IONIX

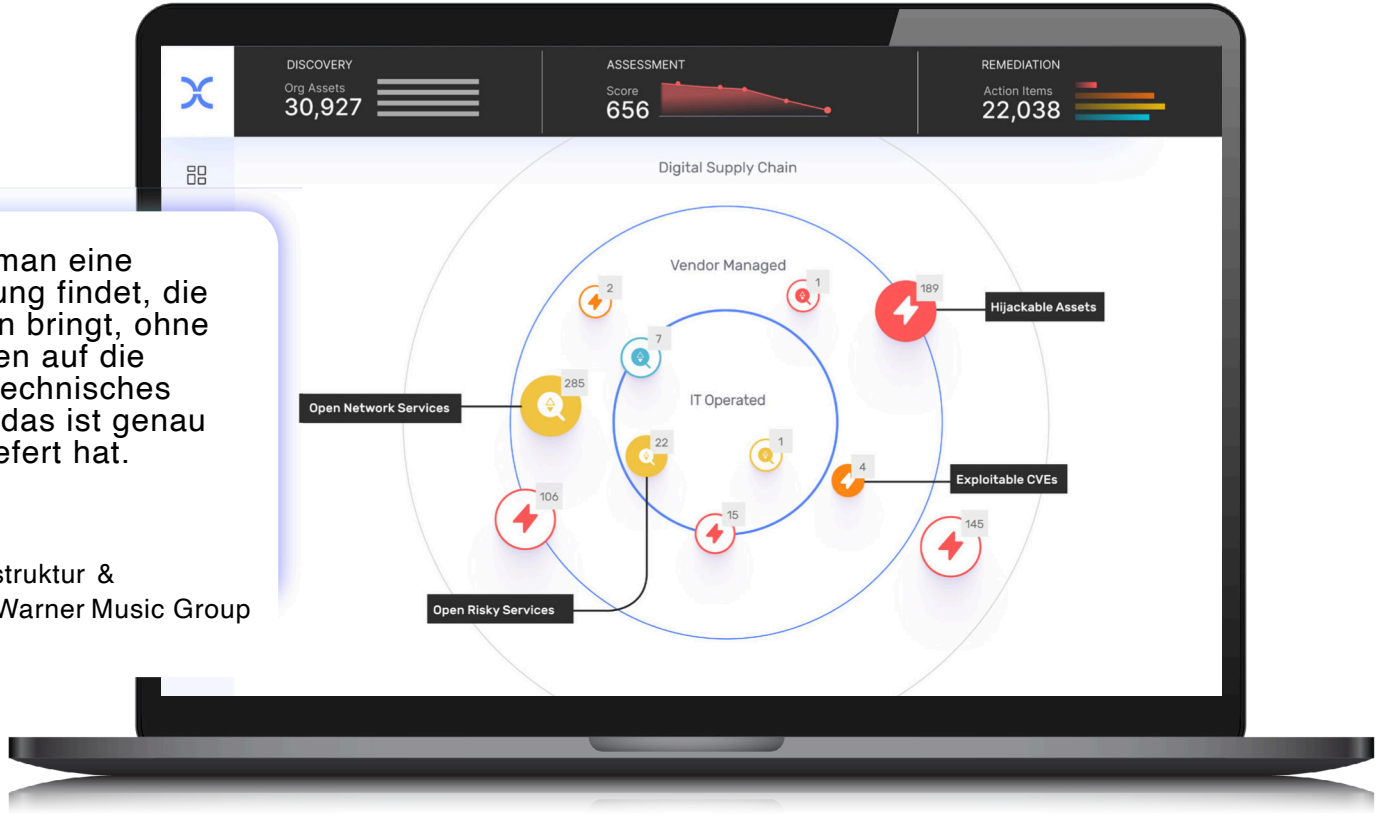
ICOS

DATASHEET

IONIX

MANAGEMENT DER EXTERNEN ANGRIFFSOBERFLÄCHE IHRES UNTERNEHMENS

AUFDECKEN VON EXTERNEN BEDROHUNGEN AUF IHR UNTERNEHMEN



"Es ist selten, dass man eine Cybersicherheitslösung findet, die unmittelbaren Nutzen bringt, ohne dass es Auswirkungen auf die Verfügbarkeit Ihres technisches Personals hat. Aber das ist genau das, was IONIX geliefert hat.

John Remo
SVP Global Cloud / Infrastruktur & Cybersicherheit bei der Warner Music Group

MEHR ALS 20% IHRES EXTERNEN ANGRIFFSRISIKOS LIEGEN IN IHRER DIGITALEN LIEFERKETTE

IONIX Attack Surface Management fokusiert sich auf die größten Angriffsrisiken - auch in Ihrer digitalen Wertschöpfungskette.

SEHEN SIE IHRE ANGRIFFSOBERFLÄCHE WIE EIN ANGREIFER, VON AUSSEN NACH INNEN

Das Risiko für die Angriffsoberfläche Ihres Unternehmens geht über die Anlagen hinaus, die Sie selber besitzen. Einem Angreifer, der in Ihr Unternehmen eindringen will, ist es egal, ob er Ihre digitale Infrastruktur direkt angreift oder eine Schwachstelle in einem digitalen Dienst eines Drittanbieters ausnutzt. Nur IONIX überwacht jeden internetfähigen Asset und jede Verbindung dorthin und liefert somit einen Fokus auf die kritischsten Risiken für Ihr Unternehmen. IONIX liefert Empfehlungen für die Beseitigung ausnutzbarer Schwachstellen, um eine schnelle Gefahrenbeseitigung zu gewährleisten.

IONIX VORTEILE

- Mehr entdecken - vollständige Abdeckung der Angriffsoberfläche
- Weitergehende Bewertung - Verstehen, was behoben werden muss bei Vermeidung unklarer Alarme
- Automatisch validieren - nicht-inversive Tests für kritische Schwachstellen
- Prioritäten intelligenter setzen - keine neue Inventarisierung von Assets, sondern eine vernetzte Karte der Angreifbarkeit
- Schnellere Abhilfe - MTTR von Tagen, nicht Monaten

> "Nachdem wir über ein Jahr mit IONIX zusammengearbeitet haben, sind wir überzeugt, dass die ASM-Plattform von IONIX uns den entscheidenden Einblick verschafft, den wir brauchen, um die schwierige Herausforderung des Managements von Risiken und Schwachstellen in unserer gesamten digitalen Lieferkette zu lösen."
>
> René Rindermann
> CISO, E.ON

EINSATZFÄLLE

Kontinuierliche Verwaltung der Angriffsoberfläche

Automatische Anpassung an Veränderungen und Überwachung der Risiken.

Sicherheit der digitalen Lieferkette

Schützen Sie Ihr Unternehmen vor Bedrohungen aus der digitalen Lieferkette.

Reduzierung der Angriffsfläche

Reduzieren Sie kritische Risiken systematisch und entfernen Sie ungenutzte und vernachlässigbare Assets.

M&A-Risikomanagement

Verwalten Sie Cyber-Risiken während des gesamten Übernahmeprozesses, von der Bewertung bis zur Integration.

Risikominimierung in Außenstellen

Zentralisieren Sie die Verwaltung und lokalisieren Sie das Attack Service Management mit automatischer Zuordnung.

Sicherheit im Cloud-Betrieb

Verschaffen Sie sich einen Überblick und analysieren Sie das Risiko auf öffentlichen Cloud-Plattformen.

Verwaltung von Schwachstellen

Erweitern Sie Ihr bestehendes Programm mit automatischer Erkennung, Bewertung und Priorisierung von Angriffsoberflächen.

Validierung von Angriffsoberflächen

Automatisierte Tests zur Validierung von Schwachstellen und zur Ermittlung der Ausnutzbarkeit von Zero-Day-Bedrohungen.

ICOS IONIX

WIE FUNKTIONIERT IONIX?

AUFKLÄRUNG DER ANGRIFFS-OBERFLÄCHE | RISIKO-BEWERTUNG | EXPOSITIONS-VALIDIERUNG | RISIKO-PRIORISIERUNG | BESCHLEUNIGTE SANIERUNG

AUFKLÄRUNG DER ANGRIFFSFLÄCHE

Entdecken Sie Ihre tatsächliche Angriffsoberfläche und die dazugehörige digitale Lieferkette

Die mehrschichtige Erkennungs-Engine von IONIX erstellt ein umfassendes Inventar Ihres Unternehmens aus der Sicht des externen Angreifers - einschließlich der 20 % Ihrer ausnutzbaren Angriffsoberfläche aus Ihrer digitalen Lieferkette:

- Globale Ereignisverfolgung - Überwachung der globalen PKI und Domainregistrierung
- FQDN- und IP-Erkennung - maschinelles Lernen zur Erkennung aller Domains, Subdomains und IPs
- Reverse-Indexierung - Domains, IP-Blöcke und Cloud-Plattformen
- Reduzierte False Positives - "Discovery Evidence"-Funde nutzen Machine Learning, um jedes Asset genau zuzuordnen

IONIX stellt Ihre Angriffsoberfläche mit einem dynamischen, graphischen ML-Modell dar - mit Nodes und Abhängigkeiten die kontinuierlich aktualisiert werden, und einer sich ständig weiterentwickelnden Reihe potenzieller Kill Chains, die bewertet werden.

RISIKOBEWERTUNG

Skalierbare Identifizierung von Risiken im dazugehörigen Kontext

IONIX führt eine gründliche Bewertung jedes Assets nach 13 Asset-Kategorien durch, darunter Cloud, PKI, Web, DNS - automatisiert und skalierbar über Ihre gesamten Umgebung. Mithilfe der patentierten Connective Intelligence erstreckt sich die Risikobewertung von IONIX rekursiv von Ihren eigenen Assets auf Ihre digitale Lieferkette. Durch die Bewertung von Assets und Verbindungen identifiziert IONIX riskante Verbindungsschwachstellen; externe Risiken durch verbundene DNS-Ketten, Webservices von Drittanbietern und externe Abhängigkeiten die sich auf Ihre Sicherheitslage auswirken. Darüber hinaus fassen die IONIX Risk Scores Sicherheitsprobleme und -risiken in Form von Benchmarks für die Angriffsoberfläche in verschiedenen Kategorien zusammen, und bieten so konkrete Möglichkeiten zur Verbesserung Ihrer Sicherheitsarchitektur.

EXPOSITIONSVALIDIERUNG

Automatisierte Exploit-Simulation

IONIX führt aktive, nicht-inversive Sicherheitstests durch, die externe Angriffe simulieren, und zwar über Ihre gesamte Angriffsoberfläche. Ohne Betriebsunterbrechung prüft IONIX Exposure Validation Ihre Umgebung auf Tausende von Risiken, die permanent aktualisiert werden. Dies beinhaltet Bedrohungen einschließlich ausnutzbarer Schwachstellen, kritische Fehlkonfigurationen, Datengefährdung und mehr. Der IONIX-Ansatz identifiziert kritische Schwachstellen und sorgt dafür, dass sich Sicherheitsteams mit knappen Ressourcen auf die wichtigsten Risiken für ihr Unternehmen konzentrieren können. Dies bietet zusätzlich die Möglichkeit die Zustimmung der Entscheider im Unternehmen für eine beschleunigte Remediation einzuholen.

ICOS IONIX

WIE FUNKTIONIERT IONIX?

AUFKLÄRUNG DER ANGRIFFS-OBERFLÄCHE

RISIKO-BEWERTUNG

EXPOSITIONS-VALIDIERUNG

RISIKO-PRIORISIERUNG

BESCHLEUNIGTE SANIERUNG

RISIKOPRIORISIERUNG

Fokus auf die wichtigsten Risiken

Sicherheitsteams müssen den einzigartigen Geschäftskontext eines gefährdeten Assets berücksichtigen. Das IONIX-Priorisierungs-Framework kombiniert Größe des Risikos, Ausnutzbarkeit, Explosionsradius und threat intelligence, um Sicherheitsteams zu helfen, sich auf die Risiken zu konzentrieren, die für ihr Unternehmen am wichtigsten sind. IONIX priorisiert Bedrohungen dynamisch auf der Grundlage der Wichtigkeit von Assets in vier Dimensionen: Zugriff auf sensible Daten, Geschäftskontext, Markenreputation und betriebliche Auswirkungen von Abhängigkeiten. Die risikobasierte Priorisierung von IONIX stützt sich auf den Schweregrad (CVSS & EPSS) sowie auf Angriffsvektoren wie Fehlkonfigurationen und andere kritische Sicherheitsprobleme, z. B. unsichere DNS-Einträge, ungeschützter Speicher, Cross-Site-Scripting-Risiken sowie schwache/keine Passwörter.

BESCHLEUNIGTE SANIERUNG

Angriffe verhindern, bevor sie passieren

Die intelligenten Workflows von IONIX passen die Abhilfemaßnahmen an die Arbeitsweise der Sicherheitsprozesse an - so verbringen Sie weniger Zeit mit der Weiterleitung von Tickets und mehr Zeit mit der Lösung kritischer Risiken. Sicherheitsprobleme werden in prägnante Aktionspunkte gegliedert, so dass weniger Unruhe entsteht und sofort klar ist, was getan werden muss. Aktionen werden automatisch der richtigen Geschäftseinheit oder Tochtergesellschaft zugeordnet - und den zuständigen Mitarbeitern zugewiesen -, um eine schnellere Lösung zu erreichen. IONIX lässt sich mit SIEM-Systemen (Security Information and Event Management), SOAR (Security Orchestration, Automation and Respronse), SOC-Software (Security Operations Center) und Ticketing-Systemen integrieren und beschleunigt so die Abhilfemaßnahmen durch optimierte Arbeitsabläufe in allen Teams.

STARTEN SIE NOCH HEUTE

Kontaktieren Sie unser Team, um einen kostenlosen Scan zu erhalten.

Erhalten Sie einen kostenlosen Scan I Erfahren Sie mehr unter icosvad.de

ICOS IONIX