DATENBLATT

DeCYFIR™

Die Lösung für Cyber Defender, um das Risiko externer Bedrohungen zu mindern und Cyberangriffe abzuwehren

DeCYFIR ist eine SaaS-basierte Plattform zur Verwaltung externer Bedrohungslandschaften. Sie wurde entwickelt, um Ihr Unternehmen zu schützen. Dabei erkennt sie Angriffsoberflächen, erstellt ein digitales Risikoprofil und nutzt personalisierte Cyber-Intelligenz, um bevorstehende Angriffe vorherzusagen.
Mithilfe von DeCYFIR erhalten Kunden einen klaren Überblick über ihre externe Bedrohungslandschaft und wissen genau, welche Gegenmaßnahmen erforderlich sind, um Sicherheitslücken zu schließen. So können Cyber Defender und Ressourcen dort eingesetzt werden, wo sie am dringendsten benötigt werden, und Angreifer auf Abstand halten.

DeCYFIR ist eine nicht-intrusive Cloud-Plattform, die über modernste Cyber-Intelligenz-Technologien verfügt und dabei folgende strenge Kriterien erfüllt:

Vorausschauende Erkenntnisse, die Kunden frühzeitig vor potenziellen Cyberangriffen warnen.

Personalisierte Informationen, die auf die Branche, die Technologie und den Standort des Kunden zugeschnitten sind.

Vielschichtige Intelligenz, die strategische, verwaltungstechnische und operative Komponenten umfassend abdeckt.

Kontextbezogene Erkenntnisse, die eine Verknüpfung zwischen Hacker, Motiv, Kampagne und Methode herstellen.

Die **„Outside-in“**-Perspektive bietet Einblicke in die externe Bedrohungslandschaft, sodass der Kunde durch die Brille des Hackers blickt.

DeCYFIR stellt Kunden ein Paket priorisierter Lösungen zur Verfügung, um das Auftreten von Sicherheitsverletzungen zu verhindern.

DeCYFIR ist eine einheitliche Plattform zur Verwaltung von externen Bedrohungslandschaften, die eine Erkennung von Angriffsoberflächen, Schwachstellen, Markeninformationen, Schutz vor digitalen Risiken und Situationsbewusstsein bietet.

DECYFIR®
BY CYFIRMA

DeCYFIR™

HAUPTMERKMAL	BESCHREIBUNG	VORTEILE
VORAUSSCHAUEND	Identifiziert potenzielle Cyberangriffe auf Ihr Unternehmen und Ihre Tochtergesellschaften bereits in einem frühen Stadium, bevor Cyberkriminelle Ihrem Unternehmen Schaden zufügen können.	Frühwarnungen und Alerts, um auf Angriffe vorbereitet zu sein
PERSONALISIERT	Sämtliche Daten und Erkenntnisse sind auf die von Ihnen verwendete Technologie, Ihre Branche und Ihren Standort zugeschnitten.	Störgeräusche werden entfernt und False Positives reduziert
KONTEXTBEZOGEN	Wir liefern vollständige kontextbezogene Details zum Indikator für eine Kompromittierung [was ist es, Hintergrunddetails, böswillig / nicht böswillig, Standortdetails, wofür wird es verwendet [C&C, Angriffspunkt, böswillige Hosting-Site], Zugehörigkeit Cybercrime-Kampagne, Cyberkriminelle.	Bietet ein profundes Verständnis von Cyber-Bedrohungen, um wirksame Verteidigungsstrategien zu entwickeln
CYBER-INTELLIGENZ	Detaillierte Einblicke in Ihre externe Bedrohungslandschaft - wer sind die Cyberkriminellen, die sich für Sie interessieren? Welche Motivation haben sie? Was wollen sie von Ihnen? Wann können sie angreifen und wie werden sie angreifen? Welche Tools und Techniken können sie einsetzen?	Umfassender Überblick, um sicherzustellen, dass Cyber Defender nicht „überrumpelt“ werden
ERKENNUNG DER ANGRIFFSOBERFLÄCHE	Proaktive Identifizierung von ungeschützten externen Assets, Schatten-IT, übersehenen Systemen und vielem mehr, was von Cyberkriminellen ausgenutzt werden kann.	Das Wissen um Angriffsoberflächen lässt Sie potenzielle Angriffspfade erkennen. So können Sie Maßnahmen ergreifen, um das Risiko zu verringern und einzudämmen.
INTELLIGENTE SCHWACHSTELLENANALYSE	Identifizierung von Schwachstellen in Ihren externen Assets. Sie erfahren, wie Cyberkriminelle versuchen, diese Schwachstellen auszunutzen.	Unterstützung bei der Priorisierung von Patch-Management-Programmen und Abhilfemaßnahmen
INTELLIGENTE ERKENNUNG VON MARKENINFORMATIONEN	Identifizierung von Rechtsverletzungen und Identitätsmissbrauch in Bezug auf Marken, Produkte, Lösungen und Personen	Verringern Sie das Risiko für Ihre Marke, Ihre Produkte und Ihre Lösungen
SITUATIONSBEWUSSTSEIN	Erkennt Trends und neue Bedrohungen in Ihrer Branche, für die von Ihnen verwendeten Technologien und für die Region, in der Sie tätig sind	Verringern Sie das Risiko für Ihre Marke, Ihre Produkte und Ihre Lösungen

DECYFIR BY CYFIRMA

DeCYFIR™

HAUPTMERKMAL	BESCHREIBUNG	VORTEILE
SCHUTZ VOR DIGITALEN RISIKEN	Proaktive Identifizierung von Datenlecks, Verstößen, Ausspähungen und Identitätsmissbrauch, um	das Risiko zu verringern, dass Cyberkriminelle Ihrer Marke schaden oder sie für neue Cyberangriffe gegen Sie verwenden
INDIVIDUELL ANGEPASSTES DASHBOARD	• Executive View ist ein risikobasierter Ansatz, der Führungskräften einen schnellen Überblick über externe Risiken und das Risiko eines potenziellen Hackerangriffs ermöglicht • Management View ist ein geführter Ansatz zur systematischen Wiederherstellung • Operational View liefert Ihnen technische Details zu Ergebnissen und Abhilfemaßnahmen	Hierarchie- und funktionsübergreifend, damit alle Beteiligten auf dem gleichen Stand sind
HEURISTISCHE SUCHE	Die Suchfunktion unterstützt Sie bei der Suche nach Bedrohungen, Cyberangriffen, Sicherheitsverletzungen, Bedrohungsakteuren, Malware und Phishing-Kampagnen über eine einzige Plattform	Sofortige Klärung dringender Fragen in Bezug auf externe Bedrohungen
RISIKODOSSIER	Risikodossier, das die Korrelation zu IOCs, Schwachstellen, Angriffsoberfläche, digitalen Risiken und mehr zeigt	So können Sie sich schnell einen ganzheitlichen Überblick darüber verschaffen, wie eine Sicherheitslücke durch eine bestimmte Kampagne ausgenutzt werden könnte und welche Cyberkriminellen dahinter stecken. Verstehen sie, welche Auswirkungen Cyberangriffe auf Ihre Assets haben
ALERT-ZENTRALE	Eine individuell auf Ihr Unternehmen zugeschnittene Alert-Zentrale, die die wichtigsten Bedrohungen und Risiken für Ihr Unternehmen erkennt	Ermöglicht eine schnelle Priorisierung von Abhilfemaßnahmen
TAKEDOWN-SERVICES	Wir bieten Takedown-Services mit 3 Informationsanfragen pro Monat an. Hierbei stellen wir nachrichtendienstliche Recherchen und ausführliche Berichte zu Themen, Ereignissen und sich entwickelnden Cyber-Trends bereit, die von Ihnen identifiziert wurden	Wir können Sie dabei unterstützen, das Risiko mit konkreten Maßnahmen zu mindern
INTEGRATION MIT SICHERHEITSKONTROLLEN	Sie können die Erkenntnisse aus STIX und TAXII in Ihre Sicherheitskontrollen integrieren	Mithilfe der DeCYFIR Intelligence Hunting-Funktion können Sie auf Ereignisse reagieren und Sie erhalten ausführliche, kontextbezogene Informationen
REAKTION AUF EREIGNISSE	Mithilfe der DeCYFIR Intelligence Hunting-Funktion können Sie auf Ereignisse reagieren und Sie erhalten ausführliche, kontextbezogene Informationen	Beschleunigen Sie die Reaktion auf Ereignisse mit einer vollständigen Analyse externer Bedrohungen
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.

EXECUTIVE VIEW

Das Dashboard von DeCYFIR ist ein Entscheidungsinstrument für Führungskräfte, das ihnen hilft, die sich verändernde Dynamik zu verstehen und kritische Entscheidungen schneller zu treffen.

- Dashboards für Führungskräfte, um die sich verändernde Dynamik zu verstehen und wichtige Entscheidungen schneller treffen zu können
- Risiko- und Hackability-Scores, um die Bedrohungslandschaft im Handumdrehen zu prüfen
- Telemetrie wichtiger Statistiken
- Überblick über Cyber-Bedrohungen, die für Ihr Unternehmen relevant sind

Risiko- und Hackability-Score und Trends verstehen

Ansicht der Externen Bedrohungs-landschaft in Echtzeit

Kritische Bedrohungsindi-katoren werden deutlich auf dem Dashboard angezeigt, um eine rechtzeitige und genaue Entscheidungs-findung zu erleichtern

Profunde Einblicke in die Zuordnung von Bedrohungs-akteuren, Motiven, Kampagnen und Auswirkungen

Sorgt für ein Situationsbewusstsein im Hinblick darauf, was weltweit geschieht und inwieweit diese Veränderungen eine Bedrohung für das digitale Profil des Unternehmens darstellen könnten. Machen Sie sich die Risiken bewusst, die auf Sie zukommen könnten.

MANAGEMENT VIEW

Mithilfe einer Schritt-für-Schritt-Anleitung erleichtert der systematische Best-Practice-Ansatz die Risikominderung beim Sicherheitsmanagement. DeCYFIR deckt methodisch Angriffsoberflächen, Schwachstellen, Angriffsmethoden, digitale Risiken und Beobachtungen im Dark Web auf und schafft Situationsbewusstsein.

Handeln Sie schnell, um das Risiko mithilfe von Schritt-für-Schritt-Anleitungen zu minimieren

Systematische Aufdeckung von:

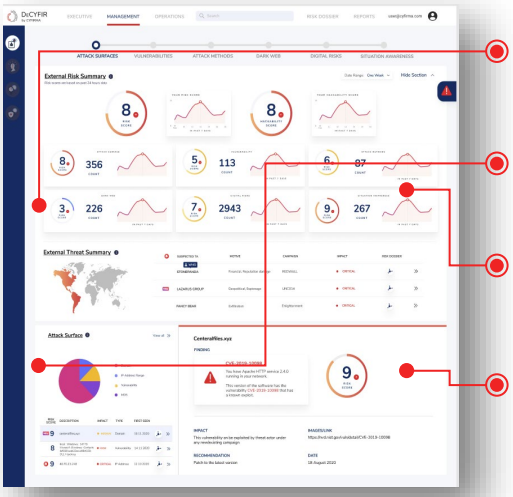
- Angriffsoberfläche
- Schwachstellen
- Angriffsmethoden
- Risikopotenzial für digitale Systeme
- Beobachtungen im Dark Web
- Situationsbewusstsein

1 ANGRIFFSOBERFLÄCHE IDENTIFIZIEREN

IDENTIFIZIERUNG POTENZIELLER EINSTIEGSPUNKTE FÜR ANGREIFER

MÖGLICHE EINSTIEGSPUNKTE FÜR CYBER-ANGREIFER

- Unterstützung des Kunden bei der Identifizierung von Assets – wie Domain, Subdomain, IP-Adressbereich, Softwareversionen, Schwachstellen usw., die möglichen Hackerangriffen ausgesetzt sind
- Unterstützung des Kunden, um einen vollständigen Überblick über die von Angreifern gefährdeten Assets zu erhalten, Methoden zu finden und das Risiko für das Unternehmen zu bewerten
- Unterstützung der Kunden bei der Entwicklung einer wirksamen Sicherheitsstrategie



Ein Counter informiert Sie über die Expositionen der letzten 7 Tage

Die Angriffsoberfläche bietet Einstiegspunkte, durch die sich Hacker Zugang zu Ihrem Unternehmen verschaffen können

Trends zeigen, wie Sie in einer bestimmten Zeitspanne für jede Kategorie abschneiden

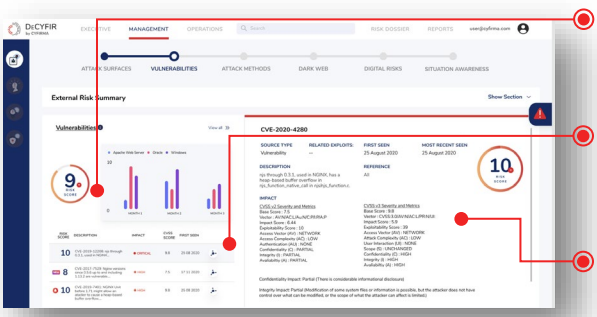
Detailansicht einer individuellen Angriffsoberfläche, die Ihnen anzeigt, wie ernst die Situation ist und welche Attribute damit verbunden sind

2 SCHWACHSTELLEN AUFDECKEN

SICHERHEITSVERANTWORTLICHE WERDEN ZU PROAKTIVEN RISIKOBERATERN STATT NUR ZU REAGIEREN

EINSTIEGSPUNKTE, DIE VON CYBERKRIMINELLEN GENUTZT WERDEN KÖNNEN

- Unterstützung des Kunden, sich in die Sichtweise des Cyber-Angreifers hineinzuversetzen
- Erkennen von Schwachstellen und potenziellen Angriffspunkten
- Mithilfe der intelligenten Schwachstellenanalyse lassen sich Bedrohungsmodelle und Sicherheitspläne erstellen



3-Monats-Trends helfen den Verantwortlichen zu verstehen, welche ihrer Assets besonders anfällig sind

Liste der kritischen Schwachstellen der letzten 3 Monate, auf die das Unternehmen besonders achten sollte

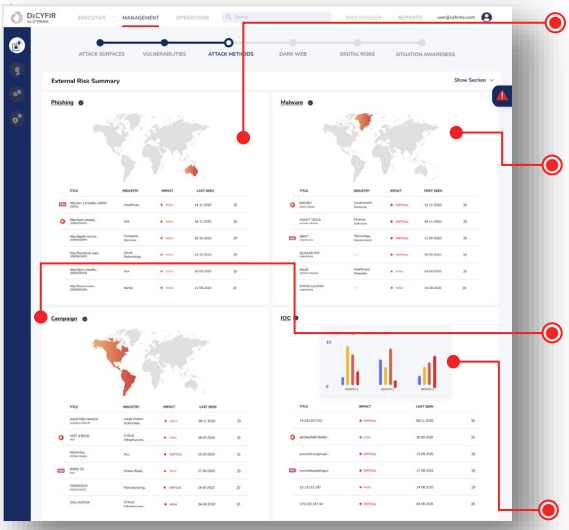
Details/Attribute der kritischen Schwachstelle

3 ANGRIFFSMETHODEN VERSTEHEN

VERBESSERTE SICHERHEITSTELEMETRIE MIT TIEFEREN EINBLICKEN IN POTENZIELLE ANGRIFFE

VERSTEHEN SIE, WIE HACKER VERSUCHEN, IN IHR UNTERNEHMEN EINZUDRINGEN, UM EINE WIRKSAME ANTWORT ZU FINDEN

- Erfahren Sie mehr über die Methoden und Werkzeuge des Gegners
- Erhalten Sie Informationen über Einzelheiten der Kampagne bereits in einem frühen Stadium der Planung



Aktuelle Phishing-Angriffe, die für Ihr Unternehmen relevant sind

Für Führungskräfte ist es wichtig, die Listen der kürzlich von Hackern entwickelten Schadprogramme einzusehen, die für Ihr Unternehmen gefährlich werden können,

Cyberangriffe werden von Bedrohungsakteuren oftmals als Teil einer koordinierten Kampagne gegen Ihr Unternehmen eingesetzt

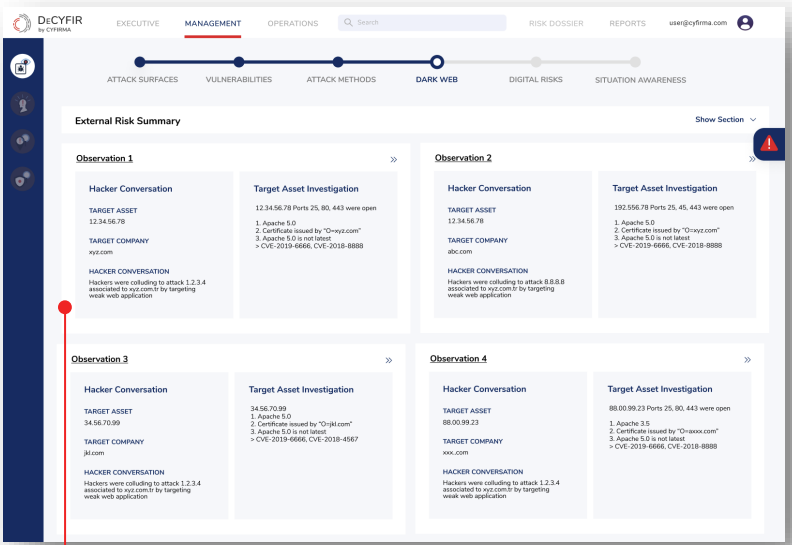
Ausführliche Aufstellung relevanter Indikatoren für eine Kompromittierung - MD5, SHA, IP, DOMAIN, HOSTNAME, URL, EMAIL, CVE, EXPLOIT, MUTEX, FILE, SSL usw.

4 BEOBACHTUNGEN IM DARK WEB

KI-ENGINES DECKEN HINWEISE AUF CYBER-RISIKEN UND ANGRIFFE AUF IHR UNTERNEHMEN AUF

BEGEBEN SIE SICH IN DIE SCHÜTZENGRÄBEN DER HACKER UND FINDEN SIE ANHALTSPUNKTE FÜR POTENZIELLE ANGRIFFE

- Bleiben Sie Cyberkriminellen einen Schritt voraus und erhalten Sie Einblicke, welche Bedrohungen lauern
- Verschaffen Sie sich einen Vorsprung durch nutzbare Cyber-Intelligenz
- Wenn Sie frühzeitig informiert werden, können Sie eine wirksame Verteidigungsstrategie entwickeln



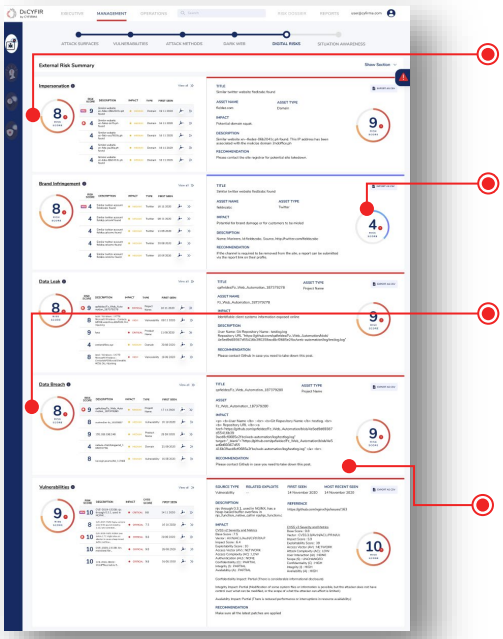
Informationen über Bedrohungen aus dem Deep/Dark Web und aus Hackerforen, geschlossenen Gemeinschaften

5 DIGITALES RISIKOPROFIL

PASSEN SIE IHRE SICHERHEITSARCHITEKTUR AN DEN KONTEXT DER DIGITALEN RISIKEN AN

ÜBERNEHMEN SIE SELBST WIEDER DIE KONTROLLE ÜBER IHRE DIGITALE LANDSCHAFT

- Decken Sie Verstöße gegen Marken-/Produktrechte auf
- Verhindern Sie, dass sich Betrüger als Führungskräfte ausgeben
- Erfahren Sie als Erster, wenn es zu Datenlecks, Datenschutzverletzungen und Identitätsmissbrauch kommt
- Entwickeln Sie eine wirksame Verteidigungsstrategie, um zu verhindern, dass sich der Vorfall wiederholt



Alle Online-Entitäten, die sich das digitale Profil und die Assets des Unternehmens auf der Grundlage des angegebenen Domainnamens zu eigen machen.

Digitale Profile können dem Ruf Ihrer Marke schaden.

Sie sollten wissen, welche Daten aus Ihrem Unternehmen in die Hände von Hackern gelangt sind, die sie für Angriffe auf Sie nutzen könnten. Dies können Dateien/Benutzernamen/Kennwörter usw. sein.

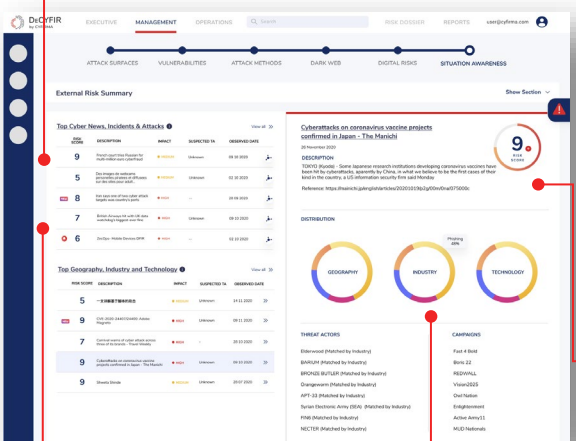
Hacker können diese Schwachstellen und Angriffsvektoren ausnutzen, Ihr Unternehmen in Verruf bringen, sensible Daten exfiltrieren und vieles mehr.

6 SITUATIONSBEWUSSTSEIN

ERREICHEN SIE MEHR EFFIZIENZ, EFFEKTIVITÄT UND GENAUIGKEIT BEI DER ENTSCHEIDUNGSFINDUNG

BEHALTEN SIE DIE KONTROLLE ÜBER SICH SCHNELL VERÄNDERNDE LANDSCHAFTEN UND ERKENNEN SIE DROHENDE GEFAHREN

- Wappnen Sie sich mit relevanten Informationen zu den neuesten Cyberangriffen in Ihrer Branche, Änderungen der Cybergesetze und anderen wichtigen Themen
- Einblicke in die strategische, organisatorische und taktische Entscheidungs-findung



Selbst in den finanziell am besten aufgestellten und erfahrensten Unternehmen gibt es Informationslücken, wenn es darum geht, den aktuellen Stand zu kennen und zu wissen, wie er sein sollte. Hier wird das Situationsbewusstsein zur Notwendigkeit, um kritische Entscheidungen treffen zu können.

Wappnen Sie Ihr Unternehmen mit den neuesten Entwicklungen in der Landschaft der Cyber-Bedrohungen und verstehen Sie, wie diese sich auf Ihr Unternehmen auswirken können.

Risiko-Scoring für spezifische Erkenntnisse, um die Priorisierung von Ressourcen zur Abwehr von Risiken und Bedrohungen zu unterstützen.

Grafische Darstellung der Arten von Bedrohungen und Malware, um sich einen schnellen Überblick über die Bedrohungslandschaft zu verschaffen. Aufschlüsselung nach Region, Branche und Technologie.

Die Informationen werden speziell für das Unternehmen zusammengestellt und sind für die jeweilige Region, Branche und Technologie relevant.

OPERATIONAL VIEW

Mithilfe von DeCYFIR behält das Betriebsteam den Überblick und erkennt Schwachstellen, die es unverzüglich zu beheben gilt.

Der Hackability-Score quantifiziert die Wahrscheinlichkeit, dass das digitale Profil und die Assets des Unternehmens des Kunden gehackt werden. Dabei werden die kürzlich aufgetretenen schädlichen Entwicklungen in der externen Bedrohungslandschaft des Unternehmens des Kunden berücksichtigt.

Der Risiko-Score zeigt an, wie hoch das Risiko für das Unternehmen des Kunden aufgrund der jüngsten Entwicklungen in der externen Bedrohungslandschaft ist.

Bedrohungsakteure, ihre Kampagnen und die Auswirkungen auf Ihr Unternehmen

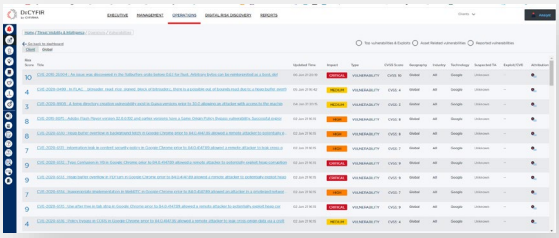
Bei mehreren hunderttausend Software-, Middleware- und Hardware-Anwendungen in einem Unternehmen ist es sehr aufwendig, die Systeme mit Patches zu versorgen. DeCYFIR listet alle betroffenen Systeme und die jeweiligen Schwachstellen auf. Beim Schwachstellen-Management richtet sich die Priorität nach den potenziellen Auswirkungen und der einfachen Verfügbarkeit von Exploits.

DeCYFIR deckt Digitale Risiken auf. Dies gilt insbesondere für Datenlecks, Datenschutzverletzungen, Markenrechtsverletzungen, Identitätsmissbrauch, Verbreitung in sozialen Netzwerken, im Dark Web usw.

Durch die Überwachung der für bestimmte Schwachstellen verfügbaren Exploits, sowohl im Surface Web als auch im Dark Web, behält das verantwortliche Sicherheitsteam den Überblick und kann die Schwachstellen identifizieren, die sofortige Aufmerksamkeit erfordern.

VORRANGIG ZU ERGREIFENDE, RELEVANTE UND TAKTISCHE ABHILFEMASSNAHMEN FÜR SOC-TEAMS

- Betriebsteams können Ressourcen optimieren und die Effizienz und Effektivität steigern
- Bereitstellung umsetzbarer Erkenntnisse über Schwachstellen, IoCs und Hashes, die für Ihre Branche, Ihre Region und Ihre Technologie relevant sind
- DeCYFIR überprüft einen Indikator und verknüpft einzelne Indikatoren mit Kampagnen, Bedrohungsakteuren und Techniken



Ausführliche Aufstellung relevanter Indikatoren für eine Kompromittierung - MD5, SHA, IP, DOMAIN, HOSTNAME, URL, EMAIL, CVE, EXPLOIT, MUTEX, FILE, SSL usw.

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.

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