PRESENTACIÓN

Estimados clientes:

Es un placer hacerles llegar nuestro catálogo de servicios y agradecerles de antemano el tiempo dedicado a conocernos.

En Jaymon Security nuestro foco es la ciberseguridad. Nuestra empresa nació de la unión de dos profesionales con amplia trayectoria en informática empresarial y ciberseguridad que decidimos ofrecer soluciones diferenciales, basadas en la excelencia técnica y la atención personalizada.

Nuestra propuesta de servicios se sustenta en tres pilares:

Metodología propia orientada a la calidad:
Aplicamos procesos de calidad rigurosos en cada fase del proyecto: desde el análisis inicial hasta la entrega de informes y seguimiento, asegurando resultados fiables, transparentes y adaptados a su negocio.

Equipo senior multidisciplinar:
Contamos con especialistas senior en todas las ramas clave de la ciberseguridad (pentesting, auditorías, hardening, forense digital, etc.) así como en cumplimiento normativo (RGPD, ENS, ISO 27001, etc.) y servicios tradicionales de TI (desarrollo, mantenimiento y consultoría).

Formación y concienciación:
Creemos que la mejor defensa comienza por el usuario. Por eso diseñamos programas de formación a medida y campañas de sensibilización para minimizar riesgos derivados de usos inseguros de sistemas y aplicaciones.

Sin más, les invitamos a explorar nuestro catálogo de servicios. Confiamos en que encontrarán en él la solución más adecuada para sus necesidades presentes y futuras.

Fernando Romero

Director de Operaciones

INTRODUCCIÓN

Para facilitar su revisión, los servicios recogidos en este catálogo se encuentran agrupados en las siguientes categorías:

- **Ciberseguridad:** Auditorías de ciberseguridad, operaciones Red Team (RTO) y servicios de consultoría, soporte ante incidentes y análisis forense digital.

- **Ciberinteligencia:** Servicios de inteligencia sobre fuentes abiertas. Incluye Deep Web, Dark Web y Marianas.

- **Seguridad de la información y cumplimiento normativo (compliance):** Servicios de auditoría interna y consultoría para el cumplimiento de normativas (ENS, RGPD, 27001, etc.).

- **Desarrollo de aplicaciones e infraestructuras cloud**: Servicios de consultoría y desarrollo para la creación de aplicaciones a medida e infraestructuras seguras en la nube.

- **Formación presencial y on-line:** Servicios a medida de concienciación y formación práctica.

- **CISO como servicio:** Cobertura en las labores de Responsable de Seguridad de la Información por parte de un equipo senior multidisciplinar.

- **Consultoría, montaje e integración de herramientas ciber y SOC:** Servicio integral para la instalación, operación y mantenimiento de aplicaciones de ciberseguridad.

Con esta variedad de servicios, pretendemos dar soluciones integrales a cualquier necesidad que puedan tener en el campo de la ciberseguridad.

CIBERSEGURIDAD

En el grupo de servicios relativos a la ciberseguridad, hemos incluido las siguientes categorías de servicios:

- Auditorías de ciberseguridad.
- Operaciones Red Team (RTO).
- Consultoría y soporte ante incidentes.
- Análisis Forense Digital (AFD).

A continuación, se describe y detalla cada una de estas categorías.

AUDITORÍAS DE CIBERSEGURIDAD

Esta categoría comprende todos aquellos trabajos de análisis centrados en identificar vulnerabilidades en sus sistemas y aplicaciones. En función de las actividades que se realizan y de los objetivos que se persiguen, podemos prestar los siguientes tipos de servicio de auditoría que van aumentando gradualmente en complejidad y profundidad:

- **Análisis de vulnerabilidades:** Estos servicios suponen el primer paso en el camino a la excelencia en ciberseguridad de su empresa. Comprenden actividades de escaneo y análisis para la identificación de potenciales vulnerabilidades en sus sistemas y aplicaciones Web o de escritorio, así como en sus infraestructuras en Cloud. Para su realización, se combinan las herramientas comerciales más avanzadas con la experiencia de nuestro personal auditor, dando como resultado, informes completos de vulnerabilidades.

- **Test de intrusión (pentest – caja negra):** Estos servicios, más avanzados que los anteriores, consisten en realizar distintas pruebas de penetración a los sistemas, infraestructura en Cloud o aplicaciones sin ninguna información previa sobre éstas, combinando herramientas manuales y automatizadas. El objetivo es la identificación y explotación real de las vulnerabilidades encontradas, aportando evidencia de estas a su organización y recomendaciones de subsanación.

- **Auditorías de seguridad (caja gris y blanca):** Los servicios de auditoría de seguridad engloban a los servicios anteriores, pero cubriendo una mayor superficie de exposición, ya que para su realización se cuenta con información interna del sistema a auditar (código fuente, manual de funcionamiento, etc.). Esto permite la confección de pruebas mucho más

específicas con las que alcanzar una mayor profundidad en la detección de vulnerabilidades en los análisis estático y dinámico.

- **Servicios de auditoría de redes inalámbricas:** Consisten en ejecutar distintas pruebas de detección y explotación de vulnerabilidades, con el objetivo de proporcionar las medidas adecuadas para securizarlas, evitando de esta manera el acceso no autorizado a la red por parte de cibercriminales que quieran hacer un uso indebido de la misma.

En todos los servicios anteriores, se generan informes detallados que contienen tanto las vulnerabilidades encontradas y su severidad, como las recomendaciones para subsanarlas. Se reportan principalmente aquellas vulnerabilidades explotables, acompañadas de las evidencias de su explotación.

Como complemento a los servicios anteriores, se presenta el siguiente servicio, de gran importancia para cerrar el círculo de la ciberseguridad.

- **Evaluación y mejora del ciclo de vida de desarrollo de aplicaciones:** Servicio orientado a clientes que producen su propio software, permitiendo evaluar, desde el punto de vista de la seguridad, todo el ciclo de vida de los productos y sistemas que desarrollan (análisis, diseño, implementación, integración, pruebas, mantenimiento).

OPERACIONES RED TEAM (RTO)

Servicios que consisten en reproducir la forma de proceder de un grupo cibercriminal que tiene por objetivo atacar a una organización. Este tipo de servicios son de complejidad elevada, tanto para su preparación como para su ejecución, pero constituyen un valor seguro ya que siempre arrojan resultados que ningún otro tipo de pruebas puede alcanzar, pues son reales al 100% y ponen a prueba todos los sistemas de seguridad de su organización, incluido el grado de concienciación y conocimiento de su personal.

En este tipo de operaciones el alcance está previamente pactado con el cliente, estableciéndose los criterios de éxito de la operación y hasta dónde llegará. Los ensayos, además pueden incluir la intrusión física en las instalaciones del cliente, ingeniería social (campañas de phishing dirigido), creación de malware personalizado que conecte con sistemas externos de Mando y Control (C2), evasión de sistemas de seguridad perimetrales y demás sistemas antivirus, etc.

Mediante este tipo de ejercicios se obtiene un diagnóstico claro y realista del estado de seguridad de su organización, adquiriendo información muy concreta y real tanto de las fortalezas como de las debilidades de su infraestructura, personal y procedimientos.

CONSULTORÍA, SOPORTE ANTE INCIDENTES Y ANÁLISIS FORENSE DIGITAL

En este grupo de servicios se incluyen el resto de los servicios relacionados con la ciberseguridad que podemos ofrecerle, de forma que podamos cubrir cualquiera de sus necesidades.

Consultoría

Consultoría general sobre ciberseguridad. Mejores prácticas, procedimientos, ataques más comunes, etc. Así mismo, podemos identificar, evaluar y proponer productos comerciales de acuerdo con sus necesidades que encajen en la actual infraestructura empresarial y se ajusten al presupuesto del cliente.

Soporte ante incidentes

En caso de necesitarlo, podemos asesorarle sobre las mejores formas de responder ante incidentes de seguridad concretos. Se incluye también un servicio de consultoría para la gestión de incidentes en relación al Reglamento General de Protección de Datos y la Agencia Española de Protección de Datos. Nuestros consultores les ayudarán a la gestión del incidente, su soporte documental y al reporte del mismo a la AEPD en caso de que se considere que, por su gravedad, el incidente debe reportarse.

Análisis Forense Digital (AFD)

Este servicio de análisis cubre la identificación del origen de un problema, el alcance de este y propone medidas de mitigación para que el incidente no se produzca de nuevo. Entre los tipos de análisis forense digital que se pueden realizar tenemos los siguientes:

- **De sistemas:** En este tipo se realiza el análisis de discos duros físicos, imágenes virtualizadas, memoria RAM, sistemas en ejecución, equipos, etc.

- **De Smartphone**: En este tipo se realiza el análisis de evidencias recogidas en dispositivos móviles.

- **De archivos:** En este tipo se lleva a cabo principalmente el análisis de documentos ofimáticos (Word, PowerPoint, etc.).

- **De malware:** En este tipo se lleva a cabo principalmente el análisis de binarios y scripts que supongan una amenaza a la seguridad informática (troyanos, ransomware, etc.).

- **De correos electrónicos:** En este tipo se realiza el análisis de distintos tipos de e-mails (phishing).

- **De tráfico de red:** En este tipo se realiza el análisis de tráfico de red entrante y saliente, en busca de posibles ciberataques (descarga de malware, phishing, exfiltración de información sensible, etc.).

La metodología que se utiliza en este tipo de servicios cuenta con todas las garantías para que el informe o informes generados puedan utilizarse como pruebas periciales en caso de juicio, respetando los protocolos para la extracción dela información, cadena de custodia, etc.

DOSSIERS DE CLIENTES (OSINT)

Este servicio consiste en la obtención de conocimiento útil mediante la recolección, filtrado y análisis de toda aquella información que pueda encontrarse en Internet de forma pública sobre una persona física o jurídica.

Supone una labor profunda de investigación sobre la información ofrecida en "fuentes abiertas", que son todos aquellos orígenes de información disponibles abiertamente en Internet, así como en la "Deep Web", la "Dark Web" y las "Marianas".

El resultado habitual de este tipo de servicios de investigación se recoge en un informe que contendrá toda aquella información relevante para el cliente.

¿Qué le aporta al cliente esta información?

- Permite al cliente ser consciente de su grado de exposición en Internet, y poder reducir dicha exposición en base a sus intereses.

- Así mismo, permite conocer de primera mano si, en los principales foros de cibercrimen existe información de filtraciones, resultados de ataques, etc. que no eran conocidos.

¿Por qué es relevante esta información?

- Porque puede ser utilizada para ataques posteriores por parte de cibercriminales. Conocer de primera mano qué información hay sobre una persona en esos foros, ayudará a prevenir posibles ataques y permitirá el modelado de amenazas.

- Porque puede alertarnos sobre ataques que hayamos sufrido y de los que no éramos todavía conscientes.

CUMPLIMIENTO NORMATIVO

Dentro de este grupo de servicios se incluyen todos aquellos servicios de consultoría orientados a determinar internamente el grado de cumplimiento de diferentes normativas. Se incluye también la elaboración de informes de auditoría y la recomendación de medidas de subsanación para garantizar el cumplimiento de la norma auditada.

Este tipo de servicio es de gran utilidad en caso de que se busque realizar una auditoría de cumplimiento oficial o certificación, ya que en algunos casos, la auditoría interna previa es un elemento obligatorio y en todos los casos permite afrontar el proceso con un nivel de confianza elevado sabiendo que se cumple con lo requerido.

A continuación, se detallan las normativas que actualmente estamos auditando:

- **Evaluación e implantación RGPD**: Servicio de auditoría interna y evaluación del grado de cumplimiento actual del RGPD de la organización. Auditoría de los tratamientos, finalidades de los datos, etc. Identificación de los puntos a cumplir para la implantación del RGPD y propuestas.

- **Evaluación e implantación ISO 27001:** Servicio de auditoría interna y evaluación del grado de cumplimiento de la norma ISO27001. Identificación de los puntos a cumplir para su implantación y propuestas.

- **Evaluación e implantación del ENS:** Servicio de auditoría interna y evaluación del grado de cumplimiento del Esquema Nacional de Seguridad por su organización. Identificación de los puntos a cumplir para la implantación del ENS y propuestas.

FORMACIÓN PRESENCIAL Y ON LINE

A continuación, se enumeran los tipos de formación que actualmente impartimos. Así mismo, estamos a su disposición para organizar sesiones de formación sobre estos u otros temas de acuerdo con sus necesidades específicas.

Para la realización de los cursos y concienciaciones contamos con laboratorios y herramientas para permitir que los alumnos pongan en práctica lo aprendido:

- **Formación en desarrollo seguro:** Formación a desarrolladores para que tengan la ciberseguridad presente a lo largo de todo el ciclo de vida de sus desarrollos. Esta formación incluye prácticas.

- **Formación en ciberseguridad - hacking ético:** Formación a profesionales para que puedan iniciarse y profundizar en el campo de la ciberseguridad a través de uno de los aspectos más interesantes de la misma, como es el hacking ético. Esta formación se complementa perfectamente con la formación anterior y también incluye prácticas.

- **Concienciación de seguridad:** Formación para el personal de la organización con la finalidad de concienciar sobre la criticidad de la ciberseguridad en todos los ámbitos. La formación cubre tanto la actividad del empleado dentro de la empresa como fuera de la misma. Esta formación incluye talleres prácticos y actividades colaborativas.

- **Concienciación en protección de datos:** Formación básica sobre LOPD y RGPD. Dicha formación consta de dos áreas diferenciadas: la parte legal que cubre el estudio de la ley y el reglamento, y la parte operativa que cubre el proceso de implantación.

- **Campañas de Phishing:** Acompañando a las acciones de concienciación y formación, se realizan campañas de correo malicioso dirigidas a:
    - Evaluar el estado de alerta y conocimiento de los trabajadores de una organización.
    - Comprobar el grado de penetración de las formaciones previas realizadas.

DESARROLLO DE APLICACIONES E INFRAESTRUCTURAS CLOUD

Este grupo de servicios incluye proyectos de desarrollo software “puro” y proyectos de infraestructura segura en la nube (principalmente la nube de Microsoft AZURE) así como la combinación de ambos.

La ventaja que ofrecen nuestros proyectos sobre la competencia es que la seguridad está contemplada desde el inicio, asegurando que, desde las etapas iniciales hasta el fin del proyecto, se tendrán en cuenta las buenas prácticas y metodologías que aseguren un producto robusto y seguro. Nuestras aplicaciones son auditadas internamente en cada una de las iteraciones del proceso de desarrollo, de forma que, si hubiera que hacer algún tipo de corrección relativa a la seguridad, ésta se haga lo antes posible, ahorrando tiempo y dinero.

Para terminar de asegurar los sistemas, se cuenta con la opción de desplegar las aplicaciones desarrolladas en la nube de Microsoft sobre infraestructuras diseñadas e implementadas por nosotros, una vez más teniendo la seguridad como uno de los objetivos principales. Las infraestructuras diseñadas e implementadas en Azure hacen uso de los componentes disponibles en el ecosistema de Azure (WAF, protección de DDoS, custodia de claves segura, etc.).

CISO COMO SERVICIO

El perfil de **Responsable de Seguridad de la Información (CISO)** es un perfil altamente especializado y muy demandado, por lo que la inversión necesaria en tiempo y dinero para incorporar un CISO fiable a la plantilla, excede en muchas ocasiones los plazos y el presupuesto disponible para ello. El perfil de CISO reúne conocimiento y experiencia en áreas tales como: ciberseguridad, seguridad de la información, cumplimiento normativo, ingeniería del software, etc. Como ya hemos mencionado, esto dificulta enormemente encontrar esos perfiles.

Desde nuestra empresa, hemos diseñado el servicio de "CISO como servicio" para dar cobertura a esta necesidad de forma rápida y mucho más económica que buscar y contratar el perfil por la vía tradicional.

Para la prestación del servicio se dedicará a un profesional que ejercerá las labores de CISO presenciales y de interlocutor con la organización. Tras ese perfil, estará nuestra **"Oficina del CISO"**, formada por un equipo de profesionales senior expertos en diferentes áreas. Sumamos en un solo servicio la experiencia acumulada de todos ellos.

Este servicio también se puede prestar dando apoyo a CISOS que acaben de incorporarse a la organización o que lleven poco tiempo en el rol. Desde la Oficina del CISO se dará soporte al CISO en todos aquellos temas que puedan surgirle, tanto en la estrategia general como para temas concretos.

JAYMON SECURITY
Cyberintelligence & Solutions

CONSULTORÍA, MONTAJE E INTEGRACIÓN DE HERRAMIENTAS CIBER Y SOC

Desde Jaymon Security, queremos ser sus colaboradores de referencia en el campo de la ciberseguridad y para ello, hemos desarrollado este servicio de consultoría, montaje e integración de herramientas de ciberseguridad para SOC.

Este servicio integral incluye todos los pasos necesarios desde que se identifica la necesidad hasta que se disfruta del servicio final. De esta forma, simplificamos el trabajo de incluir y explotar nuevos elementos en la seguridad de su organización.

Con este servicio podemos darles cobertura completa o, si lo desean, parcial, asesorando o interviniendo en cualquiera de los pasos del proceso.

Prestamos especial atención a pequeñas y medianas empresas en vías de cumplimiento y obtención de diferentes certificaciones como el Esquema Nacional de Seguridad. Aportamos soluciones de rápida integración y de coste inmejorable para facilitarles el cumplimiento de forma consistente en un tiempo récord.

PARA TERMINAR

Esperamos que los servicios presentados se ajusten a sus necesidades y en breve, podamos trabajar juntos.

Si hay algún otro servicio que necesite pero que no vea reflejado en esta presentación, le rogamos que nos consulte en info@jaymonsecurity.com , estaremos encantados de poder ayudarle.