**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE DIARIO**

**STEALTHWATCH**

**Preparado para:**

****

**Fecha de elaboración:**

**${fecha\_actual}**



**El presente documento contiene información estrictamente privada y confidencial para Securesoft Corporation S.A.C. y DPWORLD.**

**INICIO**

[**I. OBJETIVO 3**](#_Toc91269534)

[**II. ALCANCES 3**](#_Toc91269535)

[**III. ESTADO DE LAS PLATAFORMAS 3**](#_Toc91269536)

[**1. PLATAFORMA CISCO 3**](#_Toc91269537)

[**1.1. CONSOLA DE ADMINISTRACIÓN – STEALTHWATCH 3**](#_Toc91269538)

[**1.2. SENSOR DE TRÁFICO Y CONVERSIÓN A NETFLOW FLOW SENSOR 6**](#_Toc91269539)

[**1.3. RECOLECIÓN DE FLUJOS FLOW COLLECTOR 6**](#_Toc91269540)

[**1.4. IPS 7050 7**](#_Toc91269541)

[**1.5. FIREPOWER MANAGEMENT CENTER 8**](#_Toc91269542)

[**2. PLATAFORMA F5 10**](#_Toc91269543)

[**2.1. DPWGTM01.DPWC.LOCAL – ACTIVO 10**](#_Toc91269544)

[**2.2. DPWGTM02.DPWC.LOCAL – PASIVO 11**](#_Toc91269545)

[**2.3. DPWLTM01.DPWC.LOCAL – ACTIVO 13**](#_Toc91269546)

[**2.4. DPWLTM02.DPWC.LOCAL - PASIVO 14**](#_Toc91269547)

[**IV. CONCLUSIONES 16**](#_Toc91269548)

# OBJETIVO

Este documento dará a conocer el estado de salud y seguridad de las plataformas durante el presente día.

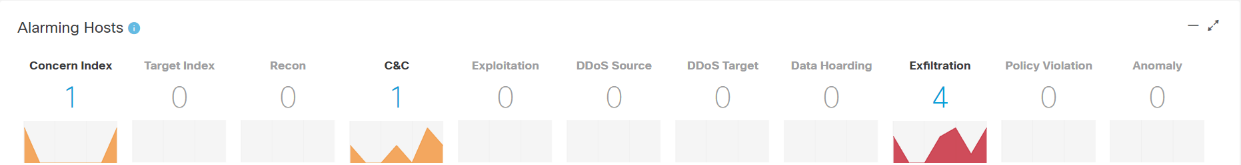
# ALCANCES

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

# ESTADO DE LAS PLATAFORMAS

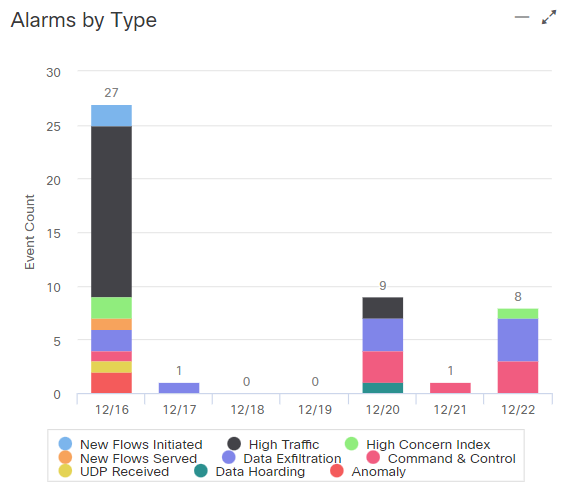
1. **PLATAFORMA CISCO**
   1. **CONSOLA DE ADMINISTRACIÓN – STEALTHWATCH**

* **EVENTOS DETECTADOS**

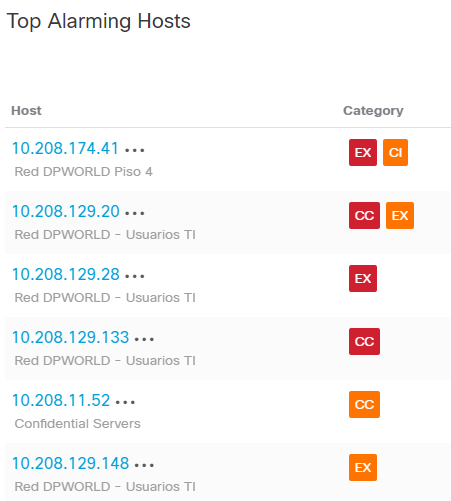


* Se observaron alertasen la consola de administración de **STEALTHWATCH.** Se observan alertas, no se consideran críticas ya que todas son de la red interna de DPW

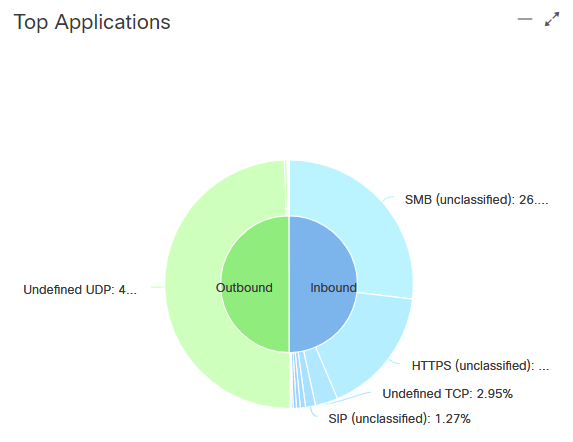
**Alarma por tipo**

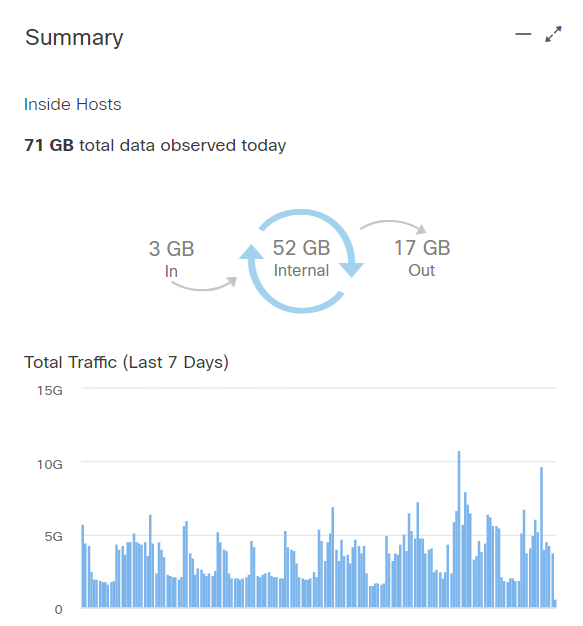


**Alarmas de los últimos 7 días**

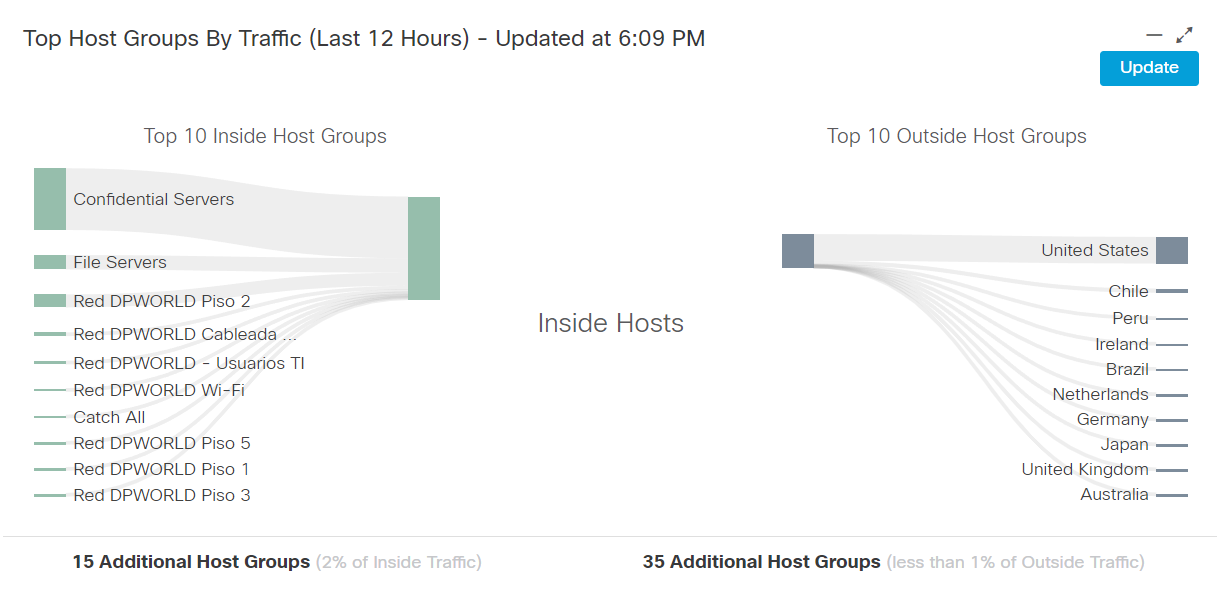


**Top aplicaciones**





**Top 10 de grupos por tráfico**



* El país donde se detectaron mayores conexiones fue **United States**.

**SALUD**

${graph36264}

* 1. **SENSOR DE TRÁFICO Y CONVERSIÓN A NETFLOW FLOW SENSOR**
* **SALUD**

${graph36265}

* 1. **RECOLECIÓN DE FLUJOS FLOW COLLECTOR**
* **SALUD**

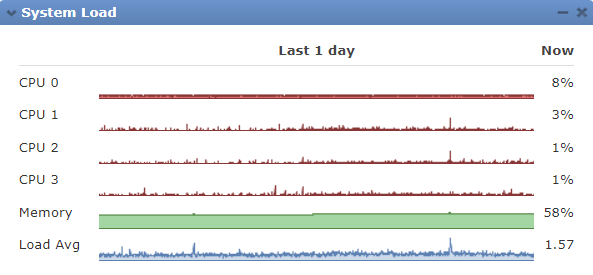
${graph36266}

* 1. **IPS 7050**
* **SALUD**

**Uptime**



**Recursos: CPU Y Memoria**

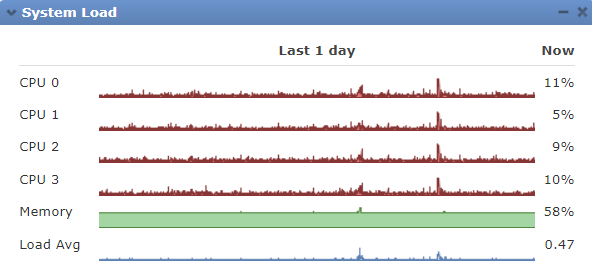


* Se puede observar que los recursos están en el umbral correcto durante las últimas 24 horas.
  1. **FIREPOWER MANAGEMENT CENTER**
* **SALUD**

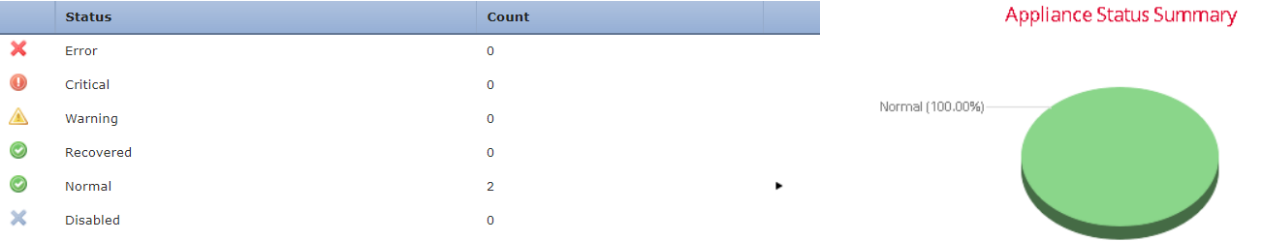
**Uptime**



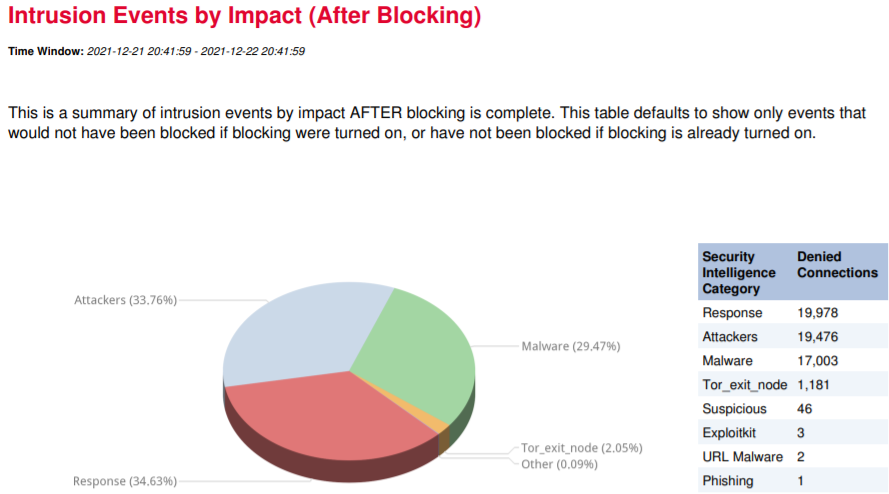
**Recursos: CPU Y Memoria**



**Consola de Administración IPS**



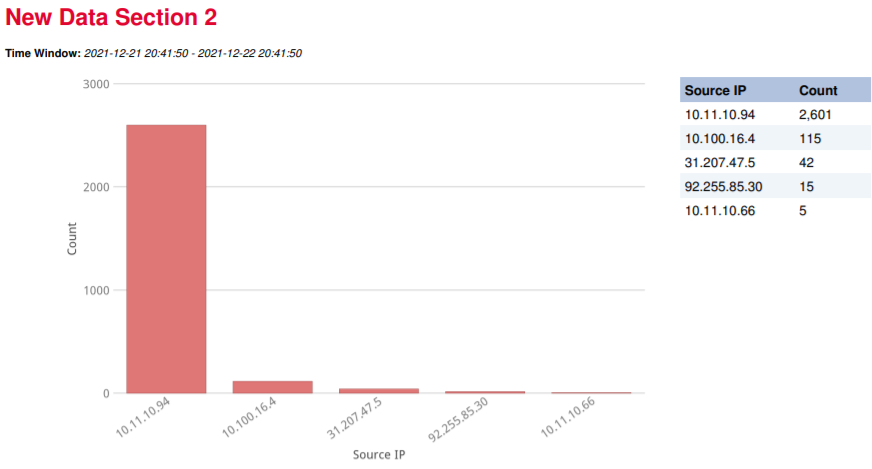
**Eventos bloqueados por el IPS**



En esta gráfica se observan los eventos bloqueados según las categorías.

* + Se verifica que la categoría **Attackers** tuvo mayores conexiones bloqueadas durante el día.

**Top de direcciones IPS atacantes**



* + La dirección **IP** **10.11.10.94** originó la mayor cantidad de eventos durante el día.

1. **PLATAFORMA F5**
   1. **DPWGTM01.DPWC.LOCAL – ACTIVO**

* **Estado del equipo**

${graph4045}

**\*3:** Estado Pasivo y **4: Estado Activo**

* **Recursos**

${graph4036}

* **Conexiones concurrentes**

${graph4038}

* **Throughput(bits)**

${graph4033}

* 1. **DPWGTM02.DPWC.LOCAL – PASIVO**
* **Estado del equipo**

${graph4064}

**\*3: Estado Pasivo** y **4:** Estado Activo

* **Recursos**

${graph4055}

* **Conexiones concurrentes**

${graph4057}

* **Throughput(bits)**

${graph4052}

* 1. **DPWLTM01.DPWC.LOCAL – ACTIVO**
* **Estado del equipo**

${graph4083}

**\*3:** Estado Pasivo y **4: Estado Activo**

* **Recursos**

${graph4074}

* **Conexiones concurrentes**

${graph4076}

* **Throughput(bits)**

${graph4071}

* 1. **DPWLTM02.DPWC.LOCAL - PASIVO**
* **Estado del equipo**

${graph4102}

**\*3: Estado Pasivo** y **4:** Estado Activo

* **Recursos**

${graph4093}

* **Conexiones concurrentes**

${graph4095}

* **Throughput(bits)**

${graph4090}

# CONCLUSIONES

* Se observa uso de recursos estables en los equipos Stealth Watch.
* Se observa un uso de recursos estables por el IPS.
* Se observa los recursos estables de los balanceadores F5.
* La dirección IP **10.11.10.94** originó la mayor cantidad de eventos.
* Se observa alto consumo de memoria en el equipo **Flow collector.** Se revisó bajo el **INC 266751**. Donde indica que la memoria está asignada a una tarea, pero es posible que la tarea no esté utilizando actualmente la memoria. Aun así, debido a que está asignado, se muestra como en uso para el hipervisor y el sistema operativo.
* Se observaron alertas de Corcern Index y Exfiltration en la consola de administración de STEALTHWATCH, No representan amenaza ya que las IP asociadas a estos eventos pertenecen a la red interna de DPW.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| a01 | ${autor} | Supervisor CyberSOC | ${fecha\_hoy} | Versión Inicial |