Kaspersky Digital Footprint Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky Digital Footprint Intelligence

Ihr Unternehmen wächst. Aber gleichzeitig nimmt auch die Komplexität Ihrer verteilten IT-Umgebung zu; eine große Herausforderung, wenn es darum geht, Ihre weit verteilte digitale Präsenz ohne direkte Kontrolle oder entsprechende Zuständigkeiten zu schützen. Dank dynamischer und verbundener Umgebungen können Unternehmen erheblichen Nutzen ziehen. Gleichzeitig bietet die wachsende Konnektivität eine immer größer werdende Angriffsfläche. Und weil die Angreifer immer raffinierter werden, brauchen Sie nicht nur einen präzisen Einblick in die Online-Präsenz Ihrer Organisation, sondern müssen auch Veränderungen nachverfolgen und schnell entsprechend reagieren können.

Auch wenn Organisationen schon eine breite Palette an Sicherheitstools einsetzen, sind sie noch lange nicht vor jeder digitalen Bedrohung geschützt: Funktionen zur Erkennung und Eindämmung von Insider-Aktivitäten, Pläne und Angriffsszenarien von Cyberkriminellen in Darknet-Foren usw. Damit Sicherheitsanalysten Unternehmensressourcen aus dem Blickwinkel des Gegners betrachten, potentielle Angriffsvektoren schnell erkennen und ihre Verteidigungsstrategie entsprechend ausrichten können, hat Kaspersky die Kaspersky Digital Footprint Intelligence entwickelt.

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 ggf. bereits stattgefundene bzw. geplante Angriffe nach.

Das Produkt bietet:

- Netzwerkperimeter-Bestandsaufnahme ohne Störung des laufenden Betriebs, um zu ermitteln, welche kundenseitigen Netzwerkressourcen und offen zugänglichen Services potentielle Angriffspunkte darstellen. Dazu gehören unter anderem versehentlich im Perimeter belassene Verwaltungsschnittstellen oder unzureichend konfigurierte Services, Geräteschnittstellen etc.
- 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).
- Identifizierung, Überwachung und Analyse aller aktiven oder geplanten zielgerichteten Angriffe auf Ihr Unternehmen, Ihre Branche oder Region abzielende APT-Kampagnen.
- Die Erkennung von Bedrohungen, die sich speziell gegen Ihre Kunden, Partner und Abonnenten richten, deren infizierte Systeme dann für Angriffe auf Ihr Unternehmen genutzt werden könnten.
- Diskrete Überwachung von Pastebin-Seiten, öffentlichen Foren, Blogs, Instant-Messaging-Kanälen, im Untergrund tätige, geheime Online-Foren und -Communities; Ermittlung von möglicherweise gefährdeten Konten, Datenlecks oder Angriffen auf Ihre Organisation, die in diesen Foren geplant und diskutiert werden.

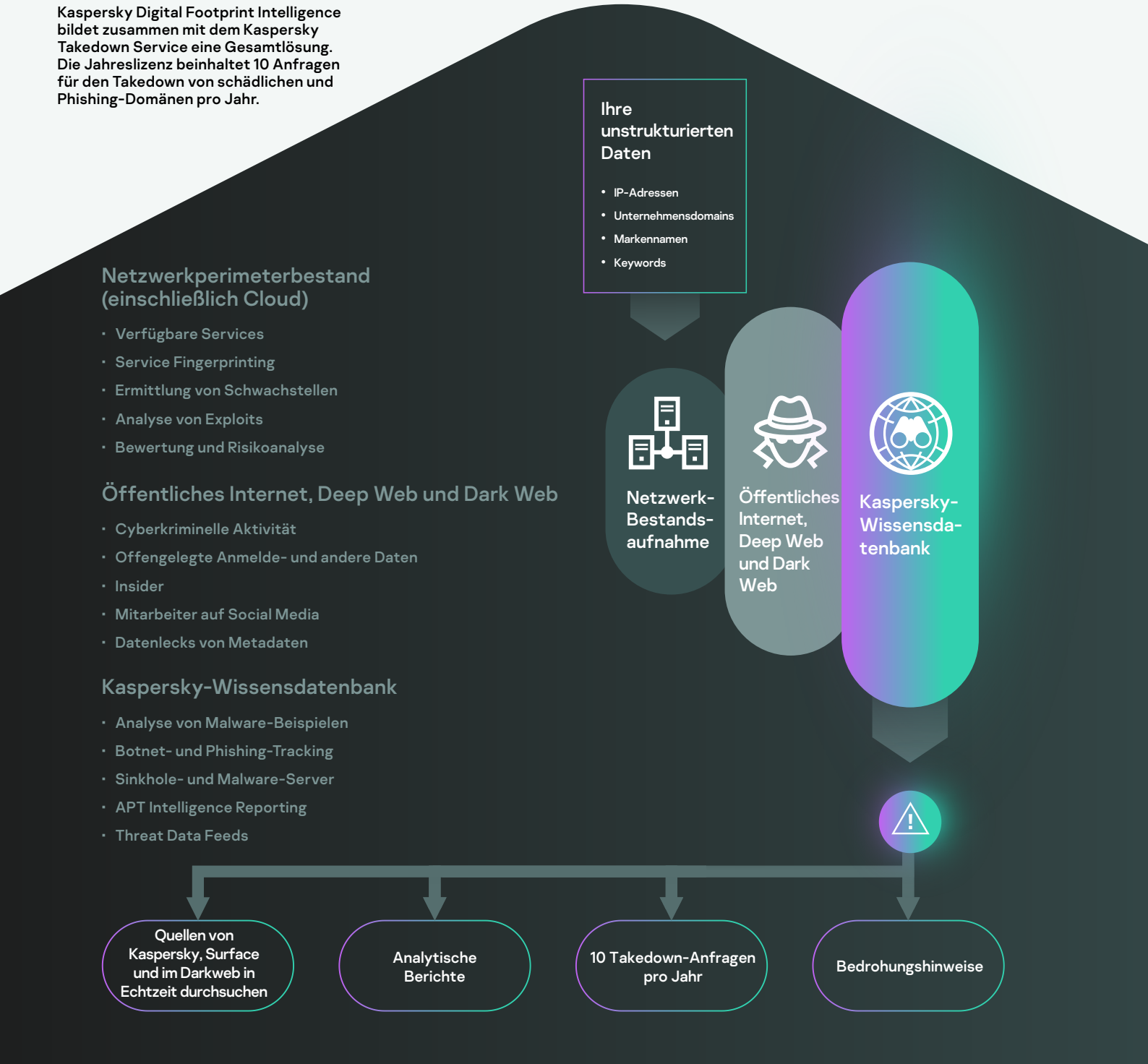
Wichtigste Vorteile

Kaspersky Digital Footprint Intelligence verwendet OSINT-Techniken in Kombination mit automatisierten und manuellen Analysen des öffentlichen Internets, Deep Web und Dark Web. Zusammen mit der internen Wissensdatenbank von Kaspersky erhalten Sie praktisch umsetzbare Einblicke und Handlungsempfehlungen

Das Produkt ist auf dem Kaspersky Threat Intelligence Portal verfügbar. Sie könnnen vier Quartalsberichte mit jährlichen Warnmeldungen zu Bedrohungen in Echtzeit oder einen Einzelbericht mit Warnungen, der sechs Monate lang aktiv ist, kaufen.

Durchsuchen Sie das öffentliche Internet und Dark Web nach Informationen in Echtzeit zu globalen Sicherheitsereignissen, die Ihre Assets bedrohen, sowie nach sensiblen Daten in geheimen Untergrund-Communities und Foren. Die Jahreslizenz umfasst 50 Suchen pro Tag über externe Quellen und die Wissensdatenbank von Kaspersky hinweg.

Kaspersky Digital Footprint Intelligence bildet zusammen mit dem Kaspersky Takedown Service eine Gesamtlösung. Die Jahreslizenz beinhaltet 10 Anfragen für den Takedown von schädlichen und Phishing-Domänen pro Jahr.



www.kaspersky.de