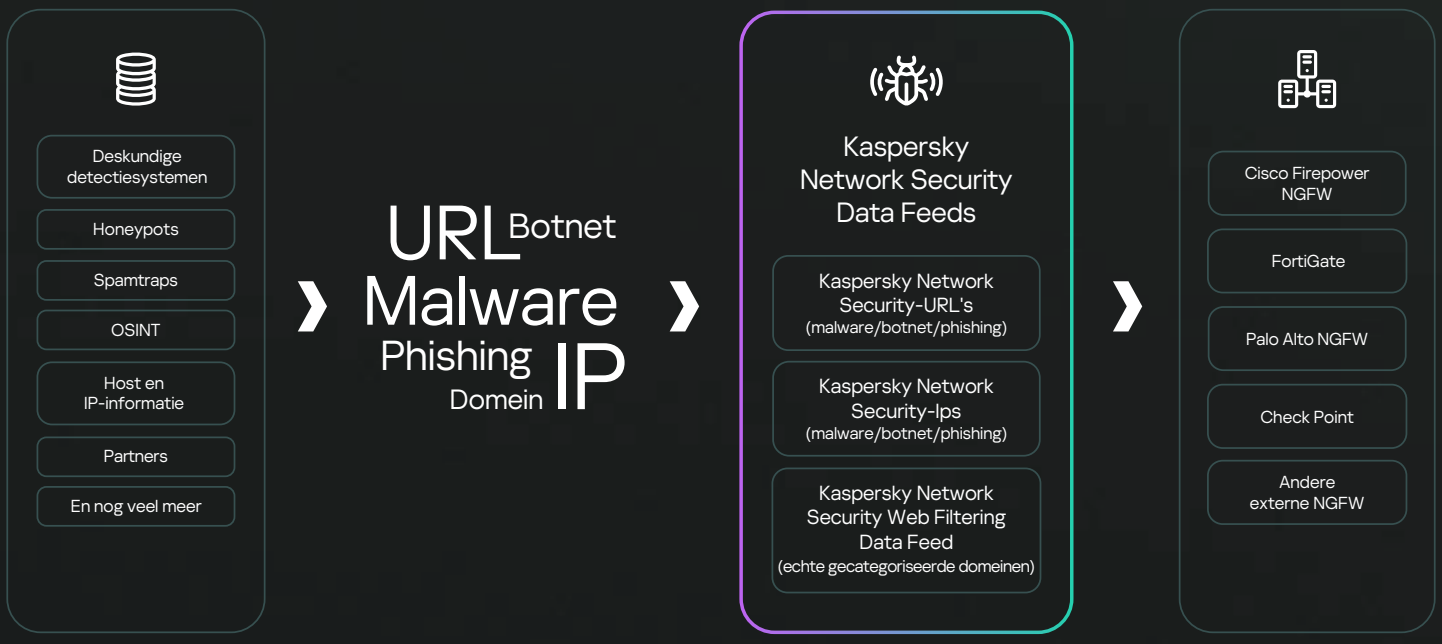
Het is bijna onmogelijk om detectieregels van NGFW's snel te configureren om aanvallen altijd voor te blijven. Daarom is externe bedreigingsinformatie essentieel. Deze zorgt voor een essentieel extra element van bescherming voor je omgeving, dat normaliter zou ontbreken.

Kaspersky biedt speciaal gemaakte verzamelingen van IoC's die, wanneer ze worden geïmporteerd in een NGFW, het beveiligingsniveau van een bedrijfsnetwerk aanzienlijk verbeteren. Ze beschermen het netwerk tegen de meest voorkomende dreigingen, zonder ingewikkelde integratie of configuratie en ze behouden de huidige netwerktopologie.

Kaspersky Network Security-feeds met dreigingsgegevens zijn gebaseerd op Kaspersky Threat Intelligence-feeds met gegevens en bevatten lijsten van verschillende soorten IoC's, zoals IP-adressen en domeinen. Deze lijsten worden regelmatig bijgewerkt. Door deze gegevens te gebruiken, kun je de gebruikerstoegang tot gevaarlijke netwerkbronnen monitoren of blokkeren.

Meer informatie

Integraties van Kaspersky Network Security-feeds met gegevens



Verzameling en verwerking van gegevens

Kaspersky Network Security-feeds met gegevens zijn samengesteld uit meerdere lijsten. Elke lijst is gericht op een specifieke soort cyberdreiging. De feeds bevatten lijsten met IP-adressen met de hoogste dreigingsscore, evenals domeinen van bronnen van het eerste en tweede niveau waarvan bekend is dat ze malware verspreiden, dienstdoen als controle- en uitvoercenters van botnets (C&C) of phishingbronnen hosten.

Feeds met gegevens worden samengesteld uit gecombineerde, heterogene en uiterst betrouwbare bronnen, zoals Kaspersky Security Network en onze eigen webcrawlers, Botnet Monitoring Service (een platform dat 24 uur per dag, 7 dagen per week, 365 dagen per jaar toezicht houdt op botnets en hun doelen en activiteiten) en host- en IP-informatieservices.

Alle samengevoegde gegevens worden zorgvuldig in realtime geïnspecteerd en verfijnd met meerdere voorverwerkingstechnieken, waaronder statische criteria, sandboxes, heuristische engines, gelijkenistools, gedragsprofilering, validering van analisten en verificatiemiddelen voor allowlisting.

Voordelen

Updates in realtime

Feeds met gegevens worden automatisch in realtime gegenereerd op basis van wereldwijde bevindingen, waardoor ze voor hoge detectiepercentages en nauwkeurigheid zorgen.

Het Kaspersky Security Network biedt zichtbaarheid voor een aanzienlijk deel van het internetverkeer en beschermt tientallen miljoenen eindgebruikers in meer dan 213 landen

Eigen ondersteuning

Eigen ondersteuning voor de meest populaire NGFW's:

- Cisco
- FortiGate
- Palo Alto
- Andere externe NGFW's (met functionaliteit van externe dynamische lijsten met basis authenticatieondersteuning)

Beveiligde authenticatie

Feeds met gegevens bieden een reeks authenticatiemethoden die voldoen aan verschillende beveiligingsbehoeften en integratievoorkeuren

Eenvoudige integratie

De aanvullende stapsgewijze configuratiegidsen voor elke ondersteunde NGFW en de technische support van Kaspersky maken eenvoudige configuratie mogelijk en bieden directe waarde

Voortdurende beschikbaarheid

Alle feeds worden gegenereerd en bewaakt via een uiterst fouttolerante infrastructuur voor een continue beschikbaarheid

100% gekeurde gegevens

Feeds met gegevens die vol staan met false positives zijn schadelijk, omdat ze legitieme bronnen kunnen blokkeren.

Kaspersky Network Security-feeds met gegevens passen uitgebreide tests toe. De filters worden toegepast voordat de feeds worden vrijgegeven, waardoor ervoor wordt gezorgd dat er 100% gekeurde gegevens worden geleverd

Voordelen

Versterk de verdedigingsoplossingen van je netwerk

met IoC's die voortdurend worden bijgewerkt om de meest voorkomende cyberdreigingen te blokkeren

Voorkom de exfiltratie van gevoelige assets

en intellectueel eigendom van geïnfecteerde machines buiten je organisatie

Blokkeer cyberdreigingen snel zodat je

je organisatie kunt beschermen tegen cyberdreigingen en je bedrijfscontinuïteit kunt behouden

Kaspersky Threat Data Feeds

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture