**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE SEMANAL**

**ESTADO DE SALUD**

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

**Fecha de elaboración:**

**17 de noviembre de 2020**

**Fecha de elaboración:**

**${fecha\_actual}**



**El presente documento contiene información estrictamente privada y confidencial para Securesoft Corporation S.A.C. y Ministerio de Relaciones Exteriores.**



**INDICE**

[**I. OBJETIVO 3**](#_Toc87613325)

[**II. ALCANCE 3**](#_Toc87613326)

[**III. ESTADO DE LAS PLATAFORMAS 3**](#_Toc87613327)

[**A. SOLUCIÓN FIREWALL DE APLICACIONES WEB 3**](#_Toc87613328)

[**a. Fortiweb WAF 1 – Master 3**](#_Toc87613329)

[**b. Fortiweb WAF 2 – Slave 4**](#_Toc87613330)

[**B. SOLUCION ANTIDDOS 4**](#_Toc87613331)

[**a. Netscout Arbor 4**](#_Toc87613332)

[**C. SEGURIDAD PERIMETRAL 5**](#_Toc87613333)

[**a. Firewall Interno 1 – Master 5**](#_Toc87613334)

[**b. Firewall Externo 1 – Master 6**](#_Toc87613335)

[**c. Fortianalyzer 7**](#_Toc87613336)

[**D. SEGURIDAD SANDBOX 7**](#_Toc87613337)

[**a. FortiSandbox 7**](#_Toc87613338)

[**E. SEGURIDAD CORREOS ELECTRÓNICOS 8**](#_Toc87613339)

[**a. FortiMail 1 – Master 8**](#_Toc87613340)

[**b. FortiMail 2 – Slave 8**](#_Toc87613341)

[**F. SEGURIDAD ENDPOINT CENTRALIZADO 9**](#_Toc87613342)

[**a. Servidor McAfee 9**](#_Toc87613343)

[**b. Consola FortiClient 9**](#_Toc87613344)

[**c. Servidor McAfee Agent Handler 10**](#_Toc87613345)

[**G. SOLUCIÓN DE ADMINISTRACIÓN DE ANCHO DE BANDA 10**](#_Toc87613346)

[**a. Exinda 10**](#_Toc87613347)

[**H. SERVICIO DEL SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD INFORMÁTICA 11**](#_Toc87613348)

[**a. FortiSIEM 11**](#_Toc87613349)

[**IV. CONCLUSIONES 12**](#_Toc87613350)

# OBJETIVO

Este documento dará a conocer el estado de salud de las plataformas de seguridad del cliente durante la última semana.

# ALCANCE

Este documento presenta información sobre el consumo de recursos de los equipos administrados, así como el estado de su disponibilidad durante los últimos 7 días.

# ESTADO DE LAS PLATAFORMAS

1. **SOLUCIÓN FIREWALL DE APLICACIONES WEB**
   1. **Fortiweb WAF 1 – Master**

* **RECURSOS**

${graph15693}

* El promedio de uso de **CPU** durante la última semana fue de **3.20%**.
* El promedio de uso de **Disco** durante la última semana fue de **78%**.
* El promedio de uso de **Memoria** durante la última semana fue de **16.49%**.
  1. **Fortiweb WAF 2 – Slave**
* **RECURSOS**

${graph15700}

* El promedio de uso de **CPU** durante la última semana fue de **4.17%**.
* El promedio de uso de **Disco** durante la última semana fue de **79%**.
* El promedio de uso de **Memoria** durante la última semana fue de **20.55%**.

1. **SOLUCION ANTIDDOS**
   1. **Netscout Arbor**

* **RECURSOS**

${graph22840}

* El promedio de uso de **Disco** durante la última semana fue de **6%**.
* El promedio de uso de **Memoria** durante la última semana fue de **33.46%**.

1. **SEGURIDAD PERIMETRAL**
   1. **Firewall Interno 1 – Master**

* **RECURSOS**

${graph15361}

* El promedio de uso de **CPU** durante la última semana fue de **1.22%**.
* El promedio de uso de **memoria** durante la última semana fue de **30.46%.**
* **CONEXIONES CONCURRENTES**

${graph15369}

* El promedio de sesiones, durante la última semana fue de **10.41 K**.
  1. **Firewall Externo 1 – Master**
* **RECURSOS**

${graph15162}

* El promedio de uso de **CPU** durante la última semana fue de **0.08%.**
* El promedio de uso de **Memoria** durante la última semana fue de **27.48%**.
* **CONEXIONES CONCURRENTES**

${graph15170}

* El promedio de sesiones es de **14.49 K** durante la última.
  1. **Fortianalyzer**
* **RECURSOS**

${graph16257}

* El promedio de uso de **disco** durante la última semana fue de **39**%.
* El promedio de uso de **memoria** durante la última semana fue de **29**%.
* No se observa data en la gráfica de CPU, fue reportado bajo ticket **SOL 231511.**

1. **SEGURIDAD SANDBOX**
   1. **FortiSandbox**

* **RECURSOS**

${graph22899}

* El promedio de uso de **CPU** durante la última semana fue de **1.26%**.
* El promedio de uso de **disco** durante la última semana fue de **8**%.
* El promedio de uso de **memoria** durante la última semana fue de **0**%.

1. **SEGURIDAD CORREOS ELECTRÓNICOS**
   1. **FortiMail 1 – Master**

* **RECURSOS**

${graph15651}

* El promedio de uso de **CPU** durante la última semana fue de **2%.**
* El promedio de uso de **memoria** durante la última semana fue de **23%**.
* El promedio de uso de **disco** durante la última semana fue de **0**%.
  1. **FortiMail 2 – Slave**
* **RECURSOS**

${graph15658}

* El promedio de uso de **CPU** durante la última semana fue de **0%**.
* El promedio de uso de **memoria** durante la última semana fue de **13.94**%.
* El promedio de uso de **disco** durante la última semana fue de **0**%.

1. **SEGURIDAD ENDPOINT CENTRALIZADO**
   1. **Servidor McAfee**

* **RECURSOS**

${graph22841}

* El promedio de uso de **CPU** durante la última semana fue de **3.52%**.
* El promedio de uso de **memoria** durante la última semana fue de **57.25%.**
* El promedio de uso de **disco** durante la última semana fue de **6%.**
  1. **Consola FortiClient**
* **RECURSOS**

${graph23181}

* El promedio de uso de **CPU** durante la última semana fue de **16.43%**.
* El promedio de uso de **disco** durante la última semana fue de **18.80%.**
* El promedio de uso de **memoria** durante la última semana fue de **39.92%.**
  1. **Servidor McAfee Agent Handler**
* **RECURSOS**

${graph26685}

* El promedio de uso de **CPU** durante la última semana fue de **0.51%**.
* El promedio de uso de **disco** durante la última semana fue de **7.40%.**
* El promedio de uso de **memoria** durante la última semana fue de **12.96%.**

1. **SOLUCIÓN DE ADMINISTRACIÓN DE ANCHO DE BANDA**
   1. **Exinda**

* **RECURSOS**

${graph15718}

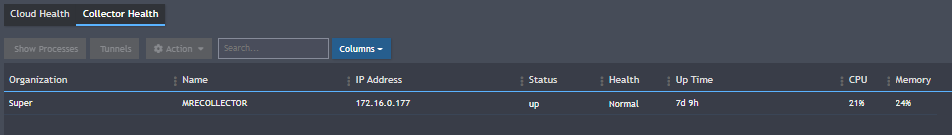
* El promedio de uso de **CPU** durante la última semana fue de **0.20%**.
* El promedio de uso de **memoria** durante la última semana fue de **16.97**%.

1. **SERVICIO DEL SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD INFORMÁTICA**
   1. **FortiSIEM**

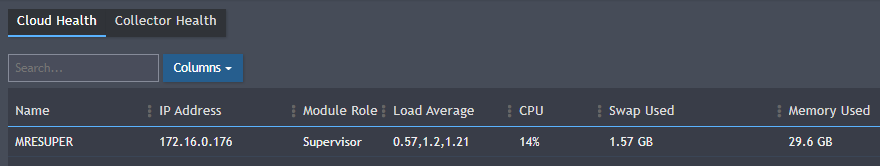
* **CONEXIÓN ICMP**

${graph23398}

* Se valida que el estado de la plataforma se mantuvo UP durante la semana.
* **SERVIDOR SIEM – COLLECTOR**

****

* El **CPU** usado es de **21%**.
* La **memoria** usada es de **24**%.
* **SERVIDOR SIEM – SUPERVISOR**



* El **CPU** usado es de **14%**.
* La **memoria** usada es de **29.6 GB.**

# CONCLUSIONES

* El uso del CPU se encuentra entre los umbrales establecidos.
* Las conexiones son estables durante la semana.
* Edwin Trejo se encuentra elaborando el PDT para las pruebas HA de las plataformas FW Externo (Slave) y FW Interno (Slave), además estará proponiendo una reunión con cliente para validar en conjunto las actividades a aplicar en el detalle del PDT.
* Los equipos Servidor SIEM Cloud Health se encuentran estables.
* Se observa perdida de SNMP en el equipo **FORTIANALYZER**, el cual está siendo revisado bajo ticket **231511.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 01 | ${autor} | Supervisor | ${fecha\_hoy} | Versión Inicial |