

# SECURESOFT CORPORATION

**e-Secure Consulting Group**

**REPORTE MENSUAL - SALUD**

### Preparado para:



**Fecha de elaboración:**

**${fecha\_actual}**

**El presente documento contiene información estrictamente privada y confidencial entre SECURESOFT CORPORATION**

**S.A.C. y HERMES S.A.C**

### OBJETIVO

Este documento dará a conocer el estado de las plataformas de seguridad durante el último mes.

### ALCANCES

Este documento servirá como herramienta para verificar el estado de las plataformas de seguridad y su correcto funcionamiento.

### ESTADO DE LAS PLATAFORMAS

* 1. **SOC.Salud.Recursos (PaloAlto)**
* **Firewall PaloAlto 1**
  + - **Certificados**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Se observa que el status de los certificados se encuentra vigentes.

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Tabla

Descripción generada automáticamente con confianza media

**Recursos**

${graph1554}

▪ Se observa un consumo promedio de CPU de ***15%*** durante el mes.

▪ Se visualiza un consumo de disco de ***72%*** durante el mes.

▪ Se visualiza un consumo de memoria de ***69%*** durante el mes.

* **Firewall PaloAlto 2**
  + - **Certificados**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Se observa que el status de los certificados se encuentra vigentes.

Imagen que contiene Escala de tiempo

Descripción generada automáticamente

Tabla

Descripción generada automáticamente con confianza baja

**Recursos**

${graph1556}

▪ Se observa un consumo promedio de CPU de ***0.84%*** durante el mes.

▪ Se visualiza un consumo de disco de ***44%*** durante el mes.

▪ Se visualiza un consumo de memoria de ***57.65%*** durante el mes.

* 1. **SOC.Seguridad.PaloAlto**
     + **Eventos de Seguridad**

Gráfico

Descripción generada automáticamente

➢ **SIPVicious Scanner Detection** fue el evento más detectado.

* + - **Aplicaciones Detectadas**

Gráfico, Gráfico de barras

Descripción generada automáticamente

* **SSL** fue la aplicación más usada.

- **Categoría de amenazas**

Gráfico, Gráfico de barras

Descripción generada automáticamente

- **Top 10 de los usuarios que realizan tráfico malicioso**

Gráfico

Descripción generada automáticamente con confianza media

1. **CONCLUSIONES**

* Los equipos se encuentran estables.
* Las conexiones concurrentes durante el mes fueron estables.
* Se observa que el status de los certificados se encuentra vigentes.
* Se observaron eventos de seguridad el día 01/02/2021, se viene revisando bajo INC 287232. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Se observaron eventos de seguridad el día 02/02/2021, se viene revisando bajo INC 290377. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Se observaron eventos de seguridad el día 07/02/2021, se viene revisando bajo INC 289873. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Se observaron eventos de seguridad el día 09/02/2021, se viene revisando bajo INC 280025. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Se observaron eventos de seguridad el día 11/02/2021, se viene revisando bajo INC 287251. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Se observaron eventos de seguridad el día 12/02/2021, se viene revisando bajo INC 286432. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Se observaron eventos de seguridad el día 16/02/2021, se viene revisando bajo INC 293056. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Se observaron eventos de seguridad el día 28/02/2021, se viene revisando bajo INC 302472. Se observa que la firma activada en el firewall tuvo la acción de Alert, el cual se derivó al área de ingeniería para su revisión.
* Durante el mes se observaron otros eventos de seguridad con firmas activadas en el firewall que tuvo la acción de **bloquear**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| a00 | ${autor} | Supervisor CyberSOC | 11/03/2022 | Versión Inicial |