TLP: AMBAR

Universidad Veracruzana

Plan para el monitoreo y seguridad de la infraestructura tecnológica

Dirección General de Tecnología de Información

"Lis de Veracruz: Arte, Ciencia, Luz

Proceso de recolección y almacenamiento de registros

La recolección de registros y su almacenamiento permiten monitorear el comportamiento de los sistemas y detectar posibles amenazas cibernéticas, esto permite identificar eventos que puedan en algún momento ser un indicador de compromiso, además da la posibilidad de que qué en caso de un incidente se pueda realizar acciones de forense para identificar patrones y establecer la ruta del incidente.

Este proceso plantea la implementación de herramientas para la recolección y almacenamiento de registro, en este momento el proceso se plantea para la recolección y almacenamiento de los registros de la solución de seguridad perimetral, para ello, se han identificado las siguientes tareas para poder llevar a cabo la implementación de este proceso:

1. **Identificación de activos:** Se identificarán los activos y los sistemas que generan logs en la red y de los cuales se puedan extraer. Se definirá también el método de recolección de los logs.

2. **Seleccionar la herramienta de recolección:** Se propondrán herramienta de recolección de logs que se ajusten a las necesidades del proceso. Se evaluarán las distintas herramientas y se seleccionará la más adecuada según lo requerido.

3. **Configuración de la herramienta seleccionada:** Se procederá a configurar la herramienta con las especificaciones del proceso, definiendo la frecuencia y el método de recolección de logs.

4. **Configuración del almacenamiento de logs:** Se definirán las políticas de almacenamiento, identificando la cantidad de espacio en disco necesario y el tiempo de retención de los logs. Se definirá también la ubicación de almacenamiento de los logs.

5. **Monitoreo y Análisis de logs:** Se realizarán pruebas de los registros obtenidos para garantizar el buen funcionamiento del proceso de recolección y almacenamiento de logs. También se implementará un proceso de monitoreo constante identificando la información que pueda ser relevante para su análisis, esto conllevará definir roles al personal del departamento para ejecutar las acciones definidas en el proceso.

En la siguiente tabla ya se han identificado algunas acciones que se estarán coordinando para reaccionar ante algún evento identificado a través de los logs que recibirán de la solución perimetral.

Avances

El avance para este proceso se concentrado específicamente en la identificación de herramientas, asi como la investigación para la instalación y configuración de estas mismas que permitan cumplir con los objetivos de los procesos planteados, para el este proceso, en este momento nos hemos centrado en los pasos 2 y 3.

1. **Seleccionar la herramienta de recolección:** Se propondrán herramienta de recolección de logs que se ajusten a las necesidades del proceso. Se evaluarán las distintas herramientas y se seleccionará la más adecuada según lo requerido.

Sobre Gray log

Se ha identificado la herramienta para poder avanzar con esta acción; Graylog es una plataforma poderosa que permite una fácil gestión de registros de datos estructurados y no estructurados junto con aplicaciones de depuración. Se basa en Elasticsearch, MongoDB y Scala. Cuenta con un servidor principal, que recibe datos de sus clientes instalados en diferentes servidores, y una interfaz web, que visualiza los datos y permite trabajar con registros agregados por el servidor principal.

Graylog es efectivo cuando se trabaja con cadenas en bruto (es decir, syslog): la herramienta lo analiza en los datos estructurados que necesitamos.

La principal ventaja de Graylog es que proporciona una única instancia perfecta de recopilación de registros para todo el sistema.

Es importante mencionar que la versión que se evaluara cuenta con una versión open source, la cual proporciona la funcionalidad central de administración de registros centralizados que necesita para recopilar, mejorar, almacenar y analizar datos. El soporte es a través de los recursos en línea, la comunidad y otros grupos abiertos de Graylog.

GrayLog cuenta también con una versión comercial que permite generar reportes y agregar módulos para la correlación de seguridad identificando amenazas a través de patrones anómalos.

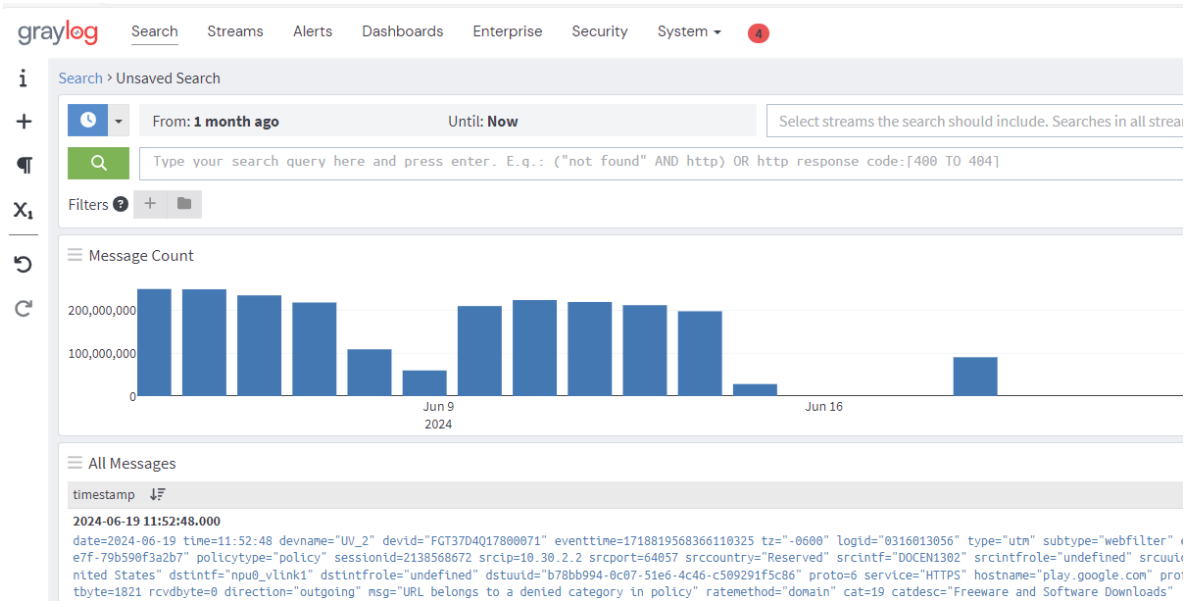
Se ha tomado como referencia el sitio oficial de la herramienta para el análisis y la implementación.

https://www.graylog.org/

Evidencias

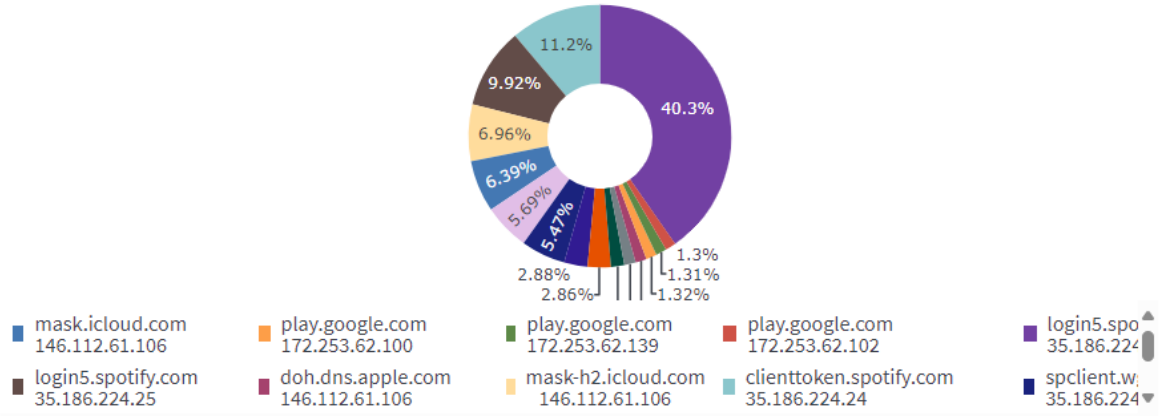
- Se ha instalado la versión libre sobre un servidor con el que cuenta el departamento, se ha instalado sistema operativo y la versión de gray log que soporta el servidor, Se trabaja en la configuración de la herramienta.

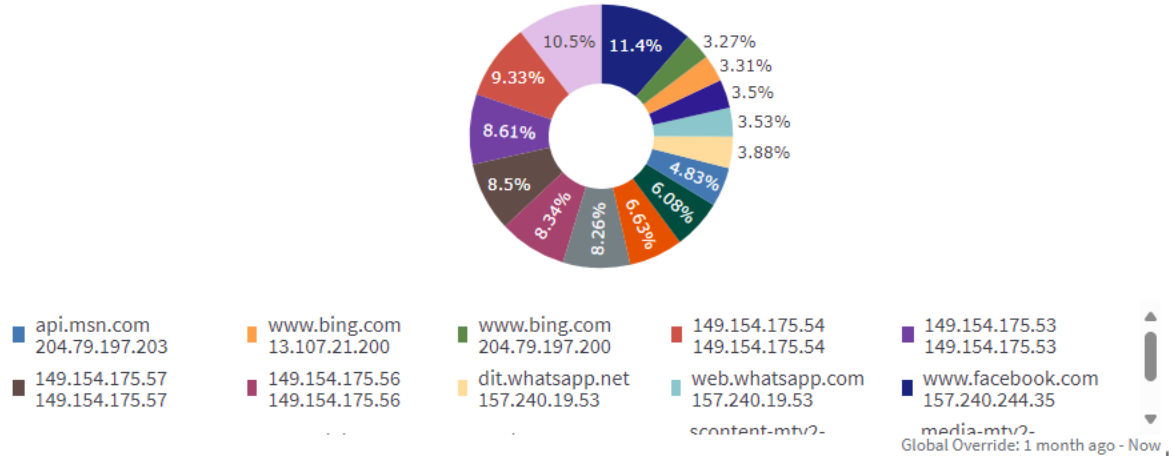
- Se ha establecido la configuración para poder recibir los registros de la solución de seguridad perimetral, actualmente se reciben todos los registros y se aplicaron configuraciones en el servidor donde se aloja esta solución para mejorar la gestión de todos los registros que se están recibiendo, tanto para almacenarlos como para poder recuperarlos y visualizarlos a través de la herramienta.



- Para poder almacenar los datos se realizó una configuración de red para poder hacer uso de una unidad de almacenamiento y ahí enviar en tiempo real los registros recibidos, esto permitirá resguardarlos y realizar búsquedas de 1 mes atrás.

- Con los registros obtenidos se personalizaron varias visualizaciones o desbordas específicos para correlacionar datos y obtener información precisa al momento de buscar indicadores maliciosos que pudieran comprometer la red.





- Se creó manual de instalación y configuración para la administración de la solución.

TLP:AMBER

Instalación y configuración de Graylog.

UV-CISRT

TLP:AMBER

Índice