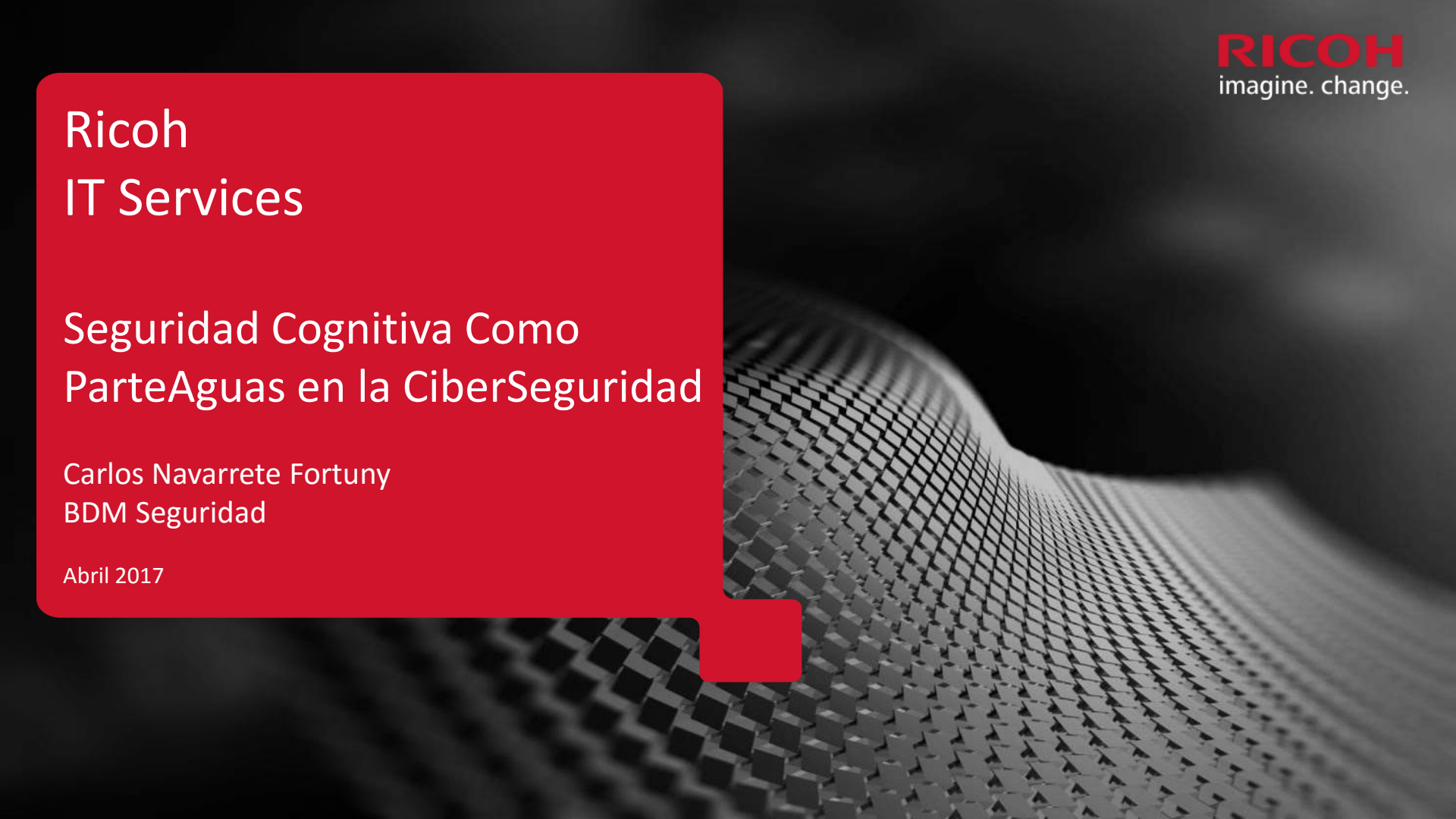


Ricoh
IT Services

Seguridad Cognitiva Como ParteAguas en la CiberSeguridad

Carlos Navarrete Fortuny
BDM Seguridad

Abril 2017

RICOH
imagine. change.

¿QUE ES LA SEGURIDAD COGNITIVA?

¿ PROBLEMÁTICA EXISTENTE EN LA CIBERSEGURIDAD?

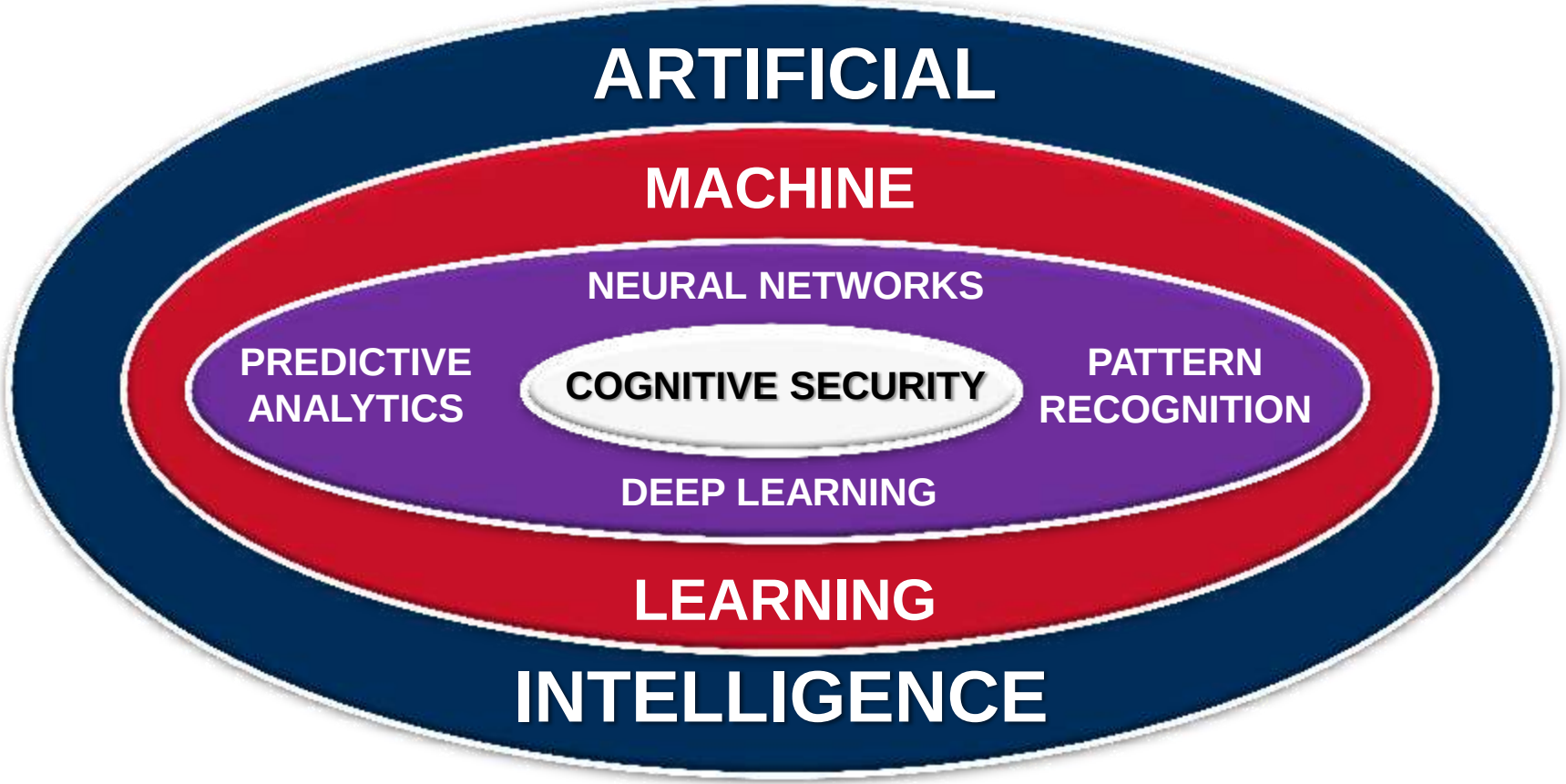
¿ COMO SOLUCIONA LA SEGURIDAD COGNITIVA ESTOS PROBLEMAS?

CARACTERISTICAS DE UN SISTEMA DE SEGURIDAD COGNITIVA

¿ QUE NOS DEPARA EL FUTURO DE LA CIBERSEGURIDAD?

¿Qué es la Seguridad Cognitiva?

RICOH
imagine. change.



RICOH
imagine. change.

¿QUE ES LA SEGURIDAD COGNITIVA?

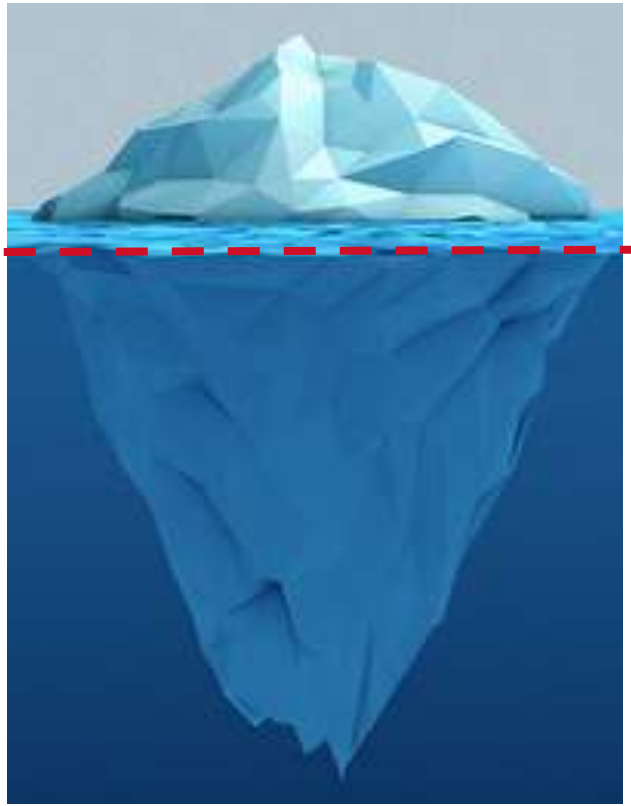
¿ PROBLEMÁTICA EXISTENTE EN LA CIBERSEGURIDAD?

¿ COMO SOLUCIONA LA SEGURIDAD COGNITIVA ESTOS PROBLEMAS?

CARACTERISTICAS DE UN SISTEMA DE SEGURIDAD COGNITIVA

¿ QUE NOS DEPARA EL FUTURO DE LA CIBERSEGURIDAD?

Las Barreras Naturales del CISO



Eventos de Seguridad Generados por Sistemas de Seguridad

- **120K** Eventos de Seguridad/Dia
- **75K** Vulnerabilidades Reportadas en SW
- Actividad de los Usuarios
- Indicadores de Compromiso

Un Universo Inexplorado por Nuestro Conocimiento

- **720K** Blogs de Seguridad al Año
- **180K** Noticias y Artículos al Año
- **10K** Reportes y Documentos de Investigación
- Publicaciones de la Industria
- Información Forense
- Wikis
- Análisis de Inteligencia

Problemática: Personal Requerido en un SOC

RICOH
imagine. change.

- **ISC2 Stack (International Information Systems Security Certification Consortium)**
- **CISSP (Certified Information Systems Security Professional**
- **SSCP (Systems Security Certified Practitioner**
- **CISM (Certified Information Security Manager)**
- **GIAC Stack (Global Information Assurance Certification)**
- **GCFW (Firewall Analyst)**
- **GPPA (Perimeter Protection Analyst)**
- **GCIA (Intrusion Analyst)**
- **GCIAH (GIAC Certified Incident Handler)**
- **GCWN (GIAC Certified Windows Security Administrator)**
- **GCUX (GIAC Certified UNIX Security Administrator)**
- **GMON (GIAC Continuous Monitoring Certification)**
- **GCFA (GIAC Certified Forensic Analyst)**
- **CompTIA Security + Certified**

Problemática de Seguridad en los Corporativos

RICOH
imagine. change.

Principales Restricciones en Seguridad

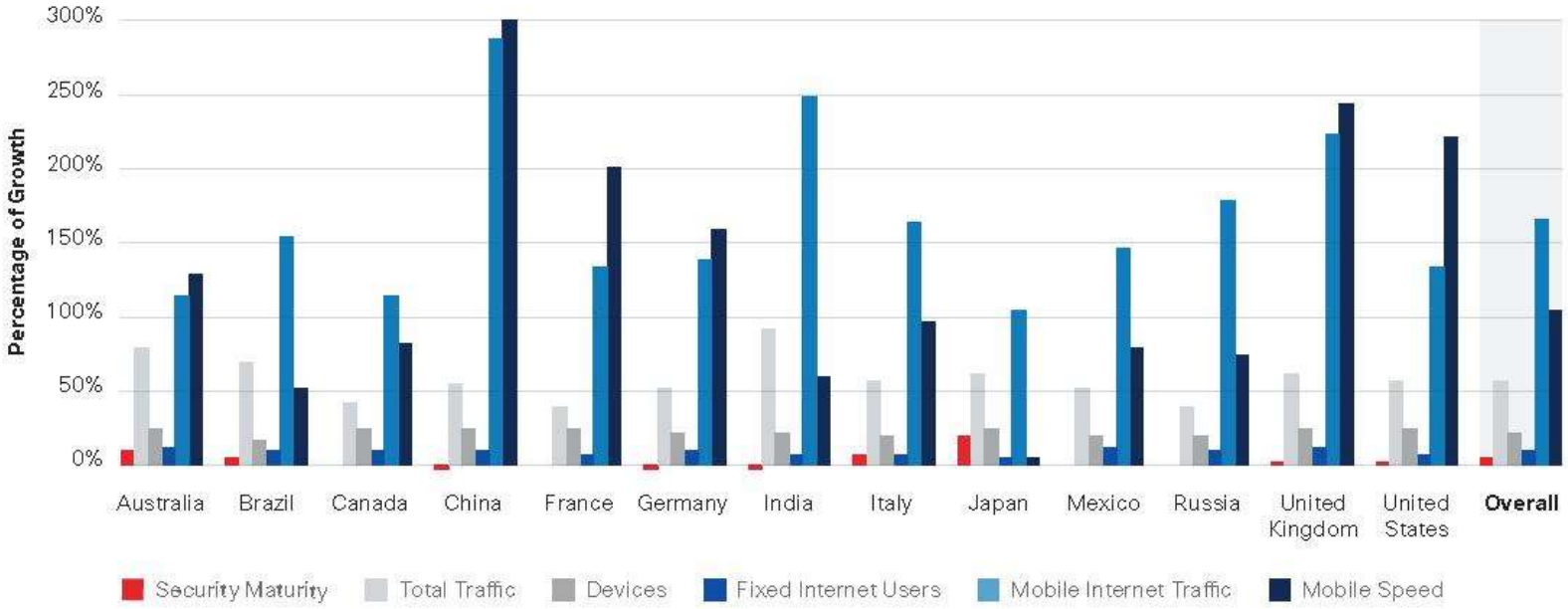
	2015 (n=2432)	2016 (n=2912)
Budget Constraints	39%	35%
Compatibility Issues	32%	28%
Certification Requirements	25%	25%
Lack of Trained Personnel	22%	25%

Mas de 1.2M de Profesionistas Requeridos Hoy!!!!!!

Porcentaje de Eventos de Seguridad Mitigados y No Mitigados

Fuente: Cisco 2017 Security Report.

Crecimiento de Usuarios y Dispositivos vs Madurez de la Seguridad



Fuente: Cisco 2017 Security Report.

Problemática General Existente en la CyberSeguridad

RICOH
imagine. change.

Evolucion Constante de Amenazas	Hasta 24Hrs para Detectar Amenazas con Infraestructura	+ 100 Días para detectar amenazas una vez Dentro
Falta de Escases de Profesionales en Seguridad	Alto Nivel de Especializacion para Mitigar Amenazas	Falta de Automatización en la Migitacion
Crecimiento Exponencial de Malware con CaaS	Personal Insuficiente para Atender Eventos	Malware cada vez mas Evasivo

RICOH
imagine. change.

¿QUE ES LA SEGURIDAD COGNITIVA?

¿ PROBLEMÁTICA EXISTENTE EN LA CIBERSEGURIDAD?

¿ COMO SOLUCIONA LA SEGURIDAD COGNITIVA ESTOS PROBLEMAS?

CARACTERISTICAS DE UN SISTEMA DE SEGURIDAD COGNITIVA

¿ QUE NOS DEPARA EL FUTURO DE LA CIBERSEGURIDAD?

El Cambio de Paradigma en La Seguridad con CS

RICOH
imagine. change.

SIN CS	CON CS
• Análisis Estático y Heurístico	• Análisis Dinámico con CS & AI
• Defensas Fácilmente Evadibles	• Detección de Evasión con AI
• Personal Altamente Especializado	• Experto Medio Apoyado de Herramientas
• Tiempos de Detección de 24 Hrs	• Detección Predictiva de Malware < 10 Hrs
• Tiempos Largos de Remediación e Investigación,	• Detección Continua Avanzada con Visión MultiCapa Correlacionada
• Reconfiguración y Adición de Reglas Perpetuas	• Reconfiguración Automática una vez ML ha entendido el modo de ataque.
• Ataques Enmascarados y Falsos Positivos Debido al Análisis de Logs	• Clasificacion Avanzada y Automatica de Malware
• Mucho Trabajo Manual para Generar Reportes	• Consolas Forenses con Análisis Raíz y Análisis Completo de Impacto
• Personal Insuficiente para Mitigar Ataques	• Mitigación Automatizada

RICOH
imagine. change.

¿QUE ES LA SEGURIDAD COGNITIVA?

¿ PROBLEMÁTICA EXISTENTE EN LA CIBERSEGURIDAD?

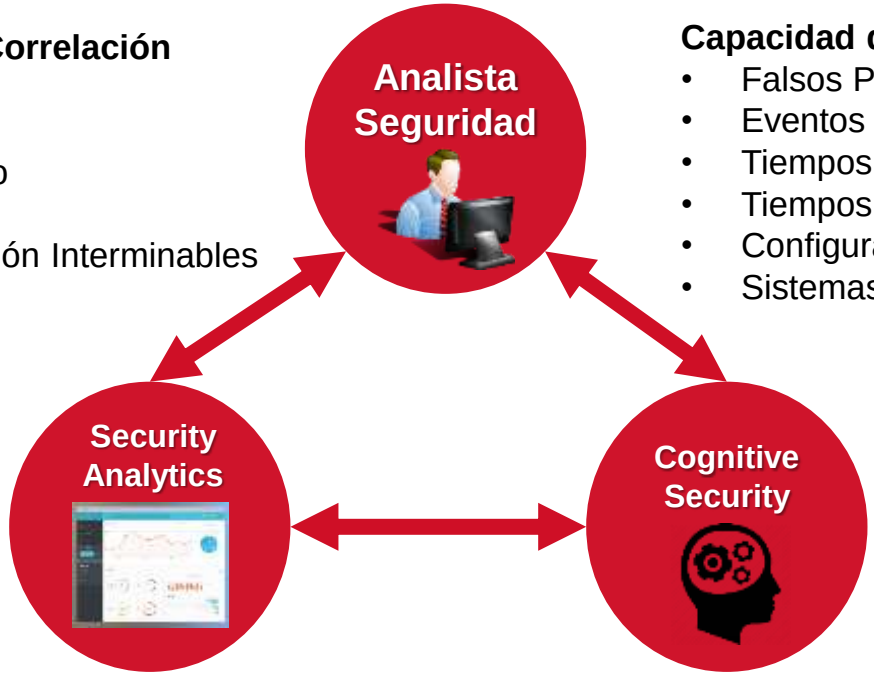
¿ COMO SOLUCIONA LA SEGURIDAD COGNITIVA ESTOS PROBLEMAS?

CARACTERISTICAS DE UN SISTEMA DE SEGURIDAD COGNITIVA

¿ QUE NOS DEPARA EL FUTURO DE LA CIBERSEGURIDAD?

Modelo General de Seguridad Cognitiva

Abstracción, Análisis y Correlación
- Exceso de Información
- Personal Insuficiente
- Personal Especializado
- Reportes Manuales
- Tiempos de Investigación Interminables



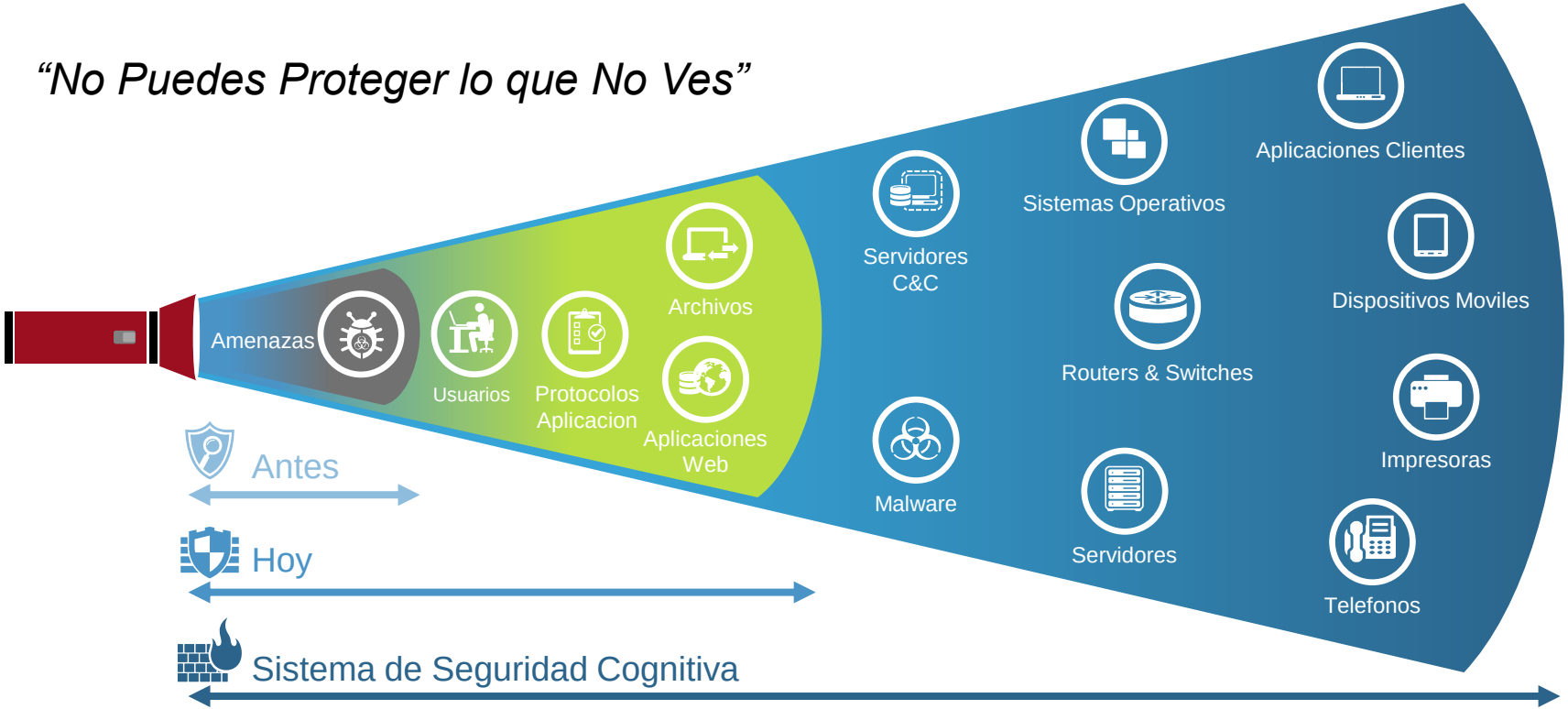
Capacidad de Detección y Automatización
- Falsos Positivos
- Eventos sin Atender
- Tiempos de Detección Largos
- Tiempos Remediación Largos
- Configuración Continua
- Sistemas en Obsolescencia

Analítica de la Seguridad
- Big Data Analytics
- Búsquedas Inteligentes
- Correlación Inteligente
- Taxonomía

Seguridad Cognitiva
- Análisis no Estructurado
- Machine Learning
- Deep Learning
- Entendimiento Incremental
- Identificación Patrones

Visibilidad Completa Al Interior y Exterior

- *“No Puedes Proteger lo que No Ves”*



Capacidades Forenses de la Administración de la Seguridad

RICOH
imagine. change.

Quien		Enfócate en estos Usuarios Primero
Que		Estas Aplicaciones Fueron Afectadas
Donde		Departamentos Afectados
Cuando		Análisis Continuo
Como		Progresión del Ataque

Preguntas a los Fabricantes de Seguridad

RICOH
imagine. change.

¿Cuantos tiempo llevan desarrollando AI para la Seguridad Cognitiva?
¿ En que fase de desarrollo de AI van en cada componente de seguridad ?
¿ Que mecanismos de AI implementan ?
¿ Que nivel de inversión están asignando a desarrollo de AI en Seguridad ?
¿ Que nivel de integración y comunicación tienen los componentes de seguridad ?
¿ Que nivel de integración multivendor se tiene con componentes ?
¿ Que Nivel y Cuantas capas de visibilidad se obtiene con el gestor de seguridad?
¿ Cual es el Tiempo de Detección Máximo para Malware Avanzado ?
¿ Los Sistemas Ejecutan Análisis Continuo en Sistemas, Usuarios e Información ?
¿ Que estrategia de AI tienen para spearfishing ?
¿ Cual es el porcentaje de falsos positivos en pruebas de desempeño ?
¿ Que Nivel de Automatización proporciona el Reporteo ?
¿ Cual es el Nivel de Automatización en la Mitigación?
¿ Con que Nivel de Automatización se Crean Nuevas Reglas de IPS?

RICOH
imagine. change.

¿QUE ES LA SEGURIDAD COGNITIVA?

¿ PROBLEMÁTICA EXISTENTE EN LA CIBERSEGURIDAD?

¿ COMO SOLUCIONA LA SEGURIDAD COGNITIVA ESTOS PROBLEMAS?

CARACTERISTICAS DE UN SISTEMA DE SEGURIDAD COGNITIVA

¿ QUE NOS DEPARA EL FUTURO DE LA CIBERSEGURIDAD?

Evolución de los Ataques en la CiberSeguridad

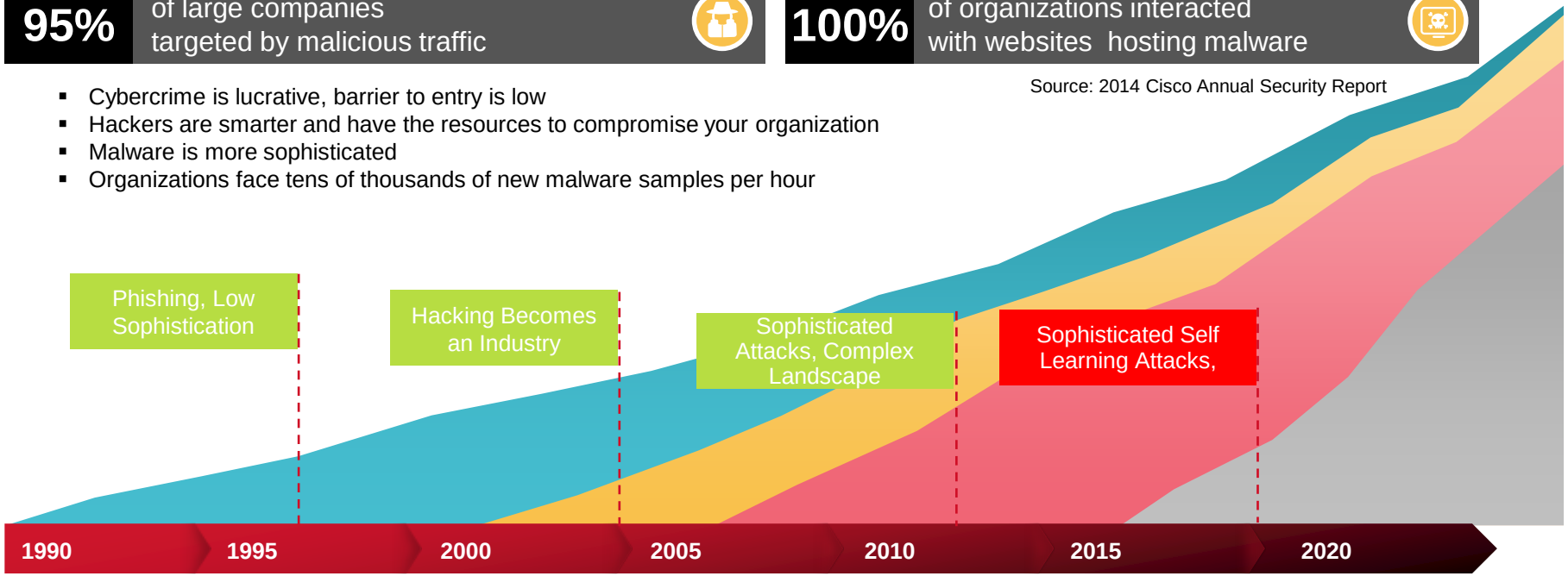
RICOH
imagine. change.

95% of large companies targeted by malicious traffic

100% of organizations interacted with websites hosting malware

Source: 2014 Cisco Annual Security Report

- Cybercrime is lucrative, barrier to entry is low
- Hackers are smarter and have the resources to compromise your organization
- Malware is more sophisticated
- Organizations face tens of thousands of new malware samples per hour



Viruses
1990-2000

Worms
2000-2005

Spyware and Rootkits
2005-Today

APTs Cyberware
Today +

Cognitive Malware
2018 +

La Guerra de Motores Cognitivos (Guerra de las Maquinas)

RICOH
imagine. change.

DEFENSA	MALWARE
A Mayor Aprendizaje mayor eficiencia de defensa	A Mayor Aprendizaje Mayor capacidad de ataque
Automatización y Correlación de la Información con BDA para Visibilidad de Ataques	BDA para obtener información de la victima y lanzar ataques dirigidos
Automatización en Remediación y Creación Nuevas Reglas	Automatización en combinación de ataques y cambio de patrones
Reducción de Tiempos de Detección	Entre mas permanezca dentro un Malware Mayor Capacidad de Evasión

Ejemplos de Malware Cognitivo

RICOH
imagine. change.

- Campañas de Spear-Fishing con Big Data Analytics!!
- PCs, Servers y Enpoints Infectados por Chat Bots basados en Deep Learning!!
- Malware con Técnicas de Evasión con Autoaprendizaje!!
- Ataques DDoS Automatizados!

RICOH

imagine. change.

Peligro En El Futuro o En El Presente???

RICOH
imagine. change.

SKYNET

Stephen Hawking

- **La Humanidad esta en el Punto Mas Critico de Su Historia**
- **El desarrollo de AI puede llevar a la destrucción del planeta**
- **Alto Riesgo de que la gente pierda sus trabajos frente al desarrollo de AI**
- **AI debe Ser Regulada y su Desarrollo no Permitido debe Ser Penado**

The Ultimate Driver to Adopt Cognitive Security

RICOH
imagine. change.

- A Cognitive Hack takes place when a user behavior is influenced by misinformation (Data Mining and Big Data Hacking Key in Success)
- The longer the attack persist inside a host the more it will learn to evade and to operate independently inside it.
- Autonomous Malware will operate without so much hacker involvement and it will evolve as more and more victims are affected.
- Cognitive Protection will become a Matter of Having the Best Cognitive Engine (Indeed the War of Cognitive Engines Will Arise!!!!)