
JaCkSecurity

Nuestra Visión
Líderes en gestionar incidentes corporativos de seguridad de la información.

Nuestra Misión
Atender la demanda de seguridad en perspectiva a las lecciones de incidentes reales.

Nuestra Filosofía
La red. Todos los problemas se pueden resolver desde el punto central de los datos.
Ofrecer servicios/tecnologías que al final del día produzcan un beneficio consistente.
Soluciones basadas en lecciones aprendidas de incidentes asistidos en la vida real.

Nuestros Valores Corporativos
Celo | Cuidamos la confidencialidad de la información de cada cliente.
Escrutinio | Analizamos cada hallazgo, antes de reportarlo como tal.
Liderazgo | Valoramos el buen ejemplo, y aspiramos a ser uno.
Organizaciones y profesionales | Siempre en un marco de ética.
Socios | Celebramos servicios para crear relaciones firmes.
Ahorro | Buscamos economizar agua, energía, y recursos.

Nuestra Tecnología
tcp13, hardware que "habilita el poder forense de la red"
waffep, "Web App Firewall for Expert Pentesters“
nanojack, un dispositivo hw "nano power auditor"
pcapgrabber, una herramienta hw "uso interno"

Nuestra Especialidad
-Consultoría basada en lo que demostró funcionar
-Estrategias aplicativas de intrusión informática
-Respuesta a incidentes y comprensión legal
-Reforzamiento sistemas y similares
-Vigilancia de redes/app

Nosotros: Compañía peruana con 8 años operación. Competencias centrales: Análisis y Detección. Visión: Líderes en el mundo de la gestión de incidentes corporativos de seguridad informática. Habilidades certificadas: Pentesting, Problemas legales en informática y seguridad, Aplicaciones Web (Pentesting / Defending). Sistemas de gestión de seguridad de la información, Respuesta a Incidentes de seguridad, Gerenciamiento de seguridad, Análisis intrusiones, Consultoría, CBK. Prontuario de sectores atendidos: Bancos, Seguros, AFP, Fondos inversión, Micro-finanzas, Servicios a la Banca, Infraestructura crítica, Gobierno y milicia extranjera, Industria alimenticia, Industria cosmética, Editoriales, Retailers,Más. Membresías: FIRST. Portafolio de servicios: Surveillance, Pentest, Hardening, Response.

hitos en 8años de labor

JaCkSecurity

En el 2004, JACKSECURITY se crea como portal web, al promover información de seguridad y cursos de SANS Institute®.

04 julio 2006, JACKSECURITY se convierte en S.A.C., al brindar soporte de respuesta a incidentes digital a dos importantes compañías, una de ellas de +1500 nodos que estuvo inoperante por 2 días, y que fuera resuelto en sólo 4 horas gracias a la asesoría de JACKSECURITY.

2007, JACKSECURITY se convierte en la primera empresa local en contar con un Authorized Trainer de (ISC)2® para la certificación CISSP®.

2008, JACKSECURITY le proporciona visibilidad ubicua 100% completa sobre el tráfico interno y externo a una importante compañía local, al implementarle una solución monitoreo de seguridad basado en red, para analistas de seguridad avanzados.

2008, JACKSECURITY ejecuta un pentesting mixto con una compañía de infraestructura regional. Elabora 03 sistemas de gestión de seguridad de la información basado en las circulares SBS G-140, y planes de gestión crisis y BCP basado en G-139.

2009, JACKSECURITY realiza el ethical hacking de una aplicación web exclusiva del sistema financiero, y prueba la seguridad de un backbone IP de máxima seguridad. Apoya en la realización de un simposio local al contactar personalmente a Mr. Bruce Schneier, el padre de la criptografía moderna.

2009, JACKSECURITY inicia operaciones de monitoreo de IDS a nivel 4, al suministrar reportes confirmados de incidentes y relevantes de seguridad, en 8x5, mediante técnicas de análisis forense de red.

2010, JACKSECURITY realiza pruebas detalladas de ethical hacking a infraestructura de sistema y de red, software y procesos de cajeros ATM (Automatic Teller Machines) de diversas marcas, en centroamérica; labor que se repite el 2011 en uno de los 4 bancos más importantes de LAC.

2010, JACKSECURITY pasa exitosamente la Visita de Sitio 1.0 realizada por representantes de FIRST® (Juniper® SIRT, en co-auspicio con Team Cymru®), y se convierte en la 3er. team de seguridad peruano en ser miembro de Forum of Incident Response and Security Teams (FIRST®).

2011, JACKSECURITY ejecuta un reforzamiento de perímetro, sistemas operativos y servicios de un entidad militar norteamericana, labor que se repite al año siguiente con tecnología de *consumerization* para otra importante organización del sector de infraestructura crítica.

2012, realiza el ejercicio de pentesting más extenso de una entidad financiera, al probar varios flancos en varias tecnologías. En este año, JACKSECURITY lanza la marca de su producto bandera **tcp13®**, que habilita la capacidad forense de la red, para diversos usos en seguridad.

2013, JACKSECURITY concreta con éxito cinco (05) Campañas de Análisis y Detección de Incidentes, para detectar fuga información, uso ilegal de la red, app inseguras de terceros, malas prácticas y actividad pirata, como demostración de su capacidad de Vigilancia y Respuesta.

2014, JACKSECURITY incursiona en proyectos de seguridad en el SDLC, más allá de las prácticas de *pentest* y *code-review*. Con su experiencia combinada en seguridad de la información e informática JACKSECURITY atiende nuevas necesidades generadas por la Ley 29733 en Perú.

A la fecha, JACKSECURITY cuenta con +13 diferentes certificaciones de seguridad en un *core-team* de +20 años de experiencia mixta, +30 clientes satisfechos, varias herramientas propias, y con acceso seguro a una red internacional para mitigar incidentes de seguridad de escala global.

Síganos en línea desde Facebook, LinkedIn, nuestro blog, y más

www.jacksecurity.com | info@jacksecurity.com | (+51)-651-0222

experiencia

registro histórico

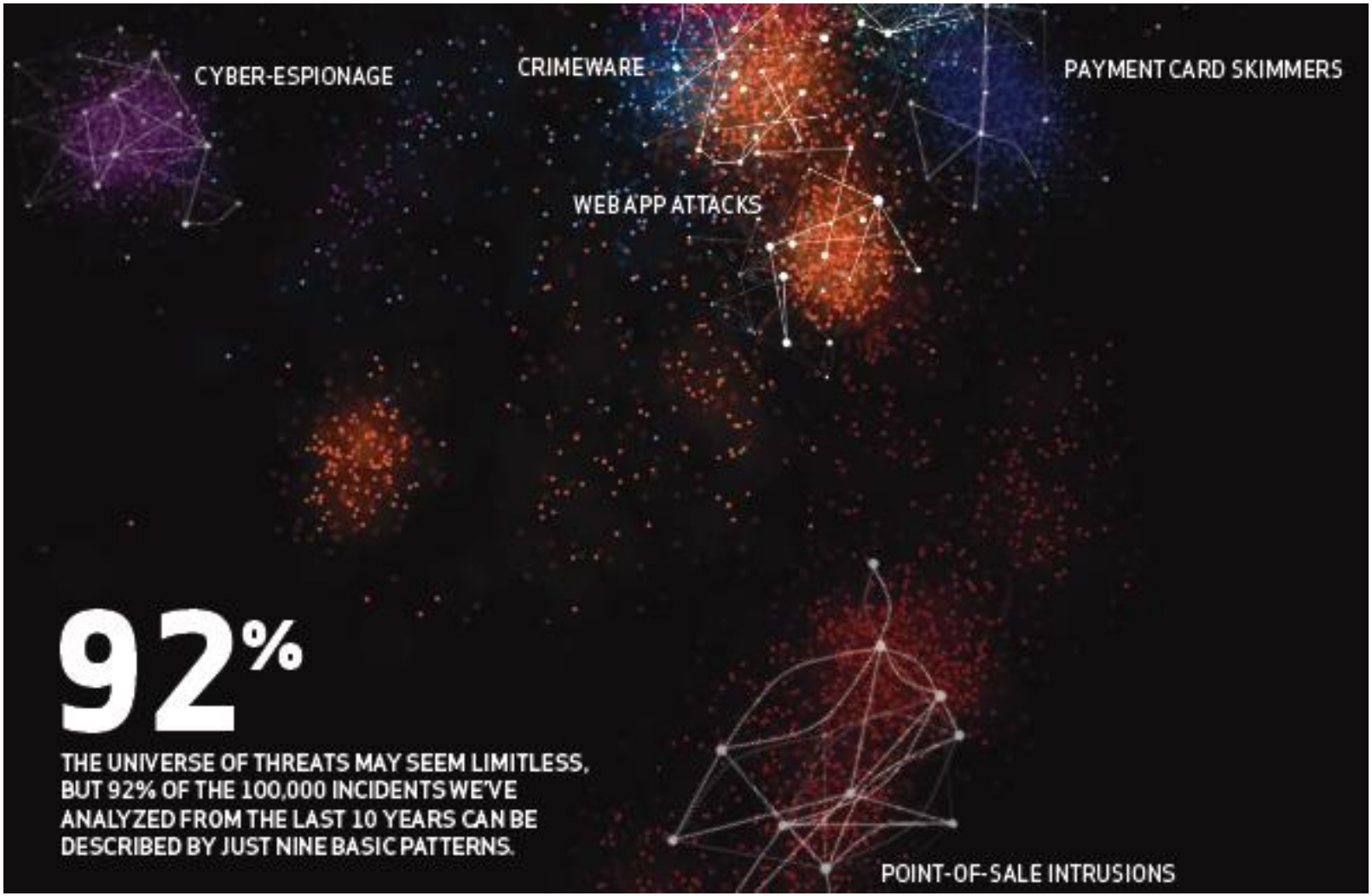
Específico a Aplicaciones Web

Cómo contratar casas desarrollo de software seguro

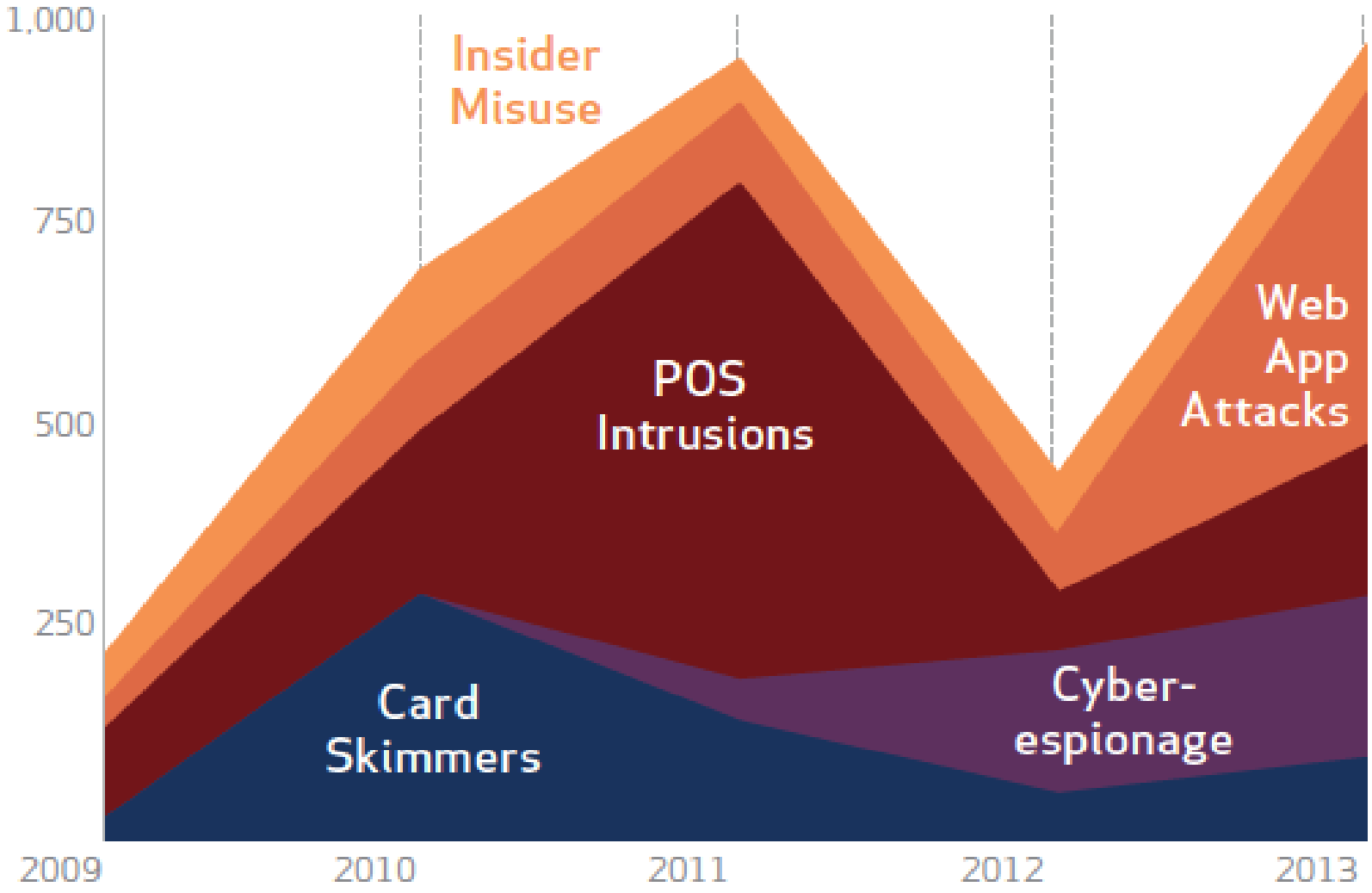
Acerca del expositor

- Javier Romero
  - CTO y co-fundador de JaCkSecurity
- +12 certificaciones en
  - IRCA, ISACA, ECCouncil, (ISC)2, y GIAC (SANS Institute)
- +15 años en
  - Análisis y detección de brechas e incidentes
  - Dirección de servicios de seguridad
  - Consultoría combinada

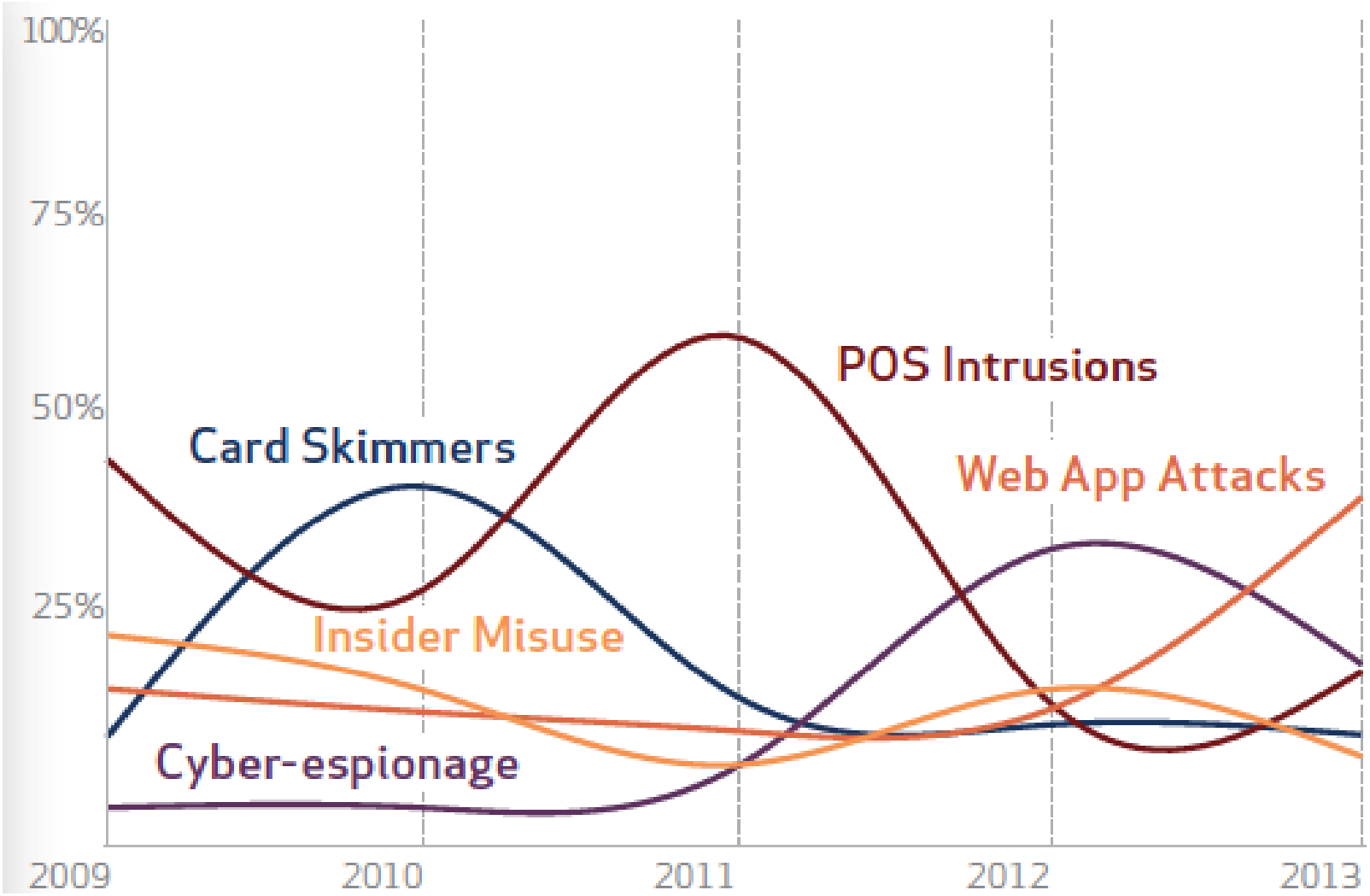
Por qué software en app web



Por qué software en app web (cont.2)



Por qué software en app web (cont.3)



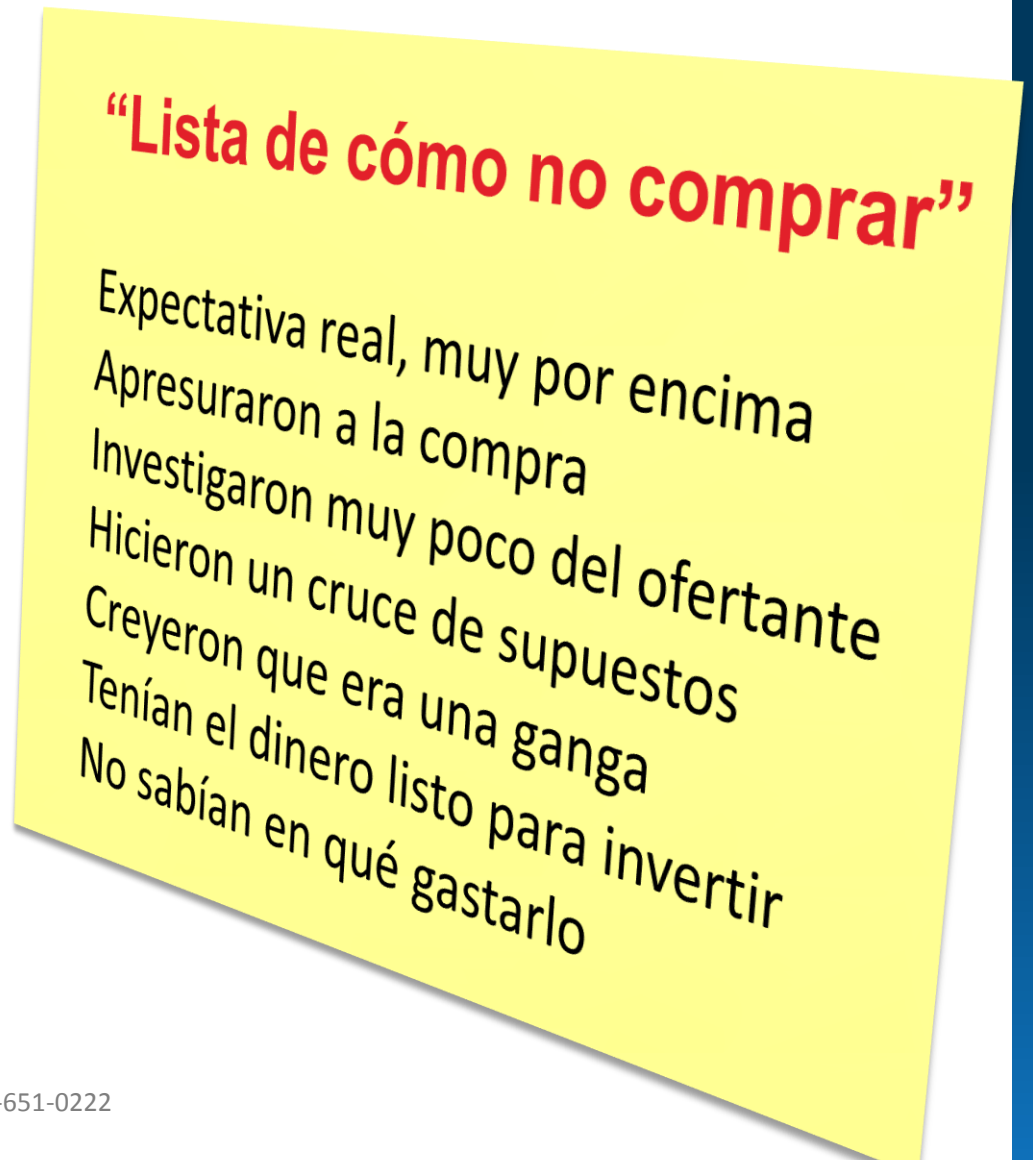
Agenda

- Introducción
  - Por qué compramos mal
  - Primeras notas de “cómo no contratar”
  - A quiénes estamos contratando
- Problema
  - Riesgos de una mala contratación
- Solución
  - Propuestas existentes
  - Propuesta evidente
- Resumen
  - Disclaimer: Trade-off
  - Preguntas

¿te ha sucedido?

Primeras notas

- Expectativa
- Prisa
- Poca investigación
- Fuente equivocada
- Sólo precio
- Exceso gasto



A quiénes estamos contratando

Grandes expectativas

- Contratamos a proveedores con:
  - ISO 9001
  - CMMIv3
  - Cartera
  - ISO 12207
  - PMP

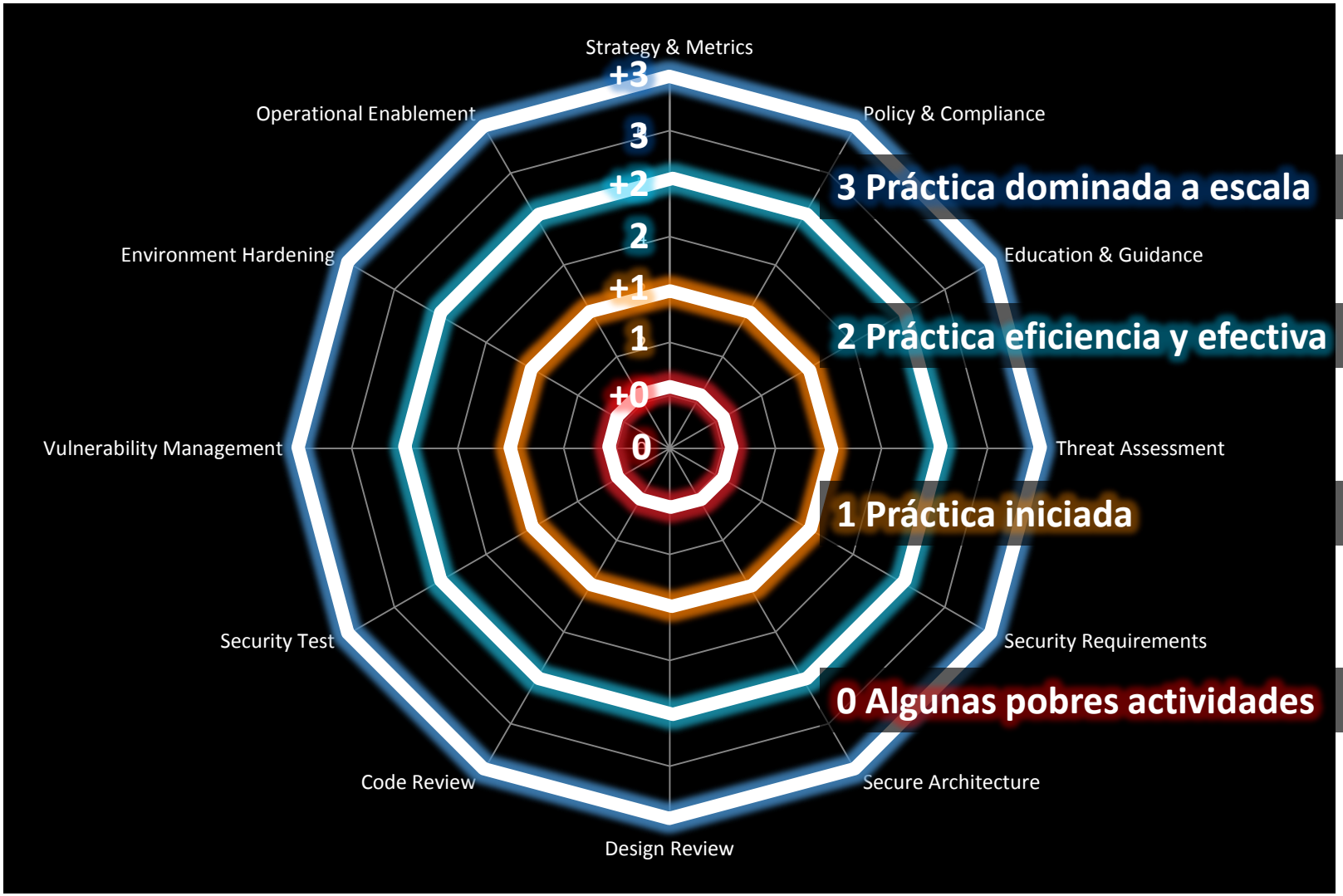
JaCkSecurity

A quiénes estamos contratando

Software Assurance Maturity Model (SAMM)

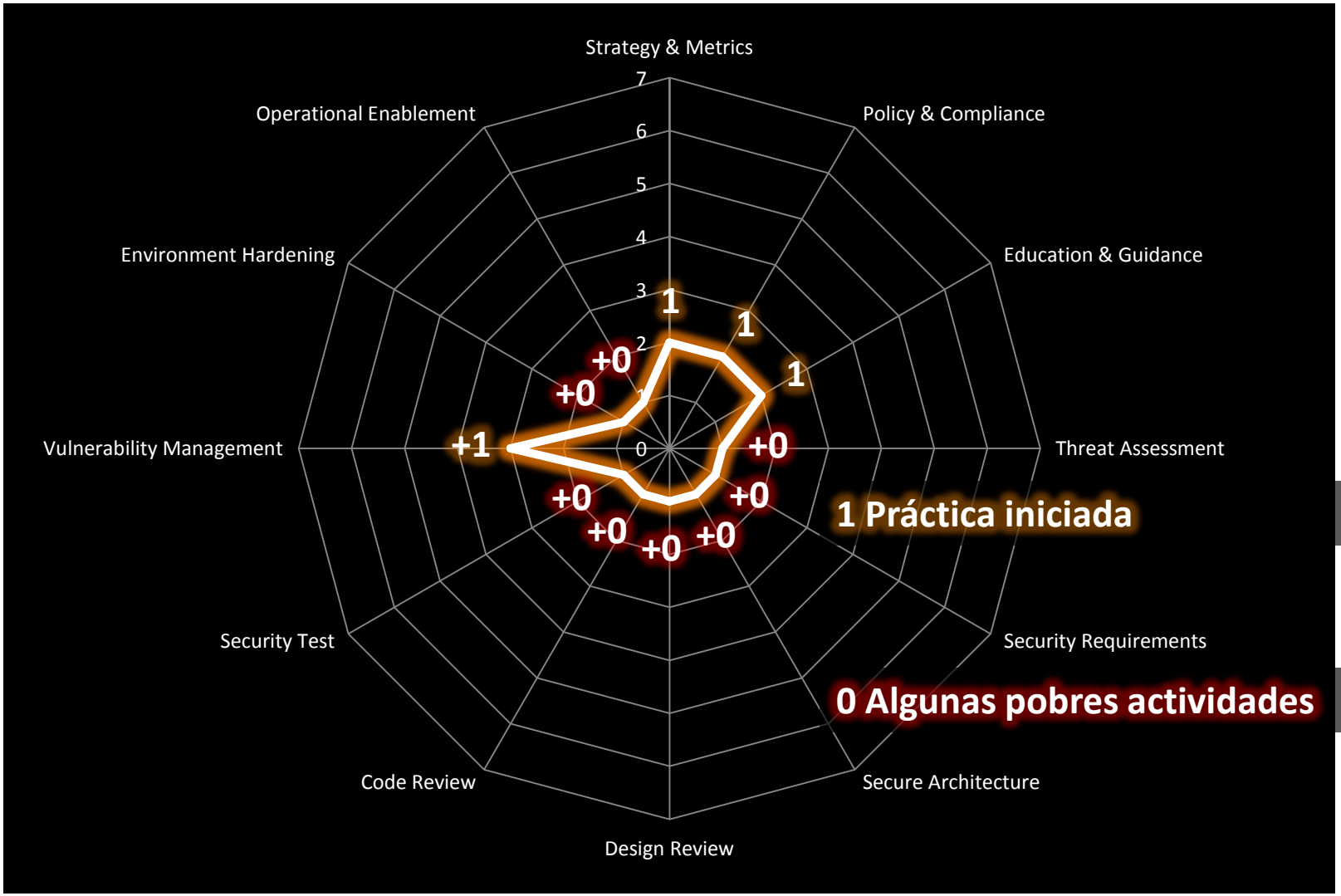
Prácticas de seguridad en el SDLC, y los niveles de maduración

JACK YOUR INCIDENTS NOW!



Software Assurance Maturity Model (SAMM)

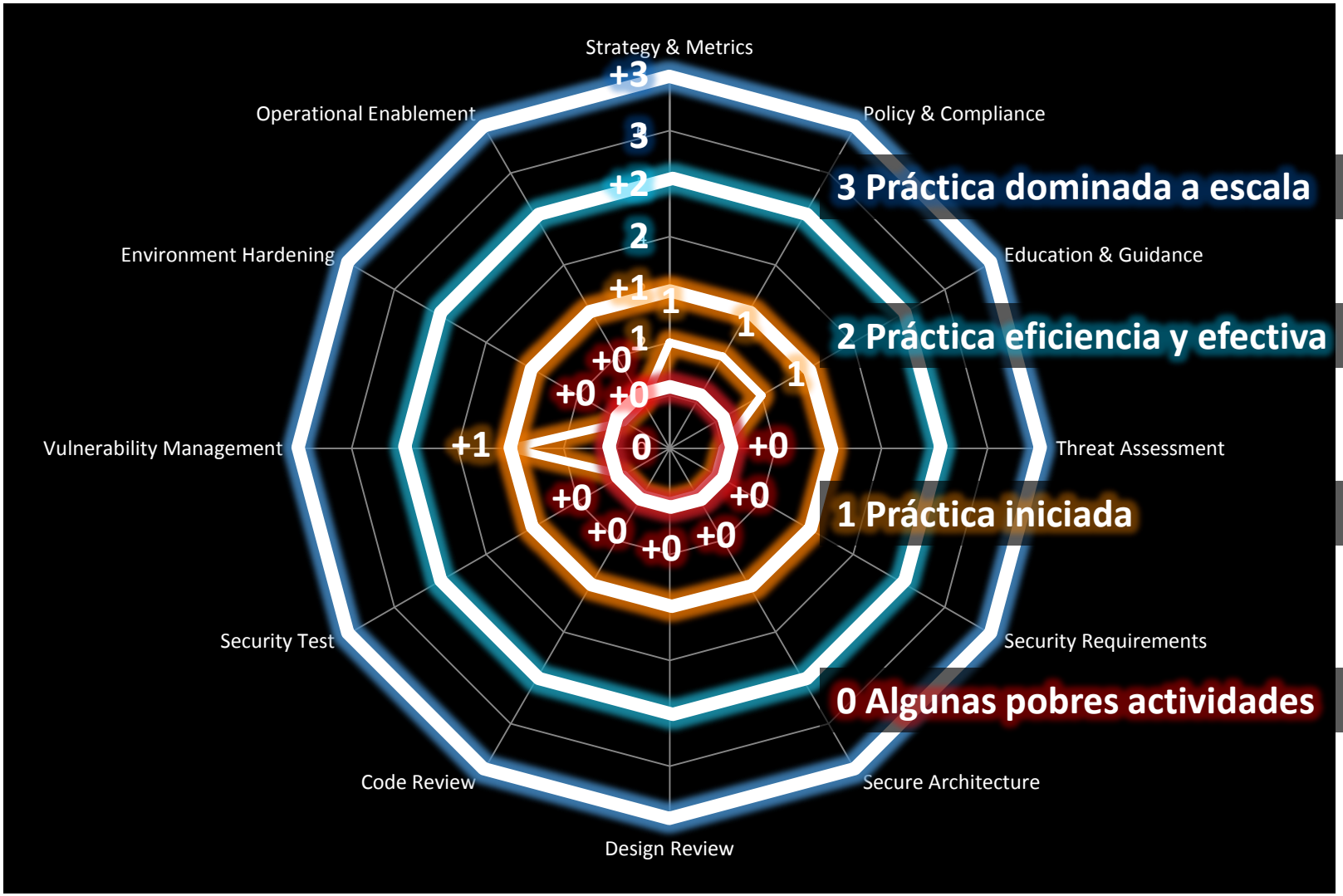
Encuesta en Perú (2013)



Software Assurance Maturity Model (SAMM)

Encuesta en Perú (2013)

JACK YOUR INCIDENTS NOW!



Software Assurance Maturity Model (SAMM)

Encuesta en Perú (2013)

Nivel	Prácticas de seguridad	Descripción
1	Strategy & Metrics	Establecer una estructura del programa, medible y alineada al negocio
1	Policy & Compliance	Asegurar los estándares internos y el cumplimiento legal/regulatorio
1	Education & Guidance	Armar al personal con el KB/recursos para diseñar/desarrollar/desplegar sw
+0	Threat Assessment	I/E el riesgo del proyecto basado en las funciones/características/entorno del sw
+0	Security Requirements	Especificar anticipadamente el las necesidades del sw respecto a la seguridad
+0	Secure Architecture	Fijar pasos para el diseño y construcción de un sw seguro por defecto
+0	Design Review	Evaluar el diseño y arquitectura del sw por problemas relacionados a la seguridad
+0	Code Review	Inspeccionar el sw a nivel de código fuente a fin de hallar vulnerabilidades
+0	Security Test	Inspeccionar el sw en el ambiente de ejecución a fin de hallar vulnerabilidades
+1	Vulnerability Management	Asegurar los procesos de manejo y respuesta a brechas e incidentes
+0	Enviroment Hardening	Asegurar el ambiente de ejecución que aloja el sw de la organización
+0	Operational Enablement	Recopilar información crítica de seguridad del team y comunicarlo a los usuarios

Software Assurance Maturity Model (SAMM)

Encuesta en Perú (2013)

Nivel	Prácticas de seguridad	Descripción
1	Strategy & Metrics	Estima el perfil de riesgo general del negocio
1	Policy & Compliance	Identifica y monitorea los ejes del cumplimiento externo
1	Education & Guidance	Conduce entrenamiento de concientización en seguridad técnica
+0	Threat Assessment	Algunas cuantas actividades por debajo de la práctica esperada
+0	Security Requirements	Algunas cuantas actividades por debajo de la práctica esperada
+0	Secure Architecture	Algunas cuantas actividades por debajo de la práctica esperada
+0	Design Review	Algunas cuantas actividades por debajo de la práctica esperada
+0	Code Review	Algunas cuantas actividades por debajo de la práctica esperada
+0	Security Test	Algunas cuantas actividades por debajo de la práctica esperada
+1	Vulnerability Management	Sabe identificar el punto de contacto para problemas de seguridad
+0	Enviroment Hardening	Algunas cuantas actividades por debajo de la práctica esperada
+0	Operational Enablement	Algunas cuantas actividades por debajo de la práctica esperada

Software Assurance Maturity Model (SAMM)

Encuesta en Perú (2013)

JACK YOUR INCIDENTS NOW!

Nivel	Prácticas de seguridad	Descripción
	Strategy & Metrics	Establecer una estructura del programa, medible y alineada al negocio Estima el perfil de riesgo general del negocio
	Policy & Compliance	Asegurar los estándares internos y el cumplimiento legal/regulatorio Identifica y monitorea los ejes del cumplimiento externo
	Education & Guidance	Armar al personal con el KB/recursos para diseñar/desarrollar/desplegar sw Conduce entrenamiento de concientización en seguridad técnica
	Threat Assessment	I/E el riesgo del proyecto basado en las funciones/características/entorno del sw Algunas cuantas actividades por debajo de la práctica esperada
	Security Requirements	Especificar anticipadamente el las necesidades del sw respecto a la seguridad Algunas cuantas actividades por debajo de la práctica esperada
	Secure Architecture	Fijar pasos para el diseño y construcción de un sw seguro por defecto Algunas cuantas actividades por debajo de la práctica esperada
	Design Review	Evaluar el diseño y arquitectura del sw por problemas relacionados a la seguridad Algunas cuantas actividades por debajo de la práctica esperada
	Code Review	Inspeccionar el sw a nivel de código fuente a fin de hallar vulnerabilidades Algunas cuantas actividades por debajo de la práctica esperada
	Security Test	Inspeccionar el sw en el ambiente de ejecución a fin de hallar vulnerabilidades Algunas cuantas actividades por debajo de la práctica esperada
	Vulnerability Management	Asegurar los procesos de manejo y respuesta a brechas e incidentes Sabe identificar el punto de contacto para problemas de seguridad
	Enviroment Hardening	Asegurar el ambiente de ejecución que aloja el sw de la organización Algunas cuantas actividades por debajo de la práctica esperada
	Operational Enablement	Recopilar información crítica de seguridad del team y comunicarlo a los usuarios Algunas cuantas actividades por debajo de la práctica esperada

Riesgos de una mala contratación

THE FOLLOWING **SCENES** ARE POS-PENTESTING TRAGEDIES

DISCLOSURE UNDER

BY THE CHATHAM HOUSE RULE SINCE JUNE 1927

THE PRESENTATION HAS BEEN RATED

JaCkSecurity

1) Re-fabricación

2) Larga espera

3) Paraíso de la auditoría del sw

4) Propiedad del código fuente

Empresas que interesados en profundizar el pentest app web, por una revisión de código exhaustiva, descubren que el proveedor de desarrollo no le entregaría el código abierto, por ser propiedad intelectual de esta última.

5) Vuelta en círculos

6) Pistolas de agua

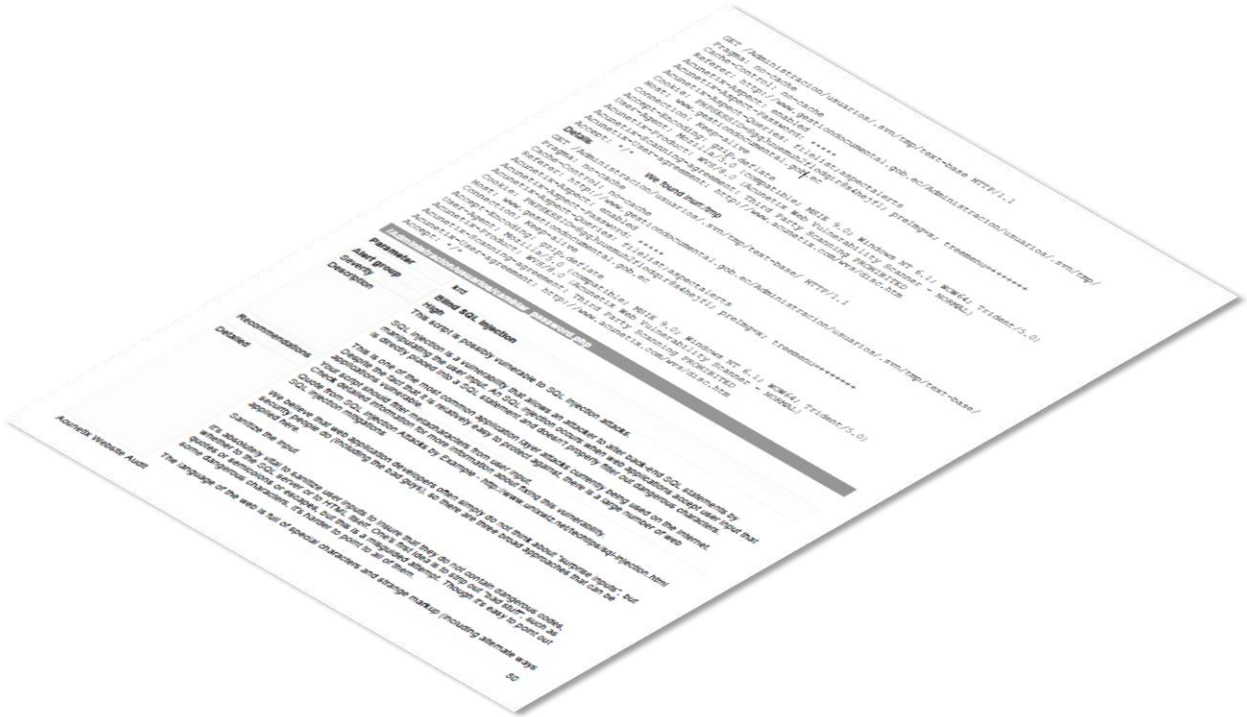
Que pierde tu compañía

- Una compañía que se **descubre** que ha contratado un proveedor de desarrollo inseguro:
  - **Pierde**
    - Fuerza competitiva
      - No volverá a usar su app web como un valor estratégico
    - Tiempo proyecto
      - Retraso su lanzamiento
    - Dinero nuevo
      - Recontratar otro desarrollador
      - Y –muy seguro- volver a empezar el desarrollo desde “0”

Por qué nos interesamos por estos problemas

¿cuáles NO son las soluciones correctas?

1. Persistir en reparar las fallas de código y lógica
   - **PELIGRO**
     - Abrir nuevas brechas

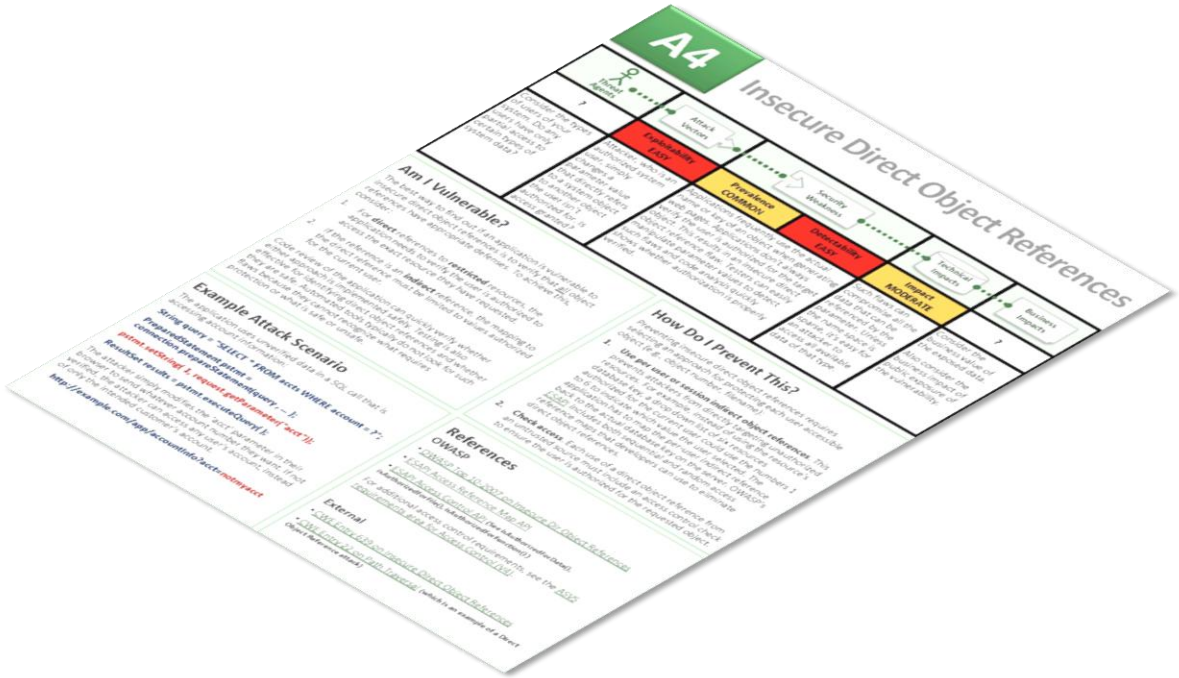


¿cuáles NO son las soluciones correctas?

2. Usar Vendor Management Using COBIT® 5
   - PELIGRO:
     - El comprador no sabe necesariamente acerca de S-SDLC

¿cuáles NO son las soluciones correctas?

3. Hacer contratos citando el Top 10 Risk – OWASP
   - PELIGRO:
     - Son 10.
     - No cubre defectos de inicio



Ingredientes empleados

S-SDLC

SAMM

Framework

Vendor Management using COBIT 5

Métricas

ASVS

Apoyo

OWASP Secure Contract Annex
STRIDE Microsoft

+ [ + ] =

- Pentest (report) App Web
- WAF (ModSecurity)

- Consultores de seguridad
- Proveedores de desarrollo

software seguro

JaCkSecurity

Diagramas: Propuesta (p1)

Contratación segura

JaCkSecurity

Trade-off

- Negocie las desventajas de la seguridad ideal:
  1. Mercado no está al nivel para proveerlo
     - Manéjelo como proyecto piloto
  2. Evite anunciar fechas de liberación con el estándar de tiempo de entrega actual
     - La **seguridad** es opuesto a **tecnología** (sw)
       - Ej. Por +seguridad Microsoft Windows Vista e IE retrasaron su salida, y además fueron muy mal recibidos por la crítica
  3. Evite abarcar todas las ventajas de un SDLC seguro
     - La guía SAMM tiene plantillas por fases según industria
     - Un pentest siempre hallará fallas
       - No combata fallas, combata riesgos OWASP Risk Rating M.

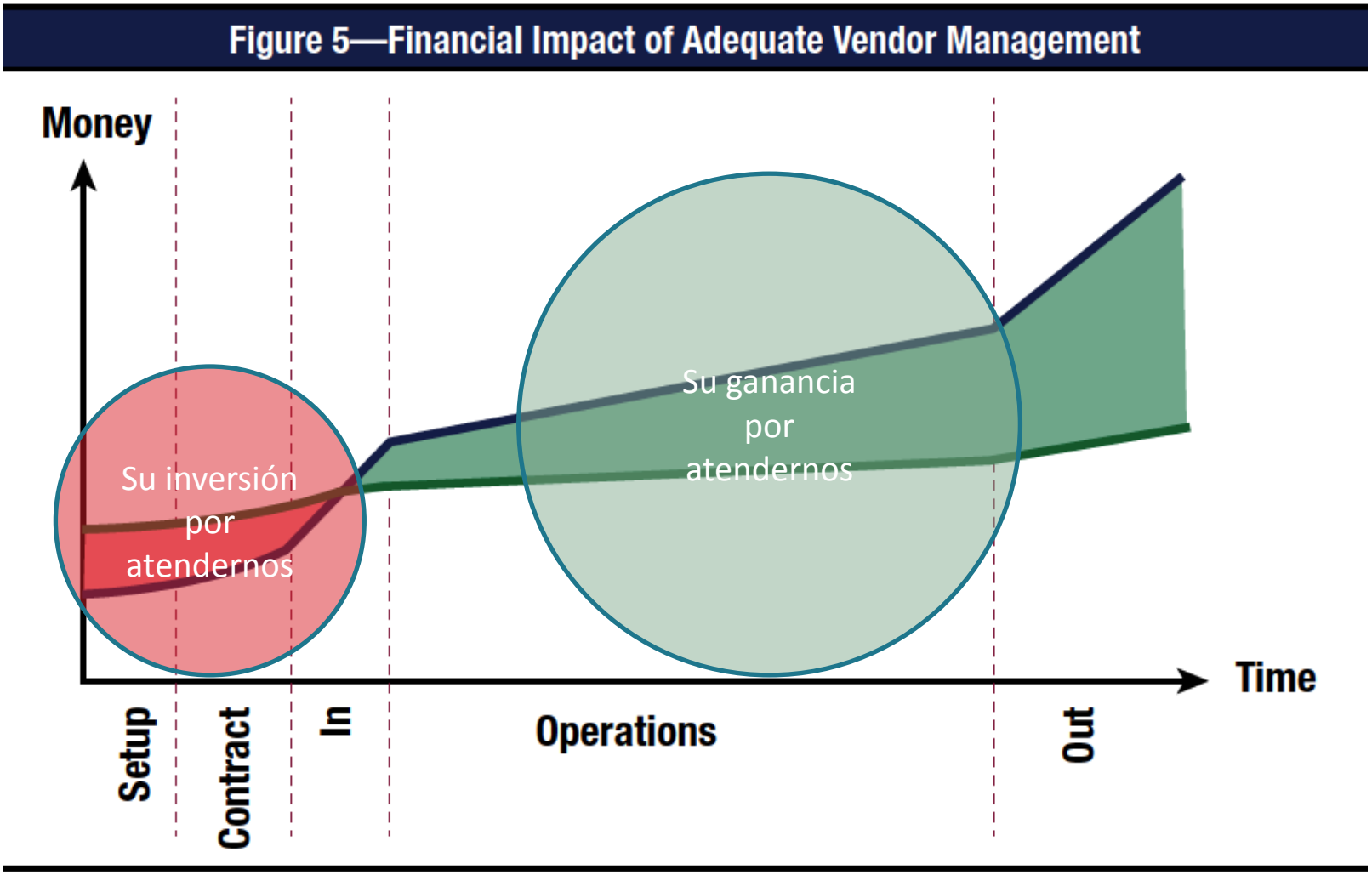
Resumen

- Madurez local:
  - La muestra local tiene 4 de 12 prácticas del S-SDLC cubiertas a su nivel más bajo (1 de 3)
- Si va a diseñar sw nuevo:
  - Añada un consultor de seguridad al proyecto
  - Utiliza un S-SDLC como SAMM
    - Evalúa en RFI, su nivel actual, y compromételo a subir su nivel madurez en la entrega de las prácticas que le compete.
  - Fíjalo a tu ciclo de gestión del proveedor
  - Fíjale metas (SLA)
- Si ya tiene sw vulnerable, que planea reemplazar:
  - Instale un WAF, para parchar virtualmente
  - Use el reporte de pentest como base de reglas mínimas
  - Evalúa tu SAMM actual
    - Según tu industria fija expectativas a las prácticas que sólo te competen como cliente, a fin de estar listo para contratar casas de sw +seguro

Evaluación y plan de madurez de tu SDLC

- Contáctenos, para más información.

Valor de la charla



JACK YOUR INCIDENTS NOW!

For information security emergencies call to (+51) 1 651 0222