Blijf aanvallen een stap voor

Kaspersky Threat-Intelligence

kaspersky bring on the future

Kaspersky
Threat Intelligence

Kaspersky Threat Intelligence

Threat Intelligence van Kaspersky Lab geeft je toegang tot de informatie die je nodig hebt om cyberdreigingen te beperken. De informatie is afkomstig van ons toonaangevende team onderzoekers en analisten.

Dankzij onze kennis, ervaring en grondige informatieverzameling ten aanzien van elk aspect van cyberbeveiliging is Kaspersky uitgegroeid tot een vertrouwde partner van vooraanstaande wetshandhavings- en overheidsinstellingen wereldwijd, waaronder INTERPOL en de belangrijkste CERT's. Met Kaspersky Threat Intelligence krijg je direct toegang tot tactische, operationele en strategische dreigingsinformatie.

Kaspersky Threat Intelligence levert een uitgebreid overzicht van het wereldwijde dreigingslandschap met informatiebronnen, feeds met dreigingsgegevens en intern onderzoek. Dit wordt allemaal door ons team van experts geanalyseerd voor bruikbare inzichten om organisaties te helpen zich te beschermen tegen cyberdreigingen.

Tactisch

Zeer vergankelijke gegevens van een laag niveau die beveiligingsactiviteiten en incidentrespons ondersteunen. Een voorbeeld van strategische informatie zijn IoC's die zijn gerelateerd aan het uitvoeren van een recentelijk ontdekte aanval.

Functies:
- SOC-analist

Systemen:
- SIEM
- NGFW
- IPS
- IDS
- SOAR

Processen:
- Dreigingsopsporing
- Monitoring

Operationeel

Dit niveau bevat gewoonlijk gegevens van campagnes en bovenliggende TTP's. Het kan gegevens over de toewijzing van specifieke aanvallers bevatten, evenals mogelijkheden en opzettelijke aanvallen.

Functies:
- SOC L3-analist
- DFIR-analist
- IR-analist

Systemen:
- SIEM
- NTA
- EDR/XDR
- TIP

Processen:
- Afhandeling van incidenten
- Dreigingsopsporing

Strategic-

Met dit niveau worden leidinggevenden en bestuursleden in de hoogste regionen ondersteund bij het nemen van belangrijke beslissingen over risicobeoordelingen, het toewijzen van middelen en organisatorische strategieën. Deze informatie omvat trends, motieven van aanvallers en hun classificaties.

Functies:
- CISO
- CTO
- CIO
- Directeur

Processen:
- Een IS-strategie ontwikkelen
- Bewustzijn creëren

Schema van de applicatieKaspersky Threat Intelligence

Kaspersky Threat Intelligence maakt je sterker

Identificeer en voorkom dreigingen proactief

Met Kaspersky Threat Intelligence blijf je op de hoogte van de laatste dreigingen en kwetsbaarheden, waardoor je proactief maatregelen kan nemen om je systemen te beschermen voordat er een aanval plaatsvindt.

Krijg inzicht in je digitale voetafdruk

Kaspersky Threat Intelligence biedt een uitgebreid overzicht van je digitale voetafdruk, waaronder assets die mogelijk kwetsbaar zijn voor aanvallen of aantastingen.

Verbeter uw dreigingsdetectie

Kaspersky Threat Intelligence helpt je je bestaande beveiligingsoplossingen uit te breiden met de nieuwste dreigingsinformatie, waardoor je geavanceerde dreigingen beter kunt detecteren en tegengaan.

Verbeter je incidentrespons

Kaspersky Threat Intelligence geeft informatie in realtime over opkomende dreigingen en Indicators of Compromise (IoC's), waardoor je snel en effectief kan reageren op incidenten.

Voldoe aan regelgevingen en normen

Alle bedrijven zijn onderhevig aan verschillende regelgevingen en normen binnen hun sector. Kaspersky Threat Intelligence ondersteunt naleving door je te helpen aan deze vereisten te voldoen.

Verrijk je interne expertise

Het expertteam van Kaspersky valt onder de meest ervaren en gerespecteerde onderzoekers in de sector en het geeft je informatiebeveiligingsteams een overvloed aan kennis en expertise.

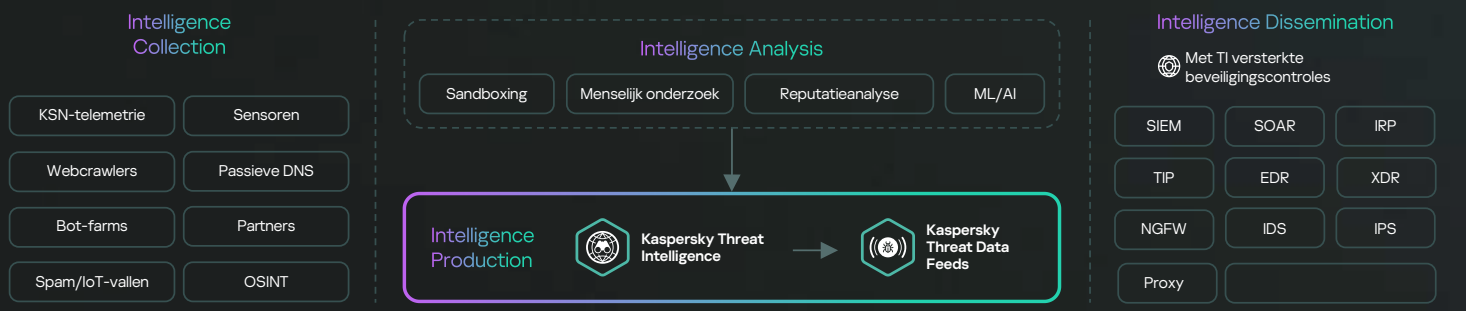
Kaspersky
Threat Data

Kaspersky Threat Data Feeds

Er vinden elke dag cyberaanvallen plaats. Cyberdreigingen komen steeds vaker voor en worden in toenemende mate complexer. Ook worden ze steeds beter verhuld in de pogingen om 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 effectieve bescherming zijn 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 Intelligence Platforms, 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.

Kaspersky Threat Data Feed geeft in realtime informatie over dreigingen om je te helpen je netwerken en systemen te beschermen tegen cyberdreigingen. Gegevensfeeds bevatten informatie over bekende malware, phishingwebsites, de laatste kwetsbaarheden en exploits en andere soorten cyberdreigingen. Deze informatie kan je helpen om gevaarlijk verkeer te blokkeren, je beveiligingssoftware bij te werken en andere maatregelen te nemen om je te beschermen tegen cyberaanvallen.



1

De gegevens worden verzameld uit een breed scala aan betrouwbare bronnen, waaronder Kaspersky Security Network en onze eigen crawlers, services voor het monitoren van botnetdreigingen (volgt botnets en hun doelwitten 24/7), spamtraps, gegevens van onderzoeksgroepen, partners en nog veel meer.

2

Alle informatie die is verzameld, wordt in real time zorgvuldig gecontroleerd en opgeschoond met verschillende methoden voor voorverwerking: sandboxen, statistische en heuristische analyse, tools voor gelijkenissen, gedragsprofilering en deskundige analyse.

3

Met gegevensfeeds kun je dreigingsinformatie over een waarschuwing of incident verzamelen en in details duiken. Het helpt ook antwoord te geven op de vragen "Wie? Wat? Waar? Waarom?" en de bron van een aanval te identificeren, waardoor je snel beslissingen kunt nemen om je bedrijf te beschermen tegen dreigingen, hoe complex dan ook.

Contextuele gegevens

Contextuele gegevens helpen bij het zichtbaar maken van het grotere geheel, wat het grootschalige gebruik van de gegevens verder valideert en ondersteunt. Vermeldingen in feeds van Kaspersky bevatten de volgende contextuele gegevens waarmee je dreigingen snel kunt bevestigen en prioriteren:

1. Namen van dreigingen
2. IP-adressen en domeinnamen van schadelijke webbronnen
3. Hashes van schadelijke bestanden
4. Kwetsbare en aangetaste objecten
5. Tactieken, technieken en procedures van aanvallen volgens de classificatie MITRE ATT&CK
6. Tijdstempels
7. Geolocatie
8. Populariteit, enzovoort

Voordelen van Kaspersky Threat Data Feeds

Verbeter en versnel je incidentrespons en forensische capaciteiten

door het aanvankelijke triageproces te automatiseren en je beveiligingsanalisten voldoende context te geven. Zo kunnen onmiddellijk de waarschuwingen worden geïdentificeerd die moeten worden onderzocht of geëscaleerd naar teams voor incidentrespons voor verder onderzoek en verdere respons.

Versterk je beveiligingsoplossingen

met onder andere SIEM's, firewalls, 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 aanvallers. Toonaangevende SIEM's (zoals ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) en TI-platformen worden volledig ondersteund.

Voorkom de exfiltratie van gevoelige assets en intellectueel eigendom

van geïnfecteerde apparaten naar buiten je 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.

Laat je zaken met MSSP groeien

door toonaangevende dreigingsinformatie als premium service aan je klanten te bieden. Als CERT kun je je cyberdreigingsdetectie en identificatiemogelijkheden verder verbeteren en uitbreiden.

Kaspersky CyberTrace

Kaspersky CyberTrace

Omdat het aantal feeds met dreigingsgegevens en het aantal bronnen voor dreigingsinformatie alsmaar groeit, is het lastig voor bedrijven om te bepalen welke informatie relevant is. Tegelijkertijd kan dreigingsinformatie veel verschillende indelingen hebben en omvat deze een groot aantal Indicators of Compromise (IoC's), waardoor SIEM's en andere netwerkbeveiligingsmechanismen de informatie moeilijk kunnen verwerken.

Door tot op de minuut nauwkeurige, door machines leesbare dreigingsinformatie te integreren in bestaande beveiligingsmechanismen, zoals SIEM-systemen, kunnen Security Operation Centers de aanvankelijke categorisering automatiseren. Tegelijk beschikken beveiligingsanalisten over voldoende context om onmiddellijk te bepalen welke meldingen moeten worden onderzocht of moeten worden geëscaleerd naar teams voor incidentrespons voor extra onderzoek en maatregelen.

Kaspersky CyberTrace is een platform met dreigingsinformatie dat feeds met dreigingsgegevens naadloos integreert met SIEM-oplossingen, zodat analisten dreigingsinformatie effectiever kunnen toepassen in hun bestaande beveiligingsworkflows. Het kan worden geïntegreerd met alle feeds met dreigingsinformatie (van Kaspersky, andere leveranciers, OSINT of je eigen klantenfeeds) in JSON-, STIX-, XML- of CSV-indeling en ondersteunt kant-en-klare integratie met allerlei SIEM-oplossingen en logboekbronnen.

Voordelen

Gedetailleerde informatie over elke indicator om een nog diepgaandere analyse te bieden. Op elke pagina staat alle informatie over een indicator, afkomstig van alle leveranciers van dreigingsinformatie (deduplicatie), zodat analisten dreigingen kunnen bespreken in de reacties en interne dreigingsinformatie over elke indicator kunnen toevoegen

Met statistieken over feedgebruik wordt de effectiviteit van de geïntegreerde feeds gemeten. In combinatie met een matrix voor feedintersectie helpen ze je om de waardevolste leveranciers van dreigingsinformatie te kiezen

IoC's taggen vereenvoudigt IoC-beheer. Maak een tag en geef het gewicht (belang) ervan op. Vervolgens kun je hiermee handmatig IoC's taggen. Je kunt IoC's ook sorteren en filteren op basis van deze tags en het bijbehorende gewicht

Met een onderzoeksgrafiek kun je gegevens en detecties die in CyberTrace zijn opgeslagen visueel verkennen en overeenkomsten tussen dreigingen ontdekken

Met de exporftunctie voor indicatoren kun je indicatorsets naar beveiligingsmechanismen zoals beleidslijsten (blokkeerlijsten) exporteren en dreigingsgegevens delen tussen Kaspersky CyberTrace-instanties of met andere TI-platformen

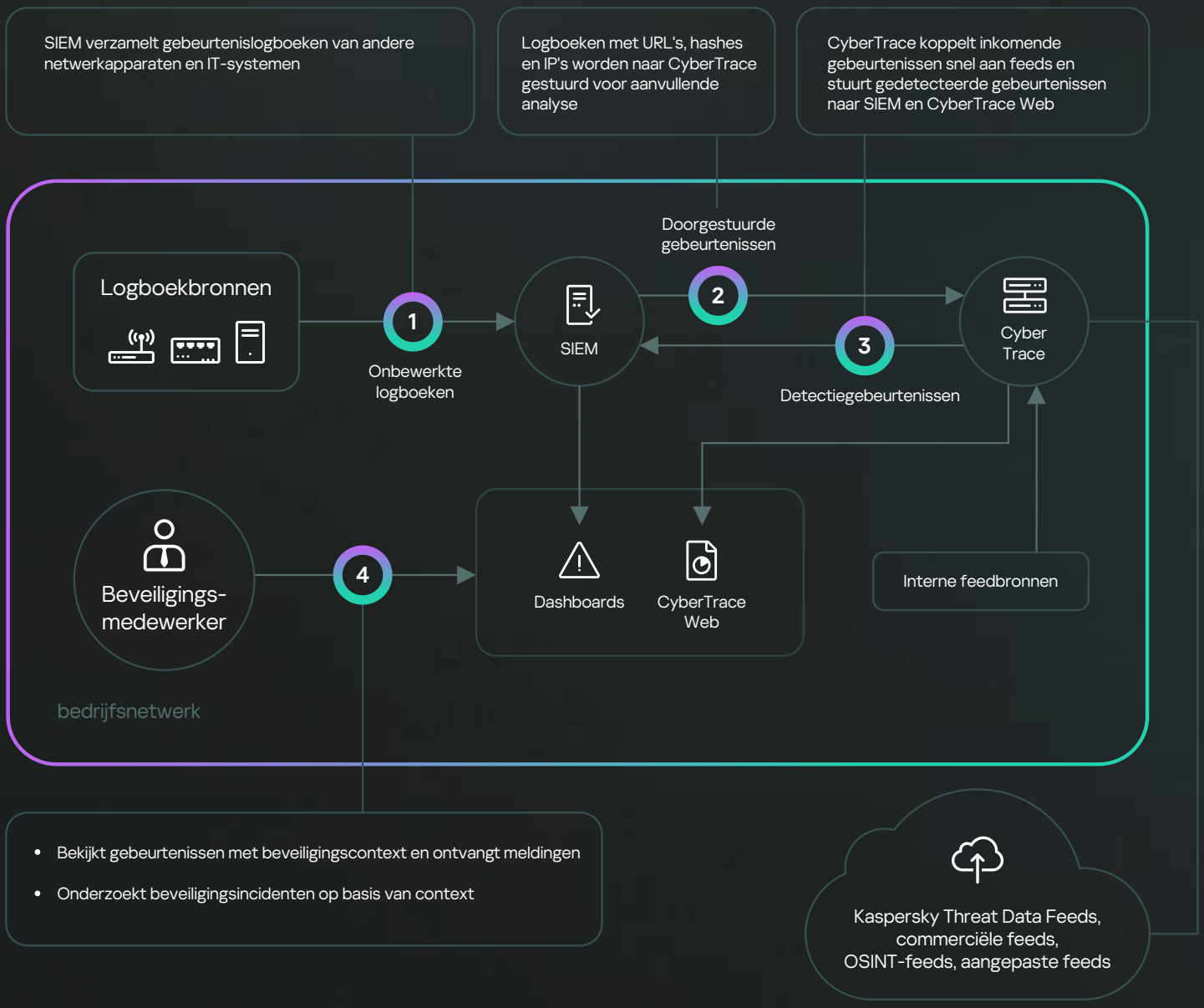
Met de functie voor historische correlatie (retroscan) kun je waarnemingen uit eerder gecontroleerde gebeurtenissen analyseren op basis van de nieuwste feeds, om zo dreigingen op te sporen die eerder werden ontdekt

Multitenancy ondersteunt gebruiksscenario's voor MSSP's en grote ondernemingen

Stuurt detectiegebeurtenissen naar SIEM-oplossingen en verkleint zo de druk op SIEM en analisten

Met de HTTP RestAPI kun je dreigingsinformatie opzoeken en beheren

Hoe het werkt



Kaspersky CyberTrace parseert inkomende logboeken en gebeurtenissen, koppelt de resulterende gegevens snel aan feeds en genereert eigen meldingen over dreigingsdetectie, wat de SIEM-werklast aanzienlijk vermindert.

Voordelen van het gebruik van CyberTrace met Kaspersky Threat Data Feeds

Grote aantallen beveiligingswaarschuwingen effectief uitfilteren en prioriteiten stellen

Processen voor categorisering en eerste respons verbeteren en versnellen

Een proactief en op gegevens gebaseerd beveiligingssysteem opbouwen

Waarschuwingen direct identificeren die van uiterst belang zijn voor je bedrijf en deze naar IR-teams escaleren

Kaspersky
Threat Lookup

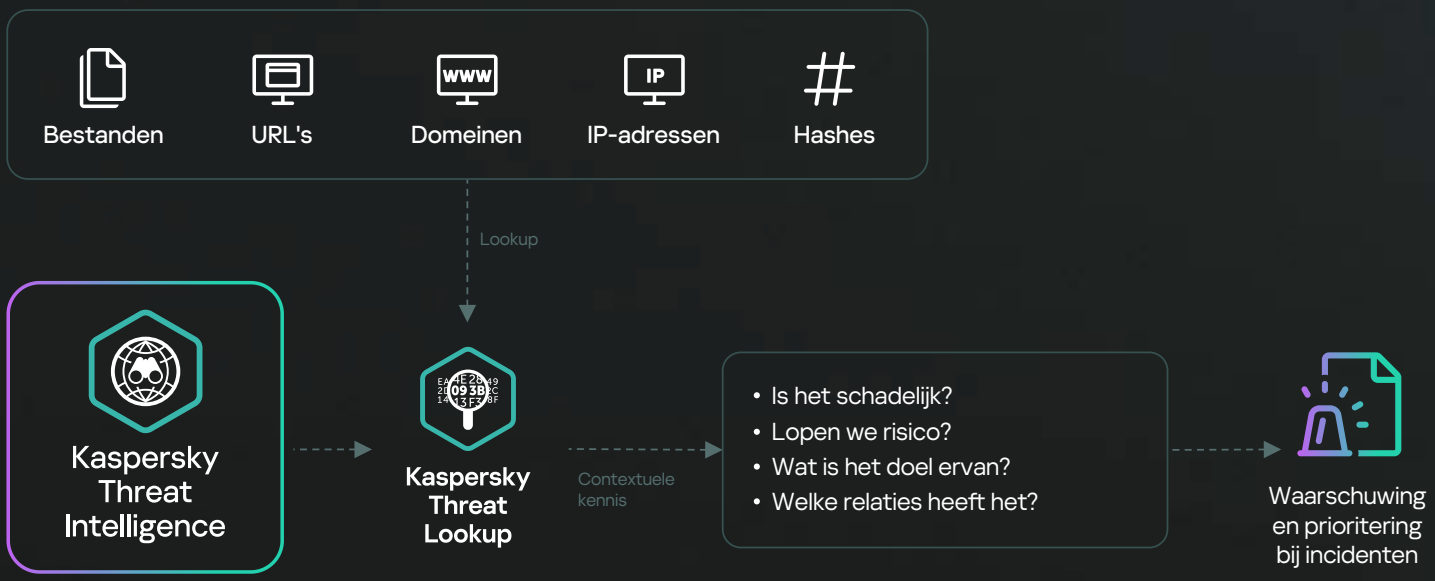
Kaspersky Threat Lookup

Cybercrime kent geen grenzen en er is op technisch vlak steeds meer mogelijk. Aanvallen worden steeds geraffineerder, ook omdat cybercriminelen gebruikmaken van bronnen op het dark web om hun doelwitten te belagen. Cyberdreigingen komen steeds vaker voor en worden in toenemende mate complexer. Ook worden ze steeds beter verhuld in de pogingen om de beveiliging te omzeilen. Aanvallers gebruiken ingewikkelde kill chains en aangepaste tactieken, technieken en procedures (TTP's) in hun campagnes om uw bedrijf te verstoren of uw klanten te benadelen.

Kaspersky Threat Lookup maakt gebruikt van alle kennis die Kaspersky heeft vergaard over cyberdreigingen en hun relaties, in de vorm van één krachtige webservice. Het doel is je beveiligingsteams te voorzien van zoveel mogelijk gegevens, waardoor cyberaanvallen kunnen worden voorkomen voor ze je organisatie treffen. Het platform haalt de nieuwste, gedetailleerde dreigingsinformatie op over URL's, domeinen, IP-adressen, bestandshashes, dreigingsnamen, statistische gegevens, gedragsgegevens, WHOIS-/DNS-gegevens, bestandskenmerken, geolocatiegegevens, downloadketens, tijdstempels etc. Het resultaat is globale zichtbaarheid van nieuwe en opkomende dreigingen, zodat je je organisatie kunt beveiligen en de incidentrespons kunt verbeteren.

Hoe het werkt

Objecten om te analyseren



Voordelen

Trusted Intelligence

Een belangrijk aspect van Kaspersky Threat Lookup is de betrouwbaarheid van onze informatie over bedreigingen, gekoppeld aan een context voor handelen. Kaspersky is toonaangevend op het gebied van anti-malwaretests. Dat blijkt uit de hoogste detectiepercentages, vrijwel zonder false positives, dankzij de ongeëvenaarde kwaliteit van onze beveiligingsinformatie.

Dreigingsopsporing

Wees proactief in het voorkomen en opsporen van, en reageren op aanvallen om de gevolgen en frequentie te minimaliseren. Spoor aanvallen op en schakel ze in een zo vroeg mogelijk stadium op agressieve wijze uit. Hoe eerder je een dreiging ontdekt, hoe minder schade deze kan aanrichten, hoe sneller je eventuele schade kunt herstellen en hoe sneller alles weer het oude is.

Makkelijk in gebruik

Webinterface of RESTful API. Gebruik de service in handmatige modus via een webinterface (via een webbrowser) of via de eenvoudige RESTful API, wat de voorkeur heeft

Uiteenlopende exportindelingen

Exporteer IoC's (Indicators of Compromise) of contexten voor handelen naar veelgebruikte, meer georganiseerde deelbare indelingen die door machines kunnen worden gelezen, zoals STIX, OpenIOC, JSON, YARA, Snort of zelfs CSV om maximaal te profiteren van de voordelen van dreigingsinformatie, operationele workflows te automatiseren of om ze met beveiligingsmaatregelen zoals SIEM's te integreren.

Voordelen van Kaspersky Threat Lookup

1. Diepgaand onderzoek uitvoeren naar indicatoren van bedreigingen met hoogwaardige, gevalideerde dreigingscontext om de prioriteit te bepalen voor aanvallen de nadruk te leggen op het beperken van die bedreigingen die het grootste risico vormen voor je bedrijf

2. Beveiligingsincidenten op hosts en het netwerk op efficiënte wijze diagnosticeren en analyseren, en de volgorde bepalen waarin signalen van interne systemen voor onbekende dreigingen worden afgehandeld

3. Je incidentrespons en mogelijkheden voor dreigingsopsporing verbeteren om de kill chain te onderbreken voordat cruciale systemen en gegevens in gevaar komen

4. Indicatoren van bedreigingen zoeken via een webgebaseerde interface of via de RESTful API

5. Geavanceerde details bekijken waaronder de certificaten, veelgebruikte namen, bestandspaden of gerelateerde URL's om nieuwe verdachte objecten te ontdekken

6. Controleren of het object dat is ontdekt, veel wordt gebruikt of uniek is, en begrijpen waarom een object als schadelijk moet worden gezien

Kaspersky
Threat Analysis

Kaspersky Threat Analysis

Als je te maken krijgt met een potentiële cyberdreiging, is het van belang welke beslissingen je neemt en op welke manier je dat doet. Het is onmogelijk om de gerichte aanvallen van tegenwoordig te voorkomen met alleen anti-virustools. Anti-virus-engines kunnen alleen bekende dreigingen en variaties hierop stoppen. Tegelijkertijd doen geraffineerde aanvallers er alles aan om automatische detectie te omzeilen. Het aantal beveiligingsmeldingen dat Security Operations Centers (SOC's) dagelijks verwerken, groeit exponentieel. Nu het aantal vormen van malware iedere dag toeneemt, is het effectief prioriteren, herkennen en valideren van waarschuwingen bijna onuitvoerbaar.

Kaspersky biedt een enkele veerkrachtige structuur om automatisch verdachte bestanden mee te analyseren, waardoor beveiligingsonderzoekers op de hoogte kunnen blijven van bestaande en opkomende dreigingen. Naast traditionele analysetechnologieën voor dreigingen zoals sandboxing, beschermt Kaspersky Threat Analysis je met geavanceerde attributie en gerelateerde gelijkenistechnologieën. Deze hybride aanpak biedt efficiënte dreigingsanalyse, zodat je goed geïnformeerde keuzes kunt maken en je infrastructuur veilig kunt houden. Kaspersky Threat Analysis wordt via een verbonden web en RESTful-interfaces aangeboden.

Componenten van Kaspersky Threat Analysis

Kaspersky
Research Sandbox

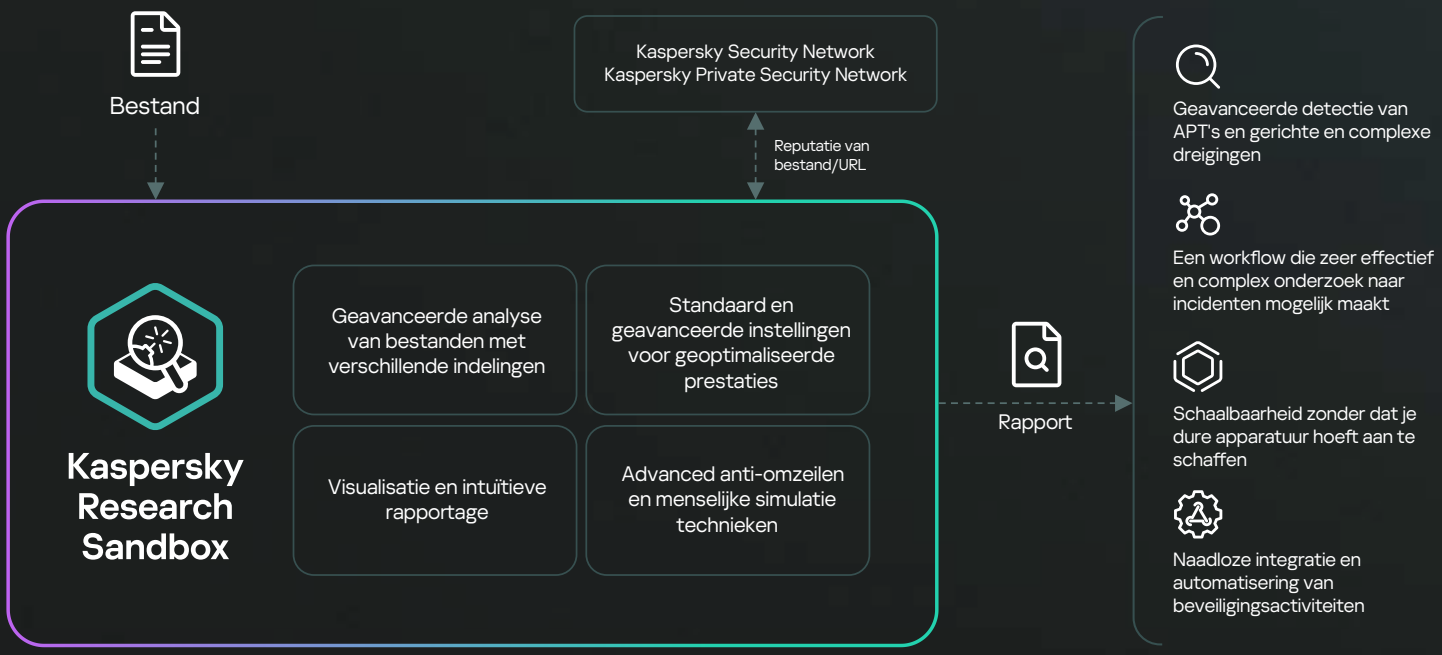
Kaspersky Onderzoekssandbox

Kaspersky Research Sandbox is een technologie die we direct vanuit ons sandbox-lab al twee decennia aan het ontwikkelen zijn. Het omvat alle kennis over malwaregedrag die we hebben opgedaan tijdens ons voortdurende dreigingsonderzoek, waardoor we elke dag meer dan 420.000 nieuwe schadelijke objecten kunnen detecteren.

Met Kaspersky Research Sandbox kun je de bronnen van bestandsexemplaren onderzoeken, IoC's verzamelen op basis van gedragsanalyse en schadelijke objecten detecteren die je nog niet eerder hebt gezien. Het biedt een hybride aanpak, waarbij gedragsanalyse en ijzersterke anti-ontwijkingstechnieken worden gecombineerd, met technologieën die menselijk gedrag nabootsen, zoals automatisch klikken, door documenten scrollen en nepprocessen.

Deze technologie wordt op locatie geïmplementeerd en voorkomt dat gegevens op straat komen te liggen. Met Kaspersky Research Sandbox kun je uitvoeringsomgevingen aanpassen aan echte omgevingen om de nauwkeurigheid van dreigingsdetectie en snelheid van het onderzoek te verhogen.

Hoe het werkt



Product voordelen

- Gepatenteerde technologie
- Geautomatiseerde objectanalyse in Windows-, Linux- en Android-omgevingen
- Ondersteuning voor analyse van meer dan 200 bestandstypen met gedetailleerde analyserapporten
- Meer dan 1000 unieke opsporingen om TTP's uit te pakken door MITRE ATT&CK
- Geavanceerde anti-ontwijkingstechnieken en technieken die menselijk gedrag nabootsen
- De dreigingsscore op basis van statistieken en gegevens die worden verkregen tijdens het uitvoeren van een bestand, geeft het risiconiveau van het geanalyseerde object weer
- Vooraf geconfigureerde Suricata-regels om het netwerkverkeer te inspecteren dat tijdens de bestandsuitvoering werd gegenereerd
- Handmatige upload van exemplaren en een geavanceerde REST API om te integreren met geautomatiseerde workflows

Kaspersky
Threat Attribution
Engine

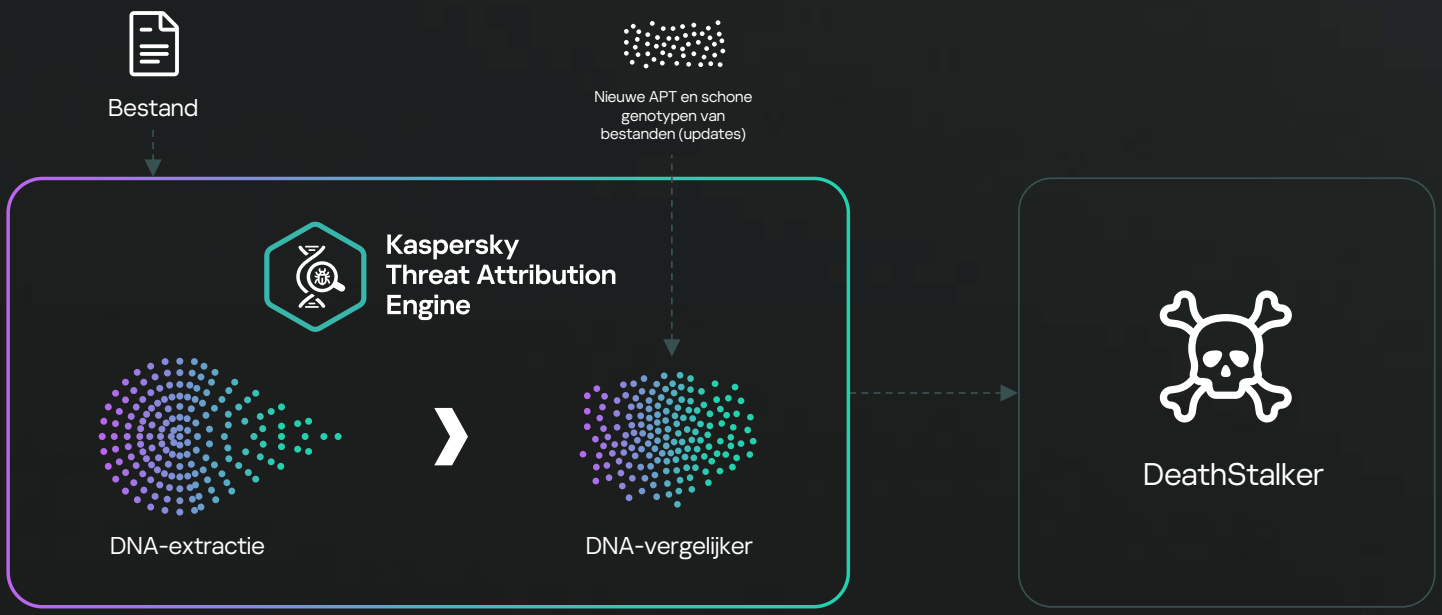
Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine is een unieke tool voor dreigingsanalyse die inzicht biedt in de herkomst van bekende malware en mogelijke ontwikkelaars. Het koppelt een verdacht bestand direct aan bekende APT-bedreigingen, -aanvallers of -campagnes door middel van een uniek algoritme en speciale database die exemplaren van APT-malware bevat en de grootste verzameling schone bestanden in de industrie. Deze bestanden zijn de afgelopen 25 jaar verzameld door experts van Kaspersky.

Per jaar houden we meer dan 1100 aanvallers en campagnes bij en leveren we meer dan 200 rapporten over dreigingsgegevens. Door ons voortdurende onderzoek wordt het verzamelen van APT's ondersteund. Deze verzameling bevat meer dan 100.000 bestanden die, samen met het gebruik van geautomatiseerde tools, voor een ongekend precies niveau van attributie zorgt.

Het product biedt een unieke aanpak voor het vergelijken van soortgelijke bestanden met een zeer lage kans op false positives. Een nieuwe aanval kan snel worden gekoppeld aan bekende APT-malware, gerichte aanvallen uit het verleden en hackergroepen, waardoor je dreigingen met een hoog risico kunt onderscheiden van minder gevaarlijke incidenten. Op deze manier kun je op tijd beschermingsmaatregelen nemen om ervoor te zorgen dat een aanvaller geen grip krijgt op je systeem. Kaspersky Threat Attribution Engine kan worden geïmplementeerd in beveiligde, geïsoleerde omgevingen, waardoor externe partijen geen toegang hebben tot de verwerkte gegevens en ingediende objecten. Met lokale implementatie heb je de extra mogelijkheid om eigen actoren en exemplaren toe te voegen om exemplaren te detecteren die hetzelfde zijn als bestanden in je privécollectie en om YARA-regels te exporteren voor verder geautomatiseerd zoeken naar dergelijke bestanden in je infrastructuur en integratie met externe oplossingen.

Hoe het werkt



Eigen zoekmethode

Om malware te koppelen aan attributie-entiteiten, wordt er bij Kaspersky Threat Attribution Engine gebruik gemaakt van een unieke eigen methode voor het zoeken naar soortgelijke genotypen en strings tussen bestanden. Deze methode omvat:

1

De genetica van een exemplaar analyseren door de volgende elementen van de code uit te pakken:

- Genotypen - kenmerkende stukjes binaire code.
- Strings - kenmerkende strings van tekens.

2

De geanalyseerde bestanden automatisch doorzoeken voor genotypen en strings die lijken op genotypen en strings van APT-exemplaren die in het verleden zijn geanalyseerd of al zijn gekoppeld aan attributie-entiteiten.

3

Op basis van dergelijke genotypen en strings die zijn gevonden in APT-exemplaren, die een rapportage bieden over de herkomst van het geanalyseerde exemplaar, gerelateerde attributie-entiteiten en gelijkenissen tussen dit exemplaar en bekende APT-exemplaren.

Belangrijke product kenmerken

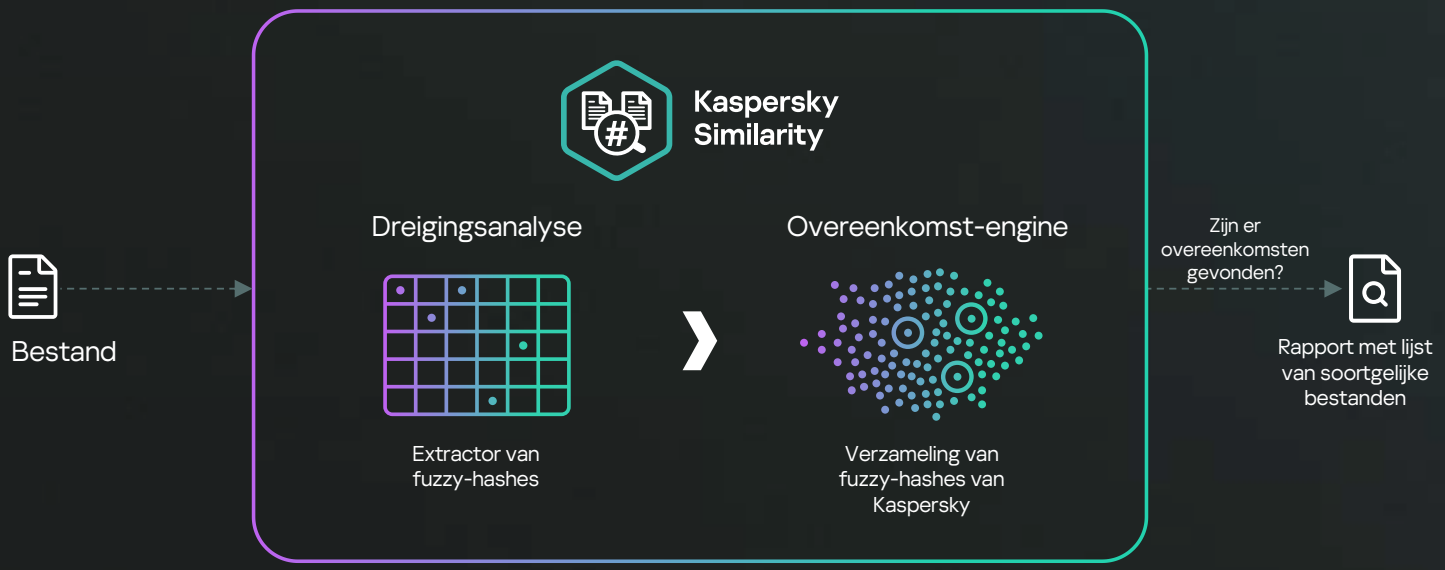
- Gepatenteerde technologie
- Directe toegang tot een bibliotheek met beheerde gegevens over duizenden APT-aanvallers, -exemplaren en -campagnes
- Handmatige upload van exemplaren en een geavanceerde REST API om te integreren met geautomatiseerde workflows
- Mogelijkheid om met wachtwoorden beveiligde archieven uit te pakken met aangepaste wachtwoorden
- Exporteren naar STIX 2.1-indeling (TXT en JSON worden ook ondersteund) voor verdere geautomatiseerde analyse van beveiligingslogs en integratie met oplossingen van externe partijen
- Ondersteunt de implementatie op cloudinfrastructuren zoals Amazon Web Services (AWS), waardoor je het product snel kunt instellen en kosten kunt besparen, aangezien je niet hoeft te investeren in hardware

Kaspersky Intelligence Reporting

Kaspersky Similarity

Kaspersky Similarity is een handige tool om bestanden met dergelijke functionaliteit te identificeren op basis van de technologie die door Kaspersky-experts is ontwikkeld om bescherming te bieden tegen onbekende en verborgen dreigingen. Voor deze technologie worden meer dan 50 unieke soorten speciale hashes en een database vol malware-exemplaren gebruikt die al meer dan 25 jaar door Kaspersky zijn verzameld en die miljoenen schadelijke bestanden bevatten om resultaten met de grootste nauwkeurigheid en betrouwbaarheid te waarborgen.

Met Kaspersky Similarity kun je soortgelijke (en ongrijpbare) malware-exemplaren zoeken in de infrastructuur zodat je zeker weet dat je op de hoogte bent van zelfs een kleine verandering in het exemplaar dat is aangebracht door de aanvaller.



Gelijkenisrapporten

De experts van Kaspersky hebben een reeks hashes ontwikkeld waarmee de gelijkenis kan worden bepaald tussen verschillende bestanden op basis van deze kenmerken.

Met Kaspersky Similarity kunnen gebruikers een verdacht bestand indienen, de hashes extraheren en deze vergelijken met hashes van bestanden die al in de dreigingsdatabase van Kaspersky zitten. Als er overeenkomsten worden gevonden, wordt er een lijst gegenereerd met hashes van de meest soortgelijke schadelijke bestanden die al bekend zijn bij Kaspersky. Vervolgens worden ze gesorteerd op basis van het aantal gelijkenissen. Het rapport bevat extra context met metagegevens voor elk soortgelijk bestand:

- Mate van gelijkenis
- Status van bestand (malware, adware of anders)
- Naam van bedreiging
- Tijdstempels van de eerste en meest recente detectie
- Hoeveelheid hits (detecties)
- Bestands-hash
- Bestandstype
- Bestandsgrootte

Voordelen

- Gepatenteerde technologie
- Het maakt gebruik van een van de grootste databases in de industrie die bestaat uit schadelijke en schone bestanden die in de afgelopen 25 jaar zijn verzameld. Hierdoor krijg je de hoogste precisie bij het vergelijken van bestanden
- Handmatige upload van exemplaren en een geavanceerde REST API om te integreren met geautomatiseerde workflows
- De technologie wordt al lang gebruikt door experts van Kaspersky om nieuwe dreigingen te onderzoeken en nog betere bescherming tegen dreigingen te bieden. Dit wordt regelmatig bewezen door onze topresultaten volgens onafhankelijke tests:

Meer informatie

Voordelen van Kaspersky Threat Lookup

1

Geef je incidentrespons en forensische activiteiten een boost met Kaspersky Research Sandbox, die je de geavanceerde dynamische analyse van verdachte bestanden geeft met de mogelijkheid om dreigingen die nog geen dag oud zijn en resultaten die zijn toegewezen aan TTP's van MITTRE ATT&CK.

2

Juiste en tijdige attributie met Kaspersky Threat Attribution Engine helpt om aanvallers te definiëren met de volledige lijst met TTP's, zodat je een uitgebreide weergave hebt van aanvalsvectoren met heldere beperkende stappen waarmee je de incidentresponstijden van maanden naar minuten kunt inkorten.

3

Onthul ontwijkende dreigingen met Kaspersky Similarity waarmee je schadelijke exemplaren kunt zoeken, die speciaal zijn ontworpen om traditionele anti-malwaretechnologieën te omzeilen om zo de meest geavanceerde APT-aanvallen te detecteren die jarenlang niet wordt opgespoord.

Kaspersky Intelligence Reporting

Kaspersky Threat Intelligence Reporting

U hebt een volledig beeld van alle tactieken, technieken en procedures van aanvallers nodig om moderne cyberdreigingen het hoofd te kunnen bieden. Alhoewel de C&C's en middelen die worden ingezet bij aanvallen regelmatig veranderen, is het lastig voor aanvallers om hun gedrag en methoden tijdens aanvallen te wijzigen. Door deze patronen direct te identificeren, kunt u direct effectieve verdedigingsmechanismen implementeren om de cybercriminelen te ontwapenen en de kill chain te verstoren.

Een abonnement op Kaspersky Threat Intelligence Reporting biedt blijvende toegang tot ons onderzoek, waarin actuele informatie staat over de meest gevaarlijke dreigingen, waardoor jij en je beveiligingsteam een effectieve strategie voor aanvalsdetectie tijdig proactief kunnen toepassen, evenals de schade van dergelijke dreigingen minimaliseren.

Terwijl slechts een klein percentage van onze onderzoeken openbaar wordt gemaakt, heb je met Kaspersky Intelligence Reporting bevoorrechte toegang tot de meest actuele informatie over de nieuwste dreigingen. Onze experts volgen voortdurend de activiteiten van cybercriminelen, waardoor ze de meest geavanceerde en gevaarlijke gerichte aanvallen, cyberspionagecampagnes, malware- en encryptie-exemplaren en de laatste trends op het gebied van cybercriminaliteit wereldwijd kunnen identificeren.

>200
privérapporten per jaar

>300
aanvallers

>500
campagnes

>2500
YARA-regels

>170.000
IoC's

Analytische rapporten omvatten:

Profielen van aanvallers

Toewijzing in MITRE ATT&CK

Samenvatting voor executives (informatie op C-niveau)

Diepgaande technische analyse omvat:

- Aanvalsmethoden
- Gebruikte exploits
- Beschrijving van malware
- Beschrijving van C&C-infrastructuur en protocollen
- Slachtofferanalyse
- Analyse van gegevensexfiltratie
- Attributies

Indicators of Compromise (IoC's) en YARA-, SIGMA- of Suricata-regels

Aanbevelingen van Kaspersky-experts

We bieden verschillende commerciële rapportagesporen op basis van je behoeften en de details van je organisatie:

Kaspersky APT Intelligence Reporting

Biedt inzichten in geavanceerde, gerichte cyberdreigingen op de lange termijn die vaak afkomstig zijn van goed georganiseerde groepen met voldoende middelen. Het omvat informatie over verschillende APT-groepen wereldwijd en hun tactieken, technieken en procedures (TTP's), evenals de sectoren en regio's waar ze zich op richten. Dit rapportagespoor is gericht op spionage-activiteiten, variërend van aanvallen op de toeleveringsketen tot vernietigende activiteiten en activiteiten van hacktivisten. Deze rapporten zijn ideaal als je organisatie een groot bedrijf, overheidsinstantie of organisatie is die is betrokken bij kritieke infrastructuur. Ze zijn ook gedeeltelijk relevant voor organisaties die gevoelige gegevens hebben die mogelijk een interessant onderwerp zijn voor overheidsinstanties.

Kaspersky Crimeware Intelligence Reporting

Focust op aanvallen en campagnes met financiële winst als hoofddoel. Dit omvat informatie over de laatste trends in cybercriminaliteit, waaronder gestolen gegevens die op het dark web zijn verkocht, financiële fraude, ransomware en ATM/PoS-malware. Ze bieden details over nieuwe soorten crimeware, hun verspreidingsmethoden en de soorten gegevens waar ze op gericht zijn. Dit rapportagespoor is met name relevant als je organisatie aanzienlijk veel online zakendoet, of als je gevoelige gegevens hebt, mogelijk als financiële instelling of e-commerce-platform.

Kaspersky ICS Threat Intelligence

Biedt diepgaande informatie en een groter bewustzijn van kwaadaardige campagnes die zijn gericht op industriële organisaties. Daarnaast wordt er informatie gegeven over kwetsbaarheden in de populairste industriële beheersystemen en onderliggende technologie. Dit rapportagespoor wordt geleverd door Kaspersky ICS CERT, een toegewijd team van meer dan 30 hooggekwalificeerde experts op het gebied van onderzoek naar ICS-dreigingen en -kwetsbaarheden, incidentrespons en beveiligingsanalyse, opgericht in 2016. Deze rapporten bieden bruikbare inzichten en ondersteuning om je kritieke bedrijfsmiddelen (waaronder je software- en hardwarecomponent) veilig te stellen en de veiligheid en continuïteit van je technologische processen te waarborgen.

Je kunt de volgende gerelateerde Kaspersky ICS Threat Intelligence-services overwegen:

ICS Threat Intelligence Reporting

Het abonnement op onze regelmatige publicaties over industriële cyberbeveiligingsdreigingen en kwetsbaarheden:

- Meldingen over dreigingen van nog geen dag oud
- Gedetailleerde technische rapporten
- Maandelijkse beoordelingen
- Aanbevelingen voor kwetsbaarheidsbeperkingen
- Statistieken en trends

ICS Threat Data Feeds

Door machines leesbare gegevensstromen over industriële cyberbeveiligingsdreigingen en -kwetsbaarheden.

Eenvoudige indelingen voor gegevensverspreiding (JSON, CSV, OpenIoC, STIX) via HTTPS, TAXII en gespecialiseerde leveringsmethoden voor integratie naar oplossingen voor informatiebeveiliging.

Vraag het aan de analist

Overleg met Kaspersky ICS CERT-experts, die je individueel advies geven over de industriële cyberbeveiligingsdreigingen en -kwetsbaarheden, dreigingsstatistieken en het landschap, industrienormen, enz. die voor jou het meest relevant zijn.

Kaspersky Threat Intelligence Reporting biedt het volgende:

Toegang met voorrang

Om verschillende redenen worden niet alle belangrijke dreigingen algemeen bekend gemaakt. We verstrekken dit soort exclusieve informatie echter aan onze klanten tijdens het onderzoeksproces, zelfs vóór de officiële publieke aankondiging.

Toegang tot technische gegevens

Waaronder een uitgebreide lijst met IoC's, beschikbaar in standaardindelingen zoals openIOC of STIX, evenals toegang tot onze YARA-, Sigma- of Suricata-regels.

Profielen van aanvallers

Inclusief verdacht land van oorsprong en hoofdactiviteit, gebruikte malwarefamilies, sectoren en regio's die doelwitten zijn en beschrijvingen van alle gebruikte TTP's, met toewijzing aan MITRE ATT&CK.

MITRE ATT&CK

Alle TTP's die in de rapporten worden beschreven, worden aan MITRE ATT&CK toegewezen. Dit maakt verbeterde detectie en respons mogelijk doordat er bijbehorende gebruiksscenario's voor veiligheidsbewaking worden ontwikkeld waaraan prioriteit wordt gegeven. Ook worden er hiaatanalyses uitgevoerd en wordt de huidige beveiliging tegen relevante TTP's getest.

Retrospectieve analyse

Toegang tot alle eerder uitgegeven particuliere rapporten gedurende je abonnement.

RESTful API-ondersteuning

Naadloze integratie en automatisering van beveiligingsworkflows.

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

Naarmate je bedrijf groeit, worden je IT-omgevingen ook meer verspreid en complexer. Dit zorgt voor een uitdaging: je wijdverspreide digitale aanwezigheid beschermen zonder rechtstreekse controle of verantwoordelijkheid. Dynamische en onderling verbonden omgevingen stellen bedrijven in staat grote voordelen te behalen. Maar naarmate de onderlinge verbondenheid toeneemt, neemt ook het aanvalsoppervlak toe. Aanvallers worden steeds vaardiger, en daarom is het niet alleen essentieel om een nauwkeurig beeld van de online aanwezigheid van je bedrijf te hebben, maar ook om wijzigingen hierin bij te kunnen houden en te reageren op externe dreigingen die zijn gericht op digitale assets.

Organisaties gebruiken uiteenlopende veiligheidstools, maar toch liggen er digitale dreigingen op de loer waarvoor je zeer specifieke vaardigheden moet hebben: om gegevenslekken te detecteren en beperken, plannen en aanvalsprogramma's van cybercriminelen op dark web-forums monitoren, etc. Kaspersky heeft Kaspersky Digital Footprint Intelligence **ontwikkeld om je beveiligingsanalisten te helpen inzicht te krijgen in het beeld van tegenstanders van je bedrijfsresources, direct de potentiële aanvalsvectoren te ontdekken die ze tot hun beschikking hebben en je beveiliging daarop aan te passen.**

Kaspersky Digital Footprint Intelligence biedt het volgende:

Detectie van dreigingen

Frauduleuze activiteiten volgen die schade kunnen toebrengen aan de reputatie van een bedrijf en/of klanten kunnen misleiden.

Netwerkverkenning

Identificatie van de netwerkresources en blootgestelde services van de klant die een mogelijk toegangspunt voor een aanval zijn. Gerichte analyses van bestaande kwetsbaarheden, met verdere score en uitgebreide risicobeoordeling op basis van de CVSS-basisscore, beschikbaarheid van openbare exploits, ervaring met penetratietesten en locatie van de netwerkresource (hosting/infrastructuur).

Het dark web volgen

Continue volgen van bronnen van het dark web (forums, ransomwareblogs, messengers, tor-sites, etc.), verwijzingen en dreigingen detecteren die aan je bedrijf, cliënten en partners zijn gerelateerd. Analyse van gerichte aanvallen, actief of gepland, en APT-campagnes gericht op je bedrijf, sector en regio's.

Ontdekking van gegevenslekken

Detectie van gecompromitteerde inloggegevens van werknemers, partners en cliënten, bankpassen, telefoonnummers en overige gevoelige informatie die kan worden gebruikt om een aanval uit te voeren of om risico's te vormen voor je bedrijf.

Ondersteuning van multitenancy

Uitgebreide mogelijkheden voor aanbieders van beheerde beveiligingsservice (MSSP's) en grote organisaties met een structuur voor meerdere branches.

Informatiebronnen

Het is essentieel dat je een uitgebreid inzicht hebt in de externe beveiliging van je bedrijf.
Om deze informatie te verstrekken, verzamelen en aggregeren beveiligingsanalisten van Kaspersky informatie van de volgende informatiebronnen:

Je ongestructureerde gegevens

- IP-adressen
- Bedrijfsdomeinen
- Merknamen
- Trefwoorden
- Netwerkbereiken
- BIN-/INN-kaartnummers
- Werknemersgegevens

Inventaris netwerkperimeter

Zoekopdrachten op het surface web, deep web en dark web

Zoekopdrachten op Kaspersky Knowledge Base

Waarschuwingen voor dreigingen

Zoeken in realtime in surface web- en dark web-bronnen van Kaspersky

Analytische rapporten*

Hoe het werkt

Configureren

Informatie over de digitale assets van het bedrijf

Verzamelen

Geautomatiseerde gegevensverzameling van surface, deep en dark webs en de Kaspersky-kennisdatabase

Filteren

Dreigingsdetectie, -analyse en -prioritering, beheerd door analisten

Kennisgeving

Snelle meldingen van dreigingen geven op Kaspersky Threat Intelligence Portal of via API

* Add-on service

Bedrijfswaarden van Digital Footprint Intelligence

Kaspersky Digital Footprint Intelligence levert krachtige voordelen en een aanzienlijke waarde voor je organisatie op:

Detectie van dreigingen

Detecteer potentiële dreigingen in realtime om je merkreputatie te beschermen, het vertrouwen van de klant te behouden en het risico op financieel verlies en schade aan zakelijke activiteiten te verminderen.

Verklein cyberrisico's

Voorzie je belangrijke belanghebbenden (CxO en bestuur) van informatie over waar de focus op uitgaven van cyberbeveiliging moet liggen door hiaten in de huidige installatie en de risico's die ze met zich meebrengen te onthullen.

Reageer sneller

Extra context voor beveiligingswaarschuwingen verbetert de incidentrespons en verkort de tijd die nodig is om een incident op te lossen (MTTR)

Verklein het aanvalsoppervlak

Beheer de digitale aanwezigheid van je bedrijf en houd toezicht op externe netwerkresources om aanvalsvectoren en kwetsbaarheden te minimaliseren die kunnen worden gebruikt voor een aanval.

Inzicht in je tegenstanders

Een gewaarschuwd mens telt voor twee. Weet wat cybercriminelen van plan zijn en over jouw bedrijf bespreken op het dark web zodat je voorbereid bent.

Herken het onbekende

Verbeter je vermogen om cyberaanvallen het hoofd te bieden en identificeer dreigingen buiten het rechtsgebied van je interne beveiligingsteams.

Efficiëntie van servicelevering

Een snelle start en snel opschalen in de multitenancy-modus bespaart tijd voor zowel aanbieders van beheerde beveiligingsservices (MSSP's) en hun klanten als grote organisaties met meerdere gelieerde ondernemingen.

Kaspersky Takedown Service

Kaspersky Takedown Service

Cybercriminelen maken kwaadaardige en phishing-domeinen om je bedrijf en merken aan te vallen. Als het na de detectie ervan niet lukt deze dreigingen snel in te perken, kan dat leiden tot verlies van inkomsten, imagoschade, een afname van het consumentenvertrouwen, gegevenslekken en meer. Het beheren van takedowns van deze domeinen is echter een complex proces waarvoor deskundigheid en tijd nodig is.

Kaspersky Takedown Service beperkt snel dreigingen van kwaadaardige en phishingdomeinen, voordat je merk en bedrijf schade oplopen. End-to-end beheer van het hele proces bespaart klanten kostbare tijd en resources. De service is wereldwijd.

Kaspersky blokkeert elke dag meer dan 15-000 phishing-/scam-URL's en voorkomt meer dan een miljoen pogingen om op dergelijke URL's te klikken. We hebben heel wat jaren ervaring met het analyseren van kwaadaardige en phishing-domeinen en weten hoe we al het nodige bewijs moeten verzamelen om te bewijzen dat ze kwaadaardig zijn. We nemen het takedown-beheer van je over en maken snelle actie mogelijk om je digitale risico's te minimaliseren, zodat je team zich kan richten op andere prioriteiten.

Kaspersky biedt klanten effectieve bescherming voor hun online services en reputatie dankzij samenwerking met internationale organisaties, nationale en regionale handhavingsinstanties (zoals INTERPOL, Europol, Microsoft Digital Crimes Unit, de National High-Tech Crime Unit (NHTCU) van de Nederlandse politie en de City of London Police), en Computer Emergency Response Teams (CERT's) wereldwijd.

Volledige zichtbaarheid

Je wordt bij elke fase van het proces op de hoogte gehouden, van de registratie van je aanvraag tot de succesvolle takedown

End-to-end beheer

We beheren het volledige takedown-proces, zodat jij er zo weinig mogelijk mee bezig hoeft te zijn

Wereldwijde dekking

Waar een kwaadaardig domein of phishingdomein ook is geregistreerd, Kaspersky vraagt de takedown ervan aan bij de regionale organisatie met de relevante juridische autoriteit

Hoe het werkt

Je kunt je aanvragen indienen via Kaspersky Company Account, onze ondersteuningsportal voor zakelijke klanten. We bereiden alle benodigde documentatie voor en sturen het takedown-verzoek naar de relevante lokale of regionale autoriteit (CERT, registratiebureau etc.) die de nodige wettelijke rechten heeft om het domein te sluiten. Je wordt bij elke stap op de hoogte gehouden, totdat de betreffende resource offline is gehaald.

Moeiteloze bescherming

De Kaspersky Takedown Service beperkt snel dreigingen van kwaadaardige en phishingdomeinen, voordat je merk en bedrijf schade oplopen. End-to-end beheer van het hele process bespaart kostbare tijd en resources.

Kaspersky
Ask the Analyst

Kaspersky Ask the Analyst

Cybercriminelen ontwikkelen voortdurend nieuwe geraffineerde manieren om bedrijven aan te vallen. In het explosieve, snel groeiende dreigingslandschap van nu komen steeds wendbaardere cybercrime-technieken voor. Organisaties krijgen te maken met complexe incidenten die worden veroorzaakt door non-malware-aanvallen, bestandsloze aanvallen, living-off-the-land-aanvallen, zero-day-exploits, en combinaties hiervan die zijn geïntegreerd in complexe dreigingen, APT-achtige en gerichte aanvallen.

In een tijd waarin bedrijven compleet plat kunnen worden gelegd door cyberaanvallen, zijn professionals op het gebied van cyberbeveiliging belangrijker dan ooit. Het kan echter lastig zijn ze te vinden en te behouden. En zelfs als je een stabiel cyberbeveiligingsteam hebt, kun je niet van je experts verwachten dat ze altijd alleen de strijd met geraffineerde dreigingen kunnen aangaan. Ze moeten kunnen terugvallen op externe experts. Door externe expertise kun je meer inzicht krijgen in het waarschijnlijke verloop van complexe aanvallen en APT's. Ook kun je actiegericht advies krijgen over de meest doeltreffende methode om deze aanvallen onschadelijk te maken.

Met voortdurend onderzoek naar dreigingen kan Kaspersky gesloten community's en dark forums die wereldwijd worden gebruikt door tegenstanders en cybercriminelen ontdekken, infiltreren en controleren. Onze analisten maken hiervan gebruik om op proactieve wijze de meest schadelijke en beruchte dreigingen, evenals dreigingen gericht op specifieke organisaties, te detecteren en onderzoeken.

Kaspersky Ask the Analyst is een uitbreiding van ons Threat Intelligence-portfolio waarmee je advies en inzicht kunt vragen over specifieke dreigingen waarmee je te maken hebt of in geïnteresseerd bent. Met deze service worden de krachtige dreigingsinformatie en onderzoeksmogelijkheden van Kaspersky op jouw behoeften afgestemd, zodat je een sterke beveiliging tegen dreigingen gericht op je organisatie kunt opbouwen.

Inhoud van Kaspersky Ask the Analyst (uniform, op aanvraag gebaseerd abonnement)

APT en crimeware

Aanvullende informatie over gepubliceerde rapporten en lopend onderzoek (bovenop APT Intelligence Reporting of Crimeware Intelligence Reporting)

Beschrijvingen van dreigingen, kwetsbaarheden en gerelateerde IoC's

- Algemene beschrijving van een specifieke malwarefamilie
- Aanvullende context voor dreigingen (gerelateerde hashes, URL's, CnC's etc.)
- Informatie over een specifieke kwetsbaarheid (hoe kritiek deze is en de corresponderende beveiligingsmechanismen in Kaspersky-producten)

Aan ICS gerelateerde aanvragen

- Aanvullende informatie over gepubliceerde rapporten
- Informatie over kwetsbaarheden in ICS
- Dreigingsstatistieken en -trends voor ICS per regio/sector
- Informatie van ICS-malware-analyses over regelgeving en standaarden

Informatie over het dark web

- Onderzoek op het dark web naar bepaalde artefacten, IP-adressen, domeinnamen, bestandsnamen, e-mailadressen, links of afbeeldingen
- Doorzoeken en analyseren van informatie

Malwareanalyse

- Analyse van malware-exemplaren
- Aanbevelingen voor verdere herstelacties

Hoe het werkt

Kaspersky Ask the Analyst kan afzonderlijk worden aangeschaft of als aanvulling op onze andere dreigingsinformatieservices. Je kunt je aanvragen indienen via Kaspersky Company Account, onze ondersteuningsportal voor zakelijke klanten. We reageren via e-mail, maar indien nodig en in afstemming met jou kunnen we een telefonische vergadering of een sessie met gedeeld scherm organiseren. Zodra je aanvraag is goedgekeurd, krijg je de geschatte verwerkingsduur te horen.

Gebruiksscenario's

1. Details in eerder gepubliceerde rapporten met dreigingsinformatie ophelderen
2. Aanvullende informatie over geleverde IoC's verkrijgen
3. Meer details over kwetsbaarheden krijgen en aanbevelingen over hoe je je tegen misbruik ervan kunt beschermen
4. Aanvullende informatie ontvangen over de specifieke dark web-acitiviteiten waarin je geïnteresseerd bent
5. Een samenvattend rapport aanvragen over een malwarefamilie dat het gedrag van de malware, de potentiële impact ervan en details over eventuele gerelateerde activiteit die Kaspersky heeft ontdekt, bevat
6. Effectief prioriteiten stellen voor waarschuwingen/incidenten met gedetailleerde contextinformatie en categorisatie voor gerelateerde IoC's die via korte rapporten worden geleverd
7. Ondersteuning aanvragen om te bepalen of gedetecteerde, afwijkende activiteit is gerelateerd aan een APT of crimeware-aanvaller
8. Malwarebestanden indienen voor uitgebreide analyse om inzicht te krijgen in het gedrag en de werking van de aangeleverde exemplaren

Voordelen van Kaspersky Ask the Analyst

Je expertise uitbreiden

Krijg directe toegang tot branche-experts zonder te hoeven zoeken en investeren in het inhuren van moeilijk vindbare fulltime specialisten

Onderzoeken versnellen

Schat incidenten effectief in en stel prioriteiten op basis van afgestemde en gedetailleerde contextinformatie

Snel reageren

Reageer snel op dreigingen en kwetsbaarheden op basis van onze richtlijnen voor het blokkeren van aanvallen via bekende vectoren

Je kennis en resources uitbreiden

Kaspersky Ask the Analyst geeft je per case toegang tot een kerngroep van Kaspersky-onderzoekers. De service biedt uitgebreide communicatie tussen experts om je bestaande mogelijkheden uit te breiden met onze unieke kennis en resources.

Conclusie

Je moet een volledig beeld hebben van alle tactieken en middelen van aanvallers om moderne cyberdreigingen het hoofd te kunnen bieden. Om deze informatie te kunnen genereren en de meest effectieve tegenmaatregelen te kunnen treffen, zijn constante toewijding en een zeer hoog expertiseniveau vereist. Met petabytes aan waardevolle dreigingsgegevens, geavanceerde technologieën voor machine learning en een unieke groep internationale experts doen we er alles aan om onze klanten te ondersteunen met de meest recente informatie over dreigingen, waar dan ook ter wereld, om ze te beschermen tegen zelfs de allernieuwste cyberaanvallen.

Belangrijkste voordelen

Maakt zichtbaarheid van dreigingen wereldwijd, tijdige detectie van cyberdreigingen, het stellen van prioriteiten voor beveiligingswaarschuwingen en een effectieve respons op incidenten betreffende informatieveiligheid mogelijk

De unieke inzichten in de tactieken, technieken en procedures van aanvallers in verschillende sectoren en regio's maken proactieve bescherming tegen gerichte en complexe dreigingen mogelijk

Een uitgebreid overzicht van de status van je beveiliging met actiegerichte aanbevelingen voor inperkingsstrategieën, zodat je je verdediging kun richten op de vlakken die primaire doelwitten voor cyberaanvallen vormen

Voorkomt dat analisten te veel werk krijgen en helpt je medewerkers zich op serieuze bedreigingen te richten

Verbeterde en snellere incidentrespons en mogelijkheden om dreigingen op te sporen helpen om de tijd dat een aanval onopgemerkt blijft te verkorten en de mogelijke schade aanzienlijk te beperken

Kaspersky Threat Intelligence

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture