Ontdek hoe je jezelf kunt verdedigen tegen je vijanden en onthul het echte bedreigingslandschap van je organisatie

Bedreigingslandschap op Kaspersky Threat Intelligence Portal

kaspersky bring on the future

Kaspersky
Threat Intelligence
Portal

Bedreigingslandschap voor je organisatie op Kaspersky Threat Intelligence Portal

Het internationale bedreigingslandschap verandert voortdurend en iedere dag komen er nieuwe aanvalsmethoden bij. Ook worden bestaande methoden steeds geavanceerder. Het wordt tegenwoordig steeds belangrijker voor beveiligingsgegevensteams om effectief de bedreigingen te prioriteren waarop snel moet worden gereageerd. Maar hoe moet je je richten op de bedreigingen die het meest relevant zijn voor je bedrijf, sector en regio?

Kaspersky Threat Intelligence Portal

Gebruikers hebben de unieke kans om hun bedreigingslandschap te bekijken in de sectie Bedreigingslandschap. Deze is speciaal ontworpen om informatie te bieden over aanvallers die zich richten op een specifieke sector en regio. Hierbij worden detectietechnologieën met internationale bedreigingsintelligentie gecombineerd. Dit biedt complete en actuele context over bedreigingen die zijn gelinkt aan mogelijke vijanden, hun tactieken, technieken en procedures (TTP's).

Bedreigingslandschap biedt informatie over de bedreigingen die worden geassocieerd met:

- geografie
- sector
- soorten bedreigingen
- aanvallers
- hun technieken, tactieken en procedures (TTP's)
- schadelijke software die ze gebruiken
- relevante indicators of compromise (IoC's)

Bedreigingsinformatie wordt in realtime verzameld met behulp van verschillendegeavanceerde systemendie Kaspersky al meer dan 25 jaar gebruikt om cybercriminaliteit te bestrijden. Dit zijn het Kaspersky Security Network, dat anonieme gegevens ontvangt van miljoenen gebruikers wereldwijd, automatisch miljoenen bestanden per dag verwerkt, evenals webcrawlers, bot-farms, spamtraps, honeypots, sensoren, passieve DNS, bronnen en partners van het open- en dark web. We hebben deze gegevens de afgelopen 25 jaar zelf gebruikt, waardoor we de hoogste scores krijgen bij onafhankelijke tests en externe beoordelingen. De verkregen gegevens worden zorgvuldig geanalyseerd door de bedreigingsonderzoeksteams van Kaspersky en worden verwerkt door moderne geautomatiseerde systemen zoals sandboxes, heuristische engines en gelijkenistools. Dit zorgt voor gegarandeerd gecontroleerde en up-to-date informatie.

Meer informatie

Hoe het werkt

Kaspersky Threat Intelligence-bronnen

KSN-telemetrie | Sensoren | Webcrawlers | Bot-farms | Spam/IoT-vallen | Passieve DNS | Partners en OSINT

Analyseren | >400.000 dagelijkse exemplaren van schadelijke bestanden

Kaspersky Threat Intelligence Portal

Profielen van aanvallers

- Namen/aliassen
- Beschrijvingen
- Landen/sectoren
- TTP's
- Software/rapporten

Softwareprofielen

- Namen/aliassen
- Beschrijvingen
- Aanvallers
- TTP's
- SIGMA-regels

Kaspersky Threat Intelligence Reporting (APT, Crimeware, ICS)

- YARA-, SIGMA-, Suricata-regels
- TTP's
- IoC's

MITRE ATT&CK TTPs

Threat Landscape

Filters: Branches | Landen | Aanvallers | Platforms

MITRE ATT&CK-heatmap

Gedetailleerde beschrijvingen van TTP's op basis van de dagelijkse gegevensstroom van schadelijke exemplaren

Top 10 statistieken
- TTP's
- Kwetsbaarheden
- Aanvallers
- Software
- Branches

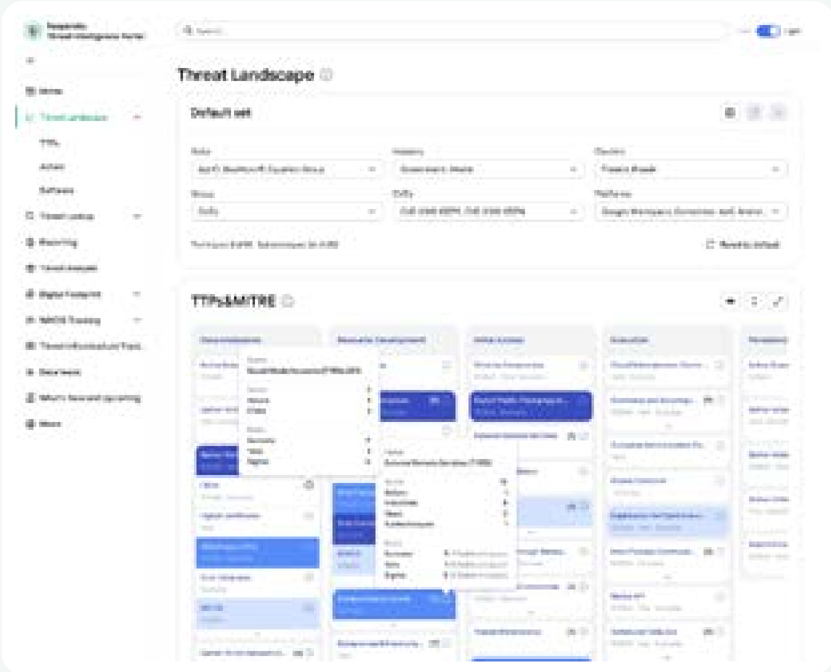
Risicobeperkingen

We verwerken dagelijks honderdduizenden exemplaren van schadelijke bestanden en extraheren de geolocatie en sectorgegevens. Vervolgens extraheren de interne systemen van Kaspersky de bijbehorende TTP's en wijzen de bestanden toe aan bestaande cybercriminele groepen en malware. De sectie Bedreigingslandschap is ook gebaseerd op een reeks echte incidenten van over de hele wereld, die we ontvangen van onze geavanceerde onderzoeksteams.

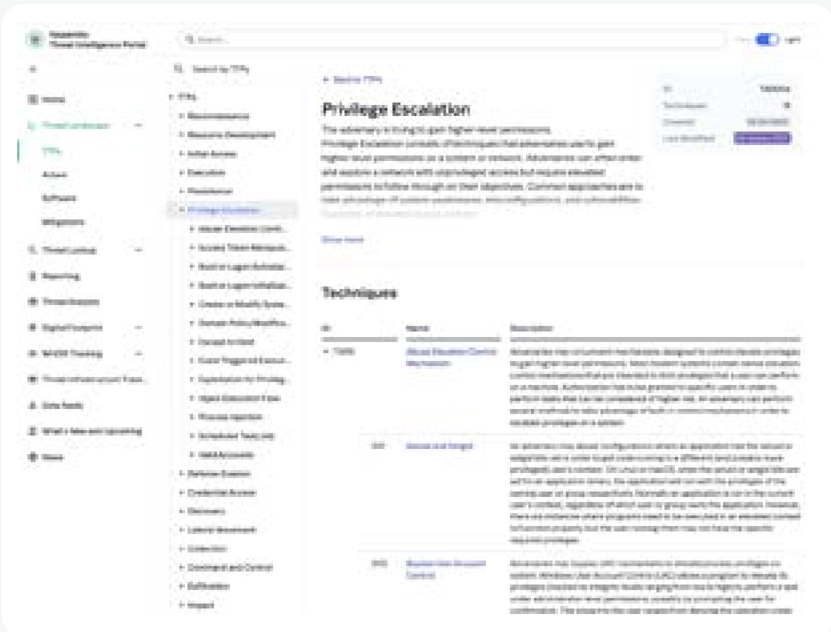
Gebruikers van het Kaspersky Threat Intelligence Portal kunnen filters toepassen en hun eigen bedreigingslandschap creëren in overeenstemming met de MITREATT&CK-structuur en de meest up-to-date gegevens verkrijgen over hun mogelijke vijanden. Hieronder vallen onder meer: technieken, tactieken en procedures die waarschijnlijk worden gebruikt voor een aanval, gedetailleerde beschrijvingen van actoren, de malware en TTP's die ze gebruiken, rapporten met gedetailleerde beschrijvingen van de aanvallen en beheersmaatregelen (specifieke aanbevelingen die kunnen worden gebruikt om te voorkomen dat een techniek wordt uitgevoerd).

Voordelen

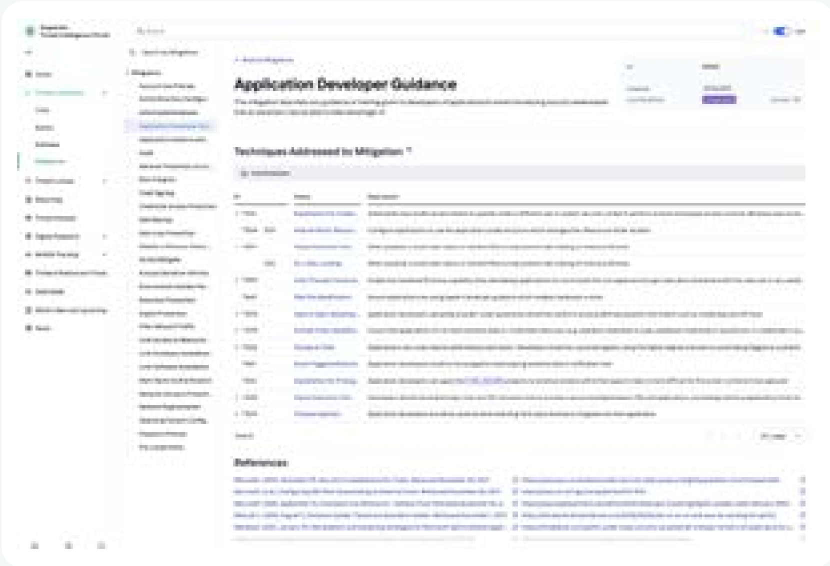
MITTRE ATT&CK-heatmap om in realtime een uniek bedreigingslandschap te ontwikkelen voor je organisatie. Door filters toe te passen, krijgt de gebruiker toegang tot de meest up-to-date gegevens, waaronder updates van de afgelopen 24 uur die worden verkregen door onze systemen en experts via voortdurend onderzoek. De mogelijkheid om lagen op te slaan voor internationale organisaties.



Live informatie in realtime over de technieken, tactieken en procedures van aanvallers op basis van de geavanceerde systemen van Kaspersky.

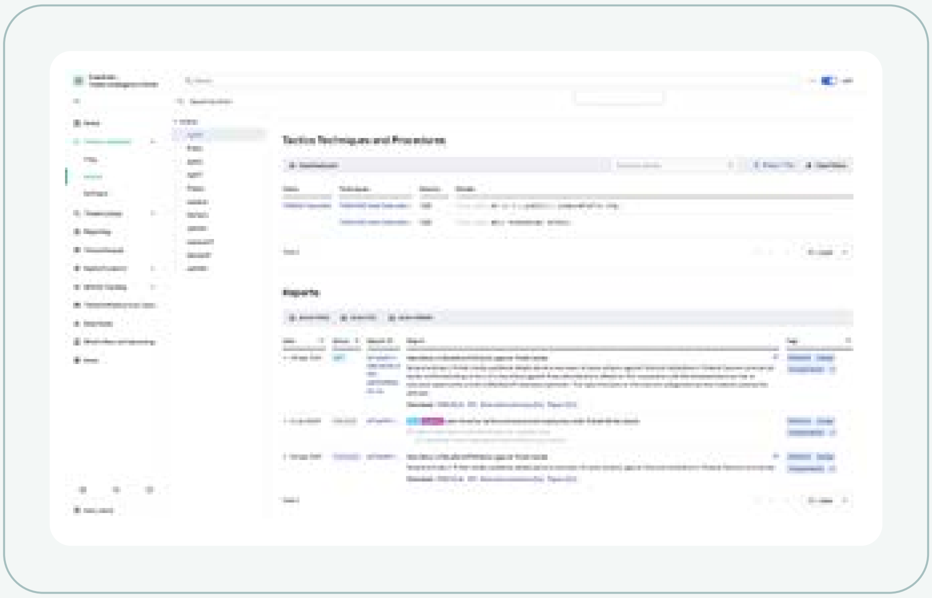


De sectie over beheersmaatregelen biedt gedetailleerde beschrijvingen van preventieve en beschermendemaatregelen voor organisaties om hiaten in de beveiliging te vermijden.

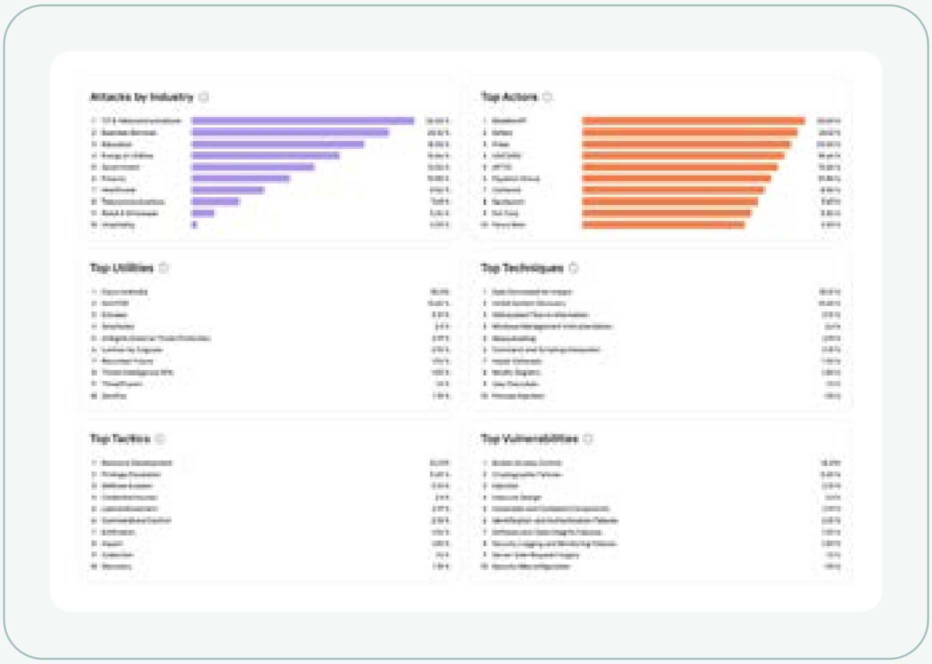


Toegang tot de meest uitgebreide respository van de sector met profielen van actoren en malware en met gedetailleerde beschrijvingen die zijn samengesteld door de experts van Kaspersky.

Toegang tot Sigma/Yara/ Suricata-regels die zijn gerelateerd aan de MITRE ATT&CK-technieken, tactieken en procedures om bedreigingen te detecteren die relevant zijn voor je organisatie.



De TOP 10 statistieken over de sectoren, actoren, TTP's, kwetsbaarheden en software.



De huidige, steeds veranderende wereld van cyberbedreigingen bevat een overvloed aan bedreigingsinformatie die beschikbaar is via een reeks producten en diensten. Als ze inzicht hebben in hun eigen bedreigingslandschap, kunnen organisaties strategische stappen nemen om zichzelf te verdedigen tegen relevante aanvallen.

Voordelen van gebruik

Proactieve verdedigingsaanpak

Krijg inzicht in de meest waarschijnlijke aanvalsvectoren om een effectieve verdedigingsstrategie te ontwikkelen

Controle van het aanvalsoppervlak

Identificeer beveiligingshiaten voordat aanvallers er misbruik van maken

Focus op relevante bedreigingen

De mogelijkheid om je te richten op de bedreigingen die het meest relevant zijn voor je bedrijf, sector en regio

Strategische planning

Gebruik informatie over het bedreigingslandschap om investeringen te plannen en tools/methoden voor bescherming te ontwikkelen

Verbeter de efficiëntie van de informatiebeveil-igingsafdelingen

Verhoog de efficiëntie van het personeel en verminder de personeelskosten door toegang tot informatie over relevante bedreigingen en internationale trends mogelijk te maken

Bedreigings bewustzijn

Informatie over de nieuwste bedreigingen en de bijbehorende internationale trends voor effectieve bescherming

Als je de vijand en jezelf kent, hoef je niet bang te zijn voor de resultaten van honderden aanvallen. Als je jezelf kent, maar niet je vijand: voor elke overwinning, lijd je verlies. Als je jezelf en je vijand niet kent, verlies je elke strijd

Sun Tzu

van The Art of War

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence biedt toegang tot een uitgebreide verzameling informatie die door onze analisten en onderzoekers van wereldklasse is verzameld. Met deze gegevens kan een organisatie de cyberbedreigingen van vandaag de dag effectief tegengaan.

Ons bedrijf heeft uitgebreide kennis en ervaring met cyberbedreigingsonderzoek en unieke inzichten in alle aspecten van cyberbeveiliging. Dit maakt Kaspersky een vertrouwde partner van wethandhavingsdiensten en overheidsdiensten over de hele wereld, waaronder Interpol en verschillende CERT-eenheden. Kaspersky Threat Intelligence biedt up-to-date tactische, operationele en strategische bedreigingsinformatie.

Kaspersky Threat Intelligence

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture