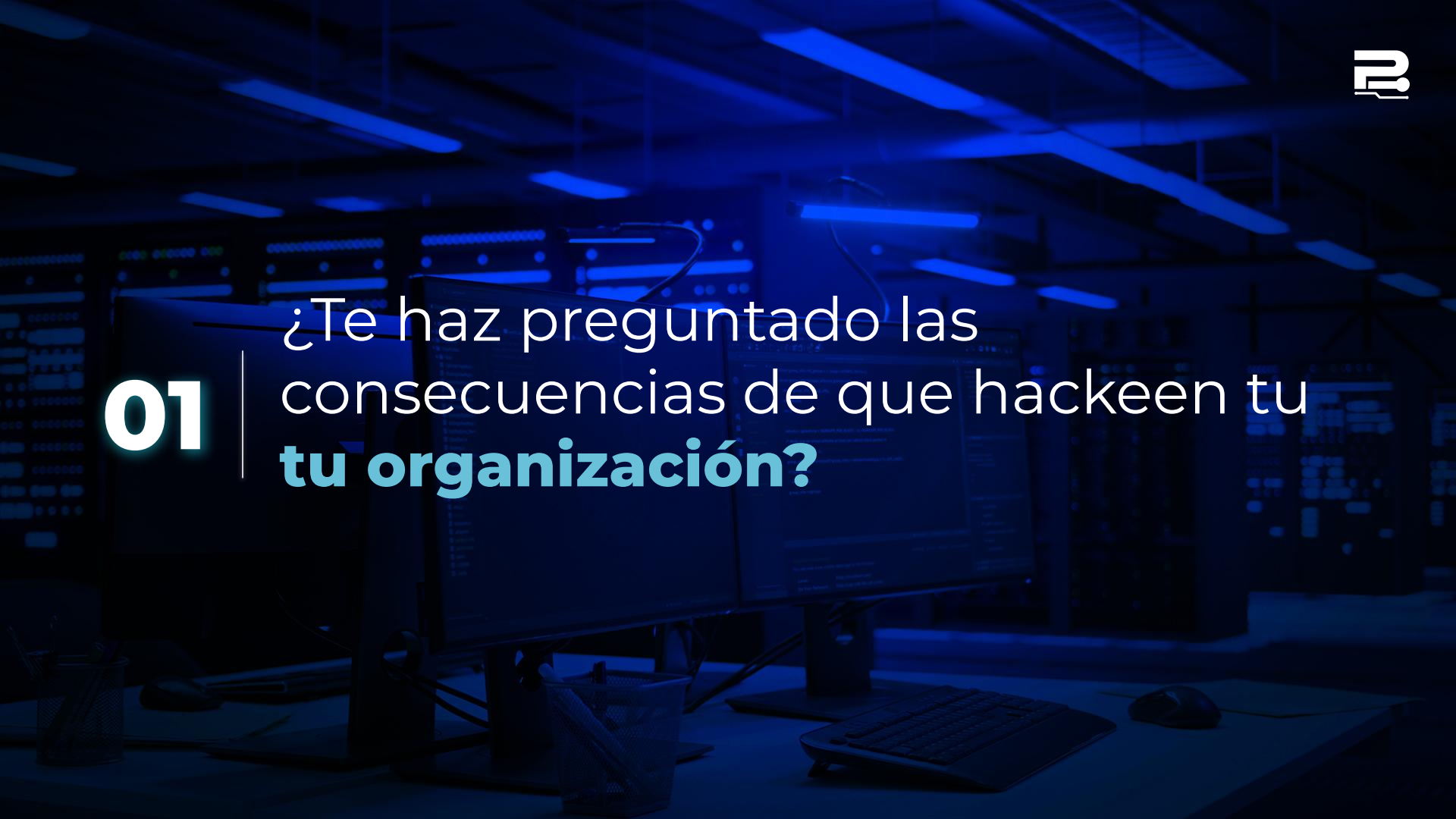


PRYSE

CYBERSECURITY

CIBERSEGURIDAD DE ALTO IMPACTO

PROTECCIÓN TOTAL.
ANTES, DURANTE Y DESPUÉS.


01
¿Te haz preguntado las consecuencias de que hackeen tu
tu organización?

Las empresas invierten en seguridad. Pero la mayoría no está lista para lo que viene.

Los ataques avanzados no se detienen adquiriendo más herramientas. Se detienen con capacidad de respuesta, inteligencia de amenazas y equipos que saben qué hacer cuando el incidente ocurre.

1 REALIDAD DEL MERCADO

Los proveedores venden tecnología. Nadie vende la capacidad de dirigir una crisis en tiempo real.

2 EL COSTO DE NO ESTAR LISTO

Un incidente sin respuesta estructurada se convierte en pérdida operativa, daño reputacional y exposición legal.

3 NUESTRA PROPUESTA

5 soluciones integradas que cubren cada fase crítica: anticipar, responder y recuperarse con control total.



02 | EL MODELO COMPLETO

01

ANTES

Anticipar, detectar y fortalecer antes de que ocurra un incidente

1.1 Cacería Proactiva de Amenazas

1.2 Ciberinteligencia, protección de Marca y Vip

1.3 Optimización de herramientas de Seguridad

02

DURANTE

Tomar el control y contener el ataque en tiempo real

2.1 Centro de Comando de Respuesta

03

DESPUÉS

Remediar, recuperar y certificar el cierre total del incidente

3.1 Remediación y Recuperación integral

Centinela Transversal

Vigilancia continua en las tres fases: detecta, contiene y escala al Centro de Comando

01

ANTES

Anticipar, detectar y fortalecer antes de que ocurra un incidente

1.1 Cacería Proactiva de Amenazas

1.2 Ciber Inteligencia, protección de Marca y Vip

1.3 Optimización de herramientas de Seguridad

SOLUCIONES ASOCIADAS

Soluciones de seguridad
defensa en profundidad, de la red al factor humano

Threat Hunting Proactivo
No esperes la alerta, encuentra al atacante antes que actúe

Inteligencias de Amenazas
Conoce a tu adversario antes de que te encuentre

Seguridad Ofensiva
Atacamos tus sistemas antes de que lo haga un adversario real

Análisis de Auditoría de Código (SAST/DAST)
Encuentra Vulnerabilidades antes de que un atacante las explote en producción

Soluciones Cloud Seguras
Hardening de entornos Híbridos

Seguridad Cloud (CSPM/CWPP/CASB)
Configura y protege y controla todo lo que corre en la nube

Formación y Concientización
Convierte el eslabón más débil en tu primera línea de defensa

1.1 Cacería Proactiva **de Amenazas**



“Asumimos que ya están dentro, vamos por ellos”

¿Hay alguien adentro ahora mismo? Es la pregunta que ningún tablero te responde. Buscamos con hipótesis sobre cómo operan los grupos que atacan a tu sector. Si está, lo encontramos y lo contenemos. Si no está, te lo demostramos y te dejamos mejor detección que antes

LO MÁS IMPORTANTE PARA TI

- Buscamos al atacante que ya está adentro y que tu EDR no ve porque no es malware. Cada campaña parte de inteligencia real sobre quién ataca a tu sector, con MITRE ATT&CK.
- Encontramos movimiento lateral, credenciales robadas y abuso de cuentas privilegiadas. Detectamos cuando usan tu propio Windows como arma: PowerShell, WMI, certutil.
- Cazamos backdoors, canales de control silenciosos y exfiltración que nadie mira. Cada cacería deja reglas nuevas dentro de tus herramientas: tu detección crece.
- Informe ejecutivo y técnico: qué encontramos, qué contuvimos y cuánto subiste.

1

¿TE SUENA CONOCIDO?

Un atacante puede llevar meses dentro sin que una sola alerta se ponga en rojo.
Entran con credenciales válidas: nada de eso dispara tu EDR.
Cerraste un incidente y todavía no puedes asegurar que el atacante se fue.

2

LO QUE GANAS

-Compruebas que estás limpio, no lo supones.
-Cada campaña mejora tu detección.
-Reduces el tiempo que alguien vive dentro.

3

CÓMO EMPIEZA

Compromise Assessment de 2 a 4 semanas para saber si hay alguien adentro hoy, o programa continuo trimestral o mensual.

1.2 Ciberinteligencia y **Protección de Marca y VIP**

“Las amenazas no empiezan en la calle. Empiezan en internet”

Lo que tú familia deja en internet rutinas, domicilios filtrados, viajes, la escuela de tus hijos, es la materia prima de extorsión y del fraude con tu nombre. Nosotros lo vemos primero, lo borramos y cuando hay amenaza, actuamos y le avisamos a tu seguridad física.

LO MÁS IMPORTANTE PARA TI

- Te decimos qué hay de ti y de tu familia allá afuera, y qué tan expuesto estás.
- Borramos tus datos personales de sitios y filtraciones, y vigilamos que no vuelvan.
- Detectamos perfiles falsos, amenazas y acoso contra ti, tu familia y tu marca.
- Te avisamos cuando alguien escala su hostilidad, antes de que se vuelva acción.
- Tiramos dominos, sitios de phishing y apps que se cuelgan de tu nombre.
- Si hay intención física, tu equipo de seguridad lo sabe con protocolo acordado.

1

¿ TE SUENA CONOCIDO?

Tú o tu familia recibieron extorsión o mensajes con datos que nadie debería tener.
Usan tu nombre para pedirle transferencias urgentes a tu director de finanzas.
Hay sitios que imitan tu marca y nadie sabe cómo tirarlos.

2

LO QUE GANAS

Tu familia y tú dejan de ser el objetivo fácil.
Tu marca deja de financiar fraudes con tu nombre.
Tu seguridad física se entera antes, no después.

3

¿CÓMO EMPIEZA?

Empieza con una evaluación de exposición tuya y de tu familia, bajo NDA. Si decides seguir, es un programa anual por persona y por marca.

1.3 OPTIMIZACIÓN DE HERRAMIENTAS DE SEGURIDAD



“Ya invertiste millones en ciberseguridad. ¿Cuánto de eso está realmente funcionando?”

Entramos, medimos cuando de lo que ya pagaste está realmente encendido, casi siempre mucho menos de lo que tu dirección cree y lo configuramos como lo haría alguien que responde a incidentes todos los días.

LO MÁS IMPORTANTE PARA TI

- Te decimos en un solo número cuánto de lo que pagaste está realmente encendido.
- Alineamos tu configuración a las gulas del fabricante y a CIS y NIST. Encendemos lo que nunca se activó: prevención del EDR, MFA, DMARC, WAF, DLP.
- Afinamos la configuración de tu SIEM para minimizar las alertas innecesarias.
- Configuramos tus herramientas para que colaboren entre sí, sin intervención manual.
- Cerramos tus huecos de telemetría: sin datos no hay detección ni respuesta.
- Capacitamos a tu equipo y le dejamos runbooks para sostener el nivel.

1

¿TE SUENA CONOCIDO?

Compraste lo mejor del mercado y tu protección real no se parece a lo que pagaste.

Tu SIEM da miles de alertas y ninguna útil; tu equipo ya dejó de verlas.

En cada auditoría te repiten que la herramienta lo podía detectar, pero no estaba configurada.

2

LO QUE GANAS

Ganas protección sin comprar una licencia más. Llegas a tu renovación sabiendo qué te sirve.

Te medimos antes y después, en un número.

3

¿CÓMO EMPIEZA?

Health Check de 2 a 3 semanas con tu plan priorizado, afinación de 4 a 10 semanas y acompañamiento trimestral. El Health Check se bonifica.

02

DURANTE

Tomar el control y contener el ataque en tiempo real

2.1 Centro de Comando de Respuesta

SOLUCIONES ASOCIADAS

Respuesta a Incidentes (DFIR)

Cada minuto cuenta; contención, erradicación y Recuperación experta

Take Down de Activos Maliciosos

Elimina infraestructura maliciosa que usa tu nombre antes que dañe a tus clientes



2.1 Centro de **Comando de Respuesta**

“Un Centro de Comando contiene y resuelve”

El día que detectas ransomware, una fuga de datos o el correo de tu director comprometido, marcas un número y en minutos tienes a un equipo de élite tomando el control técnico y sentado con tu equipo responsable. No cotizamos en medio de tu crisis: ya estamos contratados y ya conocemos tu entorno.

LO MÁS IMPORTANTE PARA TI

- Un solo número, 24x7x365. Te contesta un responsable senior, no una mesa de ayuda.
- Un líder de incidente al mando, con war room y bitácora de decisiones. Contención en horas: aislamos, bloqueamos y levantamos evidencia del ataque.
- Te decimos quién te ataca y qué hace después, con inteligencia que no está en feeds.
- Tu dirección acompañada: qué comunicar, a quién y cómo manejar el incidente. Lo legal cubierto: notificación en plazo, evidencia probatoria y denuncia.
- Oficinas BCP: Si tu sede no es segura, tu gente clave opera desde las nuestras.

1

¿TE SUENA CONOCIDO?

El día del incidente nadie sabe quién manda ni qué se le dice al consejo.

Pierdes las primeras 24 horas buscando proveedor mientras el atacante avanza.

Tu equipo lleva 72 horas sin dormir tomando decisiones irreversibles.

2

LO QUE GANAS

Nunca más pierdes las primeras 48 horas.

Tu consejo escucha una sola versión, a tiempo.

Si no hay incidente, tus horas se vuelven preparación.

3

¿CÓMO EMPIEZA?

Retainer anual en tres niveles; **Esencial** (te contestamos en ≤ 30 min), **Corporativo** (≤ 15 min y en sitio ≤ 8 h) y **Consejo** (nacional en 24 h, Especialista Senior dedicado).

03

DESPUÉS

Remediar, recuperar y certificar el cierre total del incidente

3.1 Remediación y Recuperación integral

SOLUCIONES ASOCIADAS

Forense y Asesoría Jurídica

Evidencia digital con validez legal del incidente al proceso legal

Servicios gestionados de Ciberseguridad

Defensa en profundidad, de la red al factor humano

3.1 REMEDIACIÓN Y RECUPERACIÓN INTEGRAL



“El incidente no termina cuando el atacante se va, termina cuando lo cerramos con evidencia”

Cuando el atacante se va empiez la parte que casi nadie cubre sacando de raíz, reconstruir lo que se dañó y poder demostrar que esto ya terminó.

LO MÁS IMPORTANTE PARA TI

- Sacamos al atacante de raíz: persistencias, cuentas, webshells y accesos de terceros.
- Te regresamos a la operación con controles reforzados. Nos quedamos 30, 60 o 90 días detectando posibles persistencias.
- Ejecutamos la remediación junto al equipo de TI
- Legal, RH, comunicación y TI en la misma mesa, con un solo plan y un responsable.
- Carta de cierre con evidencia para tu consejo, tu auditor y el regulador.

1

¿ESTE SUENA CONOCIDO?

Te dijeron que ya se contuvo, pero nadie garantiza que no quedó una puerta abierta.

Tienes quince recomendaciones en un reporte y nadie que las ejecute.

Tu aseguradora y tú auditor piden evidencia de remediación.

2

LO QUE GANAS

Cierras el incidente, no solo lo contienen.

Recuperas la confianza de tu consejo.

Cero reingresos durante la ventana de vigilancia.

3

CÓMO EMPIEZA

Proyecto por fases: estabilización, erradicación y reconstrucción, endurecimiento, vigilancia de reingreso 30-90 días y cierre certificado.

Centinela
Transversal

Vigilancia continua en las tres fases. Detecta, contiene y escala al Centro de Comando



“Otros te mandan alertas, nosotros defendemos”

Integramos lo que ya tienes: EDR/XDR, SIEM, firewalls, directorio, nube y correo, en una sola vista. Analistas especializados revisan cada evento con contexto, lo atienden con playbooks definidos y dejan registro de todo. Si el incidente escala, pasa directo a nuestro Centro de Comando de Respuesta.

LO MÁS IMPORTANTE PARA TI

- Te vigilamos 24x7x365 desde infraestructura propia en México, con turnos rotativos y guardias de respaldo.
- Tres niveles de atención: triage (N1), investigación y correlación (N2), cacería y forense (N3) con enlace directo a nuestro CERT.
- Casos de uso y playbooks a tu medida, mapeados a MITRE ATT&CK: ransomware, phishing/BEC, movimiento lateral, exfiltración y amenaza interna.
- Automatizamos correlación, enriquecimiento y contención: menos falsos positivos, respuesta más rápida.
- Inteligencia temprana de la comunidad internacional de respuesta a incidentes, como Liaison de FIRST en México.

ALINEADO A SOC 2 TIPO II

- Seguridad
- Disponibilidad
- Integridad de procesamiento
- Confidencialidad
- Privacidad (LFPDPPP)
- Efectividad sostenida

1 ¿TE SUENA CONOCIDO?

Tu SIEM genera miles de alertas y de noche nadie las está viendo.

Tienes EDR, firewall y nube, pero cada uno ve su parte y nadie ve el ataque completo.

Tu auditor pide evidencia de que tus controles funcionan y solo tienes capturas de pantalla.

2 LO QUE GANAS

Alguien defendiendo tu operación a toda hora, todos los días.

Tiempos de respuesta por prioridad, medidos en tu tablero ejecutivo: MTTD, MTTR y SLA.

Evidencia lista para auditoría: bitácoras inmutables y trazabilidad total.

3 ¿CÓMO EMPIEZA?

Integramos tus herramientas, diseñamos tus casos de uso y playbooks y acordamos tus SLA. Desde ahí, operación continua con reportes por incidente e informes periódicos.

Nuestras **certificaciones**

TIER II DESIGN®
Grupo de Seguridad Privada PRYSE de México
PRYSE Cybersecurity DC Cuernavaca
Expires 27 January 2028
UPTIME INSTITUTE CERTIFIED

ISO 37001:2025

ISO 27001:2022

ISO 22301:2019

ISO 20000-1:2018

ISO 9001:2015

Nuestras **metodologías**

MITRE ATT&CK™

NIST

OSSTMM 3

CYBER KILL CHAIN

Portafolio

Cinco formas de empezar con nosotros

Elige la que responda al problema que tienes hoy sobre la mesa

1

Centro de Comando de Respuesta

Marcas un número y en minutos tienes al mando a un equipo que ya ha vivido cientos de crisis.

2

Remediación y Recuperación Integral

Sacamos al atacante de raíz y te entregamos el incidente cerrado con evidencia, no un reporte.

3

Ciberinteligencia, Protección de Marca y VIP

Borramos lo que te expone, tiramos lo que suplanta tu nombre y avisamos antes de que escale.

4

Optimización de Herramientas Ecosistemas de Seguridad

Prendemos lo que pagaste y nunca se activó. La misma inversión, el doble de protección.

5

Cacería Proactiva de Amenazas

Respondemos con evidencia la pregunta que ningún tablero te contesta: ¿hay alguien adentro?



Tu operación continua, **nosotros la protegemos.**

ventas@prysecybersecurity.com prysecybersecurity.com +52 56 2080 8483