

Continuous Security Assessment

El servicio automatiza de forma periódica la revisión de vulnerabilidades en la organización, a través de la revisión mensual de las vulnerabilidades en la infraestructura objetivo.

El servicio se ejecuta desde una visión ejecutiva, con el objetivo de brindar indicadores eficientes para la toma de decisiones, como así también información concreta para la remediación de las mismas.

El servicio, que se ejecuta de forma externa, permite a los equipos de tecnología mantener actualizados los sistemas y detectar rápidamente vulnerabilidades en las aplicaciones o que hayan surgido a raíz de cambios en las configuraciones.

Objetivos principales

- ✓ Localizar debilidades y vulnerabilidades en una etapa temprana (antes que un atacante).
- ✓ Descubrir vulnerabilidades a partir de cambios en las configuraciones de la infraestructura.
- ✓ Dar seguimiento a la aplicación de parches y corrección de vulnerabilidades en la organización.

¿Por qué realizar un Continuous Security Assessment?

- ✓ Para asegurar la revisión continua del estado de las vulnerabilidades.
- ✓ Para contar con indicadores de gestión en la materia.
- ✓ Para constituir un ciclo de revisión y mejora para la seguridad.

Reportes

El servicio entrega mensualmente dos reportes. El primero de estos, lista todas las vulnerabilidades identificadas en la infraestructura y su criticidad individual, como así también un tablero resumen que compara el estado de los hallazgos respecto al mes anterior. Dicho tablero, se genera además como reporte ejecutivo de una página, de forma tal que los equipos de seguridad puedan brindar la información sin los detalles técnicos ni listado de vulnerabilidades a los actores más ejecutivos de la organización, de forma tal de dar un seguimiento y gestión al trabajo realizado.

