CORESEB®
VI CONGRESO REGIONAL DE SEGURIDAD BANCARIA Y FINANCIERA
2017

Operaciones de Seguridad Sostenibles

TECNASA
Es Confianza

Obdulio Sierra
Tecnasa/Mcafee Guatemala

McAfee™
Together is power.

Cambios fundamentales del mundo digital

Evolución de Amenazas

Mas de 500K nuevas amenazas diariamente
Ransomware-as-a-Service
La amenaza real de la cyber-guerra

Proliferación de dispositivos y datos

Miles de millones de dispositivos
Zetabytes de datos
Internet de las cosas

Nube

Transformación técnica y de negocio

Movilidad

Accesar cualquier servicio, en cualquier momento desde cualquier dispositivo

Las organizaciones deben innovar, crecer y operar con confianza

Operaciones de Seguridad – Top 3 preocupaciones

Identificar y priorizar las amenazas avanzadas rapidamente

Manejar los incidentes de una forma mas eficiente

Optimizando los recursos

Y si yo pudiera…

¿Reducir la carga del nivel 1 en un 50%?

¿Ejecutar acciones de contención y remediación?

¿ Mantener el personal actual mientras reduzco el riesgo?

Operaciones de Seguridad – Mas del Panorama….

Complejidad

564 encuestados
8 días hábiles (64 horas) para que una investigación de seguridad retorne resultados – desde la detección hasta la corrección
Al menos 4 herramientas

Multiples fuentes

La Red, La Nube, los endpoints, terceros

La Responsabilidad del CISO

Una vision complete del riesgo y el cumplimiento

La propuesta

Un modelo optimizado de seguridad que habilite las mejores practicas para el manejo de amenazas como parte de unas operaciones de seguridad eficientes.

Esto requiere la adopción de un modelo que permita integrar en forma sencilla las soluciones de seguridad y la inteligencia contra amenazas en el proceso del día a día.

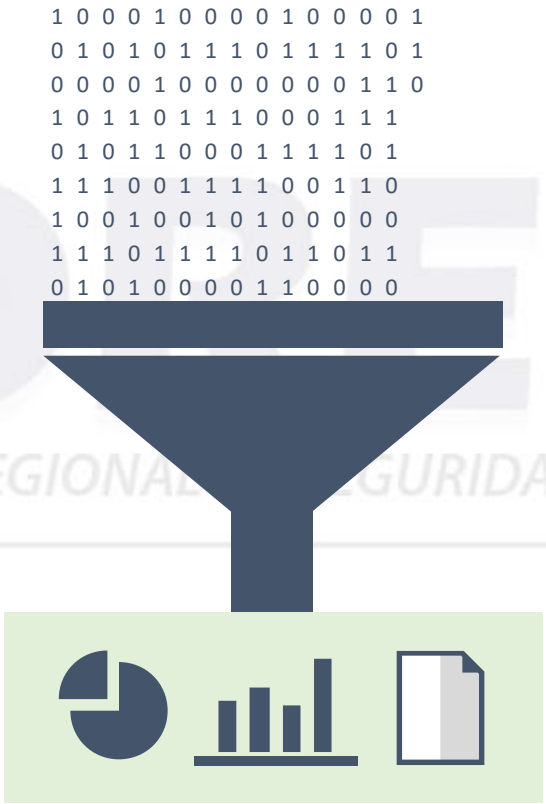
Herramientas cono dashboards centralizados y accionables que integren los datos de las amenazas y las contramedidas.

1. Evalue la madurez de su Organizacion

	Reactiva	En cumplimiento	Proactiva	Optimized
Estrategia	Falta de estrategia Falta de sponsorship del mgnt Política pobre y no reforzada No hay cumplimiento con regs	Existe una estrategia de Man de Ries Algún soporte de la gerencia Políticas deficientes Algún cumplimiento	Tolerancia al Riesgo conocido Buen soporte de la gerencia Políticas alineadas al negocio Cumplimiento efectivo	Risk gap assmts regulares Total mgmnt support e involucr Manejo del riesgo
Infraestructura	No hay una linea base o"gold image" No hay mgmt de config Perfil de vulnerabilidades descon Arquitectura pobre	Existen algunas referencias Config mgmnt debil Se conocen las vulns Arquitectura adecuada	Referencias seguras y prevalentes Buen config mgmnt Programa de mgmnt de vulns Buena arquitectura	Referencias optimizadas Pocas vulnerabilidades Métricas y reports óptimos
Aplicaciones	Estado de vulns desconocido No hay SDLC	Pruebas Ad-hoc Algún SDLC	Testeo estandarizado y periódico Pocas vulnerabilidades Seguridad parte de SDLC	Administración de Vulns SDLC seguro
Respuesta a Incidentes	No hay capacidad ni equipo No hay tecnología ni procesos No existe un plan de RI	Alguna capacidad y herramientas Puede haber una persona para RI Algún plan de RI Considerando SIEM/SOC	Totales capacidades de SOC Un plan de RI definido Alguna capacidad interna de RI	Full CERT Prevención situacional Un equipo optimizado de escalacion
Prevencion	No existe un programa de prevención	Alguna prevención Se Brinda algún entrenamiento	Programa formal de prevención Métricas lanzadas y medidas por user	Usuarios consientes de su respons Resiliencia demostrada a técnicas de ingeniería social
Metricas	No métricas/reportes No se puede medir el ROI de la seg	Métricas débiles ("hi/med/low") Reportes débiles	Algunas medidas básicas tomadas Reportes para operaciones y mgmnt	Soporte total del board ROI reconocido Framework evolucionado

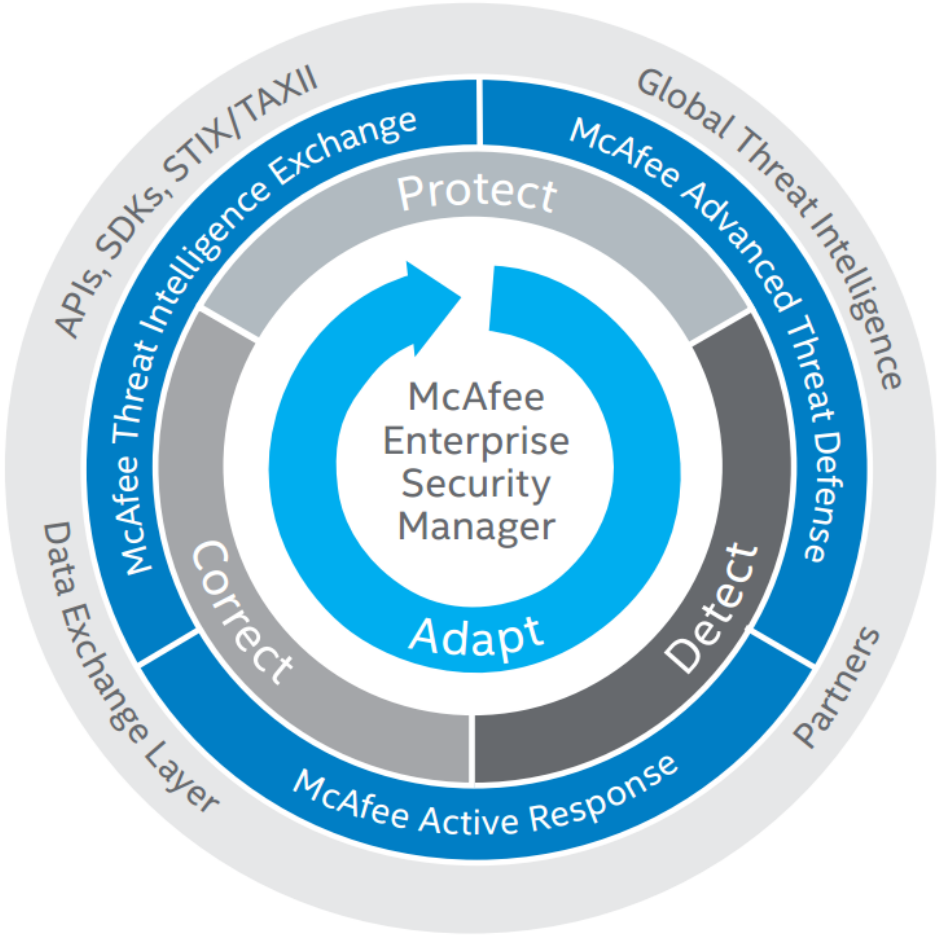
2. Integre, para mejores resultados/tiempo

3. Automatize para incrementar la eficiencia y la exactitud



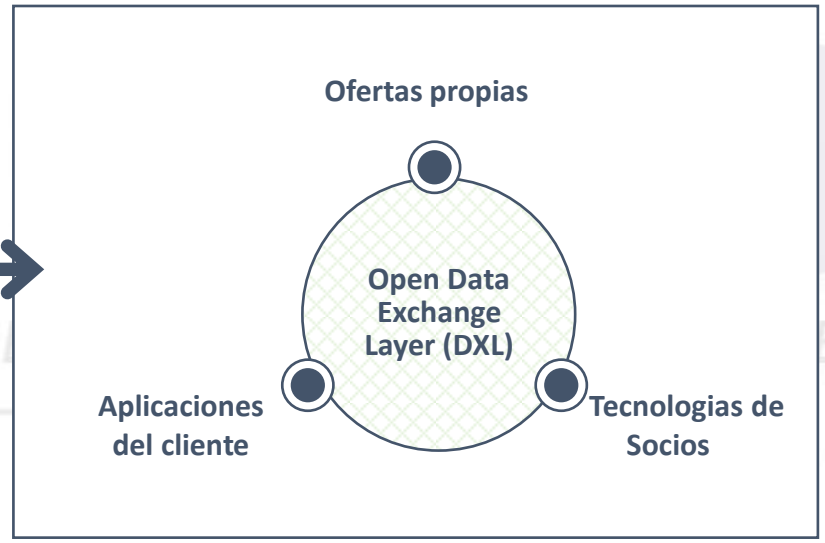
Exactitud, foco, eficiencia

Una Plataforma Optimizada para Operaciones de Seguridad



Una integración basada en un estándar comun

- Transformar tecnologia aislada en un Sistema cohesionado
- Compartir Inteligencia y sincronizar acciones entre cualquier tecnologia
- Automatizar el ciclo de defense para aprender y adaptarse inmediatamente



Una Plataforma Integrada

- Seguridad de puntos finales
- Intercambio de inteligencia contra amenazas
- Protección de datos
- Protección de red
- Protección de navegación