Protección contra riesgos digitales basada en la inteligencia

Cyberint

PROTECCIÓN CONTRA RIESGOS DIGITALES BASADA EN LA INTELIGENCIA

Aprovechando una combinación única de Argos™ - plataforma de inteligencia de amenazas patentada y analistas de inteligencia de amenazas altamente experimentados, Cyberint ofrece un nuevo enfoque para la Protección Digital de Riesgos (DRP), brindando soluciones que abordan los siguientes desafíos:

- **Determinar qué amenazas relevantes** deben ser consideradas para diseñar un programa efectivo de defensa de la ciberseguridad
- **Ilustrar el estado actualizado del riesgo cibernético** a la junta y la directiva con un plan de acción claro
- **Adquirir inteligencia predictiva** para identificar intenciones, técnicas y herramientas para mitigar las amenazas específicas antes de que se materialicen
- **Supervisar continuamente la exposición al riesgo digital** que puede ser explotada por los ciberdelincuentes
- **Detectar infracciones a medida que se propagan** fuera del perímetro de la organización
- **Obtener visibilidad de los ataques** dirigidos a su marca y a los clientes que evolucionan constantemente fuera de su red

DESAFÍOS EMPRESARIALES ABORDADOS POR CYBERINT:

- **PROTECCIÓN DE LA MARCA**
- **RIESGO CIBERNÉTICO DE TERCEROS**
- **SUPERVISIÓN DIGITAL DE SUPERFICIES DE RIESGO**
- **FRAUDE**
- **DETECCIÓN DE FUGAS DE DATOS**
- **DETECCIÓN DE ATAQUES**
- **SUPERVISIÓN DE LA WEB OSCURA**
- **INTELIGENCIA CONTRA AMENAZAS**

OFERTA DE CYBERINT

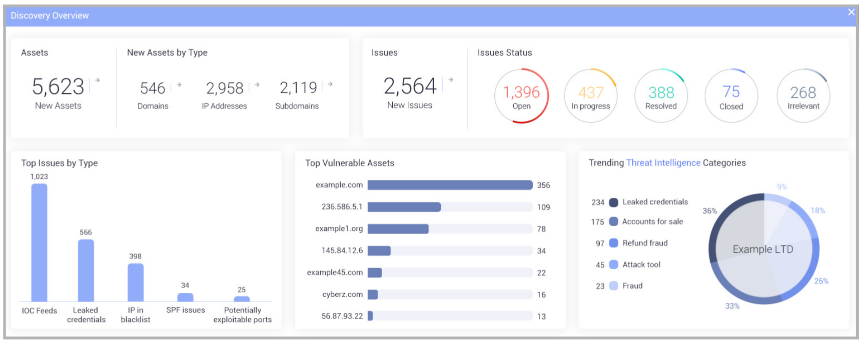
TECNOLOGÍA ARGOS™	SERVICIO GESTIONADO
INTELIGENCIA CONTRA AMENAZAS	SUPERVISIÓN DIRIGIDA
SUPERVISIÓN DE LA WEB OSCURA	HUMINT VIRTUAL
MAPEO DE SUPERFICIES DE RIESGO	INVESTIGACIONES PROFUNDAS
LIENZO FORENSE	ANÁLISIS DEL PAISAJE DE AMENAZAS
DETECCIÓN Y DETENCIÓN DE PHISHING	

PLATAFORMA DE PROTECCIÓN DIGITAL DE RIESGOS IMPULSADA POR LA INTELIGENCIA ARGOS™

Argos™ es una plataforma SaaS multiinquilino con varios módulos:

MAPEO DE SUPERFICIE DE ATAQUE

El mapeo de superficie de ataque de Argos™ identifica la huella digital de la organización y supervisa los activos más allá del perímetro de forma continua, lo que garantiza la visibilidad de dichos activos con una priorización de problemas a abordar basada en la gravedad, destacando las amenazas, vulnerabilidades y debilidades relacionadas.

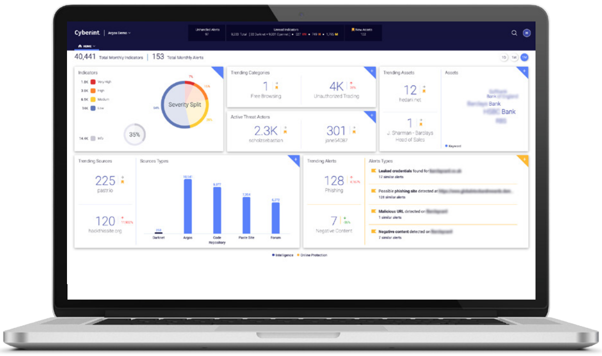


Plataforma de protección de riesgos digitales Argos™, supervisión de superficie de ataque

RECOPILACIÓN Y ANÁLISIS DE INTELIGENCIA DE AMENAZAS

La supervisión en tiempo real de Cyberint de miles de fuentes de amenazas en la web abierta, profunda y oscura conduce a la recopilación de millones de elementos de inteligencia por día en el lago de datos interno de Argos™.

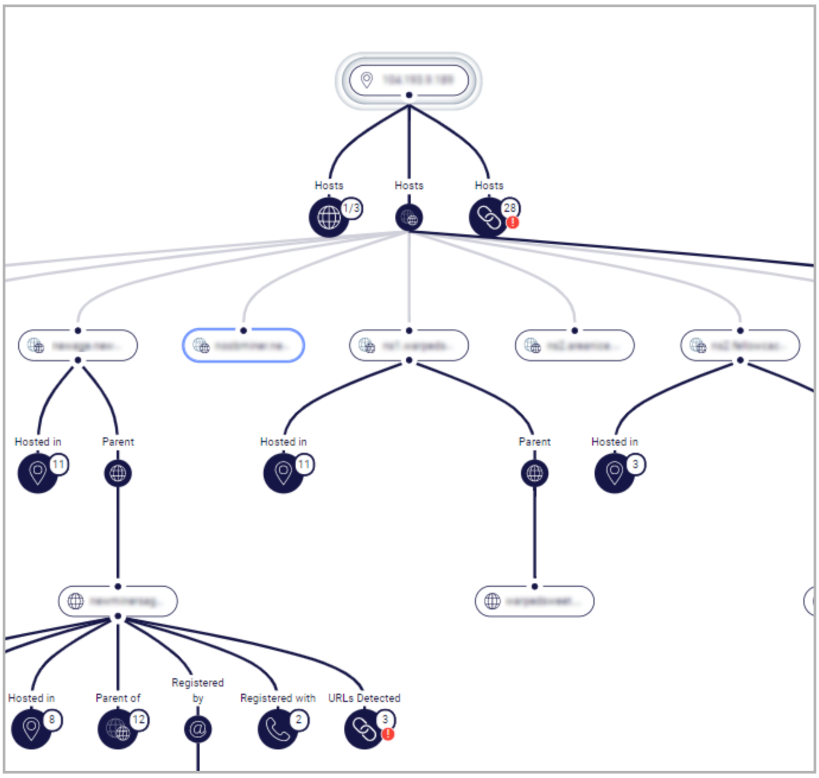
Los elementos de inteligencia sin procesar se correlacionan automáticamente con los activos de la organización (direcciones IP, dominios, marcas, ejecutivos, etc.) y se clasifican de acuerdo con un caso de uso específico: phishing, campañas de malware, relleno de credenciales, actividad fraudulenta de fuga de datos y otros. Al utilizar el algoritmo de aprendizaje automático patentado de Cyberint, esta inteligencia en bruto se prioriza de acuerdo con el riesgo y el impacto potenciales, lo que permite un análisis inteligente y rentable.



Plataforma de protección de riesgos digitales Argos™

Los motores de análisis automáticos y semiautomáticos generan alertas de inteligencia procesables que luego se difunden a los equipos de seguridad con análisis en profundidad, contexto enriquecido, perfiles de actores de amenazas y más, lo que permite a la organización tomar medidas efectivas.

LIENZO FORENSE



Plataforma de protección de riesgos digitales Argos™, Lienzo forense

El módulo de lienzo forense de Cyberint permite la identificación y la realización de un perfil de los actores de amenazas, así como la realización de una investigación profunda de las herramientas, tácticas y procedimientos (TTP) que emplean.

El lienzo forense se utiliza para enriquecer el contexto de IOC específicas o múltiples, integrando múltiples servicios en una plataforma de investigación unificada para admitir varios tipos de conexiones, incluidos la inteligencia contra amenaza Argos™, servicios de WHOIS, DNS pasivo, descubrimiento social, detección de código malicioso, etc.

TECNOLOGÍA PROACTIVA DE DETECCIÓN DE PHISHING Y DETENCIÓN

El phishing persiste como un riesgo importante para las organizaciones digitales, lo que da como resultado la toma de control de la cuenta, la pérdida de clientes y el impacto negativo en la reputación de la marca. Respondiendo a este desafío, Cyberint desarrolló el Phishing Beacon, un módulo patentado que permite la visibilidad en tiempo real de los sitios de phishing recién creados clonados del contenido del sitio web de la organización, una técnica eficaz utilizada por los actores de amenazas. La detección rápida de Cyberint nos permite eliminar los sitios de phishing en nombre de la organización para eliminar rápidamente el riesgo.

¿USTED QUÉ SACA DE ESTO?

- **REDUZCA EL RIESGO DE SEGURIDAD DE TI INVISIBLE**
- **GANE VISIBILIDAD EN SU SUPERFICIE DE ATAQUE**
- **ACORTE EL TIEMPO DE VIDA DE LA AMENAZA**
- **AMPLIE LAS CAPACIDADES DE SU EQUIPO**
- **REDUZCA EL TCO DE CIBERSEGURIDAD**

SERVICIO GESTIONADO

Servicios de ciberinteligencia personalizados que se adaptan a sus necesidades

AUMENTO DEL EQUIPO DE INTELIGENCIA DE AMENAZAS

Cyberint ofrece un programa administrado de protección contra riesgos digitales que brinda acceso a nuestra plataforma Argos™ y un equipo de analistas de amenazas cibernéticas, lo que lleva a cualquier programa de CTI a un nivel superior de calidad y rendimiento.

La asociación con el equipo de analistas de Cyberint incluye la interacción diaria con un analista dedicado que se convierte en miembro de su equipo interno. Los analistas se asignan en función de su conocimiento de las industrias y su comprensión íntima de las necesidades comerciales.

Todos los elementos de inteligencia en bruto sacados a la luz por Argos™ se verifican, contextualizan y atribuyen diligentemente a riesgos reales mediante la utilización de enormes cantidades de datos recopilados de la web abierta, profunda y oscura.

Nuestro equipo de analistas es multilingüe, lo que permite comprender a los actores de amenazas en sus respectivos idiomas. Además, el dominio del analista de la "jerga" y la cultura del ciberdelincuente le permite identificar, verificar y mitigar las amenazas que probablemente se materializarán como ataques.

Cyberint proporciona un valioso elemento humano cuando se trata de estudio, investigación y operaciones de inteligencia de amenazas. Las capacidades de HUMINT virtual, es decir, la interacción en vivo con los actores de amenazas, permiten una contextualización más profunda que se requiere para una mitigación efectiva.

INVESTIGACIÓN CYBERINT

El equipo de investigación cibernética de Cyberint explora la frontera del panorama de las amenazas cibernéticas para mantener la visibilidad estratégica de las amenazas en tendencia. El equipo de investigación cibernética analiza grandes cantidades de datos para crear informes de inteligencia de amenazas estratégicas, lo que permite a los tomadores de decisiones identificar tendencias significativas y obtener una perspectiva más amplia y profunda de los riesgos digitales que afectan a su organización. El informe incluye un análisis periódico de los riesgos del sector actual, actores de amenazas notables, análisis de TTP y más.

ÚLTIMOS INFORMES DE CYBERINT


Philippines Financial Industry
Threat Landscape Report
AUGUST 2020
Cyberint

Industria financiera de Filipinas
Informe se paisaje de amenazas

DESCARGAR


REvil
Steal, Encrypt & Auction
Ransomware Team Recent Activities and Developments
Cyberint
JUNE 2020

REvil - Robar, cifrar y subastar
Informe de investigación

DESCARGAR


Targeted Ransomware Attacks in Taiwan
May 2020
Cyberint

Ataques de ransomware dirigidos en Taiwán
Informe de investigación

DESCARGAR

BENEFICIOS DE LA ASOCIACIÓN CON LOS SERVICIOS DE INTELIGENCIA DE AMENAZAS GESTIONADOS DE CYBERINT

DETECCIÓN DE AMENAZAS

Detectar amenazas con inteligencia predictiva

IDENTIFICAR LA GRAVEDAD

Identificar la gravedad de las amenazas y comprender "el panorama general"

CAPACIDADES DE HUMINT VIRTUAL

Comunicarse directamente con los actores de amenazas, atribuir su actividad a campañas específicas y obtener más contexto e inteligencia

IDENTIFICAR OPERACIONES DE FRAUDE

Identificar y proporcionar inteligencia procesable sobre cómo responder y mitigar

DETECCIÓN DE PHISHING EN TIEMPO REAL

Operaciones de eliminación y detección de sitios web de phishing en tiempo real

INVESTIGACIONES DE AMENAZAS VIP

Supervisar la presencia en línea de sus ejecutivos para evitar que los actores de amenazas obtengan información personal para uso malintencionado

MAPEO Y SUPERVISIÓN

Mapear y supervisar la presencia digital de la organización, incluidas las fugas de credenciales, las vulnerabilidades digitales y la filtración de documentos confidenciales

Gartner peerinsights™ 4.8 ★★★★★

DE NUESTROS CLIENTES

> *Es servicio gestionado que brinda valor real al convertir los hallazgos en información relevante y alertas adaptadas a nuestro negocio.*
>
> Gran minorista con sede en EE. UU.

> *Hasta que no use Cyberint, realmente no tiene la comprensión correcta de quién está tratando de atacar su organización.*
>
> Gran minorista de comercio electrónico
> con sede en EE. UU.

CONTÁCTENOS

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

EE. UU.
214 W 29th St.
Nueva York, 10001
Tel: +1-646-568-7813

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

REINO UNIDO
14 Grays Inn Rd., Holborn
WC1X 8HN, Londres
Tel: +44-203-514-1515

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

LATAM
Ciudad de Panamá
Tel: +1-929-399-8495

Cyberint