Umfassender Service zum Schutz vor digitalen Risiken

Kaspersky Digital Footprint Intelligence

kaspersky bring on the future

Fragen an Experten

Was wäre die beste Methode, einen Angriff gegen Ihr Unternehmen zu starten?

Wie kann man Ihre Organisation 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.

Einleitung

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. Aus dynamischen und verbundenen Umgebungen können Unternehmen erheblichen Nutzen ziehen. Gleichzeitig vergrößert die zunehmende Konnektivität auch die Angriffsfläche. Die 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 zu tracken und auf externe Bedrohungen zu reagieren, die auf exponierte digitale Ressourcen abzielen.

Unternehmen setzen eine Vielzahl von Sicherheitstools ein, doch es gibt digitale Bedrohungen, die sehr spezifische Fähigkeiten erfordern – um Datenlecks aufzuspüren und einzudämmen, um Angriffspläne von Cyberkriminellen in Dark Web-Foren zu überwachen usw. Wir wollen Sicherheitsanalysten unterstützen, Unternehmensressourcen aus dem Blickwinkel des Gegners zu betrachten, potentielle Angriffsvektoren schnell zu erkennen und ihre Verteidigungsstrategie entsprechend auszurichten. Dafür haben wir Kaspersky Digital Footprint Intelligence entwickelt.

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 Internet, dem Deep Web und dem Dark Web zuverlässig erkennen können.

Netzwerk-Erkundung

Identifizierung der Netzwerkressourcen des Kunden und der gefährdeten Dienste, die als Einstiegspunkt für einen Angriff missbraucht werden könnten. Maßgeschneiderte Analyse der vorhandenen Schwachstellen mit Bewertung und umfassender Risikoeinstufung nach CVSS-Schweregrad, Verfügbarkeit von öffentlichen Exploits, Penetration Testing und Standort von Netzwerkressourcen (Hosting/Infrastruktur).

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 Ihr Einsatzgebiet 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.

Erkennung von Bedrohungen

Überwachung betrügerischer Aktivitäten, die dem Ansehen eines Unternehmens schaden und/oder Kunden täuschen können.

Mehrmandantenfähigkeit

Erweiterte Funktionen für Managed Security Service Provider (MSSP) und große Unternehmen mit einer Struktur mit mehreren Zweigstellen.

Funktionsweise

Konfigurieren

Ermittlung von Informationen über die digitalen Ressourcen des Unternehmens

Erfassen

Automatisiertes Sammeln 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. Nützliche Dashboards mit detaillierten Statistiken
2. Suchquote in der Dark Web-Datenbank
3. Bedrohungswarnungen im Threat Intelligence Portal
4. Suchquote in der Social Media-Datenbank
5. Präsentationen und Fragerunden mit Experten
6. Maschinenlesbare Daten
7. Von unseren Experten erstellte Analyseberichte*
8. Takedown-Anfragen*

*Add-On-Service

Bedrohungs-arten

Kaspersky Digital Footprint Intelligence bietet Warnhinweise in Echtzeit, damit Unternehmen schnell und effizient auf potenzielle Bedrohungen reagieren können. Damit sinkt die Wahrscheinlichkeit, dass der Ruf der Marke, das Vertrauen der Kunden und das gesamte Business Schaden nehmen. Unternehmen können die Monitoring-Features gezielt an ihren Bedarf anpassen. Umfassende Berichte und Analysen geben wertvolle Einblicke in den Umfang und die Auswirkungen von Verstößen gegen Handelsmarken und andere potenziellen Risiken.

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

Informations-quellen

Es ist wichtig, dass unsere Kunden einen umfassenden Überblick über ihre externe Sicherheitslage gewinnen. Um diese Informationen bereitzustellen, arbeiten die Sicherheitsanalysten von Kaspersky mit Informationen aus den folgenden Informationsquellen:

Ihre unstrukturierten Daten

- IP-Adressen
- Unternehmensdomains
- Markennamen
- Keywords
- IP-Adressbereich
- Bankleitzahlen/IIN-Kartennummern
- Arbeitnehmerinformationen

Netzwerk-Bestandsaufnahme

Suche im Surface, Deep und Dark Web

Suche in der Kaspersky-Wissensdatenbank

Bedrohungshinweise

Echtzeitsuche in den Bedrohungsinformationen von Kaspersky, im Internet und im Darkweb

Takedown-Anfragen*

Analytische Berichte*

Fähigkeiten zur Servicebereitstellung

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

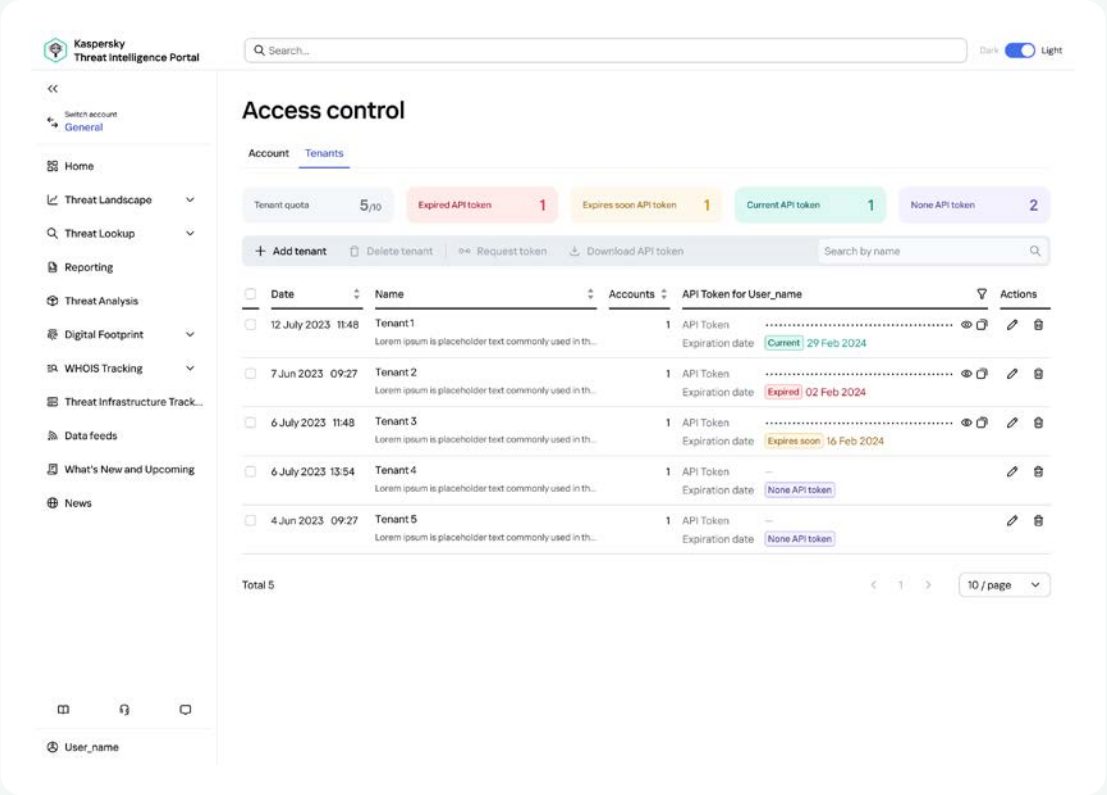
Die Schnittstelle des Threat Intelligence Portal von Kaspersky, über die der DFI-Service bereitgestellt wird, ermöglicht MSSP einen differenzierten Zugriff auf Informationen, die sich entweder auf Tochterunternehmen großer Unternehmen oder auf einzelne Organisationen beziehen, für die MSSP Sicherheitsmanagementservices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

Erstellung separater Mandanten und Konfiguration der Zugangskontrolle über den Administrationsbereich

Die Verwaltung erfolgt durch die Schaffung von Mandanten – logische Einheiten, die für jede neue Struktur geschaffen werden und die getrennt von den anderen verwaltet werden müssen.

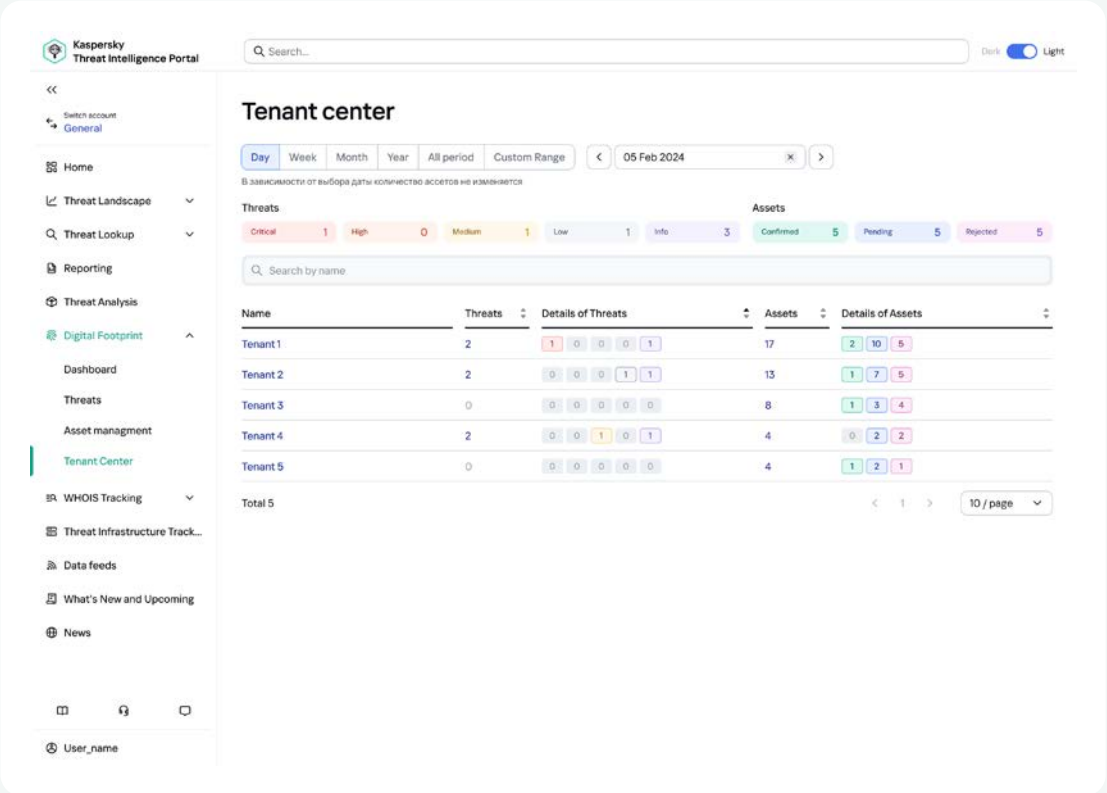
1. Zugang zu allen mandantenspezifischen Bedrohungsbenachrichtigungen und Assets
2. Nahtloser Wechsel der Mandantengruppe und Anzeige von Informationen im Namen des Mandanten
3. Zugangskontrolle durch API-Token und TOTP
4. Möglichkeit, Mandantenlizenzen zu ändern

*Add-On-Service



Zentralisierte Statistiken über die Bedrohungen und Assets jedes Mandanten

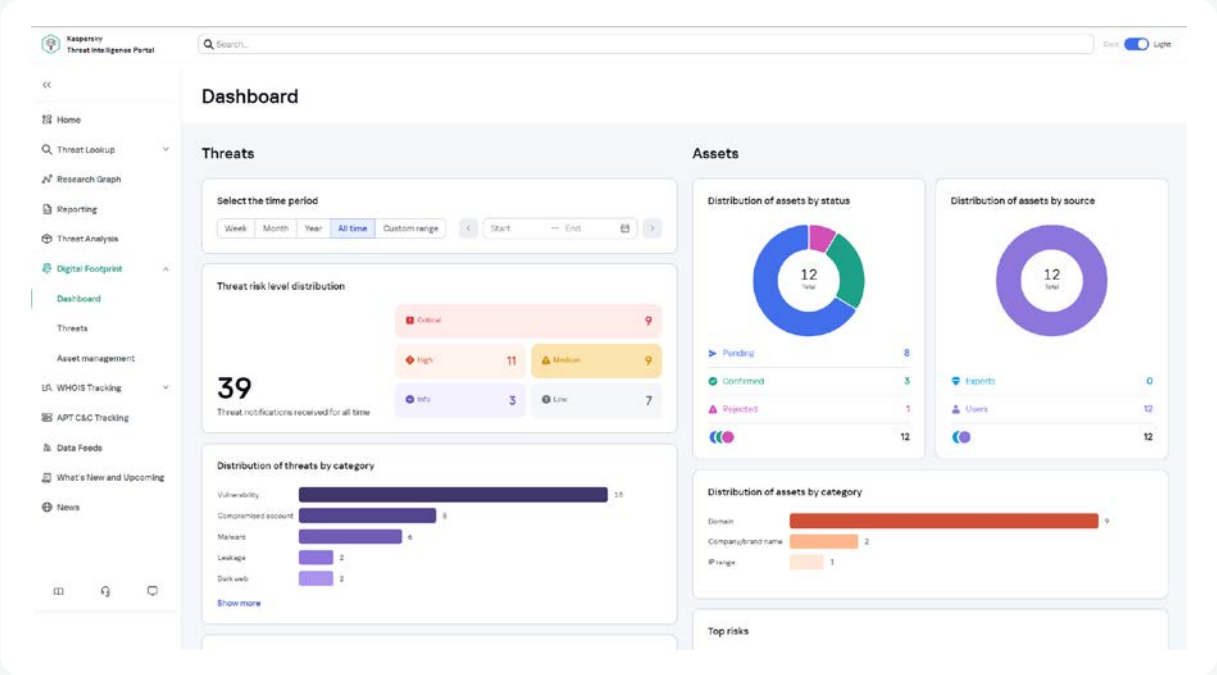
Da der Service für eine große Anzahl von Organisationen erbracht wird, sind Instrumente zur Überwachung des aktuellen Zustands der Mandanten erforderlich. Das Mandanten-Center zeigt eine Zusammenfassung für jeden Mandanten an, einschließlich der Anzahl der erkannten Bedrohungen mit ihrer Kritikalitätsstufe, sowie Informationen über die Assets, die die Mandanten überwachen möchten.



Detaillierte Überwachung

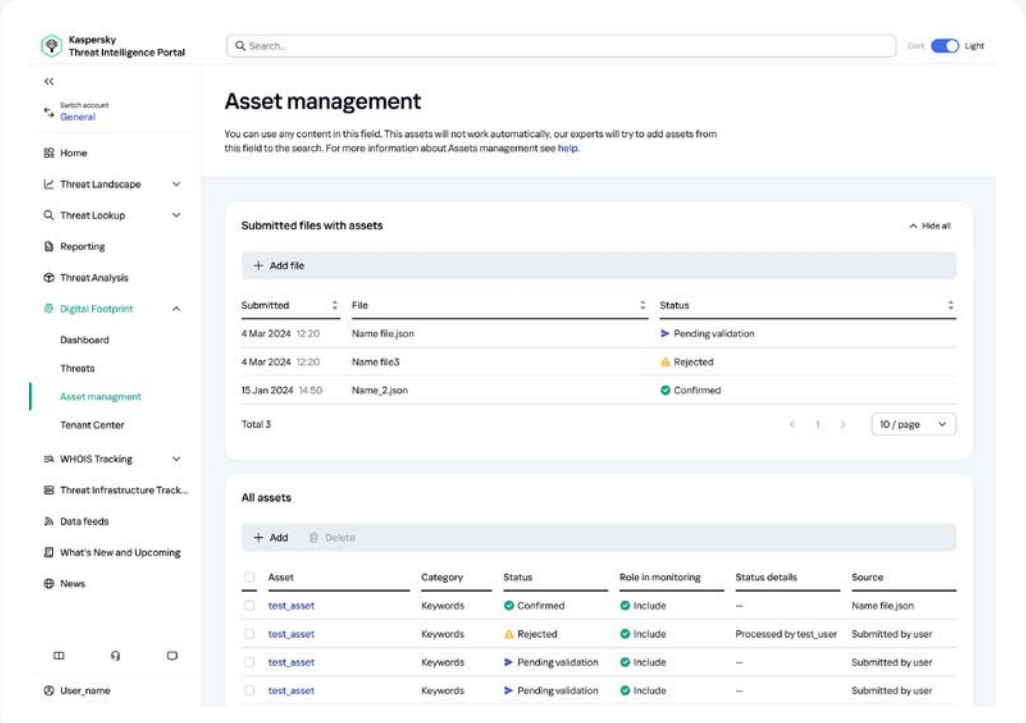
MSSP oder die Zentrale können eine detaillierte Zusammenfassung für jeden Mandanten einsehen:

- Die Gesamtzahl der in einem bestimmten Zeitraum identifizierten Bedrohungen und ihre Kritikalität für die Organisation
- Kategorisierung der entdeckten Bedrohungen
- Die Assets der schwächsten Mandanten
- Bedrohungslandschaft verändert sich mit der Zeit



Asset Management

Der Mandant kann neue Assets zur Überwachung hinzufügen, sowohl separat über die Schnittstelle des Threat Intelligence Portals von Kaspersky als auch durch Hochladen von Dateien mit einer großen Anzahl von Assets. Dieser Ansatz vereinfacht den Prozess der Aktualisierung von Assets erheblich.



Geschäftswerte

Kaspersky Digital Footprint Intelligence bietet zahlreiche Vorteile und einen erheblichen Mehrwert für Ihr Unternehmen:

Schutz Ihrer Marke

Erkennen Sie potenzielle Bedrohungen in Echtzeit, um den Ruf Ihrer Marke zu schützen, das Vertrauen Ihrer Kunden zu wahren und das Risiko von finanziellen Verlusten und Schäden für den Geschäftsbetrieb zu senken.

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

Vorbereitung ist alles. Sie müssen wissen, was Cyberkriminelle planen und über Ihr Unternehmen im Darknet sagen.

Weiße Flecken beseitigen

Verbessern Sie Ihre Fähigkeit, Cyber-Angriffe abzuwehren und Bedrohungen zu erkennen, die über den Zuständigkeitsbereich Ihrer internen Sicherheitsteams hinausgehen.

Effizienz bei der Servicebereitstellung

Der schnelle Start und die einfache Skalierung im Mehrmandanten-Modus spart Zeit, sowohl für Managed Security Service Provider (MSSP) und ihre Kunden als auch für große Organisationen mit mehreren Niederlassungen.

Für weitere Informationen zu den unterschiedlichen Abonnement-Tarifen wenden Sie sich bitte an unser Team

Kontakt

Kaspersky Digital Footprint Intelligence

Mehr erfahren

www.kaspersky.de

#kaspersky
#bringonthefuture