ONLINE

INFOSECURITY SUMMIT

Detecta y Responde a Amenazas que se Expanden en Tiempos de COVID-19

Alfredo Cristerna
Senior Management Consultant
alfredo.cristerna.guzman@ibm.com

infosecurity® MEXICO

En alianza con

ISACA. Mexico City Chapter

ISACA. Guadalajara Chapter

Organizado por Reed Exhibitions®

Un Aumento Significativo en las Amenazas.

91%

de los ataques se inician con una campaña de "*phishing*"

84%

de aumento en las herramientas de trabajo a distancia desde inicios de Feb/2020

14,000%

de aumento de "spam" y "phishing" debido a COVID-19 desde inicios de Feb/2020

Vectores clave de ataques de ciberseguridad

"Phishing";

Distribución de "*malware*";

Registro de nuevos dominios;

Ataques al acceso remoto (VPNs)

Fuente: *https://www.trustar.co/en/covid-19; https://www.ibm.com/security/COVID-19; X-Force Threat Intelligence Index; National Cyber Security Centre-CISA Cyber + Infrastructure-Advisory: COVID-19 explotado por agentes cibernéticos maliciosos.*

Organizándonos en la Incertidumbre

Visión | *Protección* | *Detección* | *Respuesta* | *Recuperación*

Gente | Procesos | Tecnologías

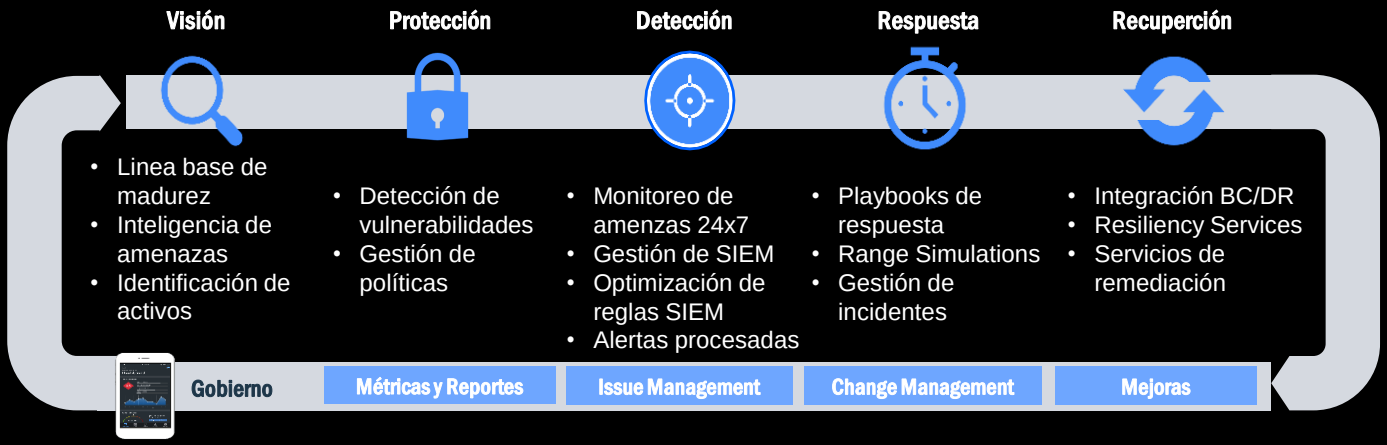
Gobierno y Mejora Continua de Procesos

Organizándonos en la Incertidumbre

Organizándonos en la Incertidumbre

SOLUCIÓN DE SEGURIDAD MÁS INTELIGENTE PARA ADMINISTRAR EL CICLO DE VIDA DE LAS AMENAZAS CON PERSPECTIVA DE 360º

Un marco programático conduce a un enfoque integrado prescriptivo que impulsa mejores resultados.



Organizado por Reed Exhibitions

Organizándonos en la Incertidumbre

SOLUCIÓN DE SEGURIDAD MÁS INTELIGENTE PARA ADMINISTRAR EL CICLO DE VIDA DE LAS AMENAZAS CON PERSPECTIVA DE 360º

Un marco programático conduce a un enfoque integrado prescriptivo que impulsa mejores resultados.

Socio de seguridad con expertos de clase mundial que pueden aportar información crítica.

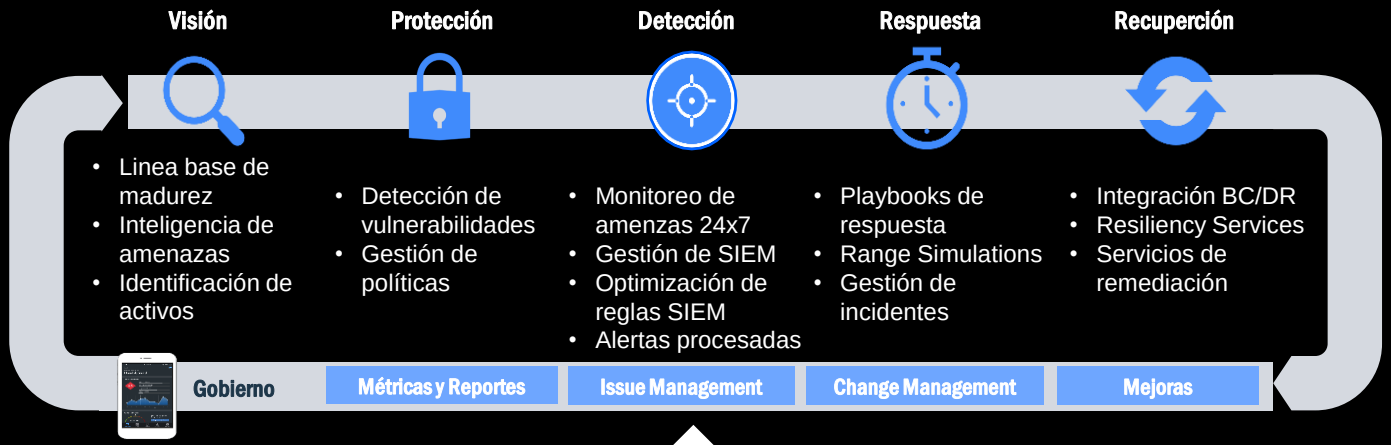
Organizándonos en la Incertidumbre

SOLUCIÓN DE SEGURIDAD MÁS INTELIGENTE PARA ADMINISTRAR EL CICLO DE VIDA DE LAS AMENAZAS CON PERSPECTIVA DE 360º

Un marco programático conduce a un enfoque integrado prescriptivo que impulsa mejores resultados.

Socio de seguridad con expertos de clase mundial que pueden aportar información crítica.

Una plataforma más inteligente que acelera la investigación y la respuesta con análisis, IA y orquestación.



Encontrar Debilidades (X-Force RED) | Detección y Análisis de Amenazas (XFTM) | Respuesta a Incidentes (IRIS) | Ciber-Recuperación (GTS)

QRadar on Cloud & Cloud Pack for Security | X-Force Exchange | Analytics Engines | Resilient Orchestration | Use Case Library | Portal & Mobile App

Partner Ecosystem — IBM Security · Carbon Black · Cisco · CrowdStrike · Fortinet · paloalto Networks · Check Point Software Technologies Ltd.

Organizado por Reed Exhibitions

Acerca de X-Force Red:

Nuestra misión: Hackear todo para asegurar todo

X-Force Red

X-Force Red es un equipo global de hackers que usa las mismas herramientas, técnicas y forma de pensar que los atacantes para identificar y ayudar a los clientes a mitigar sus vulnerabilidades más críticas:

- **Penetration Testing**
- **Vulnerability Management Services**
- **Adversary Simulation.**
- **Application Testing**

– X-Force Red can perform testing in four global hacking labs worldwide, remotely, or on-premise

X-Force Red Penetration Testing Services

— Al realizar pruebas, se deben considerar distintas posibilidades para lograr una intrusión:

- External Threat
- Insider
- Malicious user or customer
- Hacktivist

Application

- Web
- Mobile
- Terminal
- Thick-client
- Mainframe
- Middleware
- Cloud

Network

- Internal
- External
- Wireless
- Other radio frequencies
- SCADA

Human

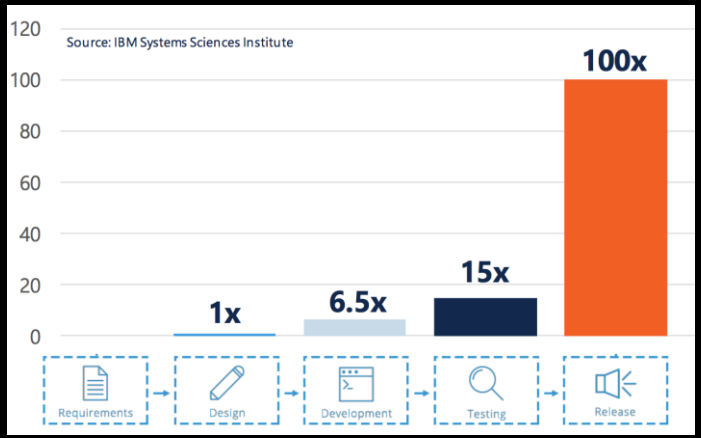
- Physical
- Social engineering
- Phishing

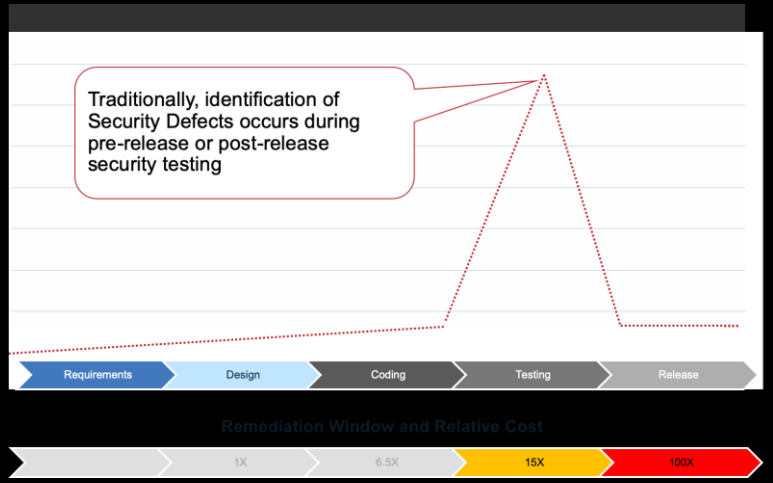
Hardware & embedded devices

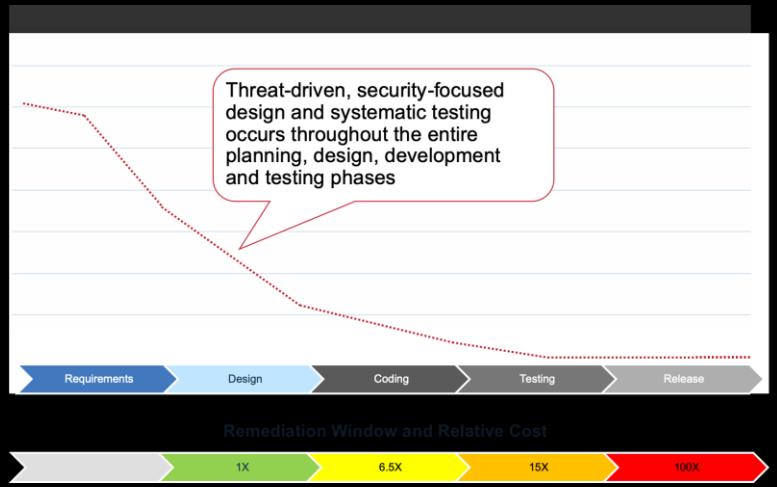
- IoT
- Wearable tech
- Point-of-sale
- ATMs
- Self-checkout kiosks

Application Testing

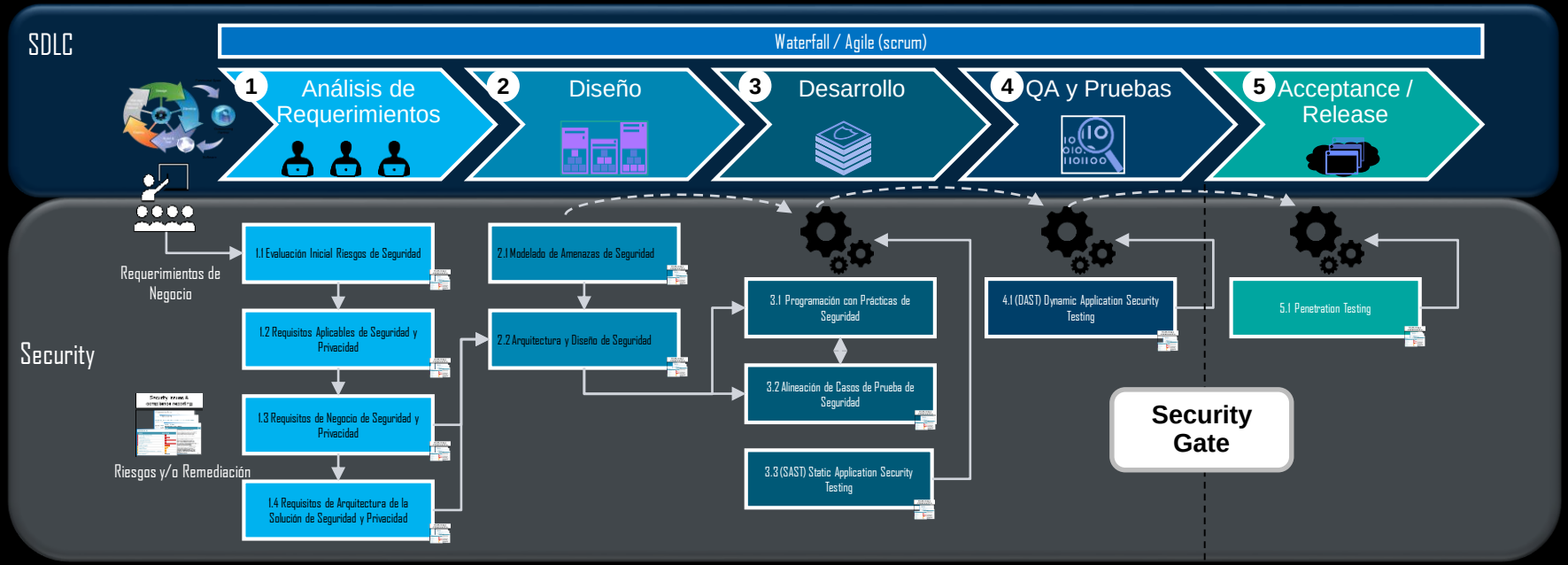
- Penetration Testing
- Vulnerability Assessment
- Source Code Review
- SSDLC







Secure SDLC



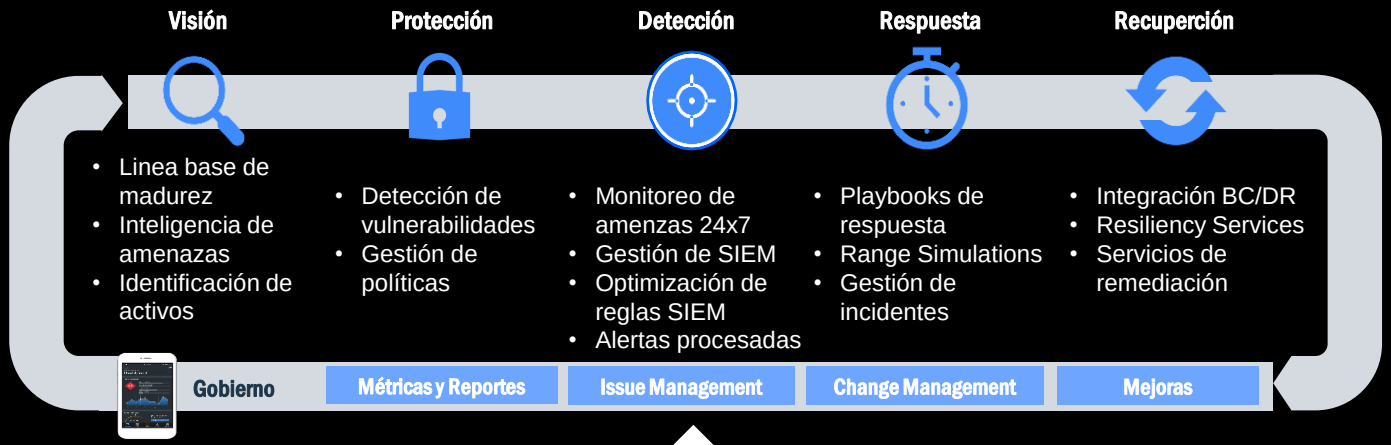
Organizándonos en la Incertidumbre

SOLUCIÓN DE SEGURIDAD MÁS INTELIGENTE PARA ADMINISTRAR EL CICLO DE VIDA DE LAS AMENAZAS CON PERSPECTIVA DE 360º

Un marco programático conduce a un enfoque integrado prescriptivo que impulsa mejores resultados.

Socio de seguridad con expertos de clase mundial que pueden aportar información crítica.

Una plataforma más inteligente que acelera la investigación y la respuesta con análisis, IA y orquestación.



Encontrar Debilidades (X-Force RED) | Detección y Análisis de Amenazas (XFTM) | Respuesta a Incidentes (IRIS) | Ciber-Recuperación (GTS)

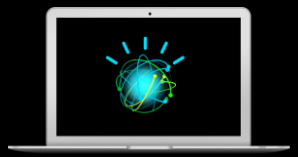
QRadar on Cloud & Cloud Pack for Security | X-Force Exchange | Analytics Engines | Resilient Orchestration | Use Case Library | Portal & Mobile App

Partner Ecosystem — IBM Security · Carbon Black · Cisco · CrowdStrike · Fortinet · paloalto Networks · Check Point Software Technologies Ltd.

Organizado por Reed Exhibitions

X-Force Threat Management

FAMILIA DE SERVICIOS



X-Force Detect (Automático)

- Servicio Global de bajo costo, manejado con AI, **alertas automáticas 24x7** hacia los grupos de investigación del cliente
- Integración de log sources y casos de uso, así como acceso a librería de casos de uso (via SCE)
- Gestión diaria de políticas y reglas en SIEM, ajustes de desempeño, parcheo y soporte a appliances
- VSOC Portal y acceso al Mobile App, reportes estándar

X-Force Detect + Investigate

- Servicio global experto con monitoreo 24x7 con Triage humano de TI (LI y L2) así como IBM Watson Analytics
- Investigación mejorada de T2 y gestión de runbook de respuesta a incidentes por analistas SOC, con hosted Resilient
- XFTM Advise Services trimestral incluido

X-Force Detect Incluido

X-Force Threat Management Program

- Marco de referencia programático gobernado por prescripción consultiva, y que maneja la seguridad del cliente y su ruta de madurez, e integra lecciones aprendidas
- Pruebas ofensivas, descubrimiento de activos, ejercicios de prueba y revisiones de IR plan, así como servicios de Respuesta a Incidentes
- Inteligecia de amenazas específica para la geografía, industria y ambiente del cliente

X-Force Investigate Incluido

X-Force Detect Incluido

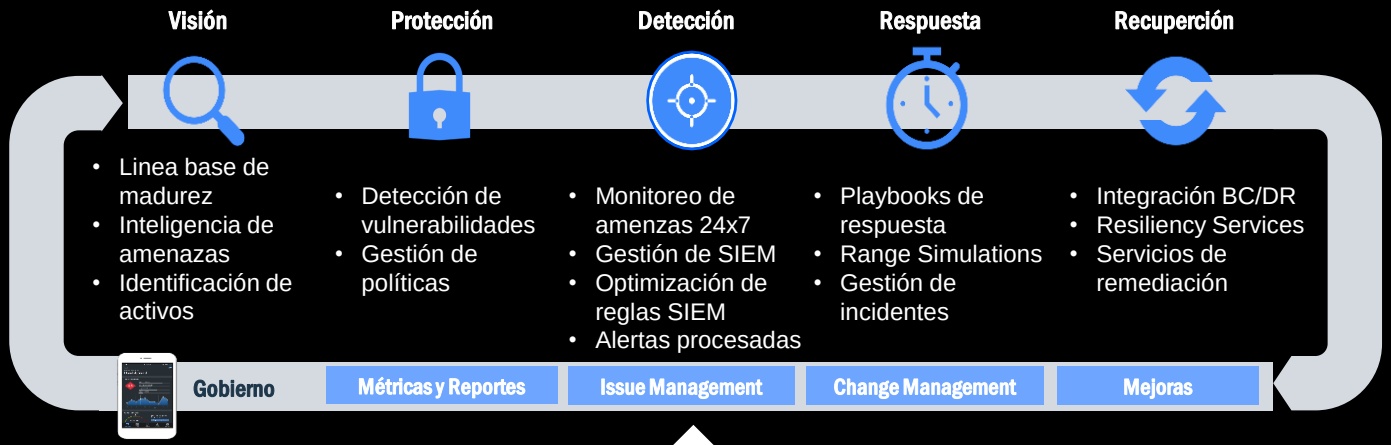
Organizándonos en la Incertidumbre

SOLUCIÓN DE SEGURIDAD MÁS INTELIGENTE PARA ADMINISTRAR EL CICLO DE VIDA DE LAS AMENAZAS CON PERSPECTIVA DE 360º

Un marco programático conduce a un enfoque integrado prescriptivo que impulsa mejores resultados.

Socio de seguridad con expertos de clase mundial que pueden aportar información crítica.

Una plataforma más inteligente que acelera la investigación y la respuesta con análisis, IA y orquestación.



Encontrar Debilidades (X-Force RED) | Detección y Análisis de Amenazas (XFTM) | Respuesta a Incidentes (IRIS) | Ciber-Recuperación (GTS)

QRadar on Cloud & Cloud Pack for Security | X-Force Exchange | Analytics Engines | Resilient Orchestration | Use Case Library | Portal & Mobile App

Partner Ecosystem — IBM Security · Carbon Black · Cisco · CrowdStrike · Fortinet · paloalto Networks · Check Point Software Technologies Ltd.

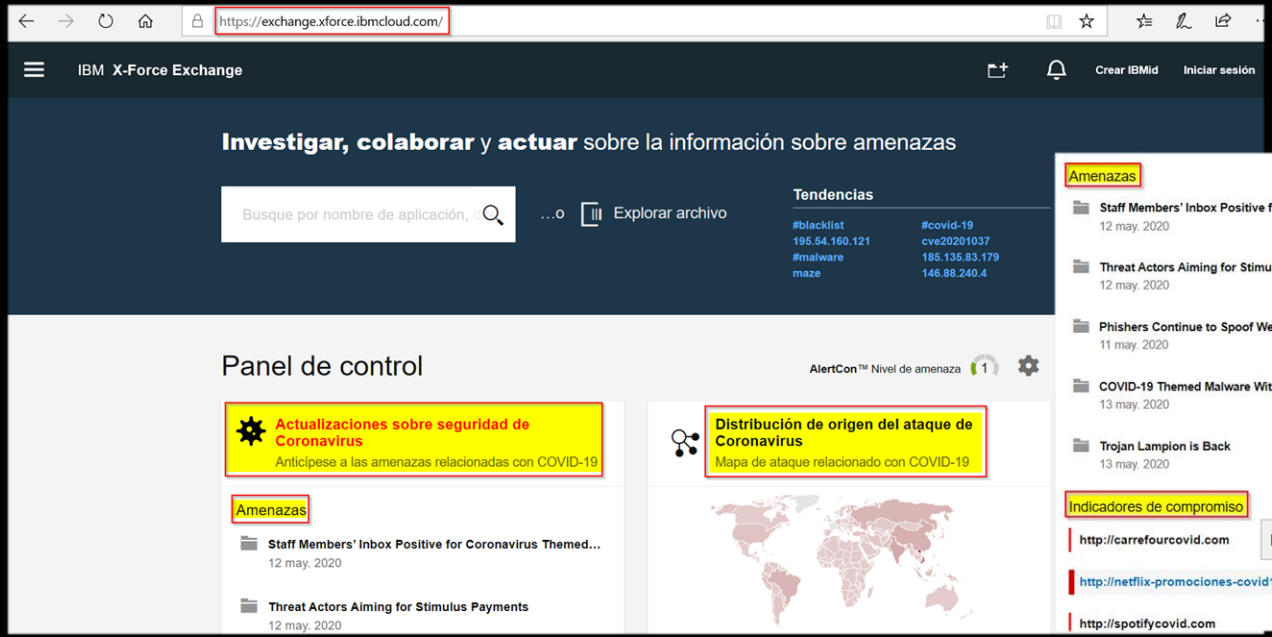
Organizado por Reed Exhibitions

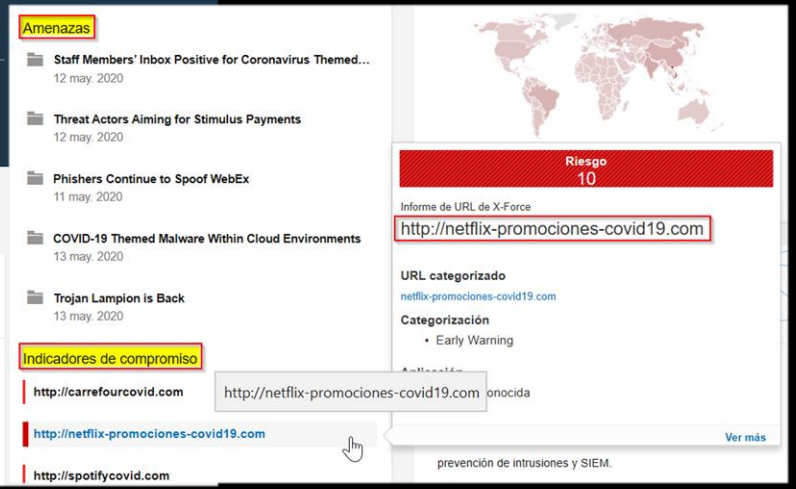
IBM X-Force Exchange

PLATAFORMA QUE CORRELACIONA INFORMACIÓN DE TODOS LOS SOC E INVESTIGACIONES DE IBM A NIVEL MUNDIAL

La URL para acceder a la plataforma es la siguiente:

- ✓ **https://exchange.xforce.ibmcloud.com/**





IBM X-Force IRIS

MENÚ DE SERVICIOS PROACTIVOS

Menú de Servicios Proactivos IRIS	Unidades Proactivas
Incident Response Program Assessment	1
CTI Program Assessment	1
Incident Response Playbook Customization	1
Standard Tabletop Exercise	1
Dark Web Search Services	1
Cybersecurity Incident Response Plan – High Level Review	1
Security Incident First Responder Training	1
Strategic Threat Assessment	1
Cybersecurity Incident Response Plan – Full Development	4
Active Threat Assessment	Custom
Custom Tabletop Exercise	Custom
Custom Cyber Range Experience	Custom

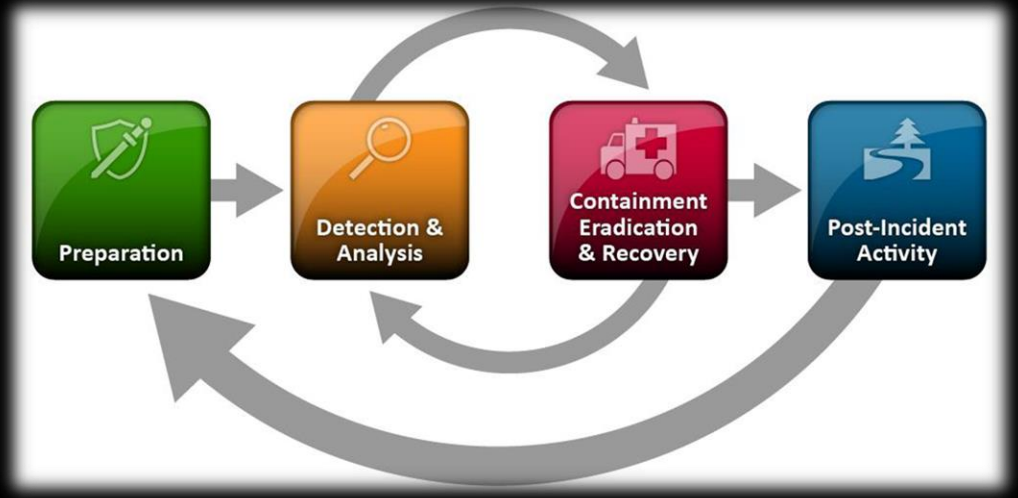
IBM X-Force IRIS

SERVICIO REACTIVO & METODOLOGÍA

Respuesta a Incidentes de Ciberseguridad

- EDR (Endpoint Detection and Response)
  - ✓ CrowdStrike
  - ✓ Carbon Black

Metodología



Caso – Infección mediante un archivo malicioso

Resumen:

El Cliente identificó un consumo anormal en los recursos de algunos de los Sistemas Operativos utilizados en la organización.

Analizando el incidente, IRIS detecto:

- **Ransomware** que cifraba los discos duros remotos excepto la unidad C.
- **Hueco de seguridad** en los sistemas de la organización.

Vector inicial:

- Correo electrónico malicioso.
- Servicio que permitía compartir archivos en Internet.

Afectación:

- 100 equipos de cómputo dentro de la organización.

Impacto:

- Los servidores críticos de la empresa se desconectaron por varios días.

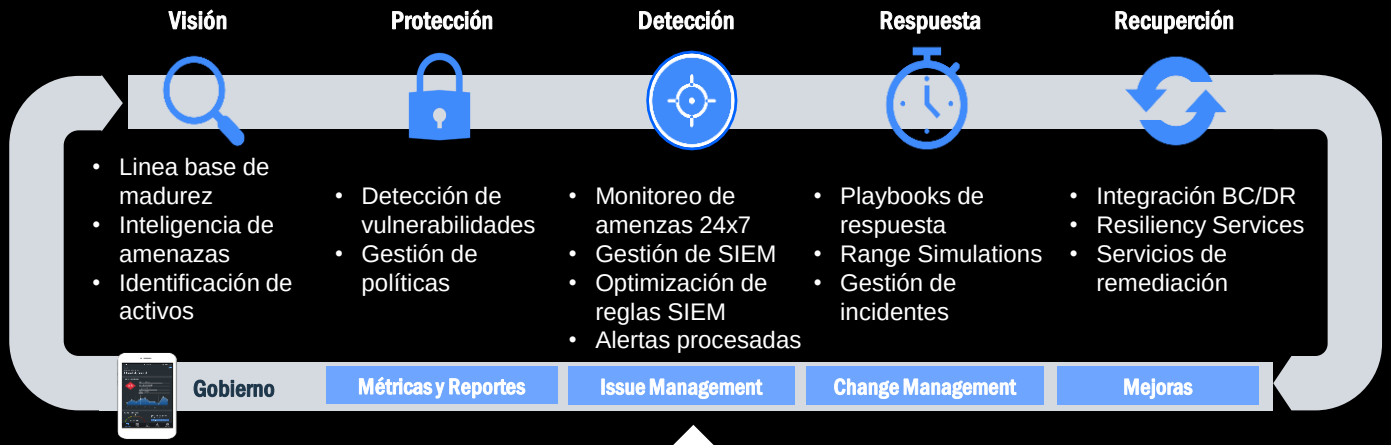
Organizándonos en la Incertidumbre

SOLUCIÓN DE SEGURIDAD MÁS INTELIGENTE PARA ADMINISTRAR EL CICLO DE VIDA DE LAS AMENAZAS CON PERSPECTIVA DE 360º

Un marco programático conduce a un enfoque integrado prescriptivo que impulsa mejores resultados.

Socio de seguridad con expertos de clase mundial que pueden aportar información crítica.

Una plataforma más inteligente que acelera la investigación y la respuesta con análisis, IA y orquestación.



Encontrar Debilidades (X-Force RED) | Detección y Análisis de Amenazas (XFTM) | Respuesta a Incidentes (IRIS) | Ciber-Recuperación (GTS)

QRadar on Cloud & Cloud Pack for Security | X-Force Exchange | Analytics Engines | Resilient Orchestration | Use Case Library | Portal & Mobile App

Partner Ecosystem — IBM Security · Carbon Black · Cisco · CrowdStrike · Fortinet · paloalto Networks · Check Point Software Technologies Ltd.

Organizado por Reed Exhibitions

Principales retos de la Ciber-Resiliencia

1

Aumento de la superficie de ataque, derivado de la transformación digital y la adopción de nube

2

Propagación de corrupción en DR y copias de respaldo que afectan la capacidad de recuperación

3

Planes de respuesta y recuperación insuficientes y mayormente manuales

4

Entorno regulador en rápida evolución y cada vez más complejo

Recuperación ante Desastres y Ciber Resiliencia

Las copias actuales de DR / respaldos son vulnerables a la corrupción y ***no son adecuadas para Ciber Resiliencia***

Exposición continua de la red

- La exposición de la red causa la propagación de corrupción a sitios de DR, haciendo que tanto la recuperación de producción como DR resulten inútiles

Copias para DR / respaldos comunes son objeto de ciberataques

- Ataca directamente a las copias para DR y respaldos comunes

Copias de Punto en el Tiempo (PIT) ineficientes

- Las copias PIT provistas por respaldos comunes tienen RTOs y RPOs altos

Para lograr la operación continua, las organizaciones requieren soluciones de DR y Recuperación ante Ciber Incidentes que les permitan ir de procedimientos manuales a modelos automáticos y de orquestación

Automatización del Ciclo de Vida de DR

Resiliencia definida por software

Workflows inteligentes

Visibilidad (Dashboard)

Almacenamiento inmutable y verificación continua

IBM Resiliency Orchestration con *Cyber Incident Recovery* permite una recuperación más rápida, reduciendo significativamente el impacto de una violación de datos

Reducción significativa sobre el impacto de la violación

Altamente confinable y escalable

Capacidad para manejar detección y recuperación a nivel de site en minutos

Facilidad de manejo mediante una sola consola

Visibilidad y control simplificados sobre tecnologías heterogéneas

Almacenamiento inmutable en Cloud

Aprovecha el almacenamiento inmutable en cloud para una protección de datos más segura

Reducción del OPEX

Detección automatizada, validación de cambios, replicación y restauración mediante air-gap

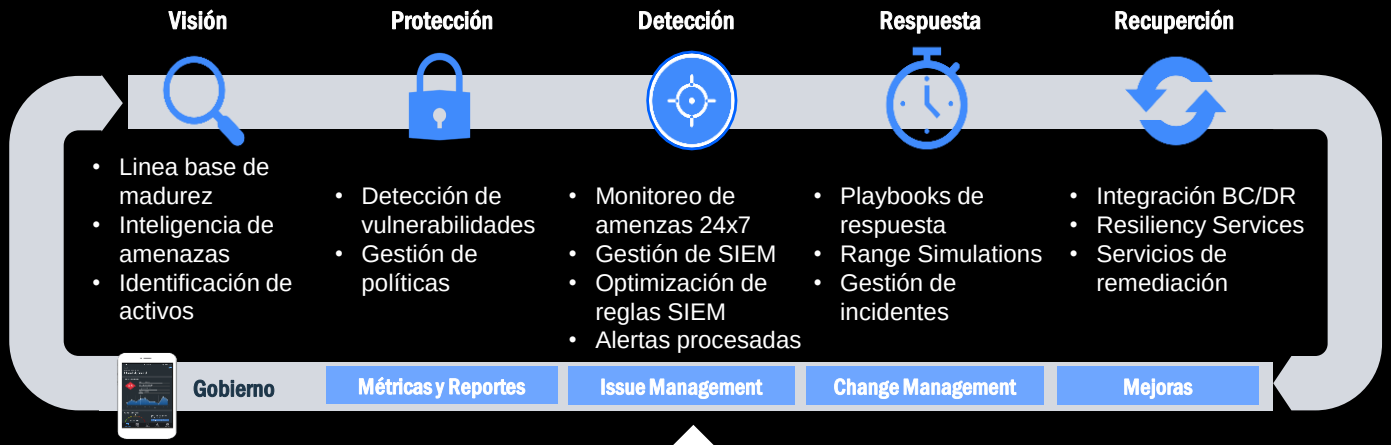
Organizándonos en la Incertidumbre

SOLUCIÓN DE SEGURIDAD MÁS INTELIGENTE PARA ADMINISTRAR EL CICLO DE VIDA DE LAS AMENAZAS CON PERSPECTIVA DE 360º

Un marco programático conduce a un enfoque integrado prescriptivo que impulsa mejores resultados.

Socio de seguridad con expertos de clase mundial que pueden aportar información crítica.

Una plataforma más inteligente que acelera la investigación y la respuesta con análisis, IA y orquestación.



Encontrar Debilidades (X-Force RED) | Detección y Análisis de Amenazas (XFTM) | Respuesta a Incidentes (IRIS) | Ciber-Recuperación (GTS)

QRadar on Cloud & Cloud Pack for Security | X-Force Exchange | Analytics Engines | Resilient Orchestration | Use Case Library | Portal & Mobile App

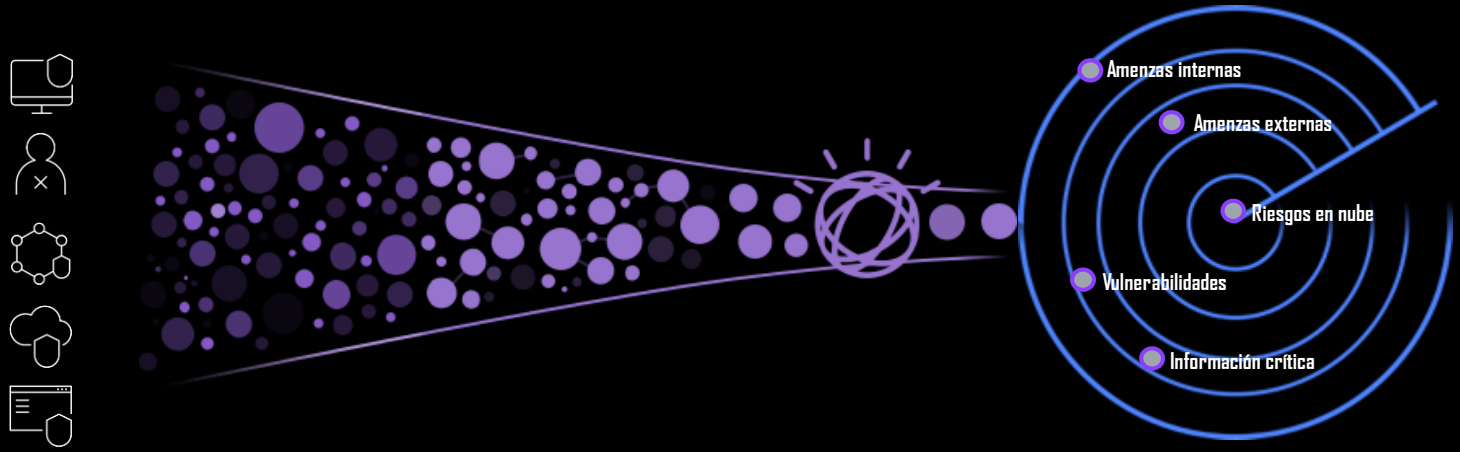
Partner Ecosystem — IBM Security · Carbon Black · Cisco · CrowdStrike · Fortinet · paloalto Networks · Check Point Software Technologies Ltd.

Organizado por Reed Exhibitions

QRadar
Cloud pak for Security

Unificar la gestión las amenazas

Visibilidad Detección Investigación Respuesta



Millones de eventos

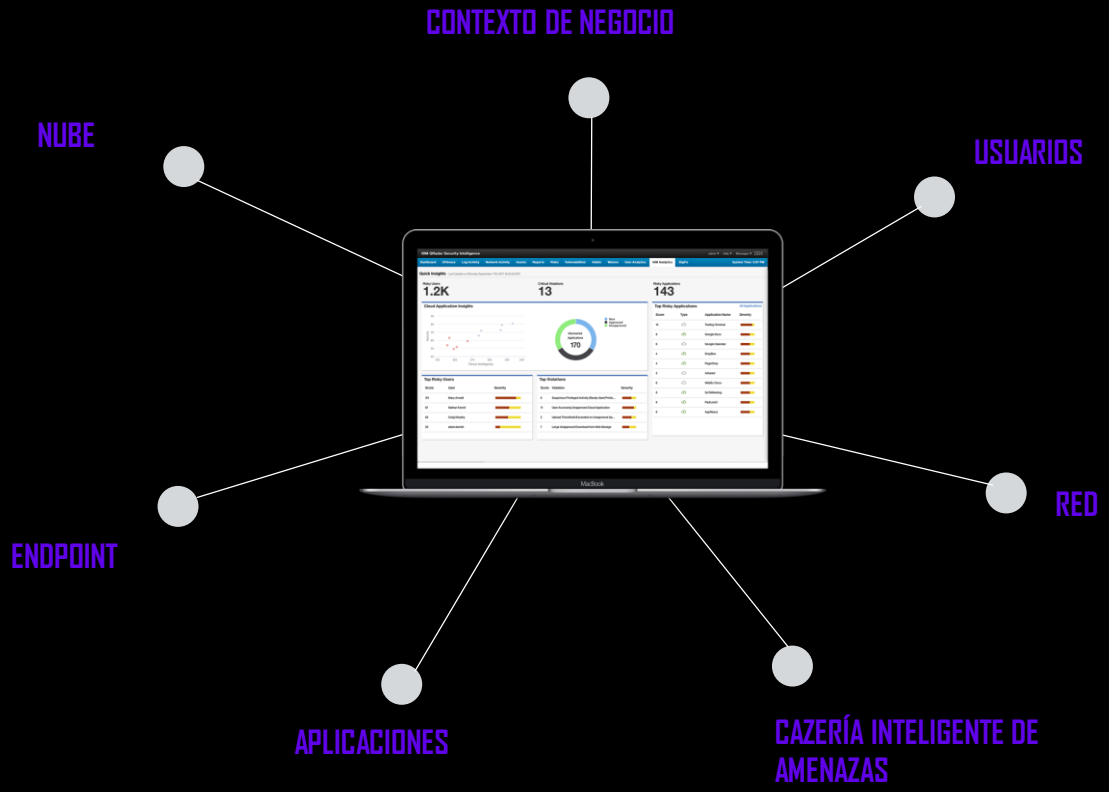
Análisis

Priorización e investigación

Resolver los incidentes de manera efectiva

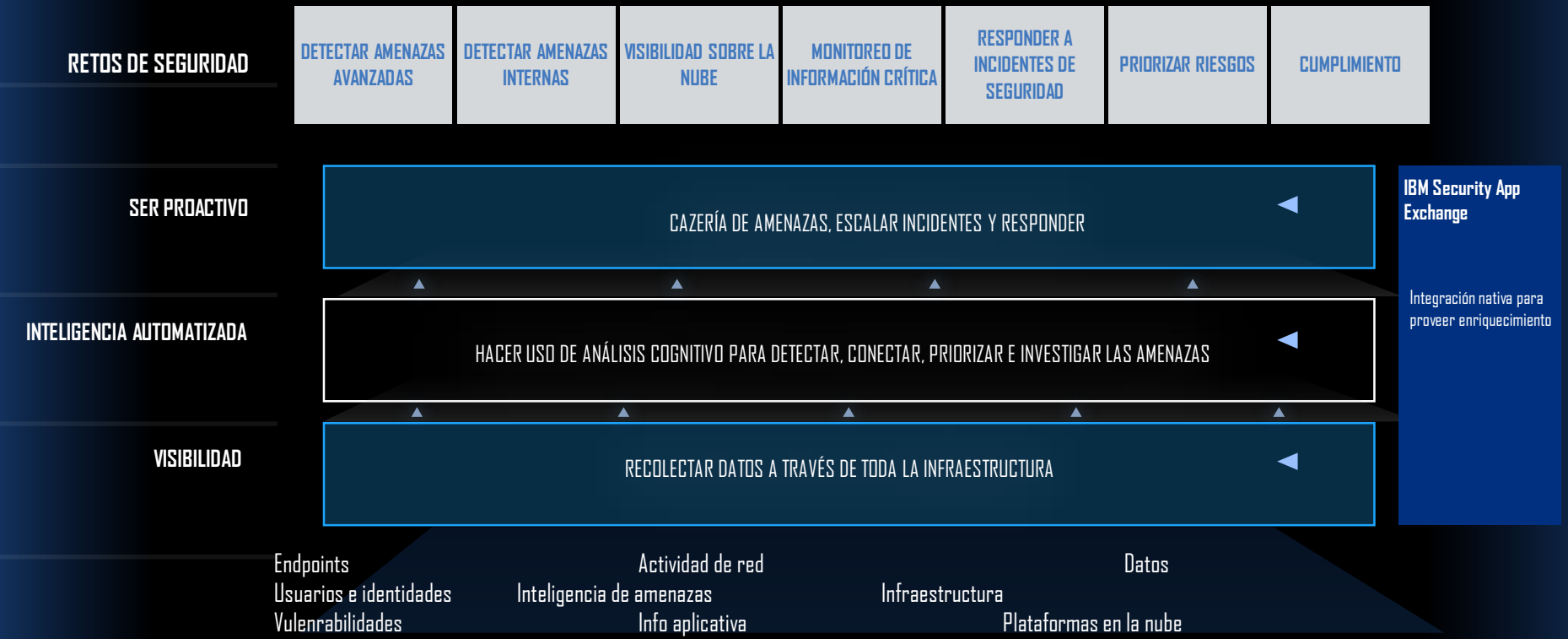
Visibilidad y monitoreo sobre todo

Contar con visibilidad analizada



QRadar

Security Intelligence Platform



Existe mucha información sobre seguridad para consumo humano

Pero la mayoría está sin explotar

- Eventos y alertas de seguridad
- Logs y datos de configuración
- Actividad de usuario y en red
- Amenazas y vulnerabilidad

Un universo de conocimiento de seguridad oculto en la defensa

Una organización tradicional aprovecha solo el 8%*

Ejemplos:

- Documentos de investigación
- Publicaciones de industria
- Información forense
- Información de amenazas
- Presentaciones y conferencias
- Reportes de analistas
- Páginas web
- Wikis
- Blogs
- Noticias
- Newsletters
- Tweets

Vincular la tecnología con el análisis

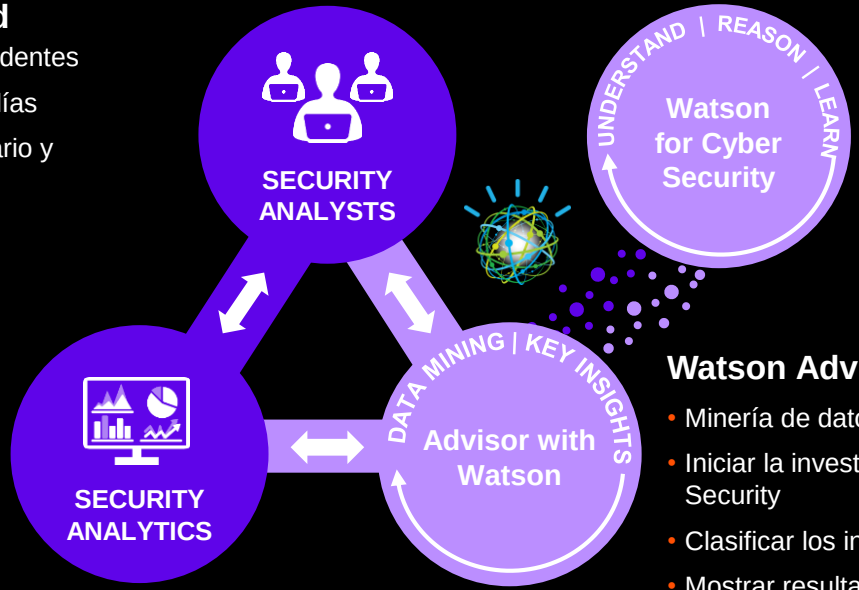
El análisis cognitivo complementa la investigación

Analista de seguridad

- Administrar los posibles incidentes
- Investigar eventos y anomalías
- Evaluar la actividad de usuario y vulnerabilidades
- Gestionar configuraciones
- Otros

Análisis de seguridad

- Correlación de datos
- Identificación de patrones
- Umbrales
- Políticas
- Detección anómala
- Jerarquía



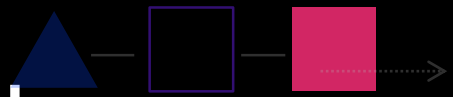
Watson for Cyber Security

- Conocimiento de seguridad
- Identificación de amenazas
- Diferentes IOCs
- Vínculos y relaciones no evidentes
- Evidencia

Watson Advisor

- Minería de datos local
- Iniciar la investigación hacia Watson for Cyber Security
- Clasificar los incidentes
- Mostrar resultados

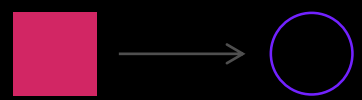
Las seguridad está fragmentada, desconectada y en multiples ambientes.

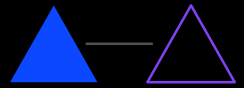


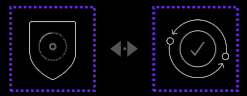
Cloud Object Store Access

Containers

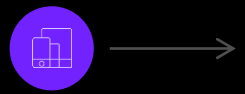
Threat Hunting



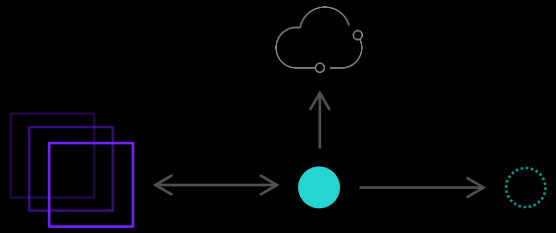




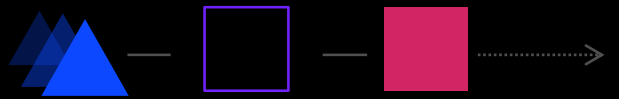
DevOps



Mobile Devices

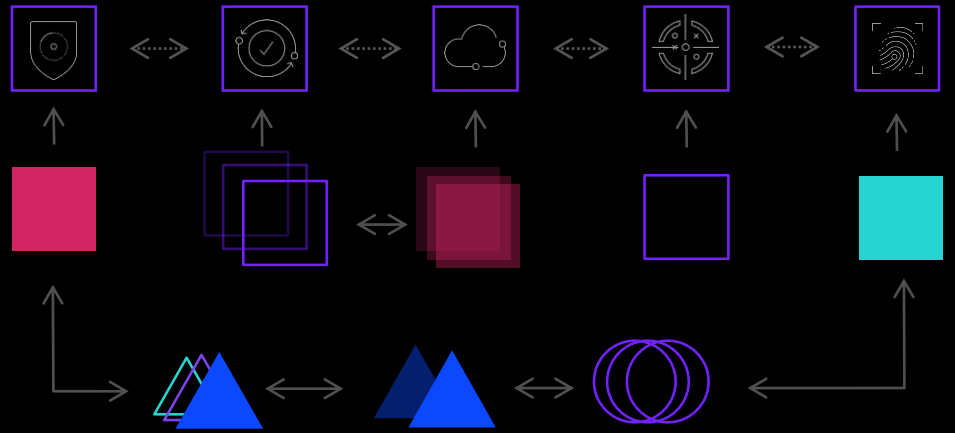


Cloud Security



Critical Data Monitoring

La seguridad debe de estar conectada e integrada



Correr donde sea

Conectar de manera abierta

Obtener contexto de seguridad

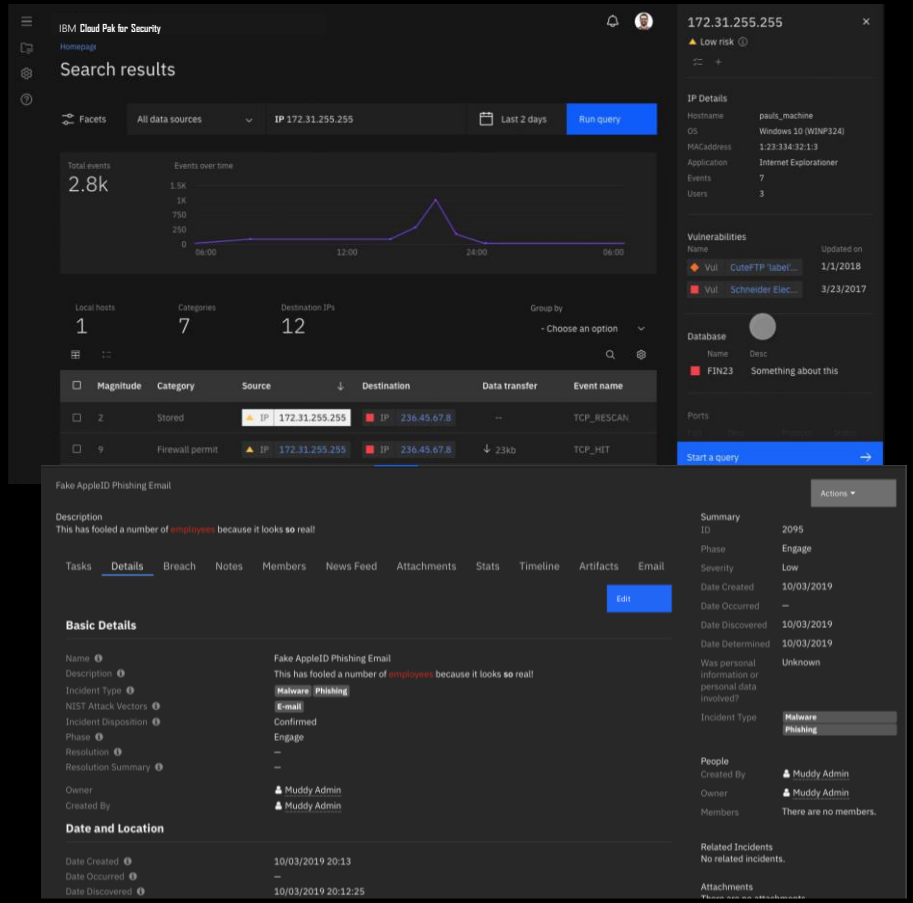
Conectar los datos

Tomar acción

Conectar flujos de trabajo

El valor

- **Investigar más rápido** a través de **búsquedas federadas** en múltiples SIEM, data lakes, ambientes de nube y cualquier fuente de datos.
- **Simplificar el trabajo con una única herramienta** de investigación y búsqueda para un entorno de nube múltiple.
- Rastrear e investigar de manera unificada con **gestión de casos**.
- Responder más rápido y más a fondo con capacidades sólidas de **orquestación y automatización**.
- **Implementar en cualquier lugar** a través de la arquitectura híbrida de varias nubes.
- **Ampliar las fuentes de datos** y las capacidades con nuevos conectores y aplicaciones.



IBM **Cloud Pak for Security en la práctica**

Fase 3 – Orquestación, automatización y respuesta

Resilient

RESPONDER

Dar el tratamiento adecuado al incidente de seguridad a través de flujos de trabajo, playbooks, automatizaciones y orquestación con todo el equipo necesario.

Aprovechar los hallazgos y patrones para enriquecer localmente los incidentes.

Fase 2 – Cazería de amenazas

Data Explorer

INVESTIGAR

Se realizan búsquedas federadas vía Data Explorer en todas las fuentes adicionales en búsqueda de los IOCs

Fase 1 – Eventos de seguridad

SIEM

Se genera una alerta (ofensa) a partir de Qradar que incluye Indicadores de Preocupación (IOCs)

Gestión de amenazas y fuentes de información

DETECTAR

Watson Advisor

QRadar

IBM · REVERSING LABS · Carbon Black. · tenable · elastic · HCL · McAfee · CROWDSTRIKE · IBM Cloud · AWS · cisco · paloalto · Symantec · Microsoft Azure · ANSIBLE · servicenow · ANOMALI · Recorded Future

Preguntas & Respuestas

ONLINE

INFOSECURITY SUMMIT

infosecurity MEXICO

En alianza con ISACA Mexico City Chapter ISACA Guadalajara Chapter

GRACIAS

Alfredo Cristerna
Senior Management Consultant
alfredo.cristerna.guzman@ibm.com