Cyberint

INTELLIGENTE DIGITAL-RISIKO-PROTEKTION

Intelligente Digital-Risiko-Protektion

Cyberint baut auf einer einzigartigen Kombination aus der firmeneigenen Bedrohungserkennungs-Plattform Argos™ und äußerst erfahrenen Bedrohungserkennungs-Analysten, und bietet damit eine neue Herangehensweise der Digital-Risiko Protektion (DRP) an, um folgende Herausforderungen zu lösen:

Ermitteln der relevanten Bedrohungen, die erwogen werden sollten, um ein effizientes Cyber-Sicherheits-Abwehrprogramm zu erstellen

Den aktuellen Cyber-Risiko-Stand der Geschäftsführung und dem Management mit einem klaren Aktionsplan darstellen

Prädiktive Analysen erwerben, um Absichten, Techniken und Werkzeuge zu identifizieren und Bedrohungen gezielt vor Eintritt zu entschärfen

Ständig die Aussetzung gegenüber Digital-Risiken überwachen, die von Cyberkriminellen ausgenutzt werden können

Sicherheitslücken aufdecken, die sich außerhalb des Unternehmensbereichs ausbreiten

Einsicht in Angriffe erhalten, die auf Ihre Marke oder Kunden abzielen und sich außerhalb Ihres Netzwerkes entwickeln

Unternehmensherausfo Rderungen, Die Cyberint Berücksichtigt:

- Markenschutz
- Cyber-Risiko Gegenüber Drittpersonen
- Digital-Risiko-Angriffsflä Chen-Überwachung
- Betrug
- Entdeckung Von Datenverlusten
- Entdeckung Von
- Cyber-Attacken
- Überwachung Des Dark Web
- Bedrohungserkennung

Cyberint-Angebot

Argos™ Technologie

Bedrohungserkennung

Überwachung Des Dark Web

Risiko-Angriffsflächen-Kartierung

Kriminaltechnische Leinwand
(Forensic Canvas)

Erkennung Und Entfernung Von
Phishing-Betrügereien

Managed Service

Gezielte Überwachung

Virtuelles Humint

Tiefgründige Ermittlungen

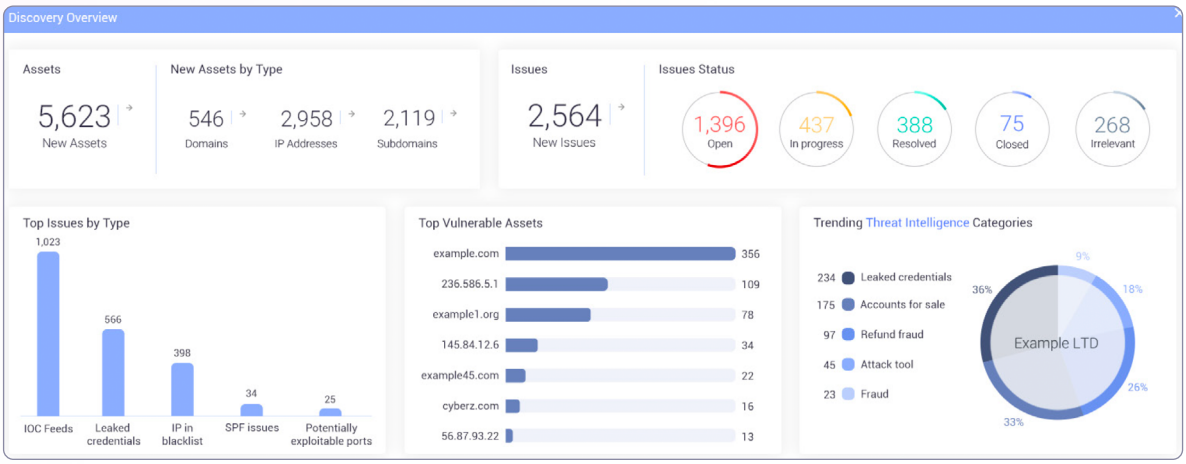
Analyse Der
Bedrohungslandschaft

Argos™ Intelligente Digital-Risiko-Protektions-Plattform

Argos™ ist eine Multi-Mandanten-SaaS-Plattform mit zahlreichen Modulen:

Angriffsflächen-Kartierung

Die Argos™-Angriffsflächen-Kart-ierung erstellt die Digitalbilanz der Organisation, überwacht ständig Unternehmensdaten auch außerh-alb der Organisationsgrenzen, gibt einen Überblick dieser Unterneh-mensdaten in Form von anzugehen-den Problemen, die nach Schwere priorisiert sind, und hebt damit verbundene Bedrohungen, Verlet-zlichkeiten und Schwächen hervor.



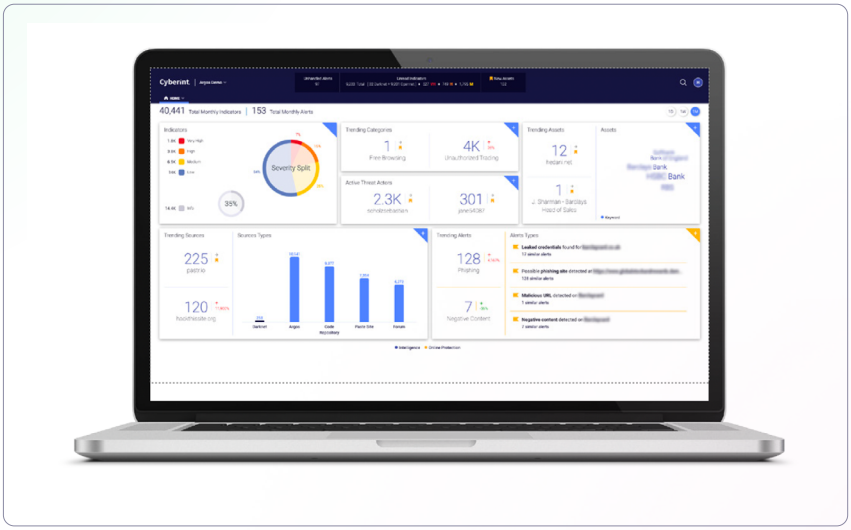
Argos™ Digital-Risiko-Protektions-Plattform, Angriffsflächen-Überwachung

Datensammlung Und -Analyse Zur Bedrohungserkennung

Die Echtzeitüberwachung tausender Gefahrenquellen im zugänglichen, Deep und Dark Web führt zur Erfassung von Millionen Nachrichtengegenständen pro Tag im internen Datensee von Argos™.

Rohdaten werden automatisch mit Unternehmensdaten korreliert (IP-Adressen, Domänen, Marken, Manager usw.) und nach Anwendungsfällen klassifiziert: Phishing, Malware-Kampagnen, Ausfüllen von Berechtigungsnachweisen, Missbrauch von Datenverlusten usw. Mithilfe des firmeneigenen Maschinenlernalgorithmus von Cyberint werden Rohdaten nach potentiellen Risiken und Auswirkungen priorisiert, was eine intelligente und kosteneffiziente Analyse erlaubt.

Automatische und halb-automatische Analysemaschinen erzeugen umsetzbare Warnhinweise, die anschließend an die Sicherheitsteams verbreitet werden mit tiefgründigen Analysen, bereichertem Kontext, Profilen der Bedrohungsakteure usw., damit das Unternehmen wirksame Aktionen ergreifen kann.

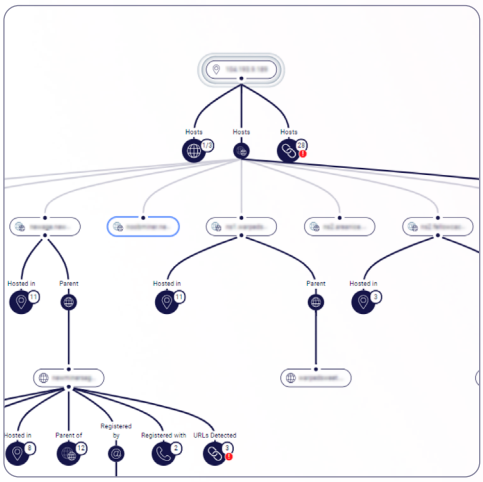


Argos™ Digital-Risiko-Protektions-Plattform

Kriminaltechnische Leinwand „Forensic Canvas“

Das Modul der kriminaltechnischen Leinwand „FORENSIC CANVAS“ von Cyberint erlaubt die Identifizierung und die Profilerstellung von Bedro-hungsakteuren sowie die tiefgrün-dige Untersuchung der verwendeten Tools, Taktiken und Prozeduren (TTPs).

Die kriminaltechnische Leinwand wird verwendet, um den Kontext spezieller oder vielfacher IOCs anzureichern und um zahlreiche Dienste in einer vereinten Untersu-chungsplattform zusammenzufassen, wie die Bedrohungserkennung von Argos™, WHOIS-Diensten, passiver DNS, Sozialbefunden, Mal-ware-Erkennung usw.



Argos™ Digital-Risiko-Protektions-Plattform, kriminaltechnische Leinwand

Proaktive Phishing-Erkennungs-Technologie Und Entschärfung

Phishing bleibt ein wesentliches Risiko für digitale Organisationen, resultiert in Kontenübernahmen und führt zu Kundenverlust und negativem Einfluss auf den Markenruf. Als Antwort auf diese Bedrohung hat Cyberint den Phishing-Leuchtturm entwickelt, ein firmeneigenes Modul, das in Echtzeit neu errichtete Phishing-Websites entdeckt, die den Inhalt einer Unternehmens-Website klonieren — eine effektive und häufig von Bedrohungsakteuren verwendete Technik. Die Schnellerkennung von Cyberint erlaubt es uns, Phishing-Websites im Namen des Unternehmens rasch zur Strecke zu bringen und damit die Gefahr rasch zu eliminieren.

Vorteile Für Sie

- Verringern Schattenhafter It-Sicherheits-Risiken
- Überblick Ihrer Angriffsfläche Erlangen
- Verkürzen Der Verweilzeit Der Bedrohung
- Erweitern Der Fähigkeiten Ihres Teams
- Reduzieren Der Gesamtbetriebskosten Der Cybersicherheit

Managed Service

**Maßgeschneiderte Cyber-Nachrichtendienste,
die Ihren Anforderungen entsprechen.**

Cyberint bietet ein verwaltetes Digital-Risiko-Protektions-Programm, das Zugang zu unserer Argos™- Plattform und einem Team aus Cyber-Bedrohungs-Analysten liefert, und damit jedes CTI-Programm auf eine höhere Qualitäts- und Leistungsstufe bringt. Die Partnerschaft mit dem Analystenteam von Cyberint umfasst tägliche Interaktionen mit einem für Sie gewidmeten Analysten, der ein Mitglied Ihres hausinternen Teams wird. Analysten werden aufgrund ihrer Kenntnisse der Industriebranche und ihrem intimen Verständnis der Unternehmensanforderungen zugewiesen.

Alle Rohdaten, die Argos™ ans Licht bringt, werden sorgfältig überprüft, in Zusammenhang gebracht und reellen Risiken zugeschrieben, und zwar unter Verwendung riesiger Datenmengen, die im zugänglichen, Deep und Dark Web gesammelt wurden.

Unser Analystenteam ist mehrsprachig und versteht daher die Bedrohungsakteure in ihrer jeweiligen Sprache. Außerdem meistert der Analyst das „Kauderwelsch“ und die Kultur der Cyberkriminellen und erlaubt Ihnen, Bedrohungen zu identifizieren, zu überprüfen und abzuwehren, die sich mit aller Wahrscheinlichkeit zu Angriffen entwickeln.

Cyberint liefert ein wertvolles menschliches Element bei den Such, Ermittlungs- und Bedrohungserkennungs-Tätigkeiten. Die virtuellen HUMINT-Fähigkeiten, d. h. Live-Interaktionen mit Bedrohungsakteuren, erlauben eine tiefgründigere Kontextualisierung, die für eine wirksame Abwehr erforderlich sind.

Cyberint-Forschung

Das Cyber-Forschungsteam von Cyberint erkundet die äußersten Grenzen der Cyber-Bedrohungslandschaft, um eine strategische Einsicht in die Bedrohungstrends zu gewinnen. Das Cyber-Forschungsteam analysiert astronomische Datenmengen, um strategische Bedrohungserkennungsberichte zu erstellen, damit Entscheidungsträger aussagekräftige Trends identifizieren können und einen breiteren und tieferen Blickwinkel der Digitalrisiken erlangen, die auf ihr Unternehmen abzielen. Der Bericht umfasst periodische Analysen der aktuellen Sektorenrisiken, nennenswerte Bedrohungsakteure, TTP-Analyse usw.

Aktuelle Berichte Von Cyberint

Finanzindustrie der Philippinen
Bericht der
Bedrohungslandschaft

Herunterladen

REvil – Stehlen, Verschlüsseln & Versteigern
Forschungsbericht

Herunterladen

Gezielte Erpressungssoftware-Attacken in Taiwan
Forschungsbericht

Herunterladen

Vorteile Einer Partnerschaft Mit Den Verwalteten Bedrohungserkennungs-Diensten Von Cyberint

Bedrohungserkennung
Erkennt Bedrohungen mittels prädiktiver Intelligenz

Bestimmen Der Schwere
Bestimmen Sie die Schwere von Bedrohungen und verstehen Sie das Gesamtbild

Betrugstätigkeiten Bestimmen
Bestimmen und erhalten Sie umsetzbare Informationen zur Reaktion und Abwehr

Echtzeiterkennung Von Phishing
Echtzeitentdeckung von Phishing-Websites und Entschärfungsaktionen

Virtuelle Humint-Fähigkeiten
Kommunizieren Sie direkt mit Bedrohungsakteuren, schreiben Sie deren Aktivitäten speziellen Kampagnen zu und erhalten Sie mehr Kontext und Informationen

Vip-Bedrohungs-Ermittlungen
Überwachen Sie die Online Präsenz Ihrer Manager, um Bedrohungsakteuren den Zugang zu persönlichen Informationen zur böswilligen Verwendung zu verwehren

Echtzeiterkennung Von Phishing
Kartieren und überwachen Sie die Digitalpräsenz des Unternehmens, wie den Verlust von Berechtigungsnachweisen, digitalen Verwundbarkeiten und sensitiven Verlusten von Dokumenten

Unsere Kunden Über Uns

> Vor allem der Managed Service ist von Wert, da er Funde in relevante Informationen und Warnungen umwandelt, die auf unser Unternehmen maßgeschneidert sind.
>
> Großer Händler in den USA

> Bevor Sie Cyberint verwenden, haben Sie kein wirkliches Verständnis davon, wer Ihr Unternehmen angreift.
>
> Großer e-Kommerz-Händler in den USA

Gartner peerinsights™ **4.8** ★★★★★

Nehmen Sie Kontakt Mit Uns Auf

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA
214 W 29th St.
New York, 10001
Tel: +1-646-568-7813

SINGAPUR
135 Cecil St. #10-01 MYP
PLAZA 069536
Tel: +65-3163-5760

ISRAEL
17 Ha-Mefalsim St.
4951447 Petah Tikva
Tel: +972-3-7286-777

GROSSBRITANNIEN
14 Grays Inn Rd., Holborn
WC1X 8HN, London
Tel: +44-203-514-1515