DeTCT
BY CYFIRMA

DATENBLATT

DeTCT™

DeTCT ist eine Plattform zur Erkennung **digitaler Risiken.** *Sie bietet Unternehmen die Möglichkeit, ihren digitalen Fußabdruck in Echtzeit zu erkennen, um so Angriffsoberflächen, anfällige Systeme, Datenlecks sowie Markenrechtsverletzungen aufzudecken und zu verhindern, dass sich Betrüger als Führungskräfte ausgeben. DeTCT* **überwacht proaktiv und 24/7** *das Dark Web, das Surface Web und die Social Media-Plattformen, damit Sie sich ganz auf das Wachstum Ihres Unternehmens konzentrieren können.*

Von Social-Engineering-Kampagnen über Ransomware bis hin zu Angriffen auf die Software-Lieferkette gibt es heute für Cyberkriminelle mehr Möglichkeiten denn je, an Ihre sensiblen Daten, wie etwa Ihr geistiges Eigentum oder Ihre Kunden- und Finanzdaten, zu gelangen und Ihr Unternehmen in Gefahr zu bringen.

Haben Sie alle externen IT-Assets im Blick?
Wissen Sie, ob Ihre Systeme und Anwendungen anfällig für Angriffe sind?
Sind Ihre Software-Patches auf dem neuesten Stand?
Ist Ihr Unternehmen eine Zielscheibe für Phishing-Kampagnen?
Sind Ihre Daten nach außen durchgesickert?
Ist Ihre Marke einem Angriff ausgesetzt?
Befinden sich Ihre sensiblen Informationen auf öffentlichen oder sozialen Plattformen?
Wissen Sie genau, was zu tun ist, um Ihre Schwachstellen zu beheben?

DeTCT gibt Antworten auf all diese Fragen. DeTCT wurde entwickelt, um dem zunehmenden Risiko digitaler Bedrohungen zu begegnen, sodass Sie stets über Ihren digitalen Fußabdruck, Datenlecks, Sicherheitsverletzungen und Identitätsmissbrauch informiert sind. DeTCT überwacht Ihr digitales Profil kontinuierlich und verschafft Ihnen in Echtzeit Klarheit darüber, wie hoch Ihr Risiko ist.
Mit diesem Wissen sind Sie bestens gewappnet, um die richtigen Abhilfemaßnahmen zum Schutz Ihres Unternehmens zu ergreifen.

DeTCT wurde speziell für die zunehmenden digitalen Risiken entwickelt, mit denen folgende Führungskräfte konfrontiert sind:

CEO/CFO
„Wie hoch ist mein Risiko? Ist mein Unternehmen in irgendeiner Weise bedroht? Halte ich mich an die Vorschriften und Richtlinien?“

Business- und Marketing-Team
„Ist meine Marke einem Angriff ausgesetzt? Gibt es Verstöße oder Fälle von Identitätsmissbrauch, die das Vertrauen der Stakeholder beeinträchtigen könnten?“

IT-Team
„Habe ich meine Angriffsoberfläche vollständig im Blick? Was sind meine kritischsten Schwachstellen? Was muss ich tun, um meine Sicherheitskontrollen zu verbessern?“

1

ERKENNUNG DER ANGRIFFSOBERFLÄCHE

Identifizierung von möglichen Einstiegspunkten in das Unternehmen

Unternehmensergebnisse: *Kontinuierliche Überwachung in Echtzeit zur Erkennung von Schatten-IT oder durchlässigen Systemen, die Zugriffsmöglichkeiten für Cyberkriminelle bieten.* **Wenn Sie die Angriffsoberfläche kennen, können Sie eine realistische Kosten-Nutzen-Analyse für jedes Asset durchführen und entscheiden, wie Sie Ihre Angriffsoberfläche minimieren können.**

2

INTELLIGENTE SCHWACHSTELLENANALYSE

Einstiegspunkte, die von Cyberkriminellen genutzt werden können

Unternehmensergebnisse: *Die Schwachstellen werden den Assets und den zugehörigen Exploits zugeordnet und nach ihrer Kritikalität eingestuft.* **So kann das Unternehmen seine Ressourcen optimieren und sich auf die wichtigsten und dringlichsten Lücken konzentrieren.**

3

INTELLIGENTE ERKENNUNG VON MARKENINFORMATIONEN

Erkennen Sie, wann Ihre Marke einem Angriff ausgesetzt ist

Unternehmensergebnisse: *Verstehen Sie, wer ihre Marke im Visier hat, warum und wie dies geschieht, und verschaffen Sie sich einen vollständigen Überblick über Markenrechtsverletzungen.* **Schützen Sie Ihre Marke und erhalten Sie sich Ihre Kundentreue, indem Sie sicherstellen, dass sie nicht durch Wirtschaftsspionage, Insider-Bedrohungen oder andere Akteure beeinträchtigt wird, die in böswilliger Absicht handeln.**

4

SCHUTZ VOR DIGITALEN RISIKEN

Mehr Klarheit über digitale Profile, Datenlecks, Datenschutzverletzungen und Identitätsmissbrauch

Unternehmensergebnisse: *Decken Sie digitale Fußabdrücke und Fälle von Identitätsmissbrauch sowie Datenlecks auf. Erhalten Sie in nahezu Echtzeit eine Warnung, wenn Ihre Daten nach außen durchsickern.* **Mit diesem Wissen, lässt sich die Lücke schließen und weiterer Image- und finanzieller Schaden abwenden.**

5

ERKENNUNG UND ÜBERWACHUNG VON RISIKEN VON DRITTANBIETERN

Entdecken Sie Schwachstellen in den digitalen Assets Ihres Lieferanten.

Unternehmensergebnisse: *Erstellen Sie ein digitales Risikoprofil des Unternehmens und erfahren Sie, ob es Datenlecks, Schwachstellen und andere Probleme gegeben hat.* **Machen Sie sich das Cyber-Risiko von Drittanbietern bewusst und erkennen Sie, welche Folgen dies für Ihr Unternehmen haben könnte.**

HAUPTMERKMAL	BESCHREIBUNG	VORTEILE
ERKENNUNG DER ANGRIFFS-OBERFLÄCHE	▪ *Proaktive Identifizierung von ungeschützten externen Assets, Schatten-IT und übersehenen Systemen, die von Cyberkriminellen ausgenutzt werden können.* ▪ *Erstellen Sie ein effektives und effizientes Programm zur Verwaltung der Angriffsoberfläche mit kontinuierlichen Überwachungsfunktionen.*	▪ *Mit einem genauen Überblick über Ihre externen Assets übernehmen Sie selbst wieder die Kontrolle und reduzieren Ihre Angriffsoberfläche, um so Ihr Unternehmen zu schützen* ▪ *Das Wissen um Angriffsoberflächen lässt Sie potenzielle Angriffspfade erkennen. So können Sie Maßnahmen ergreifen, um das Risiko zu verringern und einzudämmen.*
AUFDECKUNG VON SCHWACHSTELLEN	▪ *Verbessern Sie Ihre Programme zum Schwachstellenmanagement durch kontinuierliche Überwachung, um Schwachstellen in Ihren externen Assets zu identifizieren.* ▪ *Verstehen Sie, wie Cyberkriminelle versuchen, Ihre Schwachstellen für ihre Zwecke auszunutzen.* ▪ *Entwickeln Sie ein Programm zur Zertifikatsverwaltung, indem Sie schwache, anfällige Zertifikate identifizieren, die auf Ihren externen Assets gehostet sind.*	▪ *Verbessern Sie Ihr Schwachstellenmanagementprogramm, da Sie nun die Risiken und Bedrohungen kennen, die dringend bekämpft werden müssen.* ▪ *Priorisierung des Patch-Management-Programms und der Abhilfemaßnahmen.* ▪ *Schließen Sie Sicherheitslücken schnell, bevor weiterer Schaden entsteht.*
ÜBERWACHUNG VON DATENSCHUTZ-VERLETZUNGEN	▪ *Echtzeit-Erkennung von geistigem Eigentum, personenbezogenen Daten oder Finanzinformationen, die nach außen durchgesickert sind.* ▪ *Bereitstellung von Hintergrundinformationen, Beschreibungen und Auswirkungen für jede Art von Sicherheitsverletzung und Gefährdung.*	▪ *Sie wissen, ob und wann Ihre Daten nach außen durchgesickert sind.* ▪ *Stellen Sie sicher, dass Mitarbeiter, Geschäftspartner und externe Auftragnehmer nicht versehentlich sensible Informationen weitergegeben haben, wodurch das Unternehmen Cyberangriffen und -risiken ausgesetzt sein könnte.* ▪ *Wenn Sie wissen, dass E-Mails und Zugangsdaten kompromittiert wurden, können Sie entsprechende Maßnahmen ergreifen, um Ihr Unternehmen vor Phishing- und anderen Social-Engineering-Angriffen zu schützen.* ▪ *Stellen Sie sicher, dass Ihr geistiges Eigentum und Ihre Geschäfts-geheimnisse geschützt sind.* ▪ *Stellen Sie sicher, dass die gesetzlichen Bestimmungen eingehalten werden.* ▪ *Verhindern Sie, dass Sie im Falle einer Datenschutzverletzung oder eines Cyberangriffs mit negativen Medienberichten konfrontiert werden.*
BEDROHUNGEN IM DARK WEB	▪ *Sie erhalten Einblick in Hacker-Konversationen und verdächtige betrügerische Aktivitäten im Dark Web.* ▪ *Enttarnung von Benutzer- und Zugangsdaten für E-Mails, PII/CII-Daten und anderen vertraulichen Informationen, die in Untergrundforen und auf Marktplätzen zum Verkauf angeboten werden.*	▪ *Sie erfahren als Erster, dass Ihre Daten nach außen gelangt sind.* ▪ *Handeln Sie schnell, indem Sie z. B. bestimmte Netzwerk-Ports schließen und Passwörter und Zugangsdaten zurücksetzen, um den Schaden zu begrenzen.*
BEDROHUNGEN IN DEN SOZIALEN MEDIEN UND ÖFFENTLICHE EXPOSITION	▪ *Kontinuierliche Überwachung auf Spoof- und Lookalike-Domains und Subdomains.* ▪ *DeTCT erfasst sowohl neu registrierte als auch böswillige Domains.* ▪ *Aufdeckung gefälschter Social-Media-Profile von Unternehmen und ihren Führungskräften (LinkedIn, Facebook und Twitter).*	▪ *Vereiteln Sie Social-Engineering- und Phishing-Kampagnen von Personen, die sich als Führungskräfte des Unternehmens ausgeben oder Ihr Unternehmensprofil missbrauchen.* ▪ *Sensible Daten, die entweder absichtlich oder versehentlich nach außen gelangt sind, können von Bedrohungsakteuren für Angriffe genutzt werden. Wenn Sie diese Lecks aufspüren können, haben Sie die Möglichkeit, Gegenmaßnahmen zu ergreifen und einen größeren Angriff zu verhindern.*
IDENTITÄTS-MISSBRAUCH UND RECHTS-VERLETZUNG	▪ *Identifizierung von Rechtsverletzungen und Identitätsmissbrauch in Bezug auf Marken, Produkte, Lösungen und Personen.* ▪ *Dies sind Bedrohungsindikatoren, die auf mögliche Phishing-Kampagnen hinweisen.*	▪ *Verringern Sie das Risiko, dass Ihre Marke, Produkte und Lösungen kopiert werden.* ▪ *Schützen Sie Ihre Markenintegrität. Verhindern Sie Unterbrechungen der Geschäftstätigkeit durch Phishing- und Social-Engineering-Angriffe, die das Vertrauen der Stakeholder untergraben und sich auf die Geschäftstätigkeit auswirken könnten.* ▪ *Schützen Sie Ihre Führungskräfte vor Identitätsmissbrauch im Web und in den sozialen Medien.*
ERKENNUNG UND ÜBERWACHUNG VON RISIKEN VON DRITTANBIETERN	▪ *Wir helfen Ihnen bei der Überwachung von Drittanbietern. Hierzu greifen wir auf die Domains dieser Anbieter zu, ohne dass komplexe und auffällige Implementierungen erforderlich sind.* ▪ *Erstellen Sie ein digitales Risikoprofil des Unternehmens und erfahren Sie, ob es Datenlecks, Schwachstellen und andere Probleme gegeben hat*	▪ *Sichern Sie Ihr digitales Ökosystem und verschaffen Sie sich einen Überblick über die Cyber-Risiken von Drittanbietern.* ▪ *Entdecken Sie Schwachstellen in den digitalen Assets Ihres Lieferanten.* ▪ *Machen Sie sich das Cyber-Risiko von Drittanbietern bewusst und erkennen Sie, welche Folgen dies für Ihr Unternehmen haben könnte.*
RISIKO- UND HACKABILITY-SCORES	▪ *Verschaffen Sie sich einen schnellen Überblick über Ihre Risiko- und Hackability-Scores und verfolgen Sie, wie sich diese im Laufe der Zeit entwickeln.* ▪ *Die Risikoeinstufung erfolgt nach dem FAIR-Prinzip (Factor Analysis of Information Risk) und wird für jeden Bedrohungsindikator bzw. für jede Gefährdung erstellt.*	▪ *Verschaffen Sie sich einen Überblick über Ihre Risikosituation, damit Sie Maßnahmen zur Eindämmung von Bedrohungen ergreifen können, die zu einer Unterbrechung der Geschäftstätigkeit führen könnten.* ▪ *Erhalten Sie einen umfassenden Überblick über den Status Ihres digitalen Risikos aus Sicht des Unternehmens.*
EMPFOHLENE ABHILFEMASS-NAHMEN	▪ *Für jedes verbundene Risiko und jede Gefährdung werden Abhilfemaßnahmen empfohlen, damit die Teams schnell handeln können.*	▪ *Schnelles und entschlossenes Vorgehen mit klar festgelegten Handlungsprioritäten.* ▪ *Mobilisieren Sie die richtigen Ressourcen, um Sicherheitslücken zu schließen.*

KENNEN SIE IHRE ANGRIFFSOBERFLÄCHE

Machen Sie Ihren digitalen Fußabdruck sichtbar und erkennen Sie Ihr externes Risikoprofil

Identifizieren Sie Assets Ihrer Kunden, die möglichen Hackerangriffen ausgesetzt sind – wie Domain, Subdomain, IP-Adressbereich, Softwareversionen, Schwachstellen usw.

IDENTITÄTSMISSBRAUCH UND RECHTSVERLETZUNG

Identifizieren Sie alle Online-Entitäten, die Ihr digitales Unternehmensprofil, Ihre Assets, Ihre Produkte und Ihre Marke auf der Grundlage des angegebenen Domainnamens vortäuschen.

ÜBERWACHUNG VON DATENSCHUTZVERLETZUNGEN

Ganzheitlicher Überblick über Datenschutzverletzungen, die dazu führen können, dass kritische Daten aus Ihren IT-Systemen exfiltriert werden.

ÜBERWACHUNG VON DRITTANBIETERN

Sichern Sie Ihr digitales Ökosystem und verschaffen Sie sich einen Überblick über die Cyber-Risiken von Drittanbietern. Entdecken Sie Schwachstellen in den digitalen Assets Ihres Lieferanten und verstehen Sie, wie sich diese auf Ihr Unternehmen auswirken könnten.

SOZIALE UND ÖFFENTLICHE EXPOSITION

Identifizieren Sie Lookalike-Domains, Handler, Logos und öffentliche Informationen im Surface Web und in den sozialen Medien.

BEDROHUNGEN IM DARK WEB

Hacker-Konversationen und verdächtige betrügerische Aktivitäten im Dark Web werden sichtbar gemacht, wenn die angegebenen Domains und weitere Informationen wie beispielsweise E-Mail-ID, PII/CII-Daten übereinstimmen.

GEFÄHRDUNG DURCH SCHWACHSTELLEN

Anhand des angegebenen Domainnamens werden Schwachstellen im Asset-Design aufgezeigt, die eine potenzielle Sicherheitsgefährdung darstellen könnten.

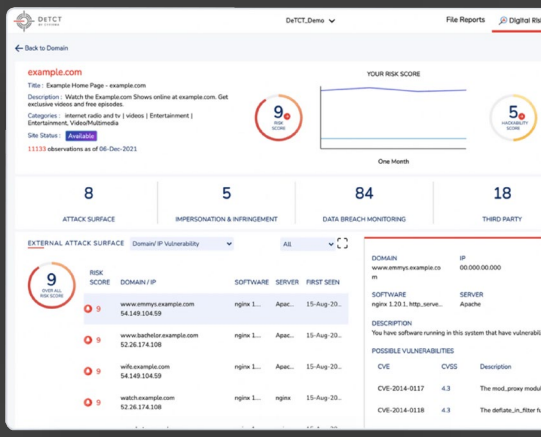
Achten Sie auf folgende digitale Risiken

- *Gefälschte Identitäten Ihrer Führungskräfte im Top-Management – hierbei könnnte es sich um gefälschte Social-Media-Profile oder gefälschte E-Mail-IDs handeln. Dies sind Anzeichen für potenzielle Phishing-Kampagnen, wobei sich die Hacker als Autoritätspersonen ausgeben, um die Mitarbeiter zum Anklicken schädlicher E-Mails zu verleiten.*
- *Lookalike -Domains und -Websites, die die Nutzer dazu verleiten sollen, auf falsche Inhalte hereinzufallen oder persönliche/finanzielle Informationen preiszugeben.*
- *Ihre IP-Adressen, Zugangsdaten von Mitarbeitern, CII/PII werden genannt und in Hackerforen, im Dark Web und auf Bin-Sites veröffentlicht. Das bedeutet, dass Hacker einen Weg gefunden haben, Ihre Abwehrmechanismen zu durchbrechen und wichtige Daten zu exfiltrieren.*

DeTCT ERKENNT AUTOMATISCH IHREN DIGITALEN FUSSABDRUCK – BESSER, ALS ALLE ANDEREN.

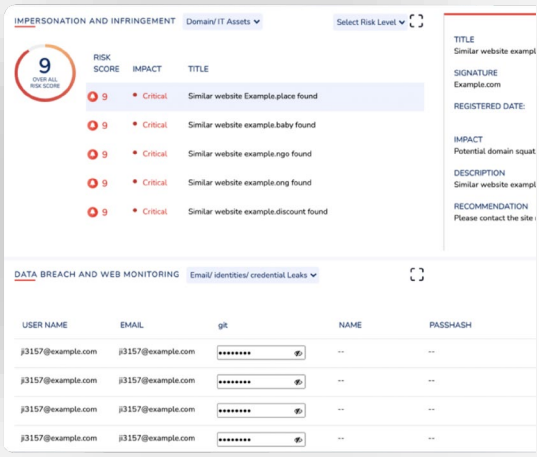
DeTCT ist der einzige proaktive Überwachungsdienst, der genau das tut, was er verspricht. Vollautomatisiert und sorgfältig – Ihr digitaler Detektiv, der 24/7 für Ihre Cybersicherheit sorgt. Risikomanagement durch die Beseitigung von Blind Spots

- Kennen Sie Ihre Angriffsoberfläche
- Identitätsmissbrauch und Rechtsverletzung
- Überwachung von Datenschutzverletzungen
- Aufdeckung von Schwachstellen
- Bedrohungen im Dark Web
- Soziale und öffentliche Exposition



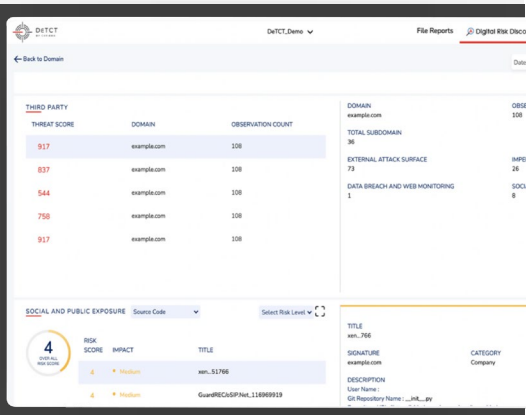
DeTCT ÜBERWACHT PROAKTIV UND 24/7 DAS DARK WEB, DAS SURFACE WEB UND SOCIAL-MEDIA-PLATTFORMEN

- Ergreifen Sie Abhilfemaßnahmen, um Datenlecks und Datenschutzverletzungen einzudämmen
- Dashboards mit schnellen Risiko- und Hackability-Scores, einschließlich Trends zur Überwachung, welche Fortschritte im Laufe der Zeit zu beobachten sind
- Details zu Marke, Domain, Identitätsmissbrauch usw. mit Risikobewertungen und Folgenabschätzung



DeTCT SICHERT IHR DIGITALES ÖKOSYSTEM UND GIBT IHNEN EINEN EINBLICK IN DIE CYBERRISIKEN VON DRITTANBIETERN

- Entdecken Sie die Schwachstellen der digitalen Assets Ihrer Lieferanten
- Erhalten Sie Benachrichtigungen über Datenlecks und Gefährdungen, die sich auf Ihr Unternehmen auswirken könnten
- Erhalten sie Empfehlungen für Abhilfemaßnahmen, um die Cybersicherheit ihrer Lieferanten zu erhöhen



ÜBER CYFIRMA

CYFIRMA ist ein Unternehmen, das eine Plattform zur Verwaltung externer Bedrohungslandschaften betreibt. Wir kombinieren Cyber-Intelligenz mit der Erkennung von Angriffsoberflächen und dem Schutz vor digitalen Risiken, um vorausschauende, personalisierte, kontextbezogene und vielschichtige Erkenntnisse zu liefern. Wir nutzen unsere Cloud-basierte KI- und ML-gestützte Analyseplattform, um Unternehmen bei der proaktiven Erkennung potenzieller Bedrohungen in der Planungsphase von Cyberangriffen zu unterstützen. Mithilfe unseres einzigartigen Ansatzes, der den Anwender in die Lage versetzt, sich in die Sichtweise eines Hackers hineinzuversetzen und profunde Einblicke in die externe Cyberlandschaft zu gewinnen, konnten sich unsere Kunden auf bevorstehende Angriffe vorbereiten.

CYFIRMA arbeitet mit vielen Unternehmen zusammen, die in der Rangliste der Fortune 500 vertreten sind. Das Unternehmen hat Niederlassungen in den USA, Japan, Singapur, der EU und Indien.

Offizielle Websites:
https://www.cyfirma.com/ https://www.cyfirma.jp/