SECURESOFT CORPORATION

e-Secure Consulting Group

1. **Reporte Mensual – EVENTOS DETECTADOS**
2. **PREPARADO PARA:**
3. 
4. **Fecha:**

**FEBRERO de 2022**



**El presente documento contiene información estrictamente privada y confidencial para SecureSoft S.A.C. y DP WORLD.**

1. **OBJETIVO**

Este documento permite mostrar los eventos detectados del mes de enero a través de los sensores de Sourcefire instalado en la red del cliente, como también el estado de recursos de las plataformas de seguridad.

1. **ALCANCES**

Este documento servirá como herramienta para saber los ataques y los incidentes de salud que se hayan presentado en la red del cliente y el impacto que tuvo.

1. **ESTADO DE LAS PLATAFORMAS**
2. **FIREWALL CHECKPOINT**

* **SMARTCENTER**

Recursos

${graph14349}

* Se observa que el uso promedio de **CPU** durante el mes fue **1.92 %.**
* Se observa que el uso promedio de **Memoria** durante el mes fue **52.45%.**
* Se observa que el uso promedio de **Disco** durante el mes fue **79.30 %.**
* **FIREWALL 01**

Recursos

${graph14374}

* Se observa que el uso promedio de **CPU** durante el mes fue **5.33 %.**
* Se observa que el uso promedio de **Memoria** durante el mes fue **40.14%.**
* Se observa que el uso promedio de Disco durante el mes fue 15.99 %

Conexiones

${graph14377}

* Se observa que el promedio de **Conexiones** durante el mes fue **7.83 K.**
* **FIREWALL 02**

Recursos

${graph14386}

* Se observa que el uso promedio de **Memoria** durante el mes fue **16%.**
* Se observa que el uso promedio de **Disco** durante el mes fue **10.95%.**

Conexiones

${graph14389}

* Se observa que el promedio de **Conexiones** durante el mes fue **7.54 K.**

1. **BALANCEADORES (F5)**

* **DPWGTM01.DPWC.local**

Recursos

${graph4036}

* Se observa que el uso promedio de **CPU** durante el mes fue **14.43 %.**
* Se observa que el uso promedio de **Memoria** durante el mes fue **3 %.**
* Se observa que el uso promedio de **Disco** durante el mes fue **25 %.**

Conexiones

${graph4038}

* Se observa que el promedio de **Conexiones** durante el mes fue **8.17 K.**

Throughput(bits)

${graph4033}

* Se observa que el promedio de **“Client Bytes Per Second”** durante el último mes es de **6.83 MB.**
* Se observa que el promedio de **“Server Bytes Per Second”** durante el último mes es de **6.83 MB.**
* **DPWGTM02.DPWC.local**

Recursos

${graph4055}

* Se observa que el uso promedio de **CPU** durante el mes fue **14 %.**
* Se observa que el uso promedio de **Memoria** durante el mes fue **3 %.**
* Se observa que el uso promedio de **Disco** durante el mes fue **25 %.**

Conexiones

${graph4057}

* Se observa que el promedio de **Conexiones** durante el mes fue **133.35.**

Throughput(bits)

${graph4052}

* Se observa que el promedio de **“Client Bytes Per Second”** durante el último mes es de **5.83 KB.**
* Se observa que el promedio de **“Server Bytes Per Second”** durante el último mes es de **3.36 KB.**
* **DPWLTM01.DPWC.local**

Recursos

${graph4074}

* Se observa que el uso promedio de **CPU** durante el mes fue **16.58 %.**
* Se observa que el uso promedio de **Memoria** durante el mes fue **5 %.**
* Se observa que el uso promedio de **Disco** durante el mes fue **46 %.**

Conexiones

${graph4076}

* Se observa que el promedio de **Conexiones** durante el mes fue **1.57 K.**

Throughput(bits)

${graph4071}

* Se observa que el promedio de **“Client Bytes Per Second”** durante el último mes es de **1.08 MB.**
* Se observa que el promedio de **“Server Bytes Per Second”** durante el último mes es de **1.09 MB.**
* **DPWLTM02.DPWC.local**

Recursos

${graph4093}

* Se observa que el uso promedio de **CPU** durante el mes fue **15.22 %.**
* Se observa que el uso promedio de **Memoria** durante el mes **fue 5 %.**
* Se observa que el uso promedio de **Disco** durante el mes fue **46 %.**

Conexiones

${graph4095}

* Se observa que el promedio de **Conexiones** durante el mes fue **1.1 K.**

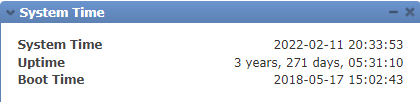
Throughput(bits)

${graph4090}

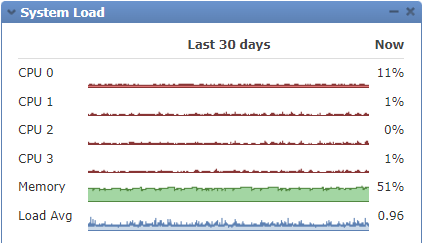
* Se observa que el promedio de **“Client Bytes Per Second”** durante el último mes es de **151.4 KB.**
* Se observa que el promedio de **“Server Bytes Per Second”** durante el último mes es de **151.29 KB.**

1. **IPS 7050 - 10.208.21.38**

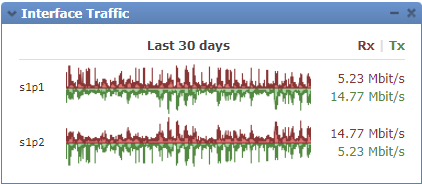
* **Uptime**



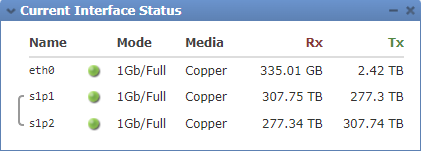
* **Cuadro de estado de recursos principales**



* **Cuadro de tráfico detectado por interfaz**

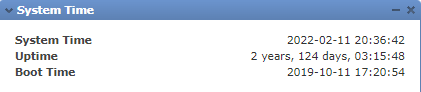


* **Cuadro de estado de interfaces**

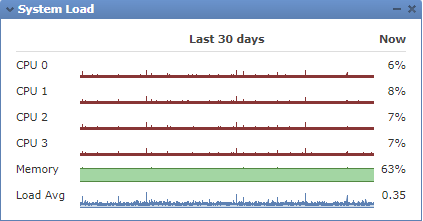


1. **FIREPOWER Management Center - 10.208.21.40**

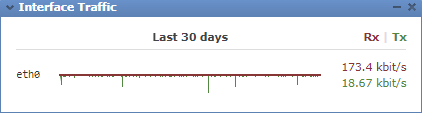
* **Uptime**



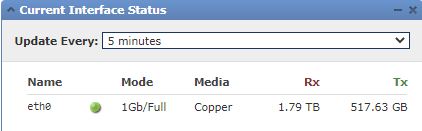
* **Cuadro de estado de recursos principales**



* **Cuadro de tráfico detectado por interfaz**

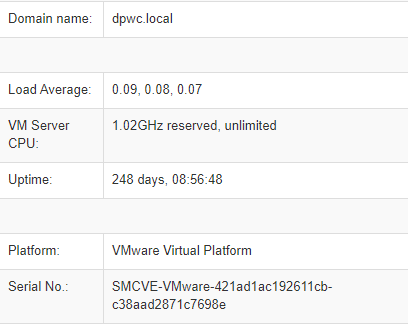


* **Cuadro de estado de interfaces**

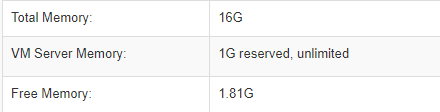


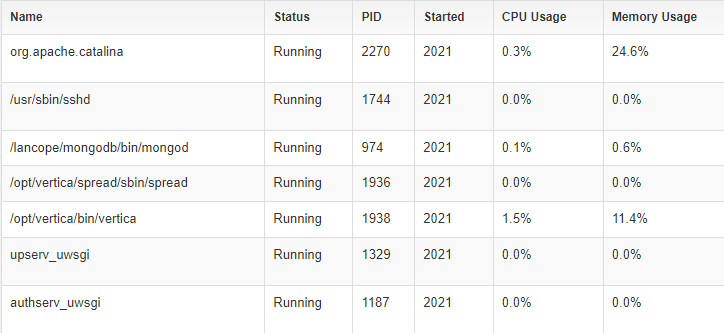
1. **Consola de Administración – Stealthwatch - 10.208.21.30**

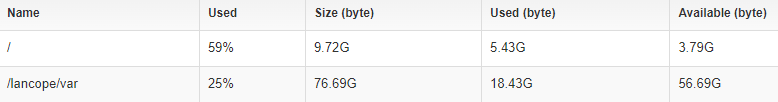
* **Uptime**



* **Recursos**

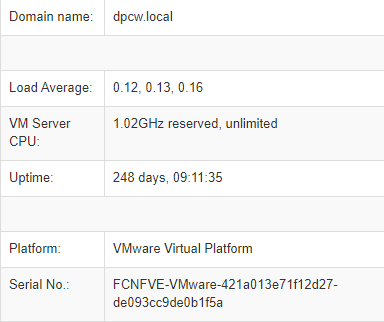




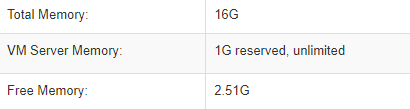


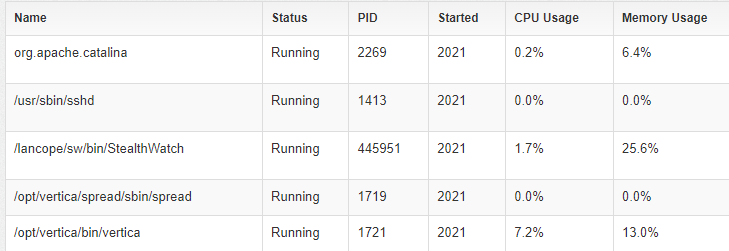
1. **Recolección de Flujos flow collector - 10.208.21.31**

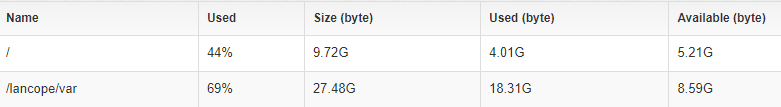
* **Uptime**



* **Recursos**

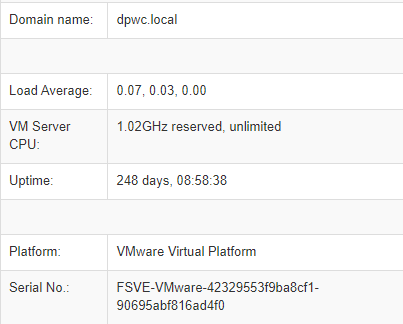




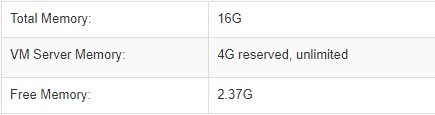


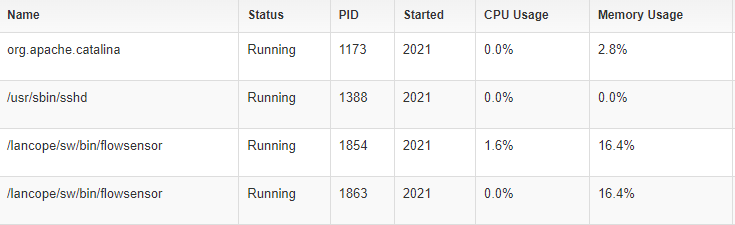
1. **Sensor de tráfico y conversión a netflow flow sensor - 10.208.21.32**

* **Uptime**



* **Recursos**







1. EVENTOS DETECTADOS
2. Consola IPS

El siguiente gráfico muestra el TOP 5 de eventos de severidad ALTA

* **Descripción de las firmas detectados de severidad alta.**

|  |  |
| --- | --- |
| **Firma** | **APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com (1:28070:3)** |
| Descripción de la Firma | Ha habido cierta controversia en torno a Qihoo y su conjunto de seguridad 360, como informar de que otro software antivirus y herramientas de búsqueda son maliciosos (referencia) y están haciendo secuestro de sesión QQ (IM / chat) (referencia). Durante el último año de publicación de Qihoo, ha habido más controversias, incluidos informes sobre espionaje, piratería y filtración de datos (referencia) de la compañía. Existen de que el software 360 ​​incluye spyware, y que pueden tener afiliaciones con el gobierno de la República Popular China para rastrear, controlar y vigilar la actividad en línea de los usuarios (referencia). |
| Recomendaciones | Actualizar a la última versión no afectada del software. Aplicar los parches apropiados provistos por el proveedor. |
| **Firma** | **SMTP\_SPECIFIC\_CMD\_OVERFLOW (124:4:2)** |
| Descripción de la Firma | Esto indica la detección de un comando de cliente SMTP demasiado largo. Los servidores SMTP que tienen una desinfección insuficiente del campo de comandos SMTP pueden ser propensos a tal ataque. Los ataques exitosos pueden permitir que un atacante remoto ejecute código arbitrario dentro del contexto del servidor web, bloquee la aplicación afectada o niegue servicios a usuarios legítimos. |
| Recomendaciones | Aplique los parches apropiados o actualice el sistema a la última versión no vulnerable. Monitoree el tráfico de esa red para detectar cualquier actividad sospechosa. |
| **Firma** | **APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn (1:28069:3)** |
| Descripción de la Firma | Ha habido cierta controversia en torno a Qihoo y su conjunto de seguridad 360, como informar de que otro software antivirus y herramientas de búsqueda son maliciosos (referencia) y están haciendo secuestro de sesión QQ (IM / chat) (referencia). Durante el último año de publicación de Qihoo, ha habido más controversias, incluidos informes sobre espionaje, piratería y filtración de datos (referencia) de la compañía. Existen de que el software 360 ​​incluye spyware, y que pueden tener afiliaciones con el gobierno de la República Popular China para rastrear, controlar y vigilar la actividad en línea de los usuarios (referencia). |
| Recomendaciones | Actualizar a la última versión no afectada del software. Aplicar los parches apropiados provistos por el proveedor. |
| **Firma** | **SSH\_EVENT\_RESPOVERFLOW (128:1:2)** |
| Descripción de la Firma | Este evento se genera cuando se intenta explotar una vulnerabilidad conocida en OpenSSH. El desbordamiento de enteros en sshd en OpenSSH 2.9.9 a 3.3 permite a los atacantes remotos ejecutar código arbitrario durante la autenticación de respuesta de desafío (ChallengeResponseAuthentication) cuando OpenSSH está usando la autenticación SKEY o BSD\_AUTH. |
| Recomendaciones | Actualizar a la última versión no afectada del software. Aplicar los parches apropiados provistos por el proveedor. |
| **Firma** | **MALWARE-BACKDOOR Arucer backdoor traffic - yes command attempt (1:16487:5)** |
| Descripción de la Firma | UsbCharger.dll en el software del cargador de batería USB Energizer DUO contiene una puerta trasera que se implementa a través del archivo Arucer.dll en el directorio% WINDIR% \ system32, que permite a los atacantes remotos descargar programas arbitrarios en una PC con Windows y ejecutar estos programas, a través de una solicitud al puerto TCP 7777. |
| Recomendaciones | Bloquear el acceso a 7777 / tcppuede mitigar esta vulnerabilidad al evitar la conectividad de red a la puerta trasera. Esto se puede lograr con dispositivos de perímetro de red o firewalls de software basados ​​en host. El software Energizer UsbCharger no agrega automáticamente una excepción al Firewall de Windows para 7777 / tcp o la aplicación de puerta trasera. Por lo tanto, la primera vez que se ejecuta Energizer UsbCharger, se le indicará al usuario que el Firewall de Windows ha bloqueado "Ejecutar una DLL como una APLICACIÓN". |

* **Resultado de Eventos Detectados**

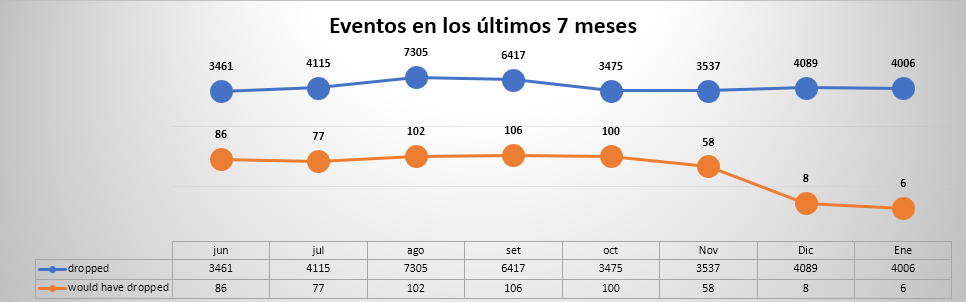
**Informacion de referencia**

|  |  |
| --- | --- |
| **Valor** | **Descripción** |
| **allowed (permitido)** | Aplica cuando el tráfico detectado cumple los parámetros de una firma, pero no necesariamente está relacionado a un ataque |
| **Dropped(bloqueado)** | Aplica cuando una directiva está en modo IPS, por tanto, es capaz de decirle a la red o dispositivo padre que bloquee la conexión cuando se haga match con las reglas de la firma. |
| **would have dropped** | Aplica cuando ciertos paquetes no se bloquean, porque al no recibir el último paquete ACK el host no realiza el reensamblado del tráfico y lo descarta. |

*El 100% (4006) de los eventos fueron bloqueados. Entre estos se encuentran los eventos asociados a infecciones en su mayoría.*



* **Eventos Detectados en los últimos 7 meses – IPS**

**Top 10 Origen**

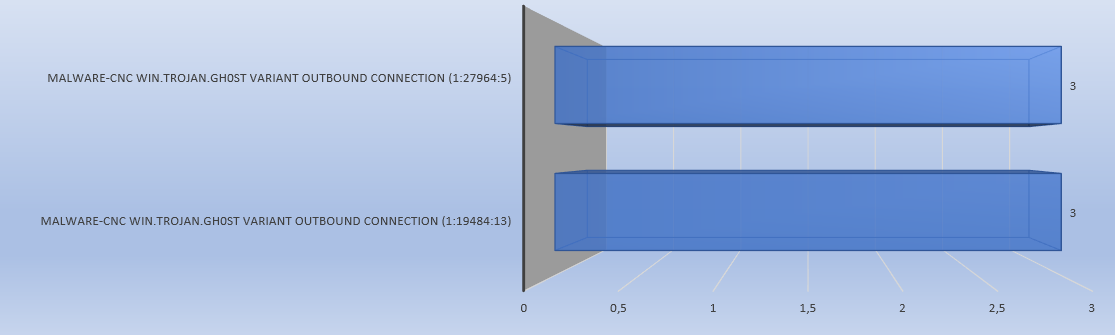
En el siguiente cuadro, se observan las 10 primeras IP’s que originaron mayor cantidad de eventos.

* **Top Destino**

En el siguiente cuadro, se observan las 10 primeras IP’s a las que fueron dirigidas la mayor cantidad de eventos.

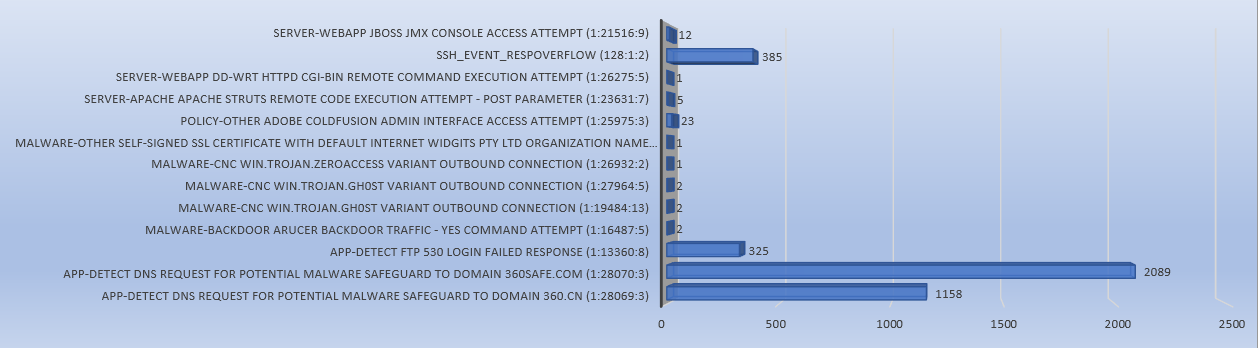
* **Resultado de Ataques Detectados -TOP 10**
* **Eventos permitidos**

En el siguiente cuadro, se observa las firmas que originó mayor cantidad de eventos.



* **Eventos bloqueados**

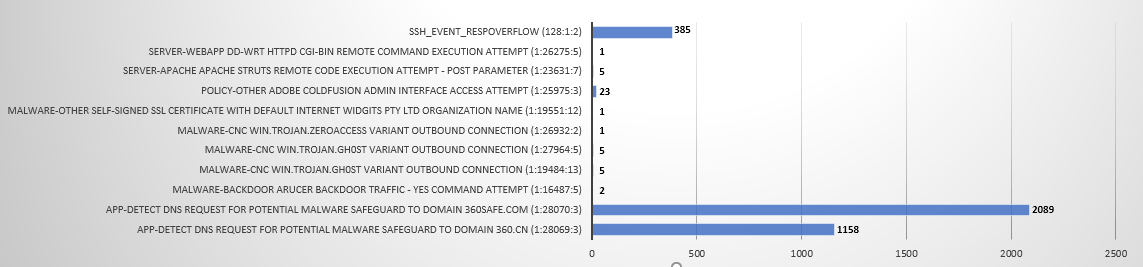
En el siguiente cuadro, se observan las firmas que originaron mayor cantidad de eventos.

****

* **Top 10 según clasificación**

En los siguientes cuadros, se observan las 10 primeras firmas según su clasificación que originaron mayor cantidad de eventos según su prioridad “ALTA “y “MEDIA”

* ***Prioridad ALTA***

******

* ***Prioridad medium***

1. **TENDENCIA DE EVENTOS**

Durante los últimos 12 meses, se incrementó la categoría de Reconocimiento.

1. **CONCLUSIONES**

* Los equipos se encontraron estables durante el mes.
* La firma de prioridad alta “APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com (1:28070:3)” originó la mayor cantidad de eventos.
* Se recomienda validar si las IPs detalladas en el TOP 10 que generaron mayor cantidad de eventos pertenecen algún proveedor del cliente.
* Los tickets generados por los analistas, ha reducido la cantidad de los eventos permitidos (Would have dropped).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| a00 | ${autor} | Supervisor | 16/02/2022 | Versión Inicial |