pyxis

Cloud Security Services

PROPUESTA DE SERVICIO

Pyxis Cloud Security Services

Relevamos, diseñamos y acompañamos a sus equipos de TI y Compliance para optimizar la seguridad de su nube. Actualmente, en ambientes de Cloud, los proveedores cumplen con varios estándares de seguridad que aplican a sus centros de datos, dejando la responsabilidad a sus clientes en mayor o menor medida sobre las configuraciones finales de seguridad y la protección de los datos. Es necesario tener estrategias y herramientas para minimizar la vulnerabilidad de su información en la nube. Asegure sus servicios de Cloud y despliegue soluciones de forma confiable y sencilla.

A continuación se describen los servicios que componen la suite Cloud Security Services:

Cloud Security Approach (CSA) - 2 months Assessment

Este servicio propone una mirada crítica sobre la infraestructura y servicios desplegados en Cloud, así como también una visión con las premisas de Security by Default y Zero Trust para nuevas soluciones. A través del CSA se identifican y ponderan las oportunidades de mejora relacionadas con la infraestructura del cliente, recomendando un diseño que cumpla con buenas prácticas y estándares de seguridad actualizados.

Cloud Security Posture (CSP) - 2 months Assessment (Powered by Guayoyo)

El servicio se enfoca en identificar vulnerabilidades a través de configuraciones incorrectas de la infraestructura Cloud sin importar si su nube es pública o privada. Mediante el CSP se mide el nivel de cumplimiento con respecto a CIS Benchmarks, advierte a los equipos sobre los problemas y recomienda una solución.

Cloud Security Deployment (CSD) - 4 months Implementation

El resultado del CSA sobre el estado de seguridad de la infraestructura y las posibles amenazas que puedan comprometerla, será la entrada para implementar soluciones de ciberseguridad en distintos puntos y con diferentes enfoques (ofensivos o defensivos), que permitan al cliente mitigar los riesgos para su organización.

Cloud Security Compliance (CSC) - 4 months Implementation

Hoy en día el entorno corporativo requiere en muchas ocasiones cumplir con distintos estándares para dar cumplimiento normativo sobre el negocio que desarrollan, por ejemplo: PCI-DSS, HIPAA, SOX. Estos requerimientos están enfocados en la protección de los activos de información, por lo que es necesario sumar un análisis especifico adicional a las buenas prácticas de seguridad en Cloud. CSC permite confirmar el cumplimiento de la norma o estándar de forma explícita a través de ejecución de pruebas sobre las soluciones a certificar.

Cloud Security Score Improvement (CSSI) - 6 months Implementation

Servicio estratégico de mantenimiento evolutivo sobre las soluciones de Cloud. Permite incorporar nuevos servicios y tecnologías bajo un proceso controlado y estable que mejora las características de seguridad. De esta manera se logra mejorar el Score del entorno Cloud y mantenerlo en el tiempo, con un acompañamiento de expertos en seguridad.

Cloud Security Services

Más Información:
www.pyxis.tech/cloud-security

Pyxis Cloud Security Approach

En la actualidad importante y cada vez más necesario seguir e implementar las buenas prácticas de Seguridad en Tecnología Informática. En particular para ambientes de Cloud, los proveedores cumplen con varios estándares de seguridad que aplican a sus centros de datos, aunque dejan la responsabilidad a sus clientes en mayor o menor medida sobre las configuraciones finales de seguridad.

Por otra parte es frecuente en la práctica que el abordaje de Cloud de muchas empresas sigue los lineamientos del negocio, sin tener en cuenta la Seguridad desde etapas tempranas de definición de la Arquitectura e Infraestructura.

Como consecuencia mas inmediata, un porcentaje muy alto de los incidentes de seguridad suceden debido a configuraciones de servicios precarias o con sus valores por defecto.

Cloud Security Approach propone una mirada obligatoria sobre la infraestructura y servicios desplegados en Cloud, así como también una visión con las premisas de Security by Default y Zero Trust para nuevas soluciones. A través del CSA se identifican y ponderan las oportunidades de mejora relacionadas con la infraestructura del cliente, recomendando un diseño que cumpla con buenas prácticas y estándares de seguridad actualizados.

A continuación se describen las fases que componen el CSA:

1.- Relevamiento de Situación Actual

Punto de partida para conocer la realidad del cliente, entender las necesidades y desafíos que actualmente tiene la infraestructura del cliente, así como los nuevos requerimientos y opciones de mejora que espera obtener. De esta manera se trabaja en conjunto en definiciones sobre las nuevas soluciones de Cloud que mejor se adapten al negocio. .

2.- Diseño de Infraestructura Segura

El desarrollo de infraestructuras de Cloud trae aparejado un conjunto de prácticas y formas de trabajo que no son totalmente comparables o equivalentes a los escenarios on-premise. Por lo cual es necesario entender como la realidad actual del cliente se adapta a un ambiente de Cloud. Se considerarán nuevas formas de acceso, la gestión de identidades y demás aspectos que hacen al diseño de la seguridad de la información en Cloud.

Esta es la principal fase del CSA, donde se define el diseño que mejor se ajusta a las necesidades del cliente teniendo en cuenta y priorizando la Seguridad según las mejores prácticas y experiencias en el área.

3.- Recomendaciones de Mejora

Luego de lograr un diseño acorde al cliente, se presentarán las recomendaciones de mejora haciendo hincapié en los beneficios que se obtendrán con la nueva infraestructura, las consideraciones que deberán tener y demás cambios que puedan implicar la nueva configuración.

4.- Acompañamiento en la Estrategia de Implementación

Confiamos en que esta fase generará el valor agregado mas importante para el cliente, donde se seguirán los lineamientos sugeridos en las fases anteriores, se logrará una nueva solución estable, confiable con las garantías de seguridad que se hayan acordado.

Acompañamos al cliente en estos primeros pasos, asesorándolo y despejando dudas que surjan ya en etapa de implementación.

Cloud Security
Approach

Más Información:
www.pyxis.tech/cloud-security

Cloud Security
Posture

pyxis

Pyxis Cloud Security Posture

Detecte y solucione infracciones de seguridad en su infraestructura de nube.

La postura de seguridad de una solución cloud se refiere al estado y medidas para protegerla de ciberamenazas. Si bien los entornos cloud se han consolidado como soluciones versátiles, son difíciles de proteger debido a su amplia superficie de ataque y gama de amenazas.

Las vulnerabilidades de configuración en ambientes cloud es uno de los errores más comunes que conducen a problemas de incumplimiento y violación de datos.

Cloud Security Posture (CSP) se enfoca en identificar vulnerabilidades a través de configuraciones incorrectas de la infraestructura cloud sin importar si su nube es pública o privada, mide el nivel de cumplimiento con respecto a CIS Benchmarks, advierte a los equipos sobre los problemas y recomienda una solución.

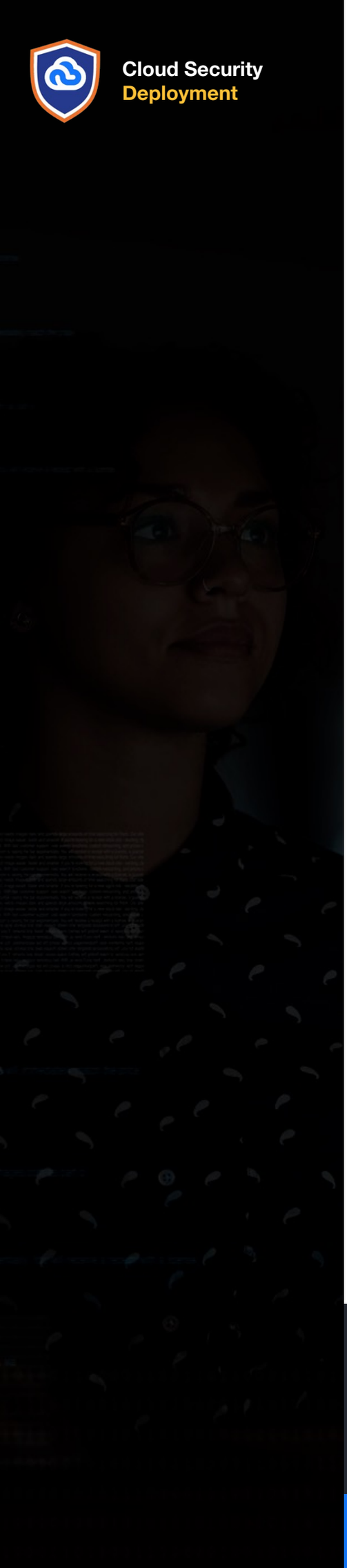
Esto se logra examinando y comparando el entorno cloud contra un set definido de pruebas de seguridad, buenas prácticas y riesgos conocidos que permitan identificar problemas de seguridad para su posterior remediación.

CSP puede ser adquirido como parte de CSS o de forma independiente para que sirva como puntapié inicial de una revisión técnica y mejora de la seguridad de su solución cloud.

Beneficios:

- Proporciona visibilidad de seguridad
- Ayuda al cumplimiento normativo y de buenas prácticas
- Previene la exposición al riesgo
- Impulsa la respuesta de remediación

Más Información:
www.pyxis.tech/cloud-security



Cloud Security
Deployment

Pyxis Cloud Security Deployment

Cloud Security Deployment (CSD) es la propuesta de valor mas conveniente para el onboarding en Cloud. CSD es el camino a seguir para implementar las arquitecturas de seguridad y de cargas de trabajo que se desprenden del relevamiento y análisis incluido.

Consideramos en esta iniciativa las siguientes fases de trabajo:

1.- Relevamiento
Se incluye como fase inicial el Cloud Security Approach. Este propone una mirada obligatoria sobre la infraestructura y servicios desplegados en Cloud, así como también una visión con las premisas de *Security by Default y Zero Trust* para nuevas soluciones. A través del CSA se identifican y ponderan las oportunidades de mejora relacionadas con la infraestructura del cliente, recomendando un diseño que cumpla con buenas prácticas y estándares de seguridad actualizados.

2.- Diseño
El resultado del CSA sobre el estado de seguridad de la infraestructura y las posibles amenazas que puedan comprometerla, será la entrada para implementar soluciones de ciberseguridad en distintos puntos y con diferentes enfoques (ofensivos o defensivos), que permitan al cliente mitigar los riesgos para su organización. En esta etapa se validan las arquitecturas propuestas y se genera el diseño de implementación, considerando las particularidades de cada ambiente teniendo en cuenta modalidades de migración, presupuesto, trabajo colaborativo, metodologías entre otras.

3.- Implementación
Una vez definido el diseño en esta instancia se realiza la implementación de las soluciones en Cloud. Esta fase consiste en la instanciación y creación de servicios de Cloud para conformar la infraestructura de seguridad propuesta.

4.- Validación
Luego de implementada la infraestructura definida, se ejecuta una instancia de validación de configuraciones, servicios, accesos, procesos y flujos de comunicación, asegurando la confiabilidad y eficacia de la solución final.

Más Información:
www.pyxis.tech/cloud-security

Cloud Security
Compliance

pyxis

Pyxis Cloud Security Compliance

Hoy en día el entorno corporativo requiere en muchas ocasiones cumplir con distintos estándares para dar cumplimiento normativo sobre el negocio que desarrollan, por ejemplo: PCI-DSS, HIPAA, SOX. Estos requerimientos están enfocados en la protección de los activos de información, por lo que es necesario sumar un análisis especifico adicional a las buenas prácticas de seguridad en Cloud.

El servicio Compliance (CSC) incluye los servicios de Approach (CSA) e implementación (CSD) y los complementa desde el inicio considerando el cumplimiento del estándar que el cliente requiera.

CSC permite confirmar el cumplimiento de la norma o estándar de forma explícita a través de ejecución de pruebas sobre las soluciones a certificar.

- Cloud Security Approach
- Cloud Security Deployment

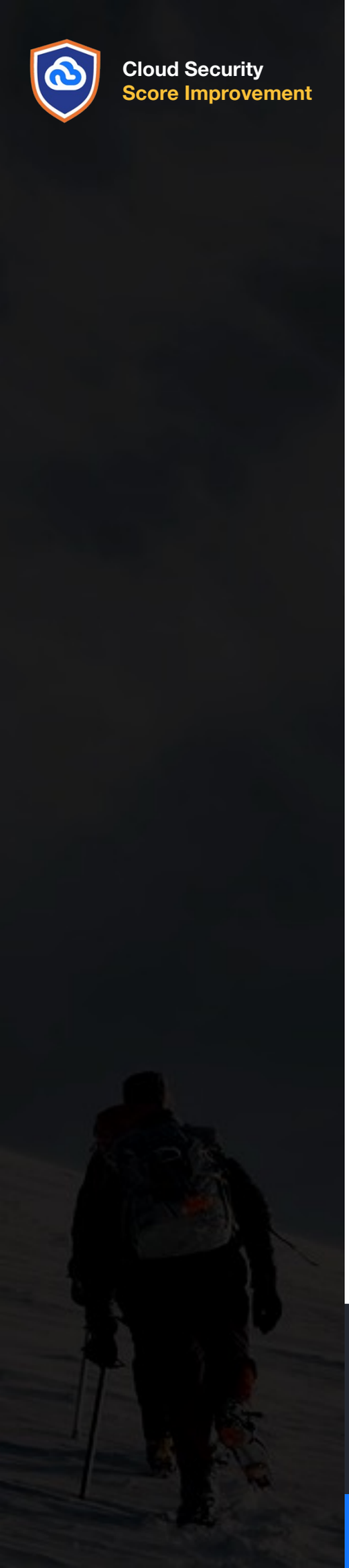
A continuación se describen las fases que componen el servicios de Compliance:

Alcance y Estándar
Lo primero que se debe establecer es el marco regulatorio exigido (estándar a cumplir) y el alcance que tendrá en la nueva infraestructura Cloud del cliente. El cumplimiento se aplica generalmente a los activos de información en relación al estándar que se sigue, por tanto en esta fase se debe acordar con el cliente el alcance de cumplimiento de las soluciones a desplegar en la nueva infraestructura.

Cumplimiento
La última fase de este servicio es la confirmación de cumplimiento del estándar de forma empírica, ya en la infraestructura implantada y con las soluciones operativas. Para esto se ejecutarán actividades de chequeo configuraciones, accesos y procedimientos importantes para los procesos de auditoría.

Más Información:
www.pyxis.tech/cloud-security

Cloud Security
Score Improvement



Pyxis Cloud Security Score Improvement

Uno de los principales desafíos que enfrentan los clientes en infraestructuras de Cloud es la gobernanza.
Los proveedores de Cloud actualizan y lanzan nuevos productos de forma constante. A su vez las organizaciones aprovechan las virtudes de estos entornos para lograr mas dinámica y agilidad en la adquisición y despliegue de nuevas soluciones tecnológicas para dar soporte al negocio.

Esto lleva a una realidad de cambio permanente, y en este escenario tener control de los activos y su estado es una tarea por demás compleja.

Para atacar esta problemática existen distintos frameworks donde se definen sus Score y Posture como forma de evaluar cada entorno Cloud, identificando niveles de madurez en que se encuentran las organizaciones.

Cloud Security Score Improvement es un servicio estratégico de mantenimiento evolutivo sobre las soluciones de Cloud. Permite incorporar nuevos servicios y tecnologías bajo un proceso controlado y estable que mejora (improve)las características de seguridad.
De esta manera se logra mejorar el Score del entorno Cloud y mantenerlo en el tiempo, con un acompañamiento de expertos en seguridad.

Ofrecemos el CSSI cómo parte del CSS, para dar una visión holística y completa sobre la infraestructura de Cloud de la organización posterior al relevamiento (CSA) e implementación (CSD).

El CSSI se puede adquirir de forma independiente ofreciendo una asesoría basada en las buenas prácticas en la materia a la hora de mejorar el Score de la empresa en sus servicios de Cloud.

Más Información:
www.pyxis.tech/cloud-security