**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE MENSUAL**

**ESTADO DE SALUD**

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

**Fecha de elaboración:**

**17 de noviembre de 2020**

**Fecha:**

**${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**](#_Toc87614901)

[**II. ALCANCE 3**](#_Toc87614902)

[**III. ESTADO DE LAS PLATAFORMAS 3**](#_Toc87614903)

[**A. SOLUCIÓN FIREWALL DE APLICACIONES WEB 3**](#_Toc87614904)

[**a. Fortiweb WAF 1 – Master 3**](#_Toc87614905)

[**b. Fortiweb WAF 2 – Slave 4**](#_Toc87614906)

[**B. SOLUCION ANTIDDOS 4**](#_Toc87614907)

[**a. Netscout Arbor 4**](#_Toc87614908)

[**C. SEGURIDAD PERIMETRAL 5**](#_Toc87614909)

[**a. Firewall Interno 1 – Master 5**](#_Toc87614910)

[**b. Firewall Externo 1 – Master 6**](#_Toc87614911)

[**c. Fortianalyzer 7**](#_Toc87614912)

[**D. SEGURIDAD SANDBOX 7**](#_Toc87614913)

[**a. FortiSandbox 7**](#_Toc87614914)

[**E. SEGURIDAD CORREOS ELECTRÓNICOS 8**](#_Toc87614915)

[**a. FortiMail 1 – Maste 8**](#_Toc87614916)

[**b. FortiMail 2 – Slave 8**](#_Toc87614917)

[**F. SEGURIDAD ENDPOINT CENTRALIZADO 9**](#_Toc87614918)

[**a. Servidor McAfee 9**](#_Toc87614919)

[**b. Consola FortiClient 9**](#_Toc87614920)

[**c. Servidor McAfee Agent Handler 10**](#_Toc87614921)

[**G. SOLUCIÓN DE ADMINISTRACIÓN DE ANCHO DE BANDA 10**](#_Toc87614922)

[**a. Exinda 10**](#_Toc87614923)

[**H. SERVICIO DEL SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD INFORMÁTICA 11**](#_Toc87614924)

[**a. FortiSIEM 11**](#_Toc87614925)

[**IV. CONCLUSIONES 12**](#_Toc87614926)

# OBJETIVO

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

# ALCANCE

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

# ESTADO DE LAS PLATAFORMAS

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

* **RECURSOS**

${graph15693}

* El promedio de uso de **CPU** durante el último mes fue de **3.25%**.
* El promedio de uso de **Disco** durante el último mes fue de **78%**.
* El promedio de uso de **Memoria** durante el último mes fue de **28.22%**.
  1. **Fortiweb WAF 2 – Slave**
* **RECURSOS**

${graph15700}

* El promedio de uso de **CPU** durante el último mes fue de **4.30%**.
* El promedio de uso de **Disco** durante el último mes fue de **79%**.
* El promedio de uso de **Memoria** durante el último mes fue de **31.55%**.

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

* **RECURSOS**

${graph22840}

* El promedio de uso de **Disco** durante el último mes fue de **6%**.
* El promedio de uso de **Memoria** durante el último mes fue de **42.67%**.

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

* **RECURSOS**

${graph15361}

* El promedio de uso de **CPU** durante el último mes fue de **0.68%.**
* El promedio de uso de **memoria** durante el último mes fue de **31.89%.**
* **CONEXIONES CONCURRENTES**

${graph15369}

* El promedio de sesiones, durante el último mes fue de **10.5 K**.
  1. **Firewall Externo 1 – Master**
* **RECURSOS**

${graph15162}

* El promedio de uso de **CPU** durante el último mes fue de **0.03%**.
* El promedio de uso de **memoria** durante el último mes fue de **28.98**%.
* **CONEXIONES CONCURRENTES**

${graph15170}

* El promedio de sesiones, durante el último mes fue de **14.42 k**.
  1. **Fortianalyzer**
* **RECURSOS**

${graph16257}

* El promedio de uso de **disco** durante el último mes fue de **28.78**%.
* El promedio de uso de **memoria** durante el último mes fue de **66.86**%.
* El promedio de uso de **CPU** durante el último mes fue de **2.93%**.

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

* **RECURSOS**

${graph22899}

* El promedio de uso de **CPU** durante el último mes fue de **10.59%**.
* El promedio de uso de **disco** durante el último mes fue de **8** %.
* El promedio de uso de **memoria** durante el último mes fue de **0**%.

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

* **RECURSOS**

${graph15651}

* El promedio de uso de **CPU** durante el último mes fue de **0%**.
* El promedio de uso de **memoria** durante el último mes fue de **26.87%**.
* El promedio de uso de **disco** durante el último mes fue de **0%**.
  1. **FortiMail 2 – Slave**
* **RECURSOS**

${graph15658}

* El promedio de uso de **CPU** durante el último mes fue de **0%**.
* El promedio de uso de **memoria** durante el último mes fue de **15.05**%.
* El promedio de uso de **disco** durante el último mes fue de **0**%.

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

* **RECURSOS**

${graph22841}

* El promedio de uso de **CPU** durante el último mes fue de **3.36%**.
* El promedio de uso de **memoria** durante el último mes fue de **59.79%**.
* El promedio de uso de **disco** durante el último mes fue de **6%**.
  1. **Consola FortiClient**
* **RECURSOS**

${graph23181}

* El promedio de uso de **CPU** durante el último mes fue de **18.52%.**
* El promedio de uso de **disco** durante el último mes fue de **17.90%**.
* El promedio de uso de **memoria** durante el último mes fue de **53.40%**.
  1. **Servidor McAfee Agent Handler**
* **RECURSOS**

${graph26685}

* El promedio de uso de **CPU** durante el último mes fue de **16.75%**.
* El promedio de uso de **memoria** durante el último mes fue de **8%.**
* El promedio de uso de **disco** durante el último mes fue de **12.94%.**

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

* **RECURSOS**

${graph15718}

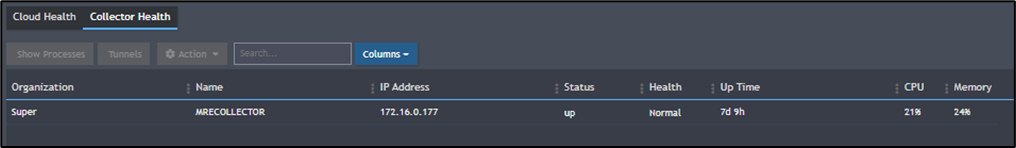
* El promedio de uso de **CPU** durante el último mes fue de **0.62%**.
* El promedio de uso de **memoria** durante el último mes fue de **29.34**%.

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

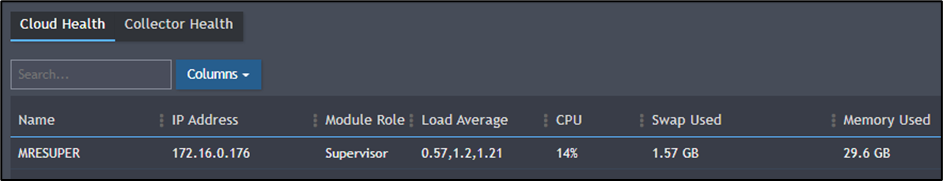
* **CONEXIÓN ICMP**

${graph23398}

* Se observan caídas, se valida que fueron falsos positivos ya que, al revisar en conjunto con el onsite, el estado de la plataforma se mantuvo UP.
* **SERVIDOR SIEM – COLLECTOR**



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



* El **CPU** usado es de **29.6%**.
* La **memoria** usada es de **1.57** **GB.**

# CONCLUSIONES

* El uso del CPU se encuentra entre los umbrales establecidos.
* 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 ICMP en el equipo **FORTISIEM** por un corto intervalo de tiempo ocasionado por intermitencia, se validó que el equipo se encontraba en estado **UP**.
* Se observa pérdida de conexión SNMP en el equipo **FORTIANALYZER,** fue reportado bajo el ticket **INC 231511.**

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