Cómo gestionar el riesgo cibernético con acciones preventivas, correctivas y mapas de ruta

Narcizo Valdés Morales

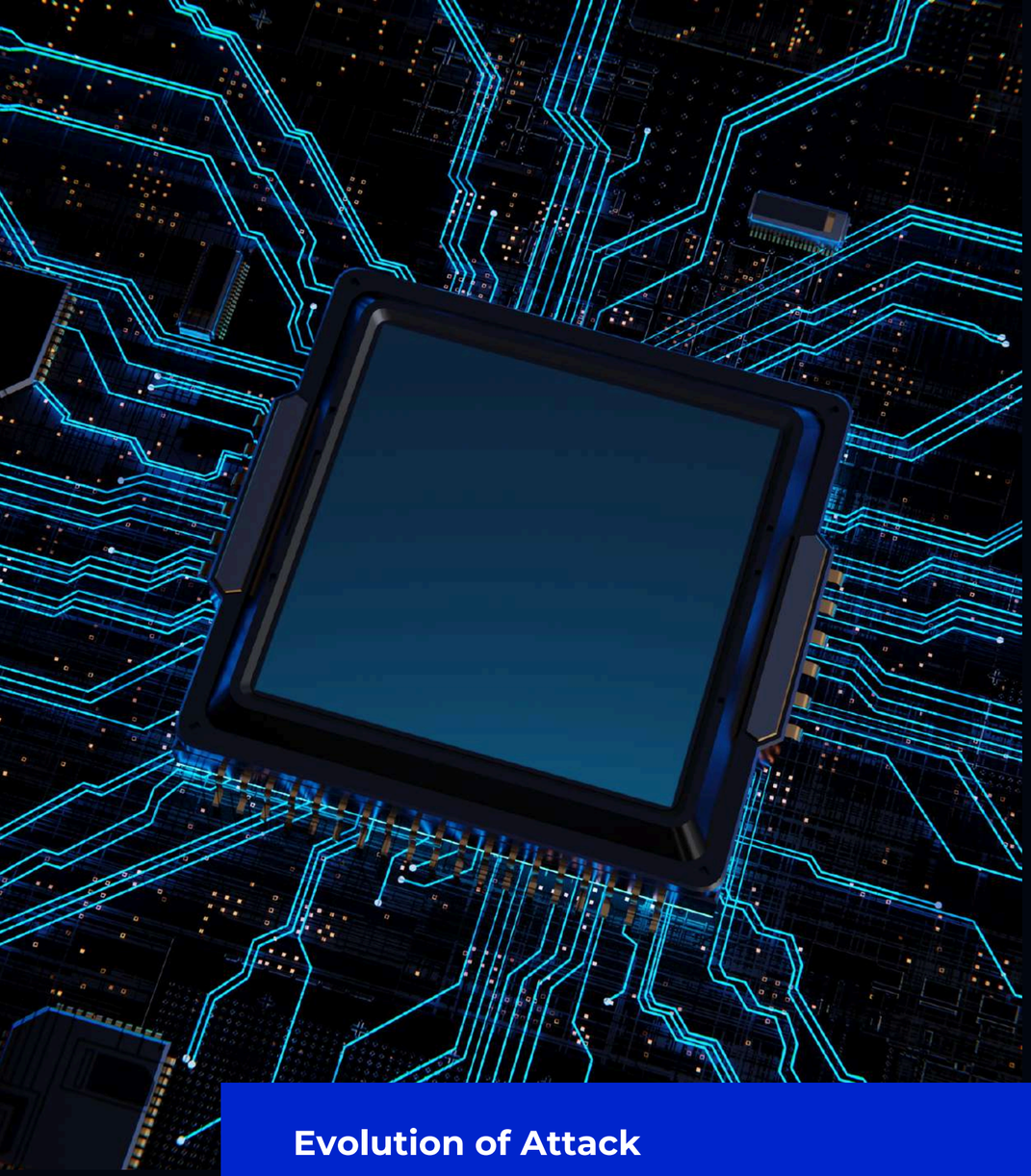
General Manager LATAM

www.inet-academy.com
www.dataonnet.com
www.benchmarklatam.com

narcizo@inet-academy.com

www.inet-academy.com

+52 3331280513



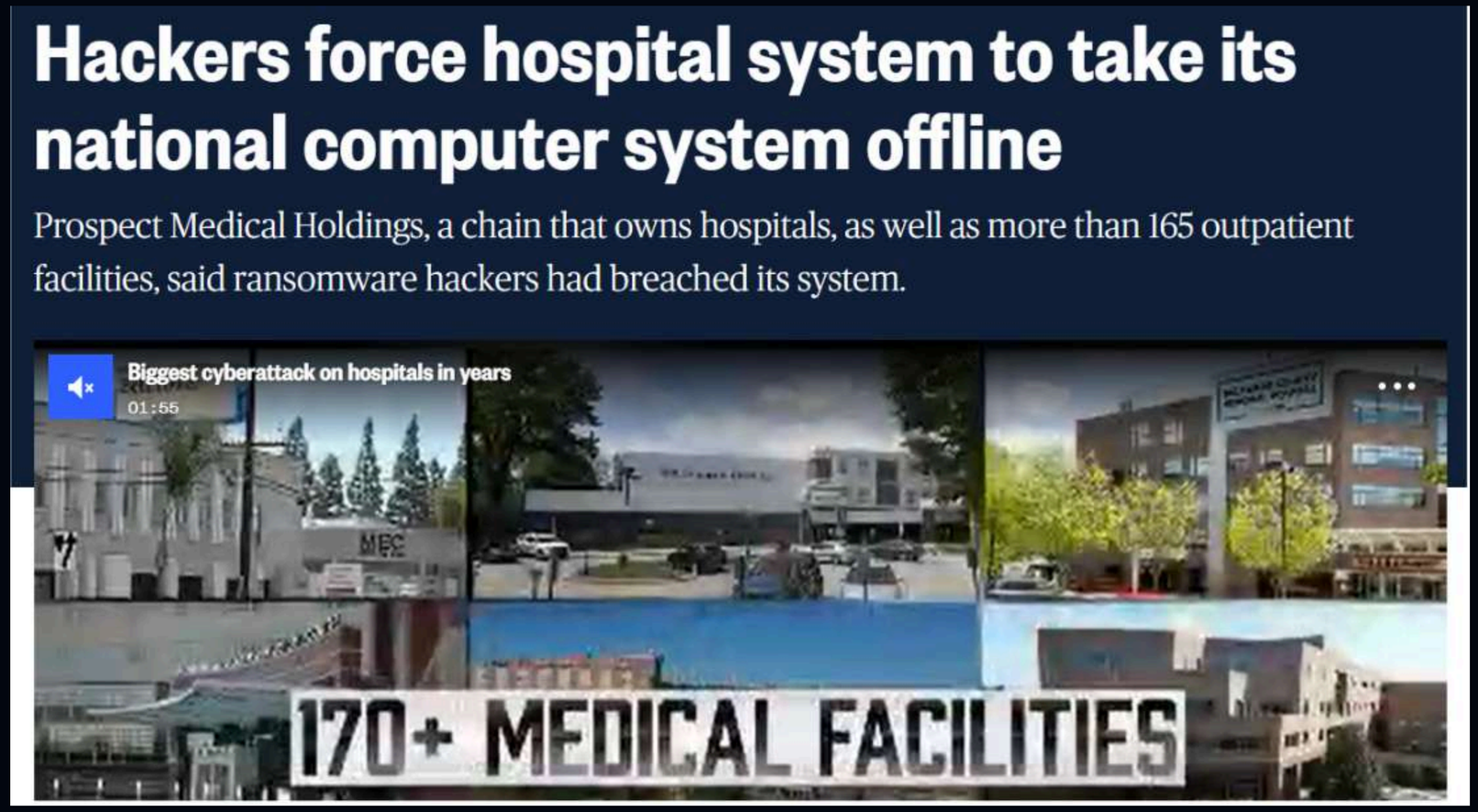
¿PORQUE PENSAR EN LOS RIESGOS CIBERNÉTICOS?

Evolution of Attack **90%**

IMPORTANT INFORMATION

Fuente:

Utilizing cutting-edge encryption to safeguard data from hackers.

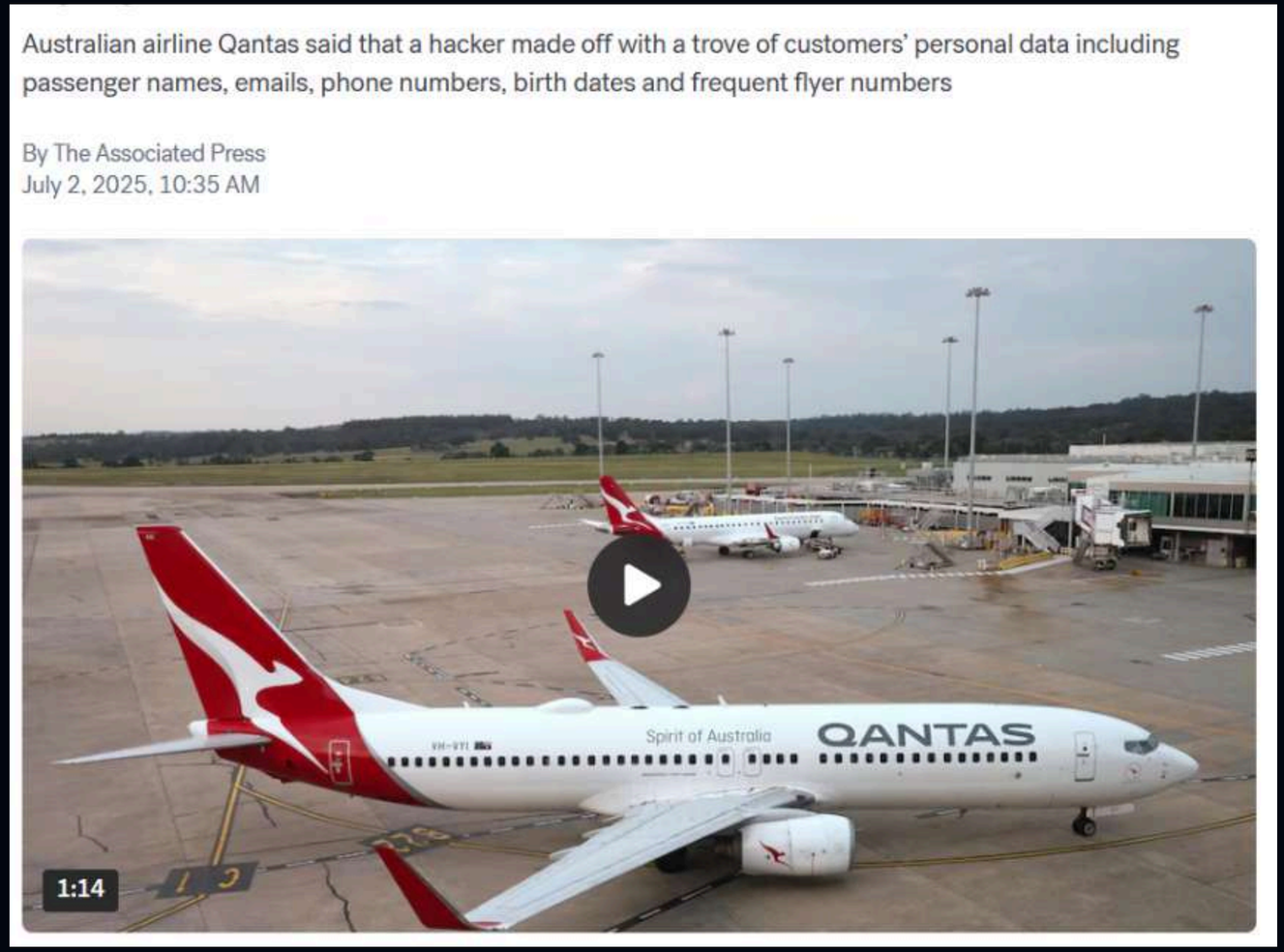


AUSTRALIAN AIRLINE QANTAS SAYS CUSTOMER DATA STOLEN BY CYBERCRIMINAL

Australian airline Qantas said Wednesday that a hacker made off with a trove of customers' personal data including passenger names, emails, phone numbers, birth dates and frequent flyer numbers.

The company said in a statement that a cybercriminal targeted one of its call centers on Monday and gained access to a **third-party customer service platform that holds records for 6 million passengers.**

Qantas apologized to customers and said that while it's still investigating the proportion of data stolen, "we expect it will be significant."



abc NEWS Live Video Shows Shop Stream on

Live Updates Trump administration | Latest Texas flooding | Inflation report | Flash flood threat | 'Zombie' fungi | College cheating scandal

Cyber attacks on the rise

One group of cyber experts say 16 billion passwords have been compromised in data leaks.

June 21, 2025

IMPORTANT INFORMATION

https://apnews.com/article/brazil-hack-cyberattack-bank-5e39633b2ce3a662b90978dcf4647510

WORLD NEWS

Police in Brazil arrest a suspect over $100M banking hack

BY ASSOCIATED PRESS
Updated 1:17 PM GMT-6, July 4, 2025

SAO PAULO (AP) — Police in Brazil arrested a suspect in connection with a cyberattack that diverted more than 540 million Brazilian reais (about $100 million) from the country's banking systems, authorities said Friday.

The breach affected Brazil's widely used instant payment system, known as PIX, which is used by 76.4% of the population. Hackers targeted C&M, a software company that connects financial institutions to the Central Bank to enable PIX transactions.

Police in Sao Paulo said the $100 million loss refers to just one financial institution that worked with C&M and total losses could be even higher.

Officials identified the suspect as João Roque, a C&M employee who worked in information technology and allegedly helped others gain unauthorized access to PIX systems.

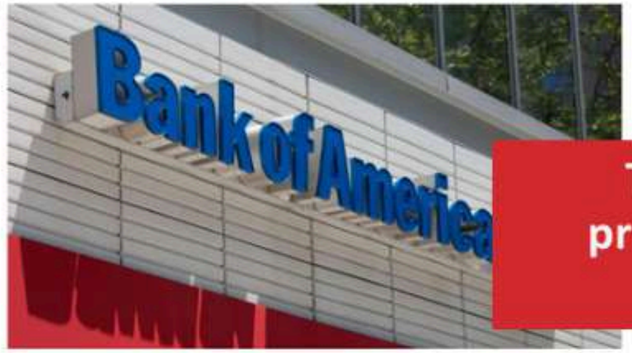
LAS BRECHAS DE SEGURIDAD ES UN TEMA DE TODOS LOS DÍAS

Forbes ADVISOR

Bank of America Customers Left In The Dark About Data Breach For 90 Days

By Natalie Campisi

Edited By Dawn Nicl



Latest Local News Live Shows ••• CBS NEWS

MONEYWATCH | Managing Your Money Your Taxes Retirement

MONEYWATCH

American Express card data exposed in third-party breach

MONEY WATCH

By Kate Gibson
Edited By Aimee Picchi
March 6, 2024 / 1:09 PM EST / CBS News

Todas relacionadas con proveedores de servicios o terceras partes

CISO

News Leaders Speak Events Webinars Brand Solutions Newsletters More

Truist Bank confirms data breach after cyberattack

The hacker, identified as Sp1d3r, is selling what they claim is data on 65,000 employees for $1 million. According to DarkTower Intelligence analyst James Hub, the data also includes bank transactions, account information, and source code for Truist's IVR system.

/S MUNDO

Internacional Hay Festival Economía Ciencia Salud

El robo masivo de datos del Banco Santander que afecta a millones de clientes en Chile, Uruguay y España, y a todos sus empleados

El Banco Santander confirmó que se había accedido a información de sus clientes.

¿CUÁL ES EL IMPACTO EMPRESARIAL?

DAÑO A LA REPUTACIÓN:

La pérdida de confianza de los clientes y socios comerciales puede tener consecuencias duraderas, afectando la imagen y la posición competitiva de la empresa

DAÑO REGULATORIO:

Multas por incumplimiento de normativas nacionales e internacionales, y costos legales asociados a demandas.

DAÑOS OPERATIVOS:

Los ataques pueden causar la paralización de sistemas informáticos, interrumpiendo la producción, la comunicación y la prestación de servicios.

PÉRDIDA DE DATOS:

La información confidencial de clientes, empleados o de la propia empresa puede ser robada, modificada o eliminada, causando graves consecuencias legales y financieras.

LA EXPLOSIÓN INFINITA DE LAS RELACIONES DIGITALES CON TERCEROS HA CONTRIBUIDO EN AUMENTAR EL CIBER RIESGO

+50% de empresas experimentaron una brecha de sus terceros.

Sólo el **34%** confía en que un tercero les informaría de sus brechas.

84% de las empresas informaron que los incidentes de riesgo de terceros conducen a interrupción operativa

Panorama dinámico de amenazas

A medida que surgen nuevas amenazas, es necesario mantener la postura cibernética de los terceros de manera proactiva y continua

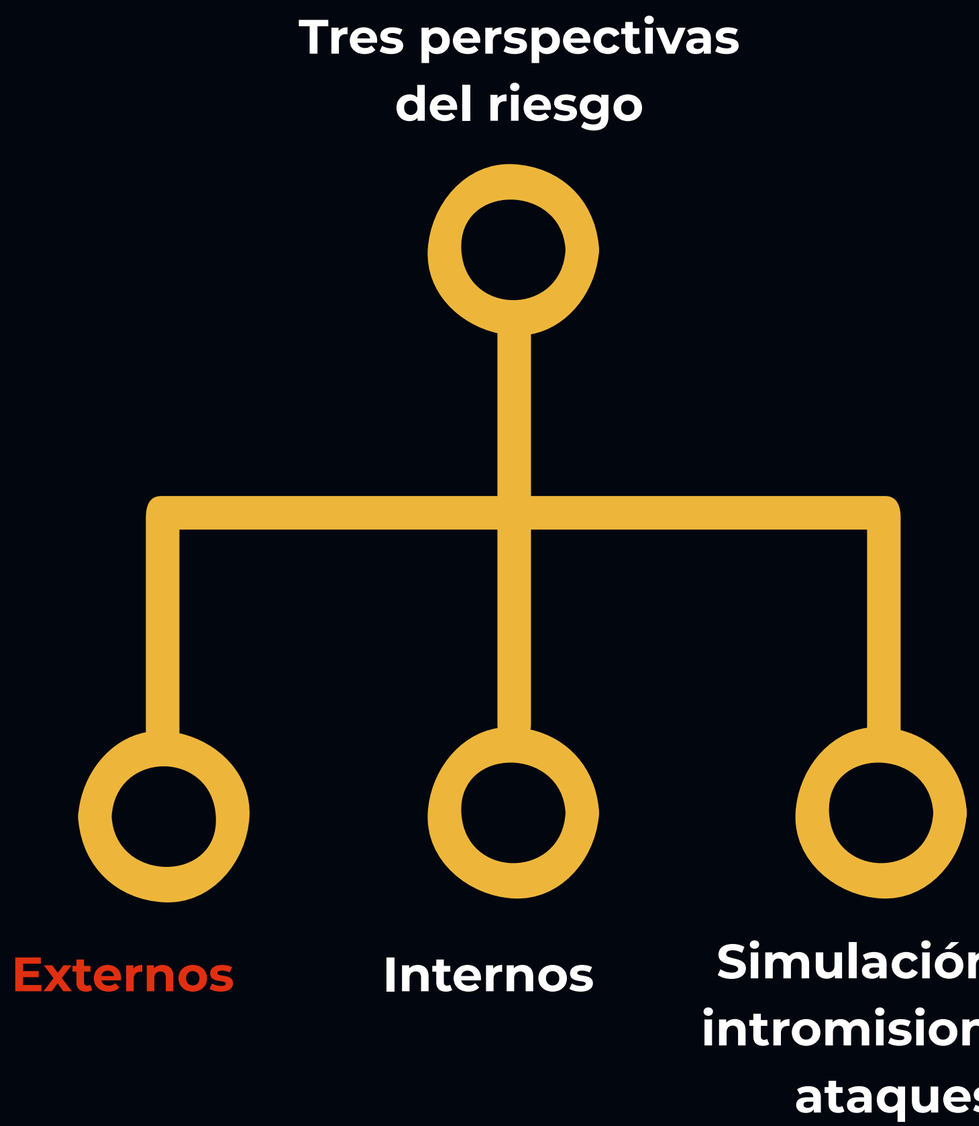
Proveedores de Proveedores

Sus 3ª Partes tienen su propio conjunto de 3ª partes, por lo que es importante tener una visibilidad holística del ecosistema

Ecosistema de Procesos

Cada proceso de negocio se compone de sistemas internos más capacidades de terceros. Categorice, priorice y agregue para comprender el riesgo organizacional

ENTENDIENDO LOS RIESGOS CIBERNÉTICOS EXTERNOS

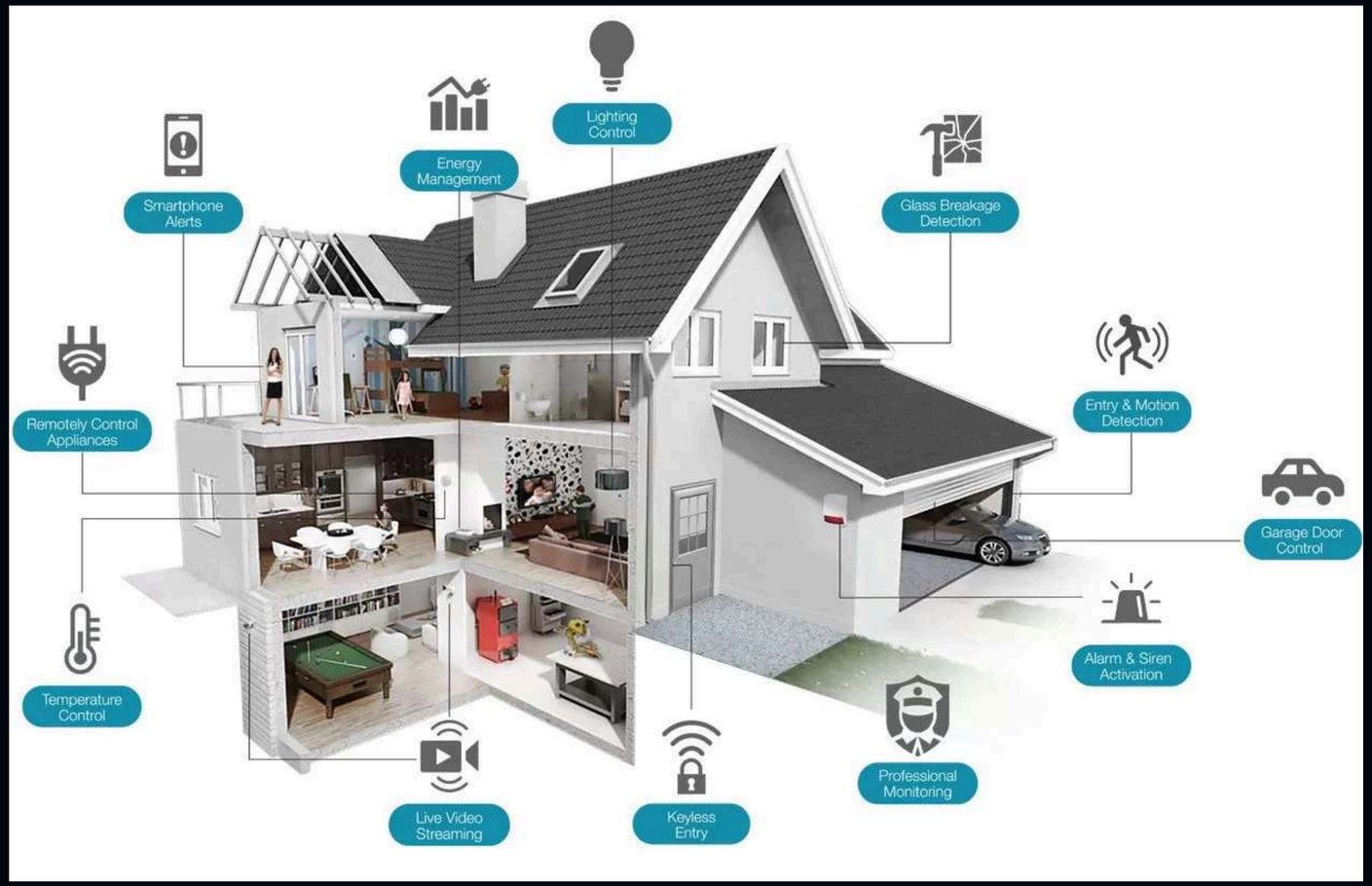


EVALUAR LA EXPOSICIÓN AL RIESGO DE TERCEROS

Cierra la puerta principal y trasera, las ventanas

Usa cerrojos y cerraduras de pomo en las puertas.

Proveedores de servicios.



Firewalls, SW patch management

Web and cctv security

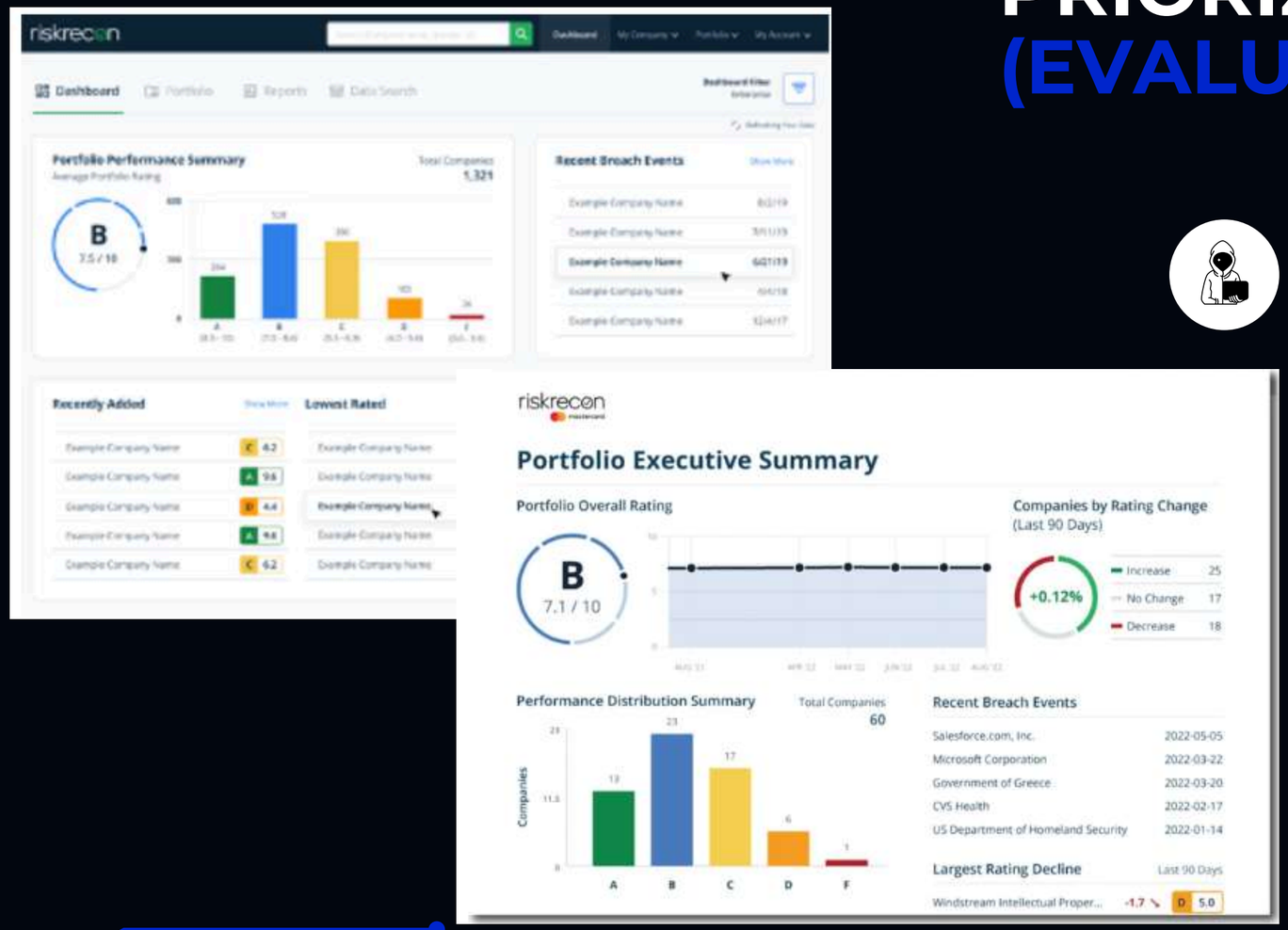
Cercas perimetrales

Piensa en las capacidades actuales de seguridad en cómo proteger tu casa de forma EXTERNA

ENTENDIENDO LOS RIESGOS DE TERCEROS

- ¿Has evaluado la exposición de riesgo en tus proveedores?
- ¿Cada cuanto tiempo es necesario evaluar a tus proveedores?
- ¿Existen hallazgos que pueden afectar tus operaciones?

DIAGNÓSTICO Y PRIORIZACIÓN DE RIESGOS (EVALUACIÓN DE TERCEROS)



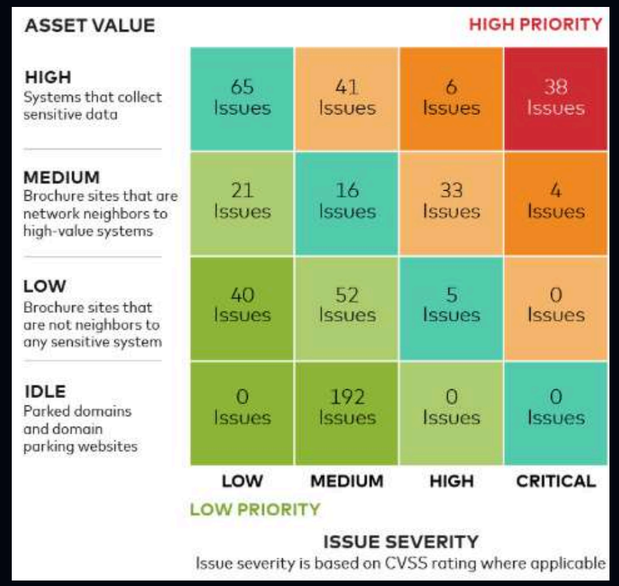
✓ Evalúe todo su ecosistema empresarial – entidades y servicios críticos, subsidiarias y proveedores – desde una perspectiva holística.

- Descubrimiento de activos.
- Evaluación profunda de riesgos.
- Priorización de Riesgos.
- Perfil de empresa & TI.
- Integrar las evaluaciones los terceros en un solo tablero.
- Continua y seguimiento (Roadmap)

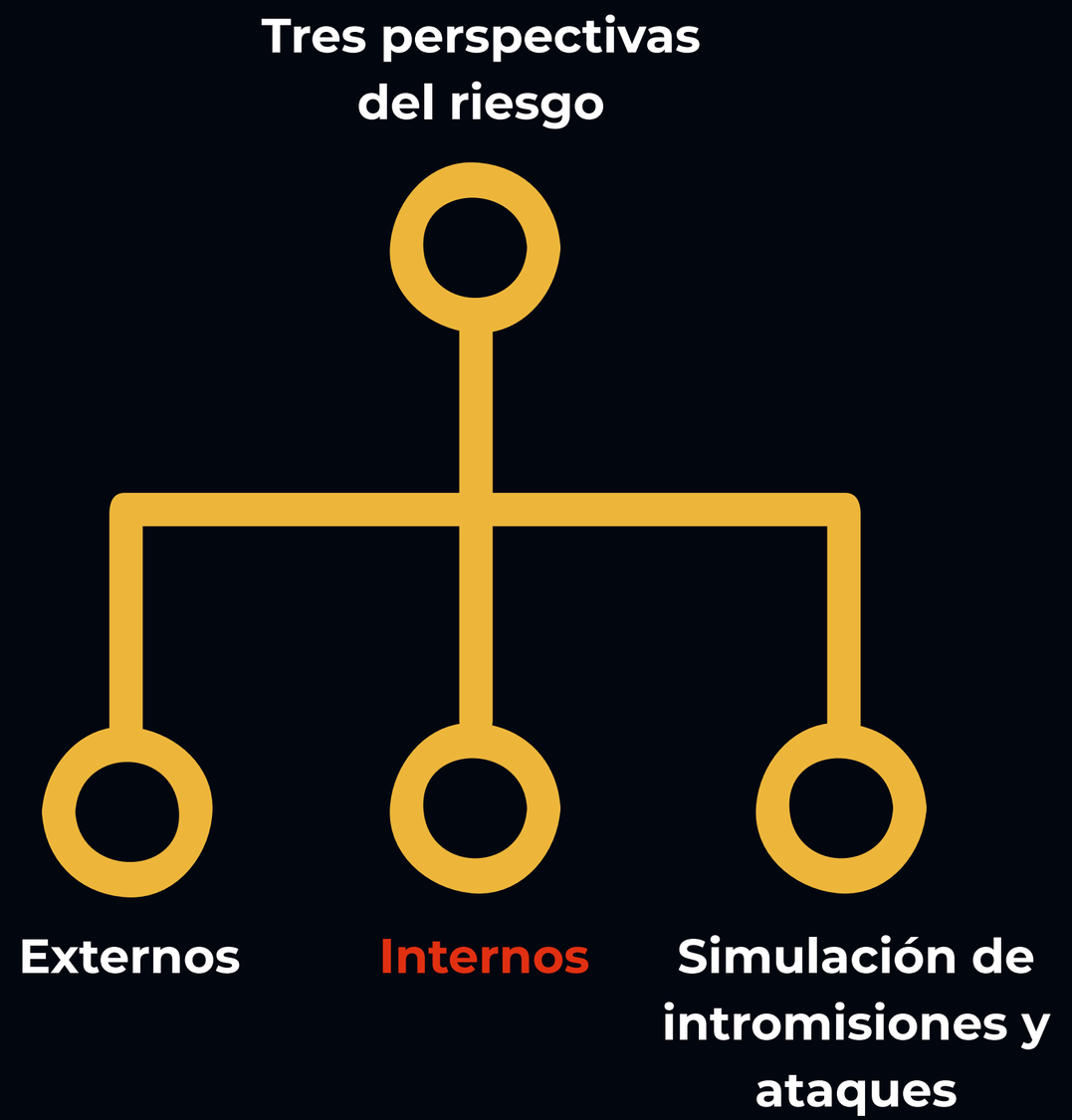
ENTENDIENDO LOS RIESGOS DE TERCEROS

- Risk Recon permite evaluar el riesgo cibernético derivado de relaciones comerciales con terceros.
- Monitoreo proactivo y continuo del entorno de cualquier entidad con presencia en línea.

- Acciones preventivas y correctivas para dar seguimiento a una mejora continua y bajar exposición de riesgos.



ENTENDIENDO LOS RIESGOS CIBERNÉTICOS INTERNOS



EVALUAR LA EXPOSICIÓN AL RIESGO INTERNO

Madurez de la ciberseguridad y cuantificación del riesgo financiero interno.

Piensa en las capacidades actuales de seguridad en tu casa pero de forma INTERNA

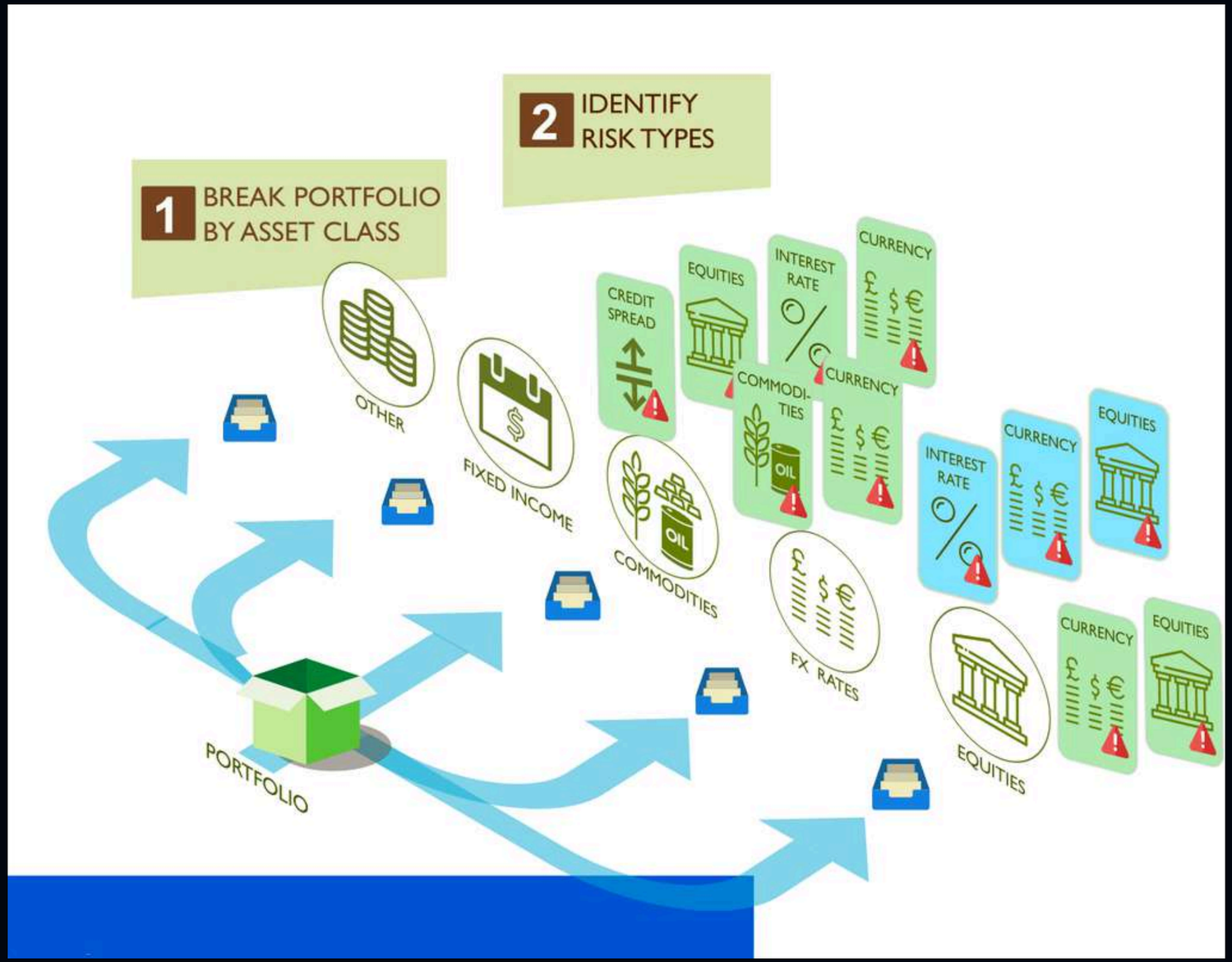
PREGUNTAS CLAVE

1. ¿Tiene catalogados cuáles son los activos más críticos en su organización?
2. ¿Conoce cuál es el impacto financiero de las brechas de seguridad en su organización?
3. ¿Conoce la postura interna de madurez (riesgos) de su organización?
4. ¿Cómo determina actualmente en que invertir para la ciberseguridad en la organización?
5. ¿Cuántas evaluaciones de riesgos realiza en el año?
6. ¿Sigue un mapa de ruta en ciberseguridad?

EVALUAR LA EXPOSICIÓN AL RIESGO INTERNO

- ¿Están identificados los activos empresariales?
  - ¿Están Catalogados los activos empresariales?
  - ¿Las tecnologías involucradas en la operación de controles y activos han sido identificadas?
    - ¿Ha evaluado la relevancia y existencia de los controles existentes en su organización?

CLASIFICACIÓN DE ACTIVOS

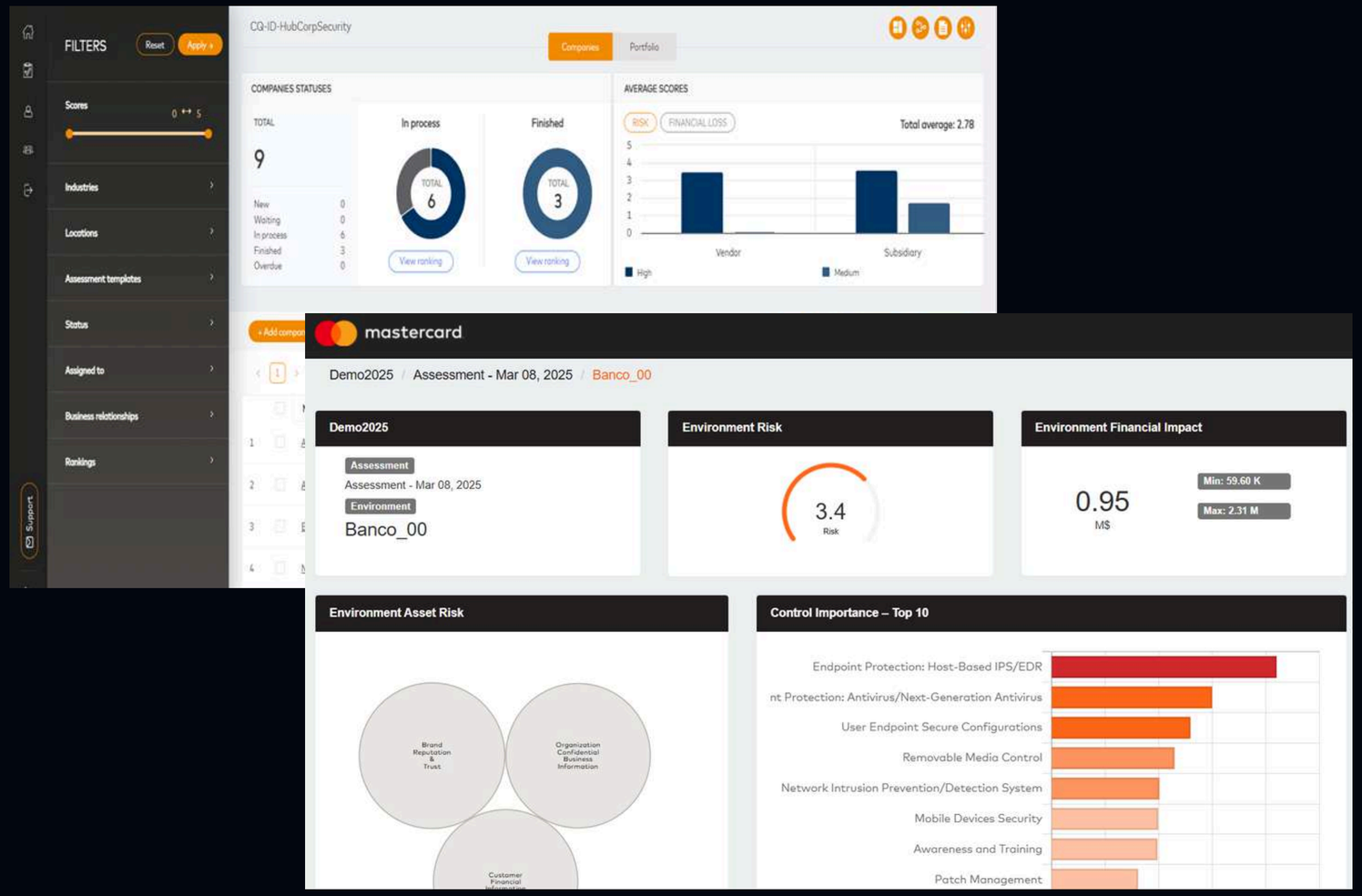


PRIORIZACIÓN DE REMEDIACIÓN DE BRECHAS PARA REDUCIR SU RIESGO CIBERNETICO

- Evaluación integral de las capacidades y riesgos de ciberseguridad en toda la organización.
- Análisis de los controles y estrategias de ciberseguridad, alineados con el panorama de amenazas.
- Reducir los costos financieros asociados a una brecha de seguridad.
- Reducción de riesgos priorizadas para maximizar el retorno de la inversión.
- Actualizaciones continuas para reflejar cambios en las prácticas y proyectos de ciberseguridad, así como en las amenazas emergentes.
- Evaluar el cumplimiento de políticas de seguridad, procedimientos y capacidades técnicas.

EVALUAR LA EXPOSICIÓN AL RIESGO INTERNO

- Motor de simulación para la evaluación continua de proyectos y toma de decisiones en ciberseguridad.



LA EXPLOSIÓN INFINITA DE LAS RELACIONES DIGITALES CON TERCEROS HA CONTRIBUIDO A AUMENTAR EL CIBER RIESGO

- Evaluar procesos y controles actuales implementados.
- Demografía y características de la organización
- Evaluar contra una normativa de cumplimiento.
- Diagnóstico / entrevistas / evidencia
- Diagnósticos técnicos internos y externos
- Revisar configuraciones de las tecnologías actuales

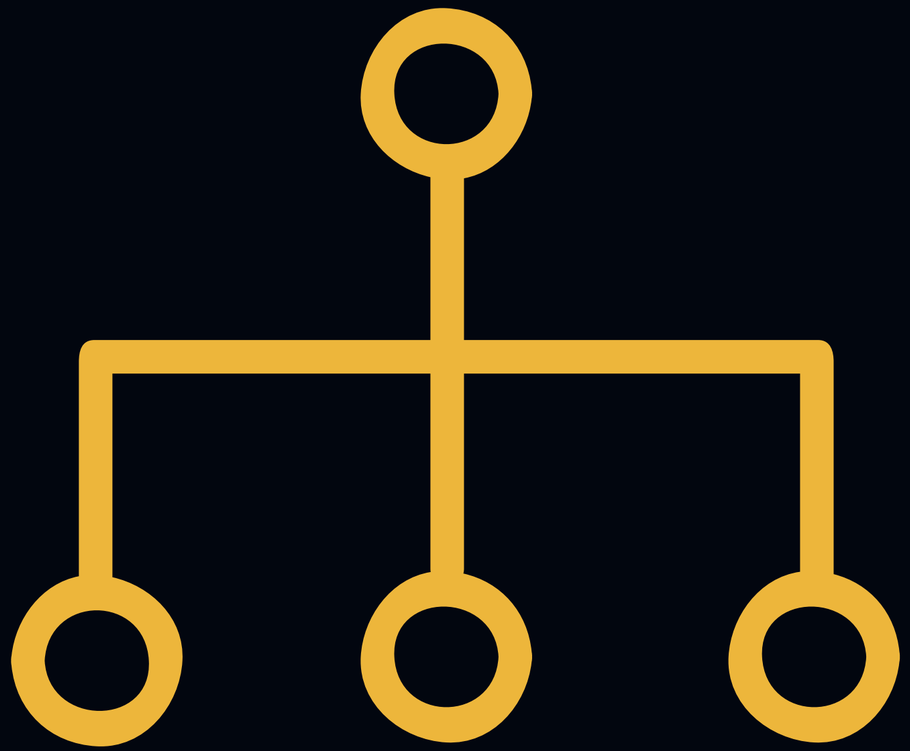
Preparación de los controles y estrategias de ciberseguridad y la criticidad de cada uno, basada en el entorno de amenazas relevante.

Cuantificación de los riesgos de ciberseguridad específicos de acuerdo con el tamaño, ingresos, región, industria y madurez de los controles de la organización.

Acciones correctivas y preventivas en un mapa de ruta.

Simulación del retorno de la inversión en caso de que se implementen controles sobre las brechas.

Tres perspectivas del riesgo



Internos

Externos

Simulación de intromisiones y ataques

SIMULACIÓN DE INTROMISIONES Y ATAQUES

SIMULACIÓN DE AMENAZAS TRADICIONAL

- Hacking ético, pruebas de penetración, auditoría técnica, etc.
- Muestra bajo una sola vez al año.
- Con enfoque solo interno, no en la cadena de 3ros.
- No se analiza impacto de pérdida financiera.
- Mayormente un enfoque técnico.
- No existen simulaciones para determinar que acciones tomar.

SIMULACIÓN DE AMENAZAS

- **Entorno cambiante:** La tecnología y los panoramas de amenazas evolucionan continuamente.
- **Recursos limitados:** Los recursos de TI son limitados para mantenerse al día con los esfuerzos de implementación, mantenimiento y remediación
- **Configuraciones erróneas:** Las configuraciones incorrectas son una de la causa principal de incidentes.
- **Incidencias:** El número de incidencias o hallazgos aumenta sin acciones concretas. Se tiene un vector predecible.

SIMULACIÓN DE ATAQUES CONTINUO
¿CÓMO FUNCIONA?

1 Amenazas globales por más de 3500 díarias con más de 10 000 acciones actualizadas diariamente

2 Se envía tráfico malicioso simulado al agente

3 Se analiza y detecta automáticamente

4 Se puede acceder al tipo de violación y escenarios de ataque probados y a los resultados de estas pruebas, así como a las recomendaciones de remediación

TODO ESTA CONECTADO

EVALUACIÓN DE TERCEROS

EVALUACIÓN INTERNA

SIMULACIÓN DE ATAQUES

SISTEMA DE GESTIÓN ANTISOBORNO

CONTINUIDAD DE NEGOCIO BCP, DRP

PREVENCIÓN DE FUGA DE DATOS

PROTECCIÓN DE DATOS PERSONALES

INFRAESTRUCTURA SEGURA E HIPERCONVERGENTE

CAPACITACIÓN

MAPA DE RUTA ...

Tomar acciones estratégicas enfocadas en la prevención, respuesta y cultura organizacional.

Establecer controles fuertes, como deshabilitar accesos no autorizados, restringir dispositivos externos, y garantizar acceso remoto seguro.

Hacer de la ciberseguridad una prioridad a nivel corporativo. Esto implica asignar recursos adecuados, crear políticas claras, y supervisar su cumplimiento.

Mantener un enfoque de mejora continua y actualización constante ante nuevas amenazas tecnológicas y regulatorias.

Movilizar equipos responsables de seguridad y definir roles y responsabilidades con claridad, para responder ágilmente ante incidentes.

Definir y aprobar planes de respuesta a incidentes, incluyendo procedimientos para identificar, contener y mitigar ataques, con enfoque en minimizar impactos.

Fomentar una cultura de ciberseguridad en toda la organización mediante formación continua y concientización en todos los niveles.

Invertir en personal capacitado en TI y ciberseguridad, que tenga certificaciones apropiadas y pueda manejar riesgos tecnológicos.

GRACIAS

Evolution of Attack **90%**