Necesito crear un SOC, ¿Y ahora?

Presenter

André Carraretto, CISSP
Cyber Security Strategist

Rafael Aguilera
Sr Systems Engineer

Date

26/04/2017

Presentadores

Rafael Aguilera
Sr. Systems Engineer
rafael_aguilera@symantec.om

Rafael es especialista en seguridad y tecnologías enfocadas en protección de datos. Como parte de sus responsabilidades apoya a empresas en México en sus proyectos de seguridad informática.

Ingeniero Cibernético y en Sistemas Computaciones por la Universidad La Salle.

André Carraretto
Cyber Security Strategist
andre_carraretto@symantec.com

Estratega de seguridad de la información de Symantec, principal portavoz y responsable de la difusión de la visión estratégica de la empresa en el mercado y para los principales clientes en Brasil y Latino América.

Responsable por la arquitectura y estrategia de Seguridad de la Información para los Juegos Olímpicos Rio 2016 para toda la cartera de productos y servicios de Symantec.

Con más de 20 años de experiencia en TI, cuenta con varias certificaciones del mercado, entre ellas ISC^2 CISSP, CCSK y PCIP.

Copyright © 2017 Symantec Corporation

Agenda

1 ¿Cuáles son algunas de las razones para invertir en seguridad?

2 ¿Qué es un SOC?

3 ¿Cómo construir un Security Operations Center (SOC)?

4 Cyber Security Services

Copyright © 2017 Symantec Corporation

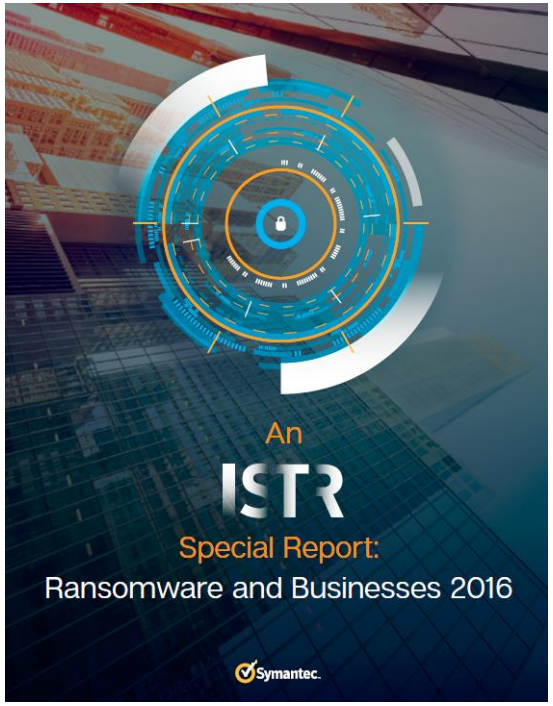
¿Cuáles son algunas de las razones para invertir en seguridad?

Section

1

Ransomware Report 2016

- Record de nuevos ransomwares
  - 100 nuevas familias identificadas en 2015. En 2014 eran 77.
- El valor para redención está subiendo. El promedio actual es $679
- Las empresas son los nuevos objetivos
  - Los empleados en las organizaciones representan el 43% de las infecciones
  - Hay familias creadas para atacar a las organizaciones
  - Ransomware dirijido utiliza técnicas avanzadas de ataque



Fuente: ISTR Insights Special Report: Ransomware and Business 2016
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

Copyright © 2017 Symantec Corporation

Cómo ellos accesan?

Email

- Phishing / Spear Phishing
- Adjunto a emails
- A través de enlaces en el cuerpo del correo

Exploit Kits

- Alojados en sitios confiables
- Enlaces enviados por email, sociale media o anuncios

Otros Vetores

- Anuncios
- Otros malwares
- Brute-force
- Vulnerabilidades
- Worm
- SMS y app stores

Fonte: ISTR Insights Special Report: Ransomware and Business 2016
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

Copyright © 2017 Symantec Corporation

¿Qué es un SOC?

Section

2

Security Operation Center vs Network Operation Center

- SOC:
  - Identifica incidentes de seguridad
  - Notifica a los diversos equipos y responsables de servidores, red, operaciones, riesgos etc. sobre incidentes de seguridad.
  - Investigación y análisis sobre nuevos ataques.
  - Coordina y lidera la investigación y resolución de incidentes de seguridad.
  - Realiza pruebas y levantamientos relacionados con seguridad.

- NOC:
  - Identifica fallas en los componentes de la red
  - Administra dispositivos de red
  - Monitores de rendimiento
  - Apoya la investigación y remediación de incidentes
  - Conduce la arquitectura de operación del entorno

El SOC “se suma al trabajo” del NOC

Copyright © 2017 Symantec Corporation

¿Porque la necesidad de un SOC?

- Mucho tiempo para detectar amenazas.
- La investigación de eventos de seguridad requiere de experiencia y conocimiento para interpretar resultados
- Presupuesto/Habilidades/Gente
- Procesos disciplinados centrados en un modelo de infraestructura tecnológica

Source: ISACA, CyberSecurity Nexus

Copyright © 2017 Symantec Corporation

¿Cómo construir un Security Operations Center (SOC)?

Section

3

La creación del SOC

¿Qué voy a entregar?

Catalogo de servicios
- Descripción y alcances

¿Cuándo lo voy a entregar?

Modelo de Madurez y las Capacidades
- Servicios Primarios y Secundarios

¿Cómo lo voy a entregar?

Procesos Clave
- Flujos de Procesos
- Tablas de Procesos

Roles & Responsabilidades (RACI)

¿Quién es el responsable?

Modelo Técnico y Organizacional

¿Cuál es mi preparación?

Modelo bien definido de Security Operation Center

Copyright © 2017 Symantec Corporation

Paso uno: Catálogo de Servicios

Componentes del éxito

C A T A L O G

	Enterprise Threats and Risks Management – Successful Components		
	Incident Handling Services	Proactive Security Services	Security Management Services
Monitoring	•Incident Identification •Incident Classification	•Real Time Device Monitor •Vulnerability Assessment •Penetration Test •Security & Compliance Audit •Cyber Security Intelligence •Performance Monitoring •Fault Monitoring •Policy Compliance •Hunting •Honeypotting	•Business Impact Analysis •Risk Assessment •Threat Assessment •Technology Watch
Advisoring	•Incident Notification	•Alerting & Warning •Trending •Technical Reporting •Security Hotline	•Executive Reporting •Security Consulting •Awareness •Countermeasures Selection
Managing	•Incident Response •Incident Recovery •Forensics Evidence Collection •Malware Analysis •Forensics Analysis •Tracking & Tracing •Post Mortem Analysis	•Secure Device Configuration •Secure Device Maintenance •Policy Management •Policy Enforcement •Patch Management •Events Data Retention •Endpoint Management •Hardening	•Business Continuity •Asset Inventory •Policy Planning •Risk Management •Education/Training •Certification

Copyright © 2017 Symantec Corporation

12

Paso 2: Modelo de Madurez y las Capacidades

Un modelo para el desarrollo en fases

	Initial	Aware	Defined	Managed	Optimized
Security Managmt		Security Awareness Executive Security Reporting	Business Impact Analysis Risk Assessment Asset Inventory	Technology Watch Security Consulting Countermeasures selection Risk Management	Business Continuity Policy Planning Education/Training Certification
Incident Handling	Incident Identification Incident Notification Incident Response	Incident Classification Tracking & Tracing	Incident Recovery	Forensics Evidence Collection Post-mortem Analysis	Forensics Analysis
Proactive Security	RT Device Monitoring Alerting & Warning Policy Management Policy Enforcement	Vulnerability Assessment Penetration Test Security Intelligence Technical Reporting Event Data Retention	Security Device Configuration Security Device Maintenance	Fault Monitoring Patch Management End Point Security Hardening	Security Audit Performance Monitoring Policy Compliance Security Hotline

INICIACIÓN
Desarrollo y atención

Servicios básicos de configuración y entrega

ADOPCIÓN
Madurar y Expandir

Mejorar y Expandir capacidades

EVOLUCIÓN
Optimizar y Mantener

Catálogo de servicios cubierto y optimizado

Copyright © 2017 Symantec Corporation

Paso 3: Diseñar y Optimizar

- *Monitoreo de ataques de ciberseguridad:*
  - 24x7 – Monitoreo en tiempo real de dispositivos de red y endpoints
  - 24x7 – Monitoreo inteligente
- *Monitoreo por regulaciones*:
  - 8x5/12x5 – Monitoreo de cumplimiento de regulaciones asociado a la empresa, la industria y a estándares nacionales o internacionales.

- *Inteligencia de ciberamenazas:*
  - Añadir inteligencia dentro de la infraestructura (Threat Intelligence)
- *Respuesta ante incidentes e incumplimiento de regulaciones:*
  - Establecer robustos procesos y procedimientos para el manejo de las amenazas y violaciones al cumplimiento de regulaciones.

Diseñar técnicas para identificar eficientemente incidentes de seguridad:

- Tendencias
- Threat Hunting
- Honeypotting

Copyright © 2017 Symantec Corporation

El tiempo IMPORTA!

¿Usted esta dispuesto a tardar 24 meses en poder implementar una estrategia de seguridad?

Algunos comentarios de nuestros clientes (antes de MSS):

- Tardamos poco mas de 5 años para construir una infraestructura de correlación que fuera capaz de entregarnos valor. *(CISO of a big Banking Group)*
- Nos costó 12 meses implementar un SIEM y estamos comenzando con la revisión de reglas de correlación debido al alto nivel de incidencias de falsos positivos. Creemos que podremos tener resultados en 12 meses más *(Global CISO of a Consulting Firm)*

Copyright © 2017 Symantec Corporation

“24x7” or not to “24x7”

Esa NO es la cuestion

- Operación 24x7 es el mínimo requerido **SIEMPRE**:
  - La integridad como mejor práctica debe mantenerse con infraestructuras de al menos dos personas.
  - Hay que tener consideraciones logísticas y de seguridad en caso de que alguna persona del staff tenga que abandonar el SOC.
  - Con múltiples analistas trabajando al mismo tiempo pueden cruzar información sobre el trabajo que están hacienda los demás. Adicionalmente ayuda a que los turnos sean menos monótonos y solitarios.
  - *Todos los turnos 24x7 requieren atención primordial donde se incluyan casos como vacaciones o enfermedades.*
  - Asumiendo 2 personas por “función”, estamos hablando de 10 recursos.

Copyright © 2017 Symantec Corporation

¿Cuánto cuesta la capacitación del personal?

Un analista con habilidades suficientes puede costar alrededor de $100K.

- 10 Analistas (para cubrir un turno 24x7) -> 1M$

Y esto es ÚNICAMENTE para los analistas

Copyright © 2017 Symantec Corporation

Estrategias para Administración de Seguridad

Co-sourcing

Utilizar personal externo para ciertas actividades reteniendo las actividades críticas internamente

Insourcing

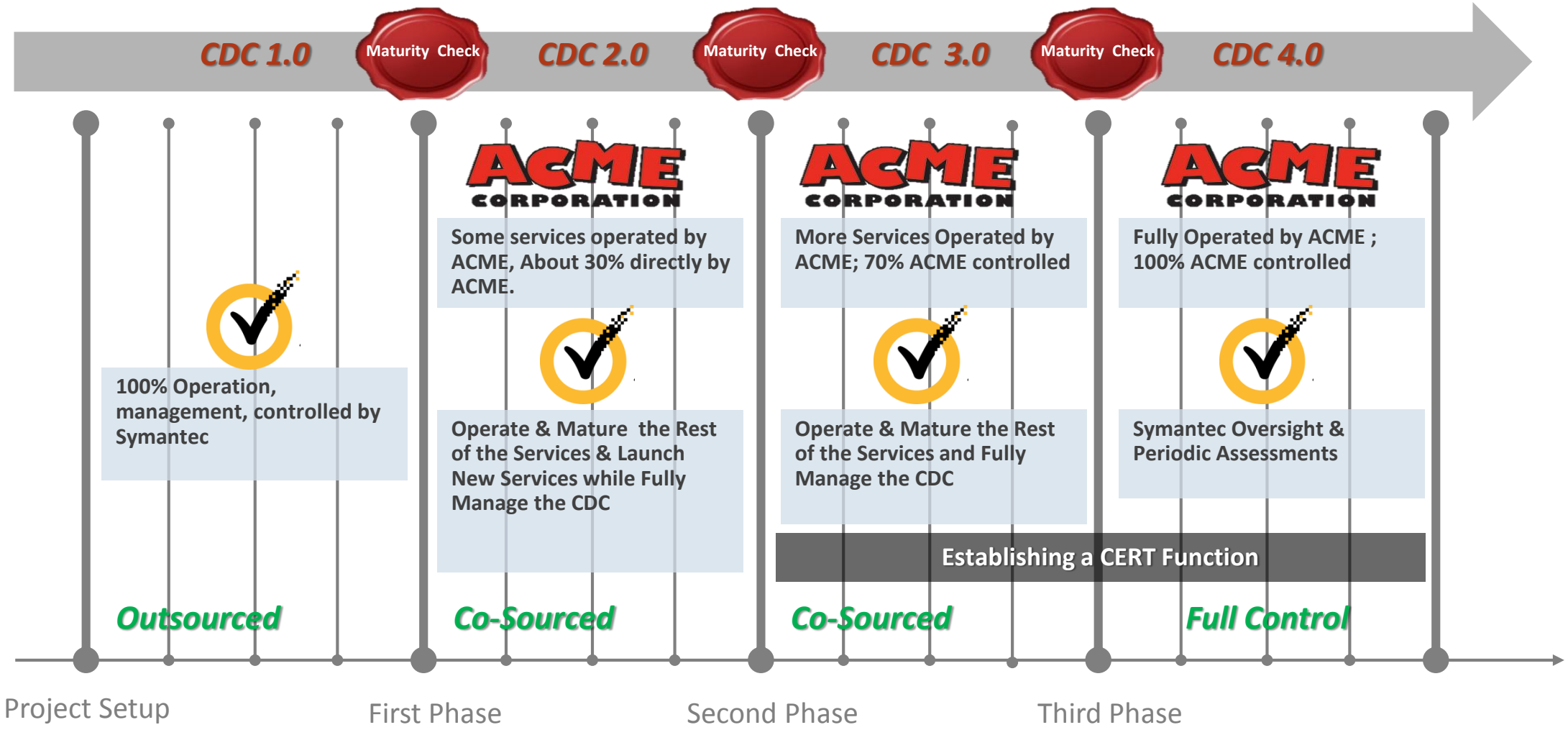
Realizar todas las actividades con mi personal y dentro de mis instalaciones

Outsourcing

Comprometer una empresa externa para realizar actividades de SOC

Copyright © 2017 Symantec Corporation

Estrategia para un SOC/CDC



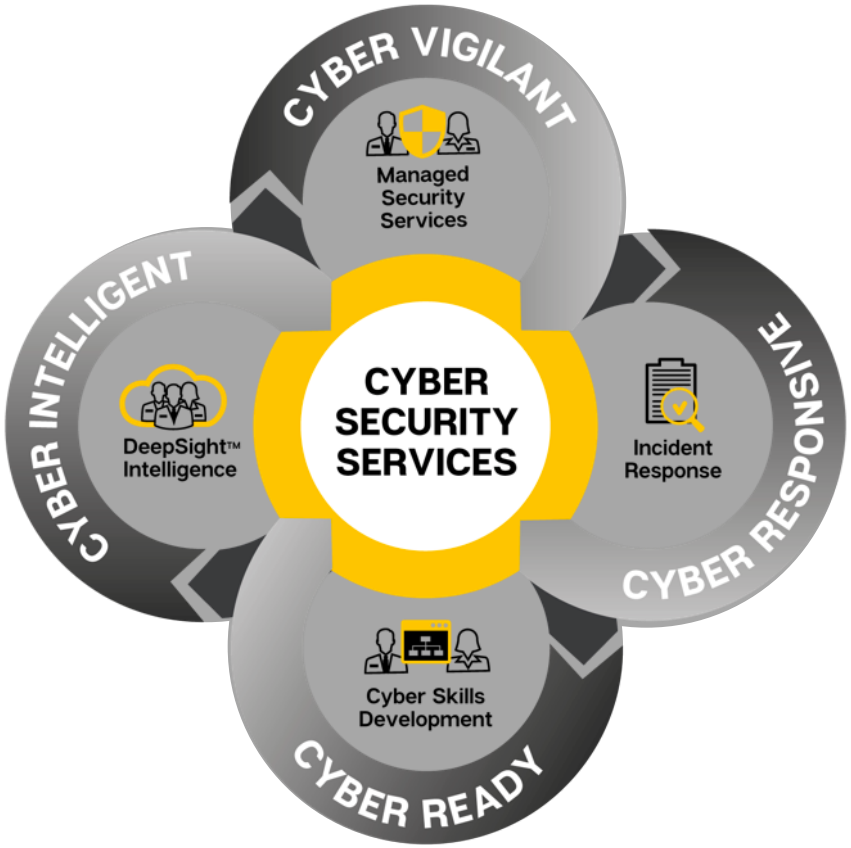
Copyright © 2017 Symantec Corporation

Cyber Security Services

Section

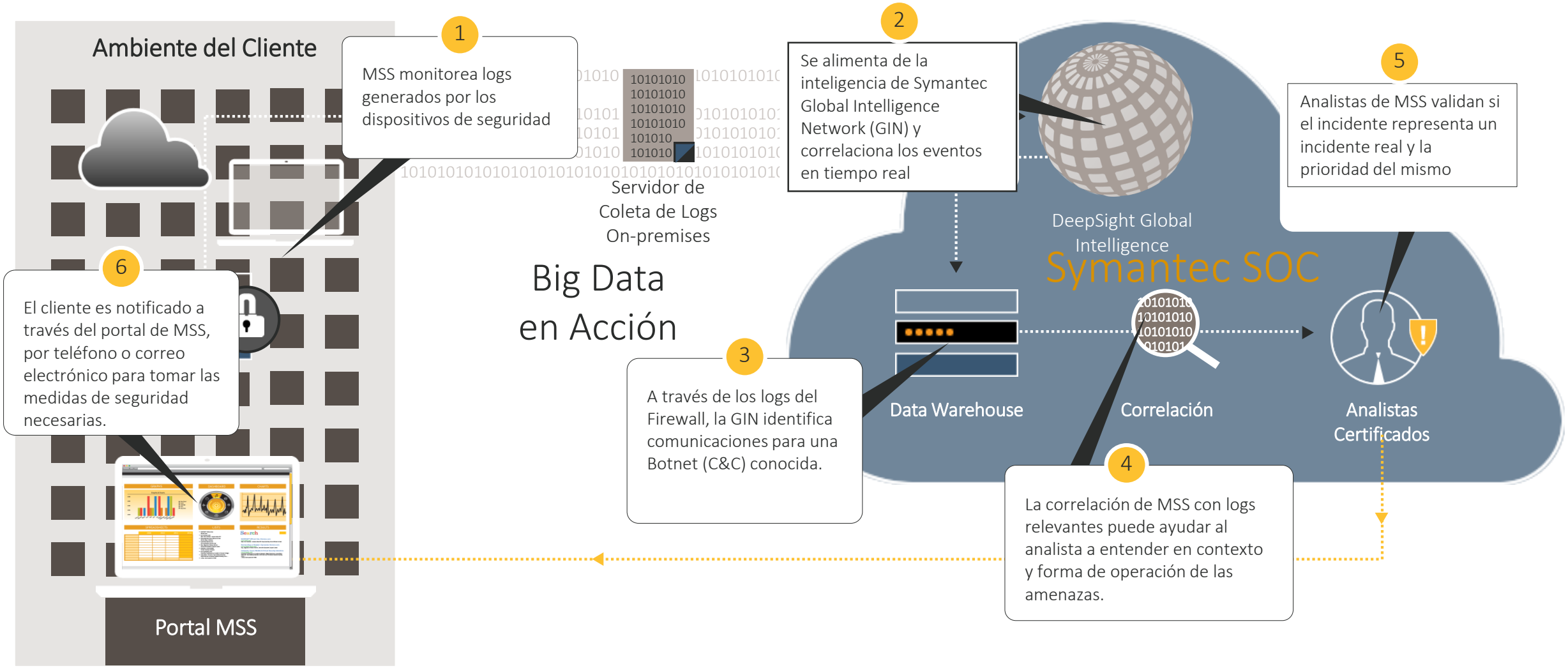
4

Cyber Security Services



Copyright © 2017 Symantec Corporation

Arquitectura



Copyright © 2017 Symantec Corporation

Diferenciadores del proyecto

Funcionalidades	Beneficios
Retención de logs por 1 año (92 días online)	Economizar costos de almacenamiento de logs
Costo fijo y mensualizado	Reducción de costos operativos
Costo por dispositivo	Permite ampliar el alcance del proyecto para mejorar la protección
Correlación con la red civil de ciberinteligencia mas grande del mundo	Reducción de falsos positivos y menores costos administrativos

Copyright © 2017 Symantec Corporation

Global Average Month		Global Average 24 Hours
2,085,321,104,588	Logs	69,510,703,486
1,043,187	Potential Incidents	34,773
232,331	Actual Incidents	7,744
5,977	Severe Incidents	199

"In Other Words"

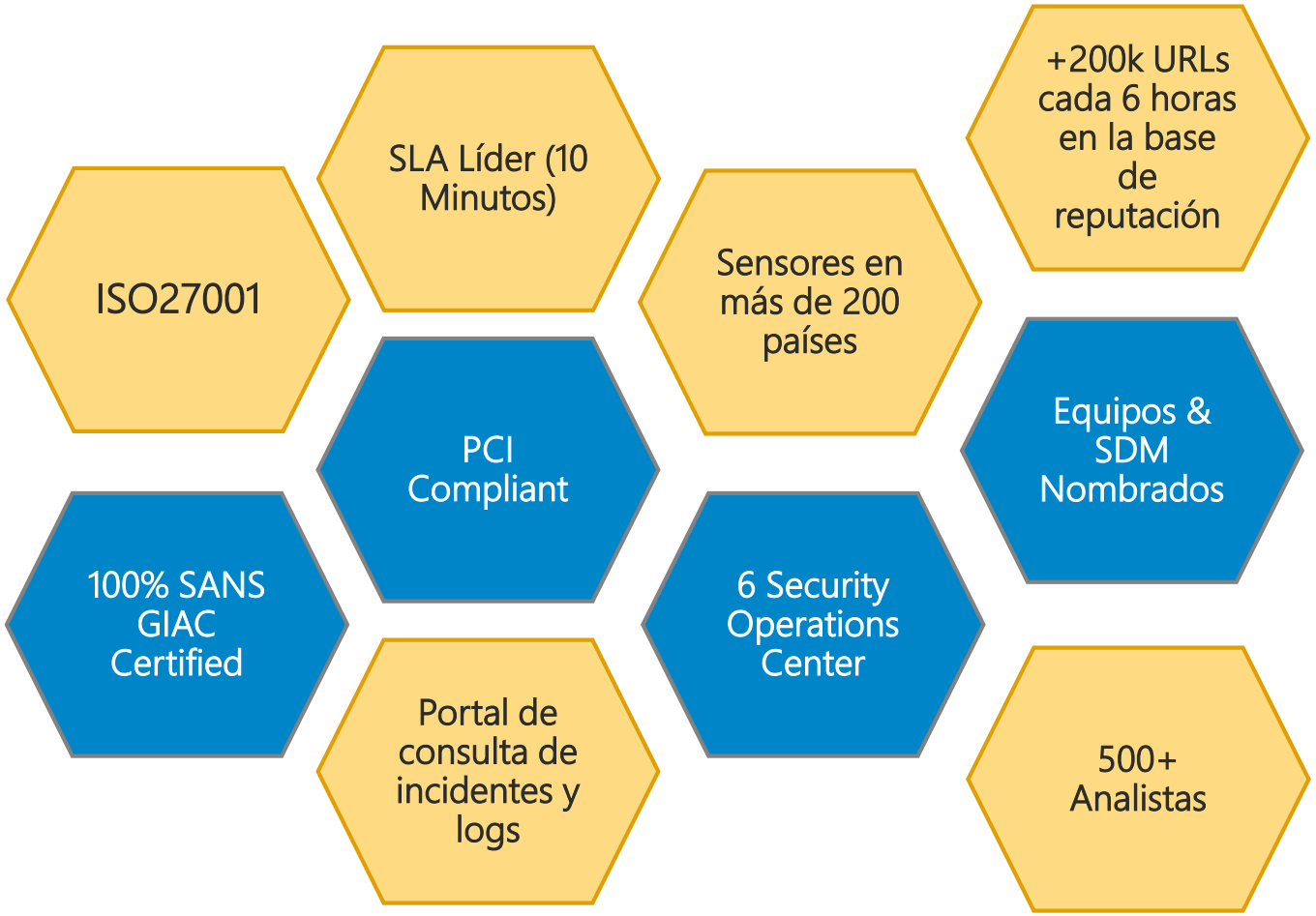
2 trilliones de eventos al mes, 70 millones al día!

Nuestros analistas y sistemas eliminan alrededor del 80% de falsos positivos, lo que resulta en aproximadamente 8,000 incidentes publicados diariamente.

Cada día, alrededor de **200** incidentes críticos se escalan a nuestros clientes dentro de los 10 minutos.

Copyright © 2017 Symantec Corporation

Diferenciadores del Symantec MSS



Copyright © 2017 Symantec Corporation

Security Operations: Where do you stand?

One of the most important things security practitioners want to know is "How secure is my organization?" Finding an answer requires a review of existing plans for **all** stages of an attack—before, during and after. Consider these questions:

- Does our threat intelligence help us make faster, better decisions?
- Does our security operations center diagnose critical threats in real time?
- How quickly and effectively do our teams respond to an incident?
- Do we focus enough resources on our people so that our organization is prepared?

These questions are integral to developing a robust security operation, yet recent IDC research shows that many organizations don't have the right solutions or resources in place to address critical security issues, including:

- Understanding user behavior and new business models (Internet of Things, mobile, social, and cloud).

https://secopsscorecard.com/

Copyright © 2017 Symantec Corporation

Preguntas por el chat

Copyright © 2017 Symantec Corporation

Próximo Webinar BE AWARE – 10/Mayo

"Aumento del umbral de seguridad contra amenazas desconocidas, ransomware y ataques de Día cero"

Copyright © 2017 Symantec Corporation