Umfassender Service zum Schutz vor digitalen Risiken

Kaspersky Digital Footprint Intelligence

kaspersky bring on the future

Einleitung

Wie kann man Ihr Unternehmen am kosteneffizientesten angreifen?

Welche Informationen stehen einem Angreifer, der es auf Ihr Unternehmen abgesehen hat, zur Verfügung?

Wurde Ihre Infrastruktur bereits ohne Ihr Wissen angegriffen?

Kaspersky Digital Footprint Intelligence beantwortet diese und weitere Fragen. Unsere Experten erstellen dazu ein umfassendes Bild Ihrer Gefährdungslage, zeigen Schwachstellen auf, die mit großer Wahrscheinlichkeit genutzt werden, und weisen bereits stattgefundene, aktuelle und sogar geplante Angriffe nach.

Ihr Unternehmen wächst. Gleichzeitig wird Ihre IT-Umgebung immer komplexer. Der Schutz Ihrer weit verstreuten digitalen Präsenz ohne direkte Kontrolle oder entsprechende Verantwortlichkeiten kann eine große Herausforderung darstellen. Unternehmen können aus dynamischen und verbundenen Umgebungen erheblichen Nutzen ziehen. Gleichzeitig vergrößert die zunehmende Konnektivität auch die Angriffsfläche. Angreifer werden immer geschickter. Deshalb ist es nicht nur wichtig, einen genauen Überblick über die Online-Präsenz Ihres Unternehmens zu haben; Sie müssen auch in der Lage sein, Änderungen nachzuverfolgen und auf externe Bedrohungen zu reagieren, die auf exponierte digitale Ressourcen abzielen.

Unternehmen setzen für ihre Sicherheitsmaßnahmen eine Vielzahl von Sicherheitstools ein, doch es bahnen sich externe Bedrohungen an, die sehr spezifische Fähigkeiten erfordern – um Datenlecks aufzuspüren und einzudämmen, um Angriffspläne und -schemata von Cyberkriminellen in Dark Web-Foren zu überwachen usw. Mit Kaspersky Digital Footprint Intelligence **unterstützen wir Sicherheitsanalysten dabei, Unternehmensressourcen aus dem Blickwinkel des Gegners zu betrachten, potentielle Angriffsvektoren schnell zu erkennen und ihre Verteidigungsstrategie entsprechend auszurichten.**

Die Vorteile von Kaspersky Digital Footprint Intelligence auf einen Blick

Kaspersky Digital Footprint Intelligence ist ein umfassender Service zum Schutz vor digitalen Risiken, mit dem Sie ihre digitalen Ressourcen überwachen und Bedrohungen aus dem öffentlichen Web, dem Deep Web und dem Dark Web zuverlässig erkennen können.

External Attack Surface

Überwachung der dem Internet ausgesetzten Ressourcen der Kunden, um eine frühzeitige Erkennung von Schwachstellen und Fehlkonfigurationen zu ermöglichen. Dies hilft Sicherheitsteams dabei, sich auf wesentliche Risiken zu konzentrieren und gleichzeitig die vollständige Transparenz der Unternehmensinfrastruktur aufrechtzuerhalten.

Dark Web Monitoring

Kontinuierliche Überwachung von Dutzenden von Dark Web-Ressourcen (Foren, Ransomware-Blogs, Messenger, Tor-Websites usw.), um Bedrohungen für Ihr Unternehmen, Ihre Kunden und Ihre Partner und alle Hinweise darauf zu erkennen Analyse aller aktiven gezielten Angriffe sowie von geplanten APT-Kampagnen, die auf Ihr Unternehmen, Ihre Branche oder Ihre Einsatzgebiete abzielen

Erkennen von Datenlecks

Erkennung von kompromittierten Anmeldedaten, Bankkarten, Telefonnummern und anderen vertraulichen Informationen von Mitarbeitern, Partnern und Kunden, die zur Durchführung eines Angriffs verwendet werden oder eine Rufschädigung für Ihr Unternehmen bedeuten können.

Bedrohungserkennung

Überwachung betrügerischer Aktivitäten, die der Reputation Ihres Unternehmens schaden oder Kunden täuschen könnten

Kaspersky Digital Footprint Intelligence ist direkt über das Kaspersky Threat Intelligence Portal verfügbar – eine einheitliche Plattform für den Zugriff auf Bedrohungsdaten, Warnungen und Analysen in Echtzeit.

Funktionsweise

Konfigurieren

Ermitteln von Informationen über die digitalen Ressourcen des Unternehmens

Erfassen

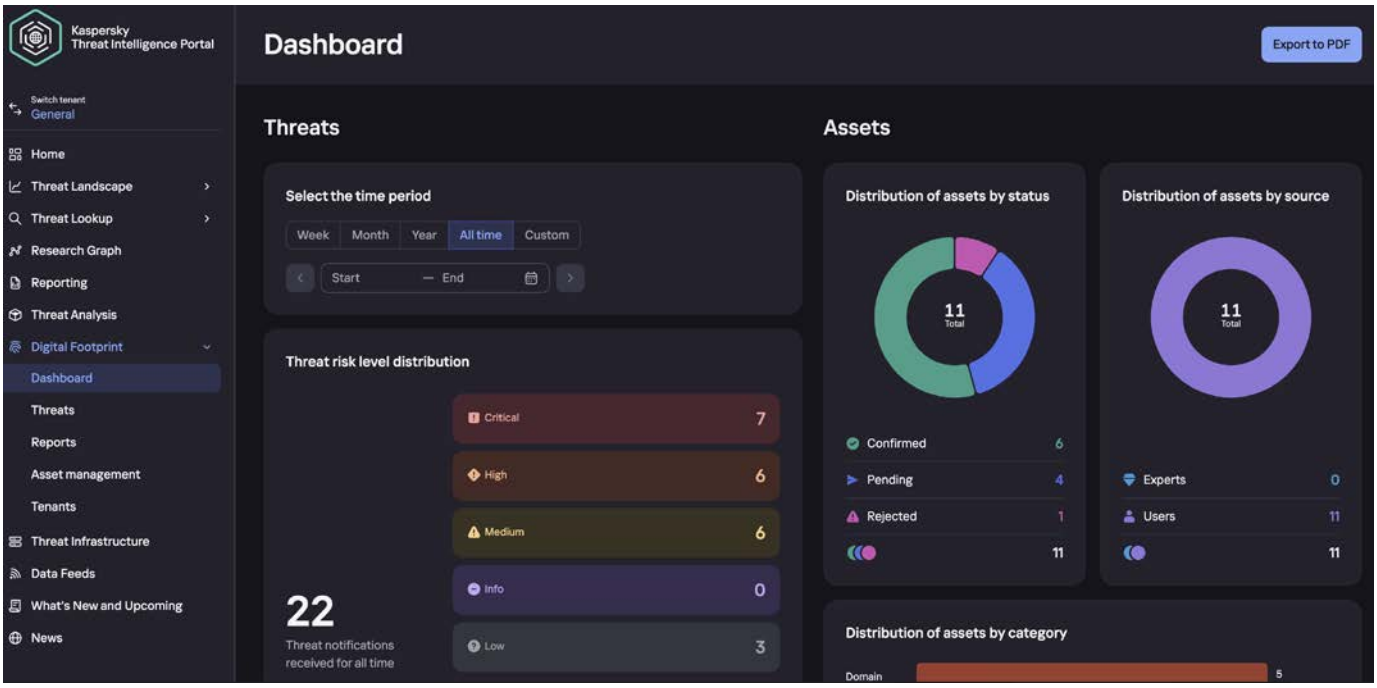
Automatisiertes Erfassen von Daten aus dem öffentlichen Internet, Deep Web und Dark Web sowie aus der Kaspersky-Wissensdatenbank

Reagieren

Bereitstellung von Benachrichtigungen über operative Bedrohungen auf dem Kaspersky Threat Intelligence Portal oder über API

Filter

Von Analysten gesteuerte Erkennung, Analyse und Priorisierung von Bedrohungen



Umfang des Serviceangebots

1. Dashboards mit Zusammenfassungs- und Drilldown-Funktionen
2. Zugriff auf Dark-, Deep- und öffentliche Internetsuchfunktionen
3. Benachrichtigungen über identifizierte Bedrohungen im Threat Intelligence Portal
4. Suchquota in der Kaspersky-Bedrohungsdatenbank (Threat Lookup) inklusive Recherche
5. Präsentationen und Fragerunden mit Experten
6. Integration über API und Möglichkeit zum Export maschinenlesbarer Daten

Zusätzliche Module

7. Von unseren Experten **erstellte Analyseberichte***
8. Unser Takedown Service mindert die Bedrohung durch bösartige Phishing-Domains, gefälschte Social-Media-Konten und gefälschte mobile Apps auf mobilen Marktplätzen
9. Fragen Sie den Analysten Direkter Zugang zu Kaspersky-Sicherheitsexperten auf Einzelfallbasis
10. Brand Monitoring Überwacht die unbefugte Verwendung Ihrer Unternehmensmarke online Identifizierung von Phishing-Websites, gefälschten Social-Media-Konten und -Programmen und anderen betrügerischen Aktivitäten, durch die der Ruf eines Unternehmens geschädigt und/oder Kunden getäuscht werden könnten

Bedrohungsarten

Kaspersky Digital Footprint Intelligence ermöglicht es Unternehmen, Bedrohungen mithilfe von Echtzeitwarnungen schnell zu erkennen und darauf zu reagieren. So werden Risiken für die Reputation der Marke, das Kundenvertrauen und die Geschäftskontinuität minimiert. Alle übermittelten Benachrichtigungen können mit Status und Benutzerzuweisungen verwaltet werden. Dies ermöglicht auch den Austausch von Feedback innerhalb von Gruppenmitgliedern und Kaspersky-Analysten.

Bedrohungen des Netzwerkperimeters

- Falsch konfigurierte Netzwerkdienste
- Ermittlung von Schwachstellen
- Unbrauchbar gemachte oder gefährdete Ressourcen

Bedrohungen aus dem Darknet

- Betrugsversuche und Pläne von Cyberkriminellen
- Verkauf kompromittierter Daten
- Insider-Aktivitäten

Datenlecks

- Gehackte Unternehmensressourcen
- Gehackte Kreditkarten
- Unterwanderte Anmeldedaten

Bedrohungen durch Malware

- Phishing-Angriffe
- Zielgerichtete Angriffe
- APT-Kampagnen

* Verfügbar als Add-on zu Kaspersky Digital Footprint Intelligence

Informationsquellen

Es ist wichtig, dass Sie ein umfassendes Verständnis ihrer externen Sicherheitslage haben.
Um diese Informationen bereitzustellen, beziehen die Sicherheitsanalysten von Kaspersky Informationen aus den folgenden Quellen:

Assets

- IP-Adressen
- IP-Adressbereich
- Domainnamen
- Bankleitzahlen/IIN-Kartennummern
- Keywords
- Markennamen
- Arbeitnehmerinformationen
- Links zu Social Media Accounts
- Links zu Mobile Apps

Quellen

- Netzwerk-Bestandsaufnahme
- Suchmaschinen für das öffentliche Web, Deep Web und Dark Web
- Suche in der Kaspersky-Wissensdatenbank

Leistungen

- Bedrohungshinweise
- Echtzeitsuche in den Bedrohungsinformationen von Kaspersky, im Internet und im Darkweb
- Analytische Berichte*

Der Service im Überblick

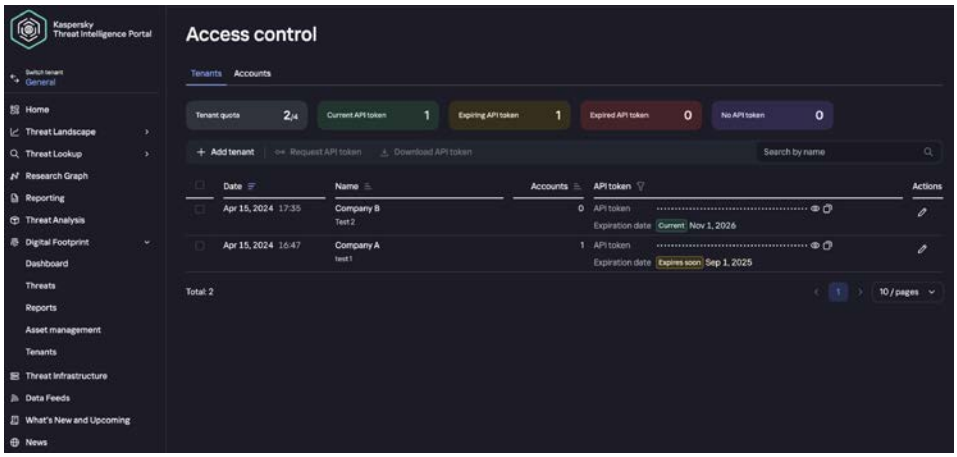
Digital Footprint Intelligence bietet fortschrittliche Funktionen für Managed Security Service Provider (MSSPs) und große Unternehmen mit mehreren Niederlassungen.

Die Schnittstelle des Threat Intelligence Portal von Kaspersky, über die der DFI-Service bereitgestellt wird, ermöglicht MSSPs einen differenzierten Zugriff auf Informationen, die sich entweder auf Tochterunternehmen großer Unternehmen oder auf einzelne Organisationen beziehen, für die Sie als MSSP Security Services anbieten.

Erstellung separater Mandanten und Konfiguration der Zugangskontrolle über den Administrationsbereich

Die Verwaltung erfolgt durch die Erstellung von Mandanten, das sind logische Einheiten, die für jede neue Struktur angelegt werden und separat voneinander verwaltet werden müssen.

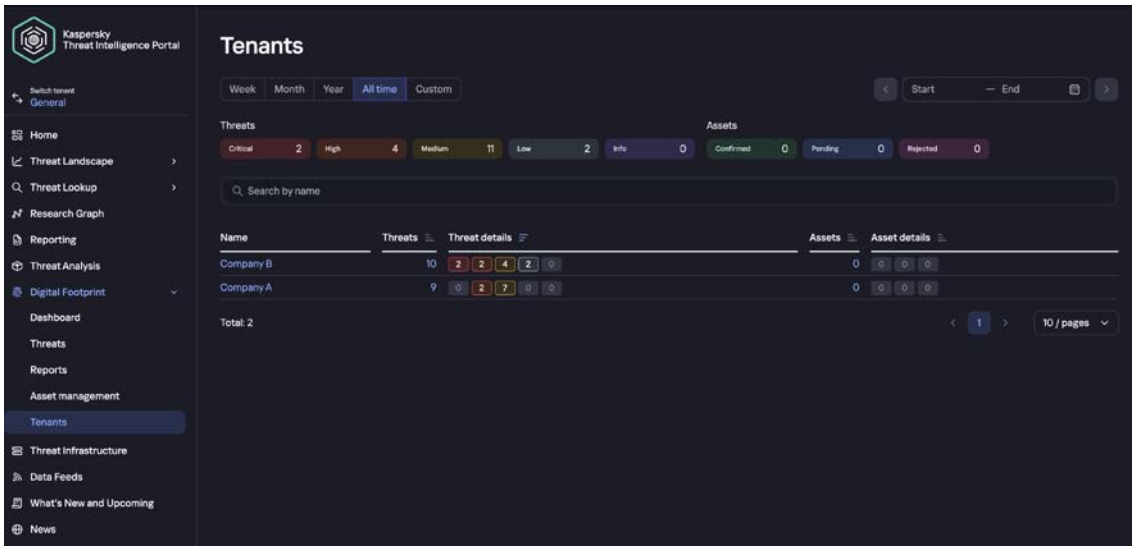
- Zugang zu allen mandantenspezifischen Bedrohungsbenachrichtigungen und Assets
- Nahtloser Wechsel der Mandantengruppe und Anzeige von Informationen im Namen des Mandanten
- Zugangskontrolle durch API-Token und TOTP
- Möglichkeit, Mandantenlizenzen zu ändern



* Add-On-Service

Zentralisierte Statistiken über die Bedrohungen und Assets jedes Mandanten

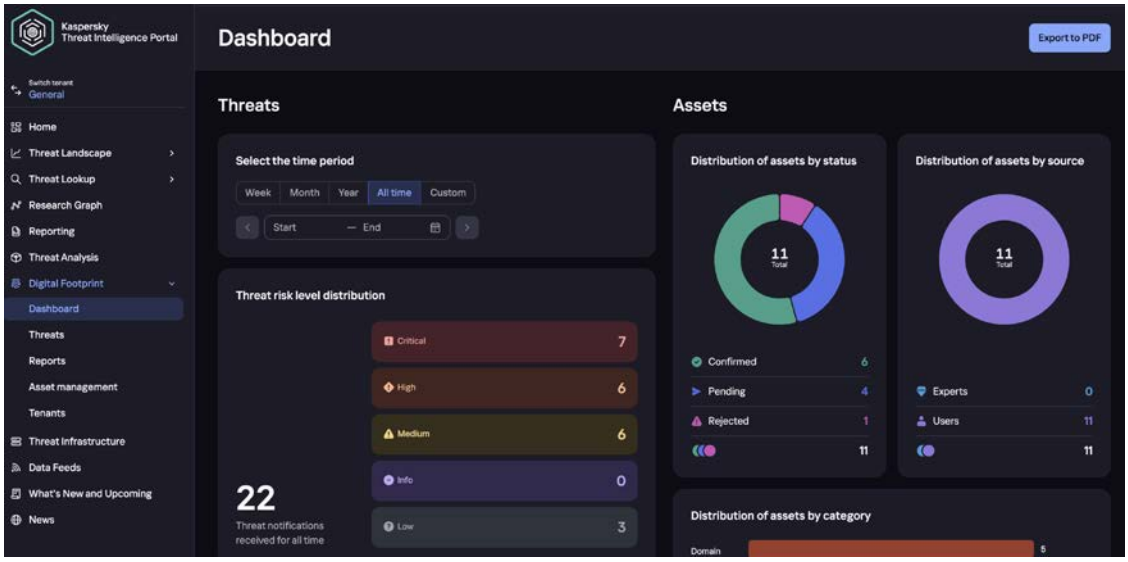
Wenn Sie den Dienst einer großen Anzahl von Organisationen bereitstellen, ist es wichtig, dass Sie über die Tools verfügen, um den aktuellen Status Ihrer Mandanten zu überwachen. Im Mandanten-Center wird für jeden Mandanten eine Zusammenfassung angezeigt, die die Anzahl der erkannten Bedrohungen mit ihrer Kritikalitätsstufe sowie Informationen über die vom Mandanten zu überwachenden Assets und deren Status enthält.



Detaillierte Überwachung

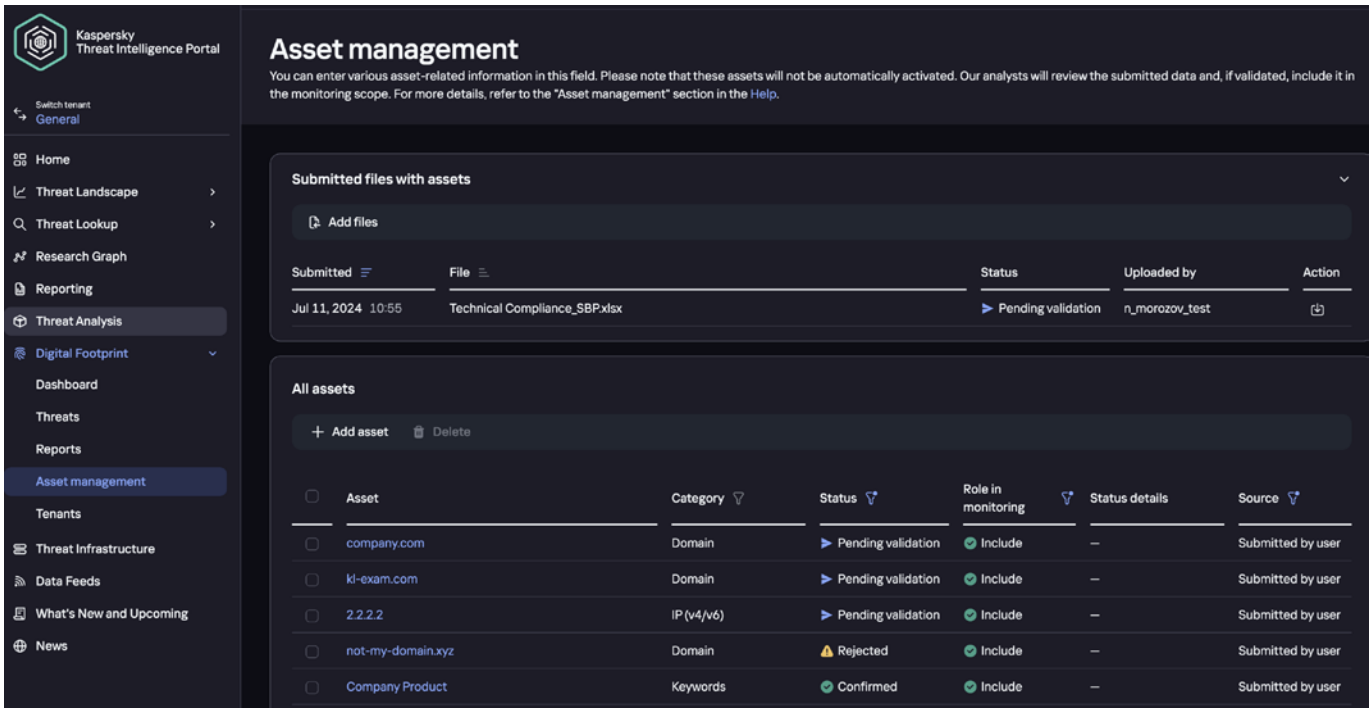
Sie als MSSP oder der Hauptsitz können eine detaillierte Zusammenfassung für jeden Mandanten einsehen:

- Die Gesamtzahl der in einem bestimmten Zeitraum identifizierten Bedrohungen und ihre Kritikalität für die Organisation
- Kategorisierung der entdeckten Bedrohungen
- Die Assets der am stärksten gefährdeten Mandanten
- Die Bedrohungslandschaft unterliegt einem stetigen Wandel



Asset Management

Der Mandant kann neue zu überwachende Assets sowohl separat über die Schnittstelle des Kaspersky Threat Intelligence Portals als auch durch Hochladen von Dateien hinzufügen, wenn es sich um eine große Menge an Assets handelt. Dieser Ansatz vereinfacht den Prozess der Aktualisierung von Assets erheblich.



Unternehmenswerte

Das sind die Vorteile von Kaspersky Digital Footprint Intelligence auf einen Blick:

Schutz Ihrer Marke

Erkennen Sie potenzielle Bedrohungen in Echtzeit, um den Ruf Ihrer Marke zu schützen, das Vertrauen Ihrer Kunden zu bewahren und das Risiko finanzieller Verluste sowie Schäden für den Geschäftsbetrieb zu minimieren.

Senken Sie die Cyberrisiken

Argumentieren Sie überzeugend gegenüber den wichtigsten Stakeholdern (CxO und Vorstand), wohin die Gelder für Cybersicherheit fließen sollten, indem Sie die Lücken im aktuellen System und die damit verbundenen Risiken aufzeigen.

Schneller reagieren

Zusätzlicher Kontext für Sicherheitswarnungen verbessert die Reaktion auf Vorfälle und verkürzt die MTTR (Mean Time To Respond).

Reduzieren Sie die Angriffsfläche

Verwalten Sie die digitale Präsenz Ihres Unternehmens und kontrollieren Sie externe Netzwerkressourcen, um Angriffsvektoren und Schwachstellen, die für Angriffe genutzt werden können, zu minimieren.

Den Gegner kennen

Gefahr erkannt, Gefahr gebannt – Sie müssen wissen, was Cyberkriminelle planen und über Ihr Unternehmen im Darknet sagen.

Blinde Flecken beseitigen

Verbessern Sie Ihre Fähigkeit, Cyberangriffe abzuwehren und Bedrohungen zu erkennen, die den Zuständigkeitsbereich Ihrer internen Sicherheitsteams überschreiten.

Effizienz der Leistungserbringung

Der schnelle Einstieg und die einfache Skalierung im Mehrmandanten-Modus spart sowohl Managed Security Service Providern (MSSP) und Ihren Kunden als auch Großunternehmen mit mehreren Niederlassungen wertvolle Zeit.

Beginnen Sie noch heute mit der Überwachung Ihrer Angriffsfläche und Bedrohungslandschaft über das Kaspersky Threat Intelligence Portal

Besuchen Sie das TIP

Möchten Sie mehr über die verschiedenen Abonnementpläne erfahren? Unser Team steht Ihnen jederzeit gerne zur Verfügung.

Kontakt

Kaspersky Digital Footprint Intelligence

Mehr erfahren

www.kaspersky.de

#kaspersky
#bringonthefuture