Kaspersky Threat Data Feeds

kaspersky bring on the future

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

Er vinden elke dag cyberaanvallen plaats. Cyberdreigingen komen steeds vaker voor en worden in toenemende mate complexer. Ook weten ze zichzelf steeds beter te verhullen in een poging de beveiliging te omzeilen. Kwaadwillenden gebruiken ingewikkelde kill chains, campagnes en aangepaste tactieken, technieken en procedures (TTP's) om je bedrijf te verstoren of je klanten te benadelen. Voor een goede bescherming zijn duidelijk nieuwe methoden op basis van dreigingsinformatie nodig.

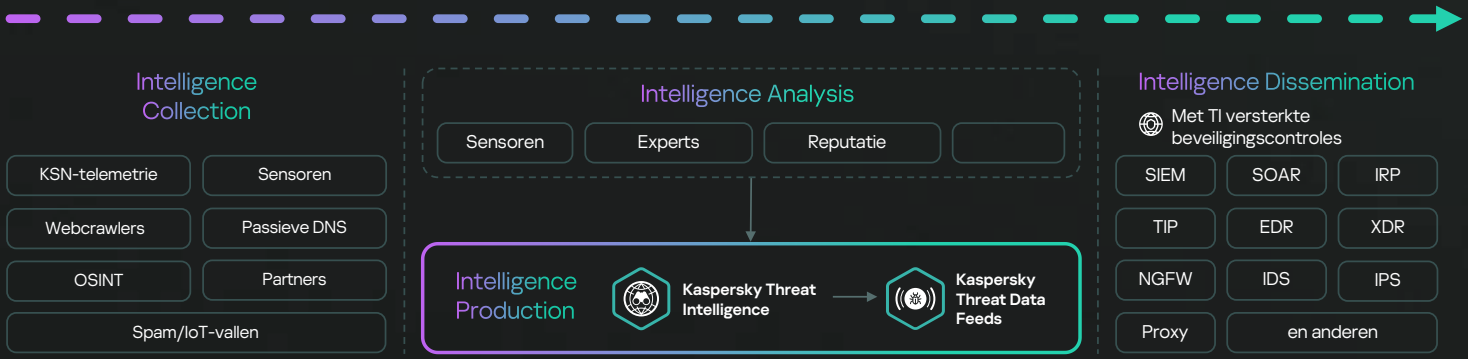
Door actuele feeds met dreigingsinformatie over verdachte en gevaarlijke IP's, URL's en bestandshashes te integreren in bestaande beveiligingssystemen zoals SIEM, SOAR en Threat IntelligencePlatforms, kunnen beveiligingsteams de initiële sortering van waarschuwingen automatiseren en hun triagespecialisten voldoende context geven. Zo kunnen ze onmiddellijk de waarschuwingen identificeren die moeten worden onderzocht of geëscaleerd naar teams voor incidentrespons voor verder onderzoek en verdere respons.

Contextuele gegevens

Vermeldingen in feeds van Kaspersky bevatten de volgende contextuele gegevens waarmee je dreigingen snel kunt bevestigen en prioriteren:

- Namen van dreigingen
- IP-adressen en domeinnamen van schadelijke webbronnen
- Hashes van schadelijke bestanden
- Kwetsbare en aangetaste objecten
- Tactieken, technieken en procedures van aanvallen volgens de classificatie MITRE ATT&CK
- Tijdstempels
- Geolocatie
- Populariteit, enzovoort

Hoe het werkt



Kaspersky Threat Data Feeds worden verzameld uit samengevoegde, heterogene en zeer betrouwbare Kaspersky-bronnen:

Kaspersky SecurityNetwork

Geavanceerde cloudinfrastructuur die anonieme cyberdreigingsgegevens van meer dan 400 miljoen vrijwillige deelnemers wereldwijd verzamelt en analyseert om de snelste respons op nieuwe dreigingen te bieden door gebruik te maken van grote gegevensanalyse, machine learning en menselijke expertise.

Webcrawlers

Verzamel nieuwe malware en legitieme exemplaren uit verschillende bronnen: OSINT, onderzoek door Kaspersky-analisten en onze eigen automatische verwerkings- en analysesystemen die URL's uit malware extraheren.

BotFarms

Het speciale botnetonderzoeksteam extraheert bot-configuraties, draait de communicatieprotocollen van engineers terug en monitort commando's vanuit commandocentra om waardevolle dreigingsinformatie te verkrijgen.

Spamtraps

Elk jaar voorkomen onze anti-phishingsystemen meer dan 500 miljoen keer dat er op een phishinglink wordt geklikt en meer dan 160 miljoen keer op schadelijke e-mailbijlagen, waaruit we extra gegevens kunnen halen om onze gegevensstromen te verrijken.

Partners

We nemen deel aan partnerschappen om schadelijke exemplaren met andere leveranciers en cyberbeveiligingsorganisaties te delen.

Sensoren

Honeypots, sinkholes en andere methoden van onderscheppende ITW-aanvallen. Bijvoorbeeld (waaronder IoT-apparaten, kwetsbare systemen, software, enz.). Kaspersky-analisten doen onderzoek naar aanvalspogingen en methoden van aanvallers, extraheren IoC's en koppelen ze aan andere gegevensbronnen.

Passieve DNS

De gegevens worden wereldwijd verzameld van vertrouwde externe partijen zoals gastorganisaties en ISP's.

OSINT

Aanvallersgegevens worden automatisch verzameld uit openbaar beschikbare bronnen zoals nieuwszenders, sociale media, openbare rapporten, dark web, etc. We gebruiken deze gegevens om naar nieuwe schadelijke exemplaren te zoeken die de infrastructuur van de aanvaller verkennen en voegen deze voortdurend toe aan onze kennisdatabase.

Elke gedetecteerde indicator ondergaat een screeningproces van meerdere fasen in een geautomatiseerd verwerkingssysteem dat gebruikmaakt van vertrouwens- en reputatietechnologieën en modellen op basis van machine learning die zijn getraind op exemplaren van honderden miljoenen daadwerkelijk vertrouwde en gevaarlijke bestanden om false positives eruit te filteren. Elke indicator wordt ook geanalyseerd in meerdere sandboxes, waarvan veel extra attributen zoals TTP's, netwerkgedrag, gedrag van het besturingssysteem en een host van andere relaties, worden geëxtraheerd.

Dit alles maakt Kaspersky Threat Intelligence een krachtige bron van tactische informatie die je bewakingscentra voor dreigingen kan versterken en aanvallers op de frontlinies van je organisatie kan detecteren.

Voordelen

Data Feeds worden automatisch, in realtime gegenereerd op basis van wereldwijde bevindingen voor hoge detectiepercentagesen nauwkeurigheid.

Eenvoudige implementatie is verzekerd door aanvullende documentatie, exemplaren, een eigen accountmanager en technische ondersteuning van Kaspersky. Dit allemaal samen maakt de integratie een eenvoudig proces.

Door eenvoudige, lichte disseminatie-indelingen (JSON, CSV, OpenIoC, STIX) via HTTP, TAXII of ad-hocleveringsmechanismen wordt de integratie van feeds in beveiligingsoplossingen zeer eenvoudig. Toonaangevende SIEM's en TI-platformen worden volledig ondersteund.

Data Feeds vol false positives zijn waardeloos. Er worden om die reden uitgebreide tests gedaan en filters toegepast voordat feeds worden vrijgegeven, zodat de gegevens 100% zijn gecontroleerd.

Honderden deskundigen, waaronder beveiligingsanalisten uit de hele wereld en gerenommeerde beveiligingsexperts uit ons GReAT- en R&D-team, dragen bij aan het genereren van deze feeds. Veiligheidsmedewerkers ontvangen kritische informatie en waarschuwingen die zijn gegenereerd uit gegevens van de hoogst mogelijkekwaliteit, zonder het risico te lopen overspoeld te worden door een overdaad aan indicatoren en waarschuwingen.

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

Voordelen

1

Verbeter de oplossingen om je netwerk te beschermen met onder andere SIEM's, firewalls, NGFW, IPS/IDS, beveiligingsproxy's, DNS-oplossingen en Anti-APT met continu bijgewerkte Indicators of Compromise (IoC's) en bruikbare context voor meer inzicht in cyberaanvallen en een beter begrip van de bedoeling, de mogelijkheden en de doelwitten van je tegenstanders.

2

Verbeter en versnel je incidentrespons en forensische capaciteit door het aanvankelijke triageproces te automatiseren en je beveiligingsanalisten voldoende context te geven om onmiddellijk de waarschuwingen te identificeren die moeten worden onderzocht of geëscaleerd naar teams voor incidentrespons voor verder onderzoek en verdere respons.

3

Voorkom de exfiltratie van gevoelige assets en intellectueel eigendom van geïnfecteerde computers buiten de organisatie. Detecteer snel geïnfecteerde assets om de reputatie van je merk te beschermen, de voorsprong op de concurrentie te behouden en zakelijke kansen veilig te stellen.

4

Als MSSP kun je je bedrijf laten groeien door toonaangevende informatieverzameling over bedreigingen als premium service aan te bieden aan klanten.

5

Als CERT kun je je cyberdreigingsdetectie en identificatiemogelijkheden verder verbeteren en uitbreiden.

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence biedt toegang tot een breed scala aan informatie die door onze analisten en onderzoekers van wereldklasse is verzameld. Met deze gegevens kan je organisatie de cyberdreigingen vandaag de dag effectief tegengaan.

Ons bedrijf heeft diepgaande kennis, ruimte ervaring op het gebied van onderzoek naar cyberdreigingen en unieke inzichten in alle aspecten van cyberbeveiliging die actuele, tactische, operationele en strategische dreigingsinformatie verschaffen.
Dit maakt ons een vertrouwde partner van wethandhavingsdiensten en overheidsdiensten over de hele wereld, waaronder Interpol en verschillende CERT-eenheden. En dit is allemaal beschikbaar als relevante, bruikbare gegevens via de Kaspersky Threat Intelligence Portal.

Kaspersky Threat Intelligence

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture