Proteja su negocio
Security Operations Center

23 de Septiembre, 2020

pwc

SkyOnline
Data & Media Center

Expositores

Diego Taich

Managing Director de Consultoría de Ciberseguridad de PwC Argentina

Horacio Fernandez Delpech

CEO de Skyonline

Viviana Basso

Gerente de Consultoría de Ciberseguridad de PwC Argentina

Introducción

Los riesgos de ciberseguridad evolucionan constantemente.

Según estudios*, se tardan **197 días** en identificar una **brecha de seguridad** y **69 días** en **contenerla***.

La buena noticia es que esto es inferior a 101 días en 2017. La mala noticia es que es todavía mucho tiempo durante el cual un cibercriminal, competidor, Estado nacional agresivo, o incluso un empleado descontento tiene **acceso no autorizado** a sus sistemas comerciales y críticos activos de información.

** IBM: Informe del coste de una brecha de seguridad - 2019*

Los desafíos

Salvaguardar las operaciones y proteger los datos

- Actualmente nos encontramos con una transformación digital forzada por la situación que lleva a las empresas a implementar cambios en sus operaciones, abrir canales nuevos de comercialización, cambiar las formas de acceso a sistemas críticos, y otras cuestiones, todo lo cual obliga a repensar dónde está el perímetro de la organización y si los datos y las operaciones están correctamente protegidas.

Cumplimiento

- Muchas empresas tienen que alcanzar objetivos de cumplimiento con normativas externas o internas, en forma rápida y madura.

Monitorear, detectar, responder

- Incluso teniendo las adecuadas herramientas de protección, se requiere de una capa de monitoreo y detección de eventos que permitan a las organizaciones adelantarse y prepararse para responder adecuadamente a las amenzas que surgen día a día en cualquier momento. Disponer de los recursos suficientes y capacitados dedidos a estas tareas es difícil y costos

Beneficios

- Monitoreo de seguridad de infraestructura y servicios (on premise y en la nube) 24x7x365
- Notificación de eventos relevantes de seguridad, llevando la comunicación durante todo el ciclo de vida del evento e incidente.
- Gestión de vulnerabilidades: visibilidad de los riesgos que las vulnerabilidades nuevas o antiguas representan para su infraestructura de TI y recomendaciones sobre cómo reducir o mitigar esos riesgos
- Detección de ataques: obtenga datos de herramientas de ciberseguridad de última generación, detecte ataques e infracciones e involucre a nuestro equipo para realizar triage de amenazas y definir con precisión los riesgos del ataque
- Informes y recomendaciones: obtenga informes detallados y personalizados con recomendaciones sobre como prevenir los invidentes
- Organizado en 3 niveles de escalamiento,
- Según el diseño establecido, se puede implementar para reportar a la nube los logs o solo alertas.
- El servicio entrega mensualmente informes técnicos y de gestión del servicio

Valor para el negocio

- Visión objetiva de los niveles de riesgo a los que está expuesta la organización.
- Preparación y mejora continua de las tecnologías que operan los servicios informáticos.
- Mitigación del riesgo a sufrir ataques cibernéticos
- Prevención ante los ataques emergentes.
- Disminución del impacto de incidentes de seguridad de TI a través de procesos y procedimientos establecidos para cada escenario.
- Optimización de los recursos propios, delegando en el servicio tareas que demandan mucho tiempo
- Alcance el cumplimiento con normativas y estándares, al adoptar rápidamente las practicas maduras de nuestro SOC

Por qué PwC?

PwC tiene una práctica global de Seguridad, reconocida en el mundo entero

Práctica extendida de servicios de monitoreo de seguridad a nivel global

PwC no es solo un proveedor de SOC, es un partner integral de soluciones de Cyberseguridad. Entre otros servicios, ofrecemos

- Forensics: Análisis Forense de equipos afectados por un incidente grave.
- IT Risk: Evaluación, diseño e implementación de herramientas de medición y seguimiento de riesgos Tecnológicos.
- Security Framework: Evaluación, diseño e implementación de SGSI acorde a estándares ISO 2700X, PCI-DSS, NIST, etc.
- Datacenter services: Servicios de Housing /Hosting, Administración de infraestructura, servicios de cloud
- CiberInteligencia: La misión del servicio es fortalecer al cliente ayudándolo a estar preparado para afrontar y resolver los mayores retos de seguridad en el mundo digital.

SOC: profesionales

Los profesionales que dan respuesta a incidentes son:

- Analistas (especialistas en Triage)
- Forenses,
- Gestión de Crisis, (Threat Hunting)
- Penentration Testers

SOC: procesos

Todos los procesos, tanto para la gestión integral del SOC como los reportes de incidentes de seguridad y de las métricas del servicio, han sido diseñados en cumplimiento de normativas y estándares ISO 27001, PCI-DSS, BCRA, HIPAA, NIST, IRMs, y GDPR.

SOC: procesos

Checklist de tareas claves ▶ Esencial para que el equipo de SOC sepa que debe hacer y cómo hacerlo correctamente.

Clasificación de eventos ▶ Se clasifican según la criticidad predefinida acorde a cada tipo de origen del evento.

Priorización y análisis ▶ Revisar cualquier actividad sospechosa que indique posible ataque.

Remediación y recuperación ▶ Se sugieren las posibles tareas a realizar: System Upgrades, Patching, Reconfig. reglas FWs, recuperación desde un Backup, desconexion del sistema comprometido de la red, etc.

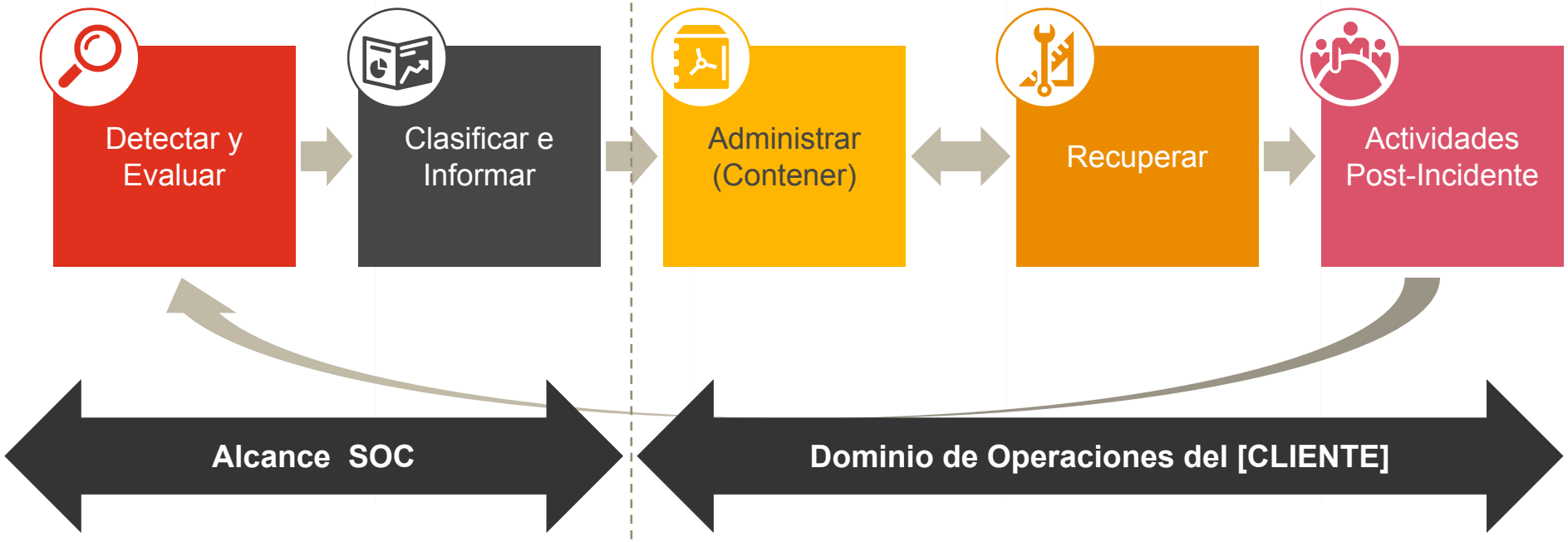
Evaluación y auditoría ▶ Tanto el Análisis de vulnerabilidades como las revisiones periódicas de Audit & Compliance son parte del proceso de mejora continua del SOC.

SOC: escalabilidad

SOC acompaña la evolución de la organización, agregando componentes para monitorear de acuerdo a sus necesidades.

Esta escalabilidad del servicio evita incurrir en grandes inversiones en servicios y herramientas de monitoreo de seguridad, lo que le permite optimizar sus esfuerzos enfocándolos al negocio.

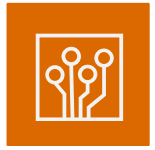
SOC: enfoque



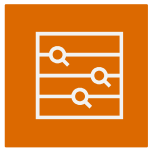
En caso de que la organización necesite, no solo asesoramiento sino también apoyo en la ejecución de la respuesta al Ciberataque, la sinergia PwC & SkyOnline puede proporcionarle servicios específicos para la respuesta a incidentes y la investigación forense, entre otras soluciones del portfolio.

Servicios adicionales...

Servicios de valor agregado que, gracias a esta sinergia, podremos brindarle generando una solución integral.

1.  Análisis Forense, Ciberinteligencia, Test de Penetración, Respuesta a Incidentes.

2.  Modelado de riesgos y amenazas, Evaluación de riesgos tecnológicos.

3.  Privacidad y protección de datos.

4.  Administración de Infraestructura Tecnológica.

5.  Servicios Cloud, Procesos de Backup y Restore, etc.

Sigamos en contacto:

Diego Taich
diego.taich@pwc.com

Horacio
Fernandez Delpech
horacio.fd@skyonline.net

Viviana Basso
viviana.basso@pwc.com