**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE MENSUAL**

**Preparado para:**



**Fecha:**

**${fecha\_actual}**

**El presente documento contiene información estrictamente privada y confidencial para Minera Volcan S.A.A y SecureSoft Corporation S.A.C.**

1. **OBJETIVO**

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

1. **ALCANCES**

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

1. **ESTADO DE LAS PLATAFORMAS**

# FIREWALL FORTIGATE 01

# ESTADO DE SALUD

* **Uso Promedio de CPU**

${graph1405}

**\* *El consumo de CPU promedio es de 5.29%, se encuentra dentro del umbral.***

* **Uso de Memoria**

${graph1412}

**\* *El consumo de Memoria promedio es de 29.61%, se encuentra dentro del umbral.***

* **Uso de disco**

${graph1409}

* **Conexiones Concurrentes**

${graph1414}

# FIREWALL FORTIGATE 02

# ESTADO DE SALUD

* **Uso Promedio de CPU**

${graph1417}

**\* *El consumo de CPU promedio es de 0.005%, se encuentra dentro del umbral.***

* **Uso de Memoria**

${graph1424}

**\* *El consumo de Memoria promedio es de 26.00%, se encuentra dentro del umbral.***

* **Uso de disco**

${graph1421}

* **Conexiones Concurrentes**

${graph1426}

# RED DE QUBO

1. **ANTIMALWARE FIREPOWER THREAT DEFENSE**

# ESTADO DE SALUD

* **Recursos**

${graph34516}

**\* *El consumo de CPU promedio es de 2.96%, se encuentra dentro del umbral.***

**\* *El consumo de MEMORIA promedio es de 39%, se encuentra dentro del umbral.***

1. **FIREPOWER MANAGEMENT CENTER (FMC01) – QUBO**

# ESTADO DE SALUD

* **Recursos**

${graph34969}

**\* *El consumo de CPU promedio es de 3.24%, se encuentra dentro del umbral.***

**\* *El consumo de MEMORIA promedio es de 43.65%, se encuentra dentro del umbral.***

1. **FIREPOWER MANAGEMENT CENTER (FMC02) – QUBO**

# ESTADO DE SALUD

* **Uso Promedio de CPU**

${graph1467}

**\* *El consumo de CPU promedio es de 2.95%, se encuentra dentro del umbral.***

* **Uso de Memoria**

${graph1464}

**\* *El consumo de MEMORIA promedio es de 41.48%, se encuentra dentro del umbral.***

1. **FIREPOWER THREAT DEFENSE (FW01) – QUBO**

# ESTADO DE SALUD

* **Recursos**

${graph34475}

**\* *El consumo de CPU promedio es de 3.05%, se encuentra dentro del umbral.***

**\* *El consumo de MEMORIA promedio es de 41.96%, se encuentra dentro del umbral.***

1. **FIREPOWER THREAT DEFENSE (FW02) – QUBO**

# ESTADO DE SALUD

* **Recursos**

${graph34517}

**\* *El consumo de CPU promedio es de 0.99%, se encuentra dentro del umbral.***

**\* *El consumo de MEMORIA promedio es de 41%, se encuentra dentro del umbral.***

1. **PROXY – SYMANTEC QUBO**

# ESTADO DE SALUD

* **Recursos**

${graph1440}

**\* *El consumo de CPU promedio es de 19.81%, se encuentra dentro del umbral.***

**\* *El consumo de MEMORIA promedio es de 32.56%, se encuentra dentro del umbral.***

# PROXY – SYMANTEC TIC 01

# ESTADO DE SALUD

* **Recursos**

${graph1448}

**\* *El consumo de CPU promedio es de 20.91%, se encuentra dentro del umbral.***

***\*El consumo de Memoria promedio es de 19%, se encuentra dentro del umbral.***

* **Conexiones concurrentes**

${graph1449}

# PROXY – SYMANTEC TIC 02

# ESTADO DE SALUD

* **Recursos**

${graph1456}

**\* *El consumo de CPU promedio es de 20.91%, se encuentra dentro del umbral.***

***\*El consumo de Memoria promedio es de 19.00%, se encuentra dentro del umbral.***

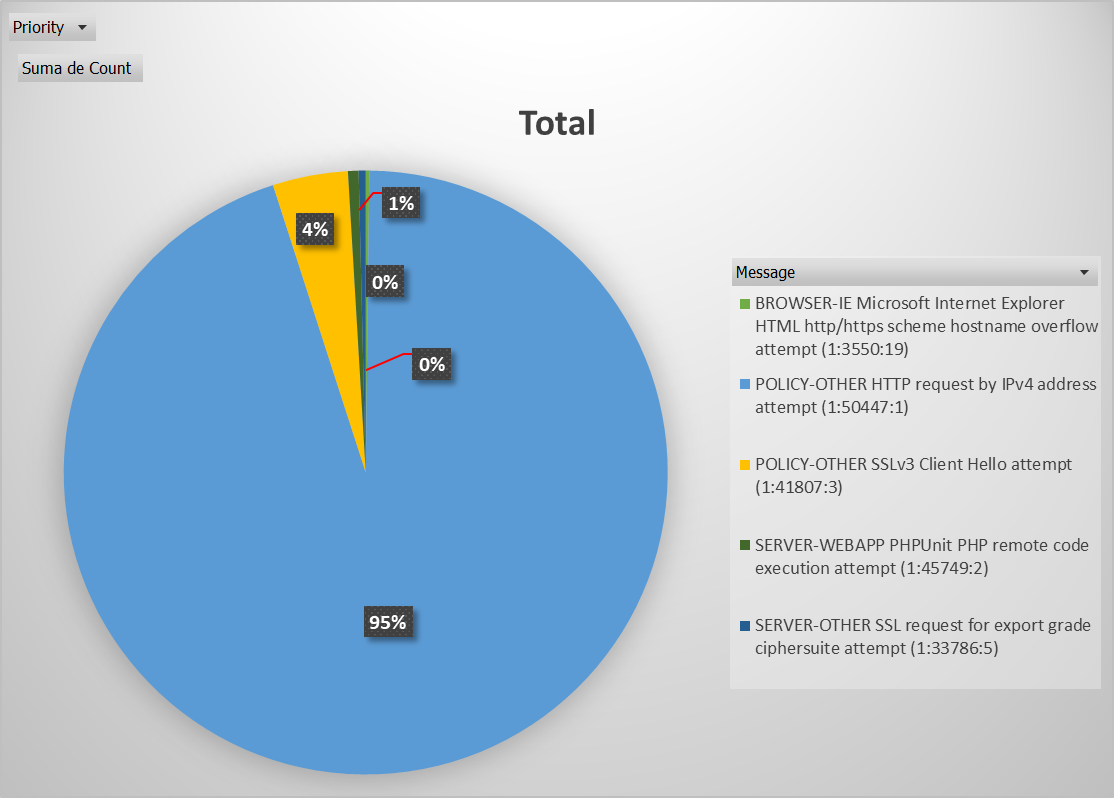
* **Conexiones concurrentes**

${graph1457}

# EVENTOS DETECTADOS

# Consola IPS

***El siguiente gráfico muestra el TOP 5 de eventos en la categoría alta y medio detectados durante el mes.***

******

* ***Se observa que se generó un total de 2658 eventos, los cuales fueron bloqueados.***

1. **CONCLUSIONES**

* El estado de todos los equipos durante el mes es estable.
* El uso promedio de CPU en el FIREWALL FORTIGATE 01 durante el mes es de 5.29%
* El uso promedio de CPU en el FIREWALL FORTIGATE 02 durante el mes es de 0.005%
* El uso promedio de CPU en el QUBO ANTIMALWARE FTD durante el mes es de 2.96%
* El uso promedio de CPU en el QUBO FMC01 durante el mes es de 3.24%
* El uso promedio de CPU en el QUBO FMC02 durante el mes es de 2.95%
* El uso promedio de CPU en el QUBO FTD FW01 durante el mes es de 3.05%
* El uso promedio de CPU en el QUBO FTD FW02 durante el mes es de 0.99%
* El uso promedio de CPU en el PROXY - SYMANTEC QUBO durante el mes es de 19.81%
* El uso promedio de CPU en el PROXY - SYMANTEC TIC 01 durante el mes es de 20.91%
* El uso promedio de CPU en el PROXY - SYMANTEC TIC 02 durante el mes es de 20.91%
* Las conexiones concurrentes durante el mes son estables.
* Se adjunta archivos Ataques Febrero IPS y AMP pdf.
* Se validó que las firmas de severidad media y alta que se presentaron a nivel de IPS fueron bloqueadas.
* Se presentaron 2658 firmas de severidad alta a nivel de IPS.
* La firma que realizó la mayor cantidad de alertas fue **POLICY-OTHER HTTP request by IPv4 address attempt (1:50447:1)** los cuales fueron bloqueados.
* Se generaron los siguientes eventos correspondientes al mes de Febrero.

|  |  |
| --- | --- |
| **N° Ticket** | **Detalle\_Contencion** |
| 303050 | Bloqueo a nivel IPS/Firewall |
| 302438 | Bloqueo a nivel IPS/Firewall |
| 301008 | Bloqueo a nivel Firewall |
| 300779 | Bloqueo a nivel IPS/Firewall |
| 300770 | Bloqueo a nivel IPS/Firewall |
| 300761 | Bloqueo a nivel IPS/Firewall |
| 299043 | Bloqueo a nivel Firewall |
| 298922 | Bloqueo a nivel IPS/Firewall |
| 298602 | Bloqueo a nivel IPS/Firewall |
| 298599 | Bloqueo a nivel IPS/Firewall |
| 298553 | Bloqueo a nivel IPS/Firewall |
| 298545 | Bloqueo a nivel IPS/Firewall |
| 298541 | Bloqueo a nivel IPS/Firewall |
| 298094 | Bloqueo a nivel Firewall |
| 298081 | Bloqueo a nivel IPS/Firewall |
| 297897 | Bloqueo a nivel IPS/Firewall |
| 297895 | Bloqueo a nivel IPS/Firewall |
| 297891 | Bloqueo a nivel IPS/Firewall |
| 297786 | Bloqueo a nivel Firewall |
| 297782 | Bloqueo a nivel Firewall |
| 297500 | Bloqueo a nivel IPS/Firewall |
| 297252 | Bloqueo a nivel IPS/Firewall |
| 297247 | Bloqueo a nivel IPS/Firewall |
| 297243 | Bloqueo a nivel IPS/Firewall |
| 297233 | Bloqueo a nivel IPS/Firewall |
| 296542 | Bloqueo a nivel IPS/Firewall |
| 296534 | Bloqueo a nivel IPS/Firewall |
| 296149 | Bloqueo a nivel Firewall |
| 295416 | Bloqueo a nivel Firewall |
| 295413 | Bloqueo a nivel Firewall |
| 295410 | Bloqueo a nivel Firewall |
| 294086 | Bloqueo a nivel IPS/Firewall |
| 294083 | Bloqueo a nivel IPS/Firewall |
| 291675 | Bloqueo a nivel IPS/Firewall |
| 291661 | Bloqueo a nivel IPS/Firewall |
| 290859 | Bloqueo a nivel IPS/Firewall |
| 290012 | Bloqueo a nivel IPS/Firewall |
| 290006 | Bloqueo a nivel IPS/Firewall |
| 290003 | Bloqueo a nivel IPS/Firewall |
| 289363 | Bloqueo a nivel IPS/Firewall |
| 289355 | Bloqueo a nivel IPS/Firewall |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| a00 | ${autor} | Supervisor | 18/03/2022 | Versión Inicial |