Deloitte.

CyberSOC
Seguridad 24/7

Una nueva realidad

Escenario actual

Las organizaciones se enfrentan hoy en día a un amplio catálogo de amenazas de seguridad que pueden materializarse tanto dentro como fuera del perímetro establecido.

La rápida evolución de estas amenazas complica asimismo la implantación de controles eficaces que, con el paso del tiempo, deberán ser revisados y actualizados para garantizar un nivel de seguridad aceptable.

En este contexto, es necesario combinar de manera inteligente los diferentes elementos que componen la estrategia de seguridad de una organización: operaciones, tecnología, equipos humanos, elementos de gestión del riesgo y procedimientos de trabajo.

Solamente con un enfoque holístico respecto a los elementos anteriores puede una organización mantener las capacidades de seguridad elementales con un rendimiento adecuado, entre ellas: capacidad de respuesta a incidentes, gestión de vulnerabilidades, control y protección de la reputación de la marca o la prevención de casos de fuga de información.

La problemática existente

Muchas organizaciones que realizan significativas inversiones en seguridad manifiestan la ausencia del retorno esperado. Esta circunstancia se produce incluso cuando existe tecnología adecuada y personal con cierto grado de especialización.

Es asimismo frecuente la ausencia de controles adecuados para un amplio abanico de amenazas que hasta el momento no presentaban un nivel de riesgo significativo, o que ni siquiera habían sido consideradas en la estrategia de seguridad.

Por último, elementos tales como la capacidad de operar en 24x7, la disponibilidad de plataformas tecnológicas de seguridad con enfoque colaborativo, las sinergias derivadas del trabajo para múltiples clientes o la capacidad de financiar una infraestructura compleja y creciente quedan fuera del alcance de la mayor parte de la organizaciones, reduciendo la eficacia de sus planteamientos en materia de seguridad TI.

Servicios de seguridad de extremo a extremo

Nuestra propuesta

Los servicios gestionados del CyberSOC se integran dentro de la solución global de Deloitte para ciberseguridad: preparar, conocer y responder; ayudando a consolidar la transformación de la organización desde una postura tradicional reactiva a una situación que permita anticiparse a los ataques y reducir los impactos que puedan causar de manera rápida.

La propuesta de Deloitte se fundamenta en la existencia de un SOC propio, con un enfoque cloud, con equipos de trabajo de alto rendimiento y con una plataforma tecnológica probada e integrada que permite resolver cualquier escenario corporativo en el que las operaciones de seguridad tengan un papel clave.

Deloitte permite a las organizaciones gestionar el riesgo tecnológico y reputacional a través de un portfolio de servicios que responden a necesidades reales, empleando las herramientas más eficaces y unos procedimientos de trabajo orientados al cliente.

Para la puesta en marcha del SOC, Deloitte ha considerado la problemática existente en clientes de los principales sectores del mercado, y ha enfocado su conocimiento en seguridad hacia los requerimientos específicos de un entorno crítico de operaciones.

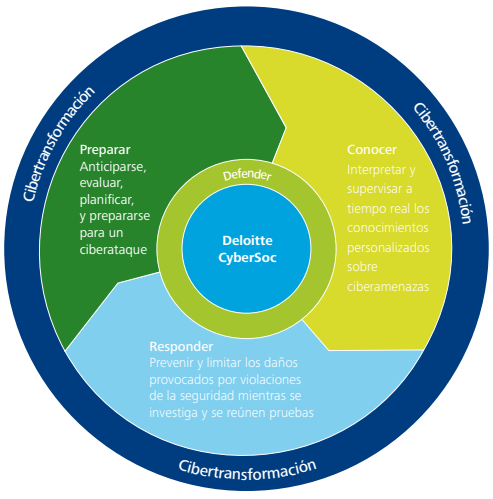
El CyberSOC de Deloitte

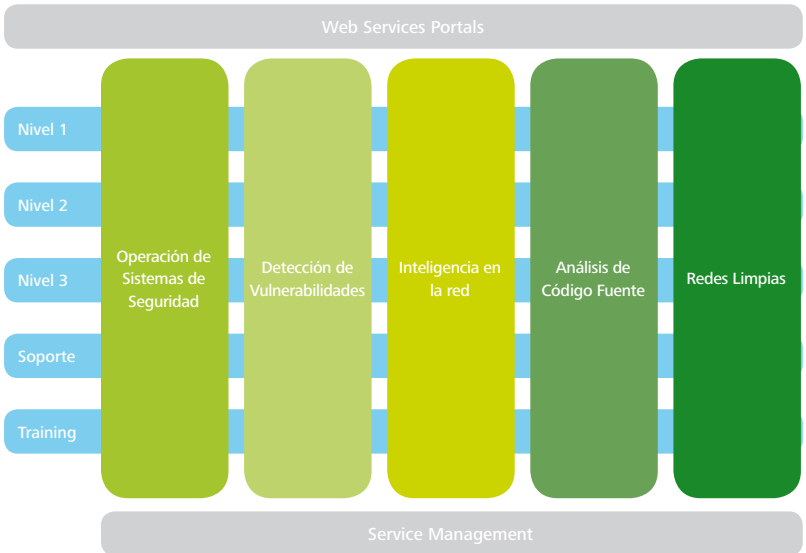
Ubicado en Madrid, en unas instalaciones dedicadas, el CyberSOC está formado por casi 100 profesionales que trabajan en modalidad 24x7 para la prestación de un amplio conjunto de servicios de operaciones de seguridad.

El CyberSOC cuenta asimismo con una plataforma tecnológica que integra la tecnología de los fabricantes más exitosos del mercado, proporcionando un único punto de gestión a través del que los clientes pueden conocer el estado del servicio, obtener métricas e indicadores de su evolución, e interactuar con los equipos responsables de cada actividad.

El CyberSOC constituye el punto de referencia de servicios SOC a nivel internacional en Deloitte. En la actualidad, empresas de todo el mundo están empleando sus capacidades para resolver de manera eficaz sus necesidades en materia de seguridad y disponer de un modelo de operación eficiente, fiable, integral y efectivo.

Por último,esta aproximación global permite asimismo disponer de procedimientos de trabajo con un elevado grado de optimización, lo que desencadena un modelo de costes mucho más eficiente y competitivo.





Una plataforma integrada

Portfolio de servicios

El portfolio de servicios del CyberSOC comprende las principales áreas de actividad en un equipo de operaciones de seguridad, atendiendo a un amplio abanico de necesidades que incluye:

Vulnerability Management

Focalizado en la detección y gestión de vulnerabilidades, en modalidad de vulnerability assessment, penetration testing, hacking gestionado, hacking on demand o hacking pasivo, a través del servicio de alerta temprana.

Managed Security Services

Focalizado en la administración, monitorización y correlación de equipamiento de seguridado, con el objetivo de explotar al máximo las capacidades de la infraestructura y extraer información relevante para la gestión de incidentes o la toma de decisiones.

Brand Services

Focalizados en la identificación, clasificación y procesamiento de información relevante publicada en Internet, incluyendo phishing, malware, amenazas a la marca, reputación de la marca y reputación de directivos.

Static Application Security Testing

Focalizado en la detección de vulnerabilidades en código fuente a través de una sofisticada tecnología que automatiza gran parte del proceso y la orquestación de las tecnologías involucradas en la aplicación revisada.

Clean Pipes

Focalizado en la protección del correo electrónico corporativo y la navegación en Internet de los empleados, a través de una plataforma en la nube que evita la instalaciones de equipamiento on premises.

Enfoque cloud

Todos los servicios del portfolio han sido diseñados para su prestación en modalidad cloud, sin necesidad de despliegue de equipamiento en la organización y con una capa de gestión de servicio que garantiza la interacción eficaz con el cliente y el control de los resultados.

Servicios corporativos 24x7 en la nube

Correlación de seguridad
Una plataforma de correlación en la nube capaz de detectar incidentes de seguridad en procesos de negocio, entornos sujetos a auditoría, despliegues DLP y otros sistemas cuya sofisticación va más allá de los sistemas de seguridad tradicionales.

Static Aplication Security Testing
Una plataforma de revisión de código fuente en la nube con soporte para aplicaciones web, aplicaciones de escritorio, aplicaciones móviles y tecnologías de bases de datos, con un entorno de colaboración que optmiza los procesos de resolución asociados.

Gestión de vulnerabilidades
Un equipo de profesionales en España y Argentina capaces de arrancar un trabajo de hacking en menos de 8 horas, conforme a nuestra capacidad On Demand, y un portal web de gestión desde el que abordar los procesos de resolución reduciendo los costes de documentación de resultados.

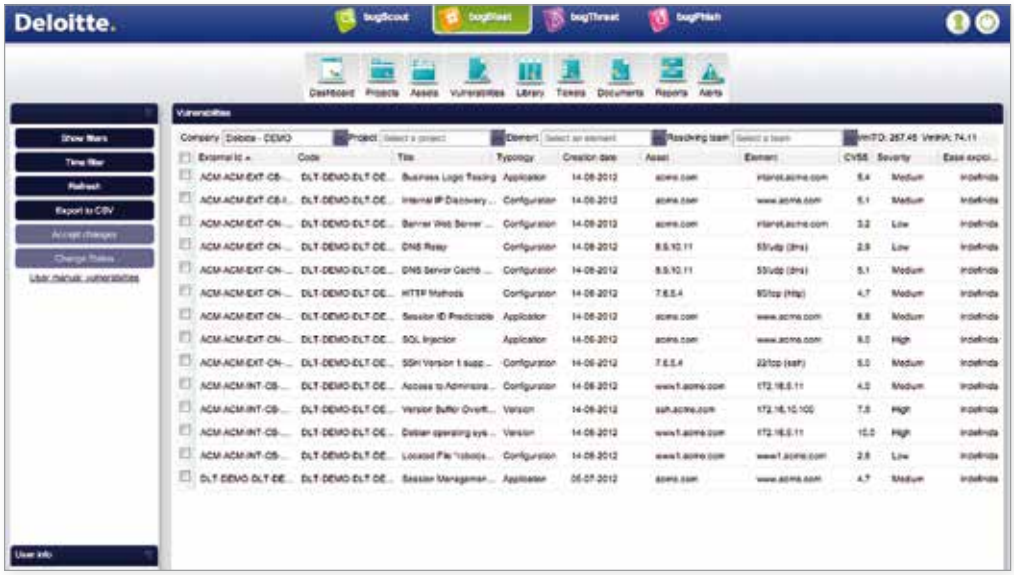
Cyber Watch
Una plataforma de monitorización en Internet y un equipo de analistas capaces de identificar información sensible publicada en foros de cibercrimen, credenciales robadas, menciones difamatorias o casos de fraude vinculadas a las marcas de nuestros clientes.

Brand 3.0
Un servicio de análisis de la presencia en la red que permite a las empresas conocer el sentimiento de sus consumidores respecto a la marca y sus productos, su posición respecto a sus competidores y el grado de posicionamiento de sus sitios web.

Mobile Device Management
Una plataforma en la nube orientada a la gestión eficaz de los dispositivos móviles bajo la filosofía BYOD, con capacidades de prevención de fuga de información e implantación de las políticas de seguridad corporativas.

Protección frente al fraude
Un equipo de especialistas capaces de eliminar sitios web fraudulentos vinculados a una organización en menos de 48 horas, detectar binarios maliciosos que afectan a una marca o analizar el comportamiento de los mismos para determinar el grado de impacto de un incidente de seguridad.

Ingeniería social
Una metodología probada para identificar el grado de madurez de la organización respecto a los ataques de ingeniería social, con indicadores fáciles de interpretar y acciones correctivas que previenen la ocurrencia de los mismos y la concienciación de los empleados de la organización.



Contactos

Alfonso Mur
Socio Riesgos Tecnológicos
amur@deloitte.es
Telf.: +34 91 514 5000

Fernando Picatoste
Socio Riesgos Tecnológicos
fpicatoste@deloitte.es
Telf.: +34 91 514 5000

César Martín
Socio Riesgos Tecnológicos
cmartinlara@deloitte.es
Telf.: +34 91 514 5000

Luis Carro
Socio Riesgos Tecnológicos
lcarro@deloitte.es
Telf.: +34 91 514 5000

Marta García
Socio Riesgos Tecnológicos
martgarcia@deloitte.es
Telf.: +34 91 514 5000

Mercedes Gutiérrez
Socio Riesgos Tecnológicos
megutierrez@deloitte.es
Telf.: +34 91 514 5000

Ricardo Martínez
Socio Riesgos Tecnológicos
rmartinezmartinez@deloitte.es
Telf.: +34 91 514 5000

Fernando Pons
Socio Riesgos Tecnológicos
fepons@deloitte.es
Telf.: +34 93 280 4040

Carmen Sánchez Tenorio
Socio Riesgos Tecnológicos
csancheztenorio@deloitte.es
Telf.: +34 91 514 5000

Si desea información adicional, por favor, visite www.deloitte.es

Diseñado y producido por CIBS, Dpto. Comunicación, Imagen Corporativa y Business Support, Madrid.