Inteligencia local en un centro de operaciones de cyber-seguridad

Valentín Reviglio[1] y Pablo Frias[1]

[1]McAfee, Av La voz del interior, 7000, Córdoba, Argentina. TE: +54 351 5541200
{Valentin_ReviglioCanepa, Pablo_Frias}@McAfee.com
http://www.mcafee.com

Abstract. Todas las organizaciones están constantemente expuestas a diversas amenazas informáticas. Aunque existen herramientas de detección, mitigación y respuesta ante incidentes, resulta de vital importancia el contar con un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés) que permita realizar un análisis más profundo de los diferentes eventos que ocurran. Se propone integrar un conjunto de herramientas existentes con el propósito de brindar a los analistas de seguridad, un instrumento adicional para cumplir con las responsabilidades que implica su rol.

Keywords: Seguridad, SOC, analista de seguridad, trabajo de pasantía.

1 Introducción

El manejo de la Seguridad Informática involucra no sólo herramientas de detección, sino también de análisis forense para poder determinar el contexto de la ejecución de un evento de seguridad, como puede ser la ejecución de un archivo malicioso o un ataque direccionado por parte de un individuo.

Existen diversos productos que proporcionan herramientas para los analistas de seguridad dentro del SOC que, trabajando individualmente resultan útiles para el cumplimiento de las tareas del rol. Lo que se propone en este trabajo de investigación es que, integrar dichas soluciones permite potenciar los servicios que las mismas facilitan.

Para el desarrollo de este trabajo se analizaron tres productos orientado a la seguridad informática: McAfee Threat Intelligence Exchange (TIE) [4], The Hive Project [7] y Cortex [8]. A partir de esto se planteó integrar estas tres tecnologías.

En la sección "*Desarrollo"* del trabajo se explicará cual es la función y que valor se espera que agregue cada una de las tecnologías mencionadas. También, se mostrará que posición se tomó para implementar la integración entre ellas y como interactuará un analista de seguridad con el resultado final. En la sección "Conclusión y siguientes pasos", se determinará si efectivamente al integrar los productos propuestos se logró obtener una solución que facilite el desarrollo de las tareas de los analistas de sistemas dentro de un SOC. También, definiremos con que otras herramientas se pueden seguir integrando el producto final, para potenciar sus funcionalidades.

Este trabajo se realizó como parte de la pasantía en la empresa McAfee que realizo Valentín Reviglio durante sus estudios de 5º año de la carrera de Ingeniería en Sistemas de Información de la Universidad Tecnológica Nacional, Facultad Regional de Córdoba.

2 Desarrollo

Contexto

El objetivo principal de esta integración es facilitar las tareas de un analista de seguridad y brindar información adicional de contexto para el cumplimiento de las funciones de su rol. Para tener una mejor comprensión de para quien está pensado esta unificación, es necesario saber que es un analista de seguridad y cuáles son las funciones del rol.

Un analista de seguridad es aquella persona responsable de identificar y corregir errores en el sistema de seguridad de la organización para la que trabaja. Está a cargo de asegurar y proteger los activos digitales de la empresa contra el acceso no autorizado. Tiene como responsabilidad encontrar y eliminar los riesgos antes de que se produzcan ataques, y en caso de que se produzcan él es el encargado de contrarrestar los mismos [12]. Resulta interesante tener en cuenta lo que plantea P. A. Legg en su ensayo *"Por lo*

tanto, los analistas de seguridad requieren herramientas sofisticadas que les permitan explorar e identificar la actividad de los usuarios, que puede llegar a ser un indicador de una amenaza inminente para la organización" [13] (traducido por el autor del presente trabajo) ya que demuestra con claridad la importancia que tienen las herramientas para facilitar la labor del analista, exponiendo el valor del trabajo propuesto.

McAfee TIE Server provee la capacidad de responder a diferentes actores acerca de la reputación de uno o más archivos o certificados, generando una forma de detección temprana de amenazas en una organización. Mediante mecanismos de comunicación encriptados a través de la plataforma McAfee Open Data Exchange Layer (OpenDXL) [6], es posible realizar consultas al sistema, a través de la identificación de archivos y certificados con funciones hash.

Cuando una alerta de seguridad ocurre en una organización, el SOC recibe el evento y genera un caso de investigación. Este proceso puede llevarse a cabo usando la plataforma open-source The Hive Project como respuesta a incidentes. Dentro de esta plataforma, se encuentra el módulo servidor Cortex, que brinda mecanismos para realizar análisis sobre distintos aspectos del incidente. Este servicio es de vital interés para la integración de McAfee TIE Server a la plataforma, que se desarrollará en la definición de la arquitectura.

Para poder llevar a cabo esta integración se tomó como referencia los analizadores de VirusTotal y de FileInfo que ya estaban integrados a la plataforma de The Hive.

Flujo de Trabajo

Se plantea la necesidad de que todo analista de seguridad pueda obtener información detallada del incidente que investiga, para poder llevar a cabo un análisis y poder establecer el grado de severidad del incidente y en caso de ser una amenaza concreta, determinar qué medidas tomar para la prevención, mitigación o eliminación de la misma.

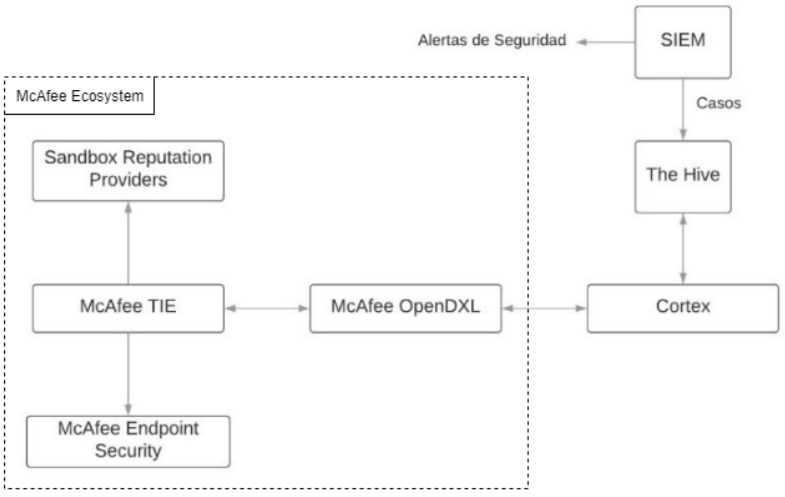

Fig. 1. Diagrama de los módulos participantes en la solución propuesta

Para poder comprender como se daría el flujo de trabajo una vez que se lleve adelante esta integración es necesario comprender como funciona el ecosistema de productos McAfee.

En primer lugar, es necesario saber de dónde obtiene la reputación de un archivo el componente TIE Server. Para poder comprender esto, se debe entender la utilidad del componente 'Sandbox Reputation Providers'. Este módulo es una de las principales fuentes de reputación de archivos de TIE. Consiste en un entorno autoadministrado de virtualización en donde, bajo condiciones controladas, se puede ejecutar un archivo y realizarle análisis extras con el fin de determinar, bajo ciertas reglas si el archivo es malicioso o no generando un índice de reputación.

Sin embargo, el potencial del producto TIE Server no está simplemente en determinar si un archivo es malicioso o no, sino también en conocer las condiciones de entorno en el que se ejecutó dicho archivo. La fuente de esta información es el módulo McAfee Endpoint Security (ENS), que es un agente instalado en cada uno de los sistemas a ser protegidos. Es el encargado de, a la hora de ejecutar un archivo, realizar una serie de análisis con el objetivo de determinar una reputación local y permitir o no la ejecución del archivo en cuestión. En caso de no poder determinar una reputación concreta, ENS delegara la responsabilidad de determinar dicha reputación al componente TIE Server. Generando un servicio de seguridad inteligente dedicado para toda la compañía.

Por otro lado, un sistema SIEM (Security Information and Event Management) permite realizar análisis de seguridad en tiempo real y genera alertas cuando detecta incidentes que pueden ser interpretados como amenazas dentro de la red [11]. Cuando esto ocurre, el sistema SIEM de la organización generará alertas para informar al analista del evento sucedido. La plataforma de The Hive proporciona herramientas para el manejo de eventos, permitiendo a los analistas generar casos de investigación. Estos últimos son la función troncal de The Hive, cada caso puede ser desglosado en una o más tareas. A su vez la plataforma proporciona la posibilidad de crear plantillas de estos casos para establecer un protocolo de acción ante eventos similares. El analista puede asignar uno o más observables a cada caso creado. Los observables son elementos que se desean analizar, y que se supone el analista considera relevantes e importantes para examinar.

Los incidentes y las amenazas dentro de la red se pueden dar por diferentes factores como pueden ser direcciones IP, URLs, mails, archivos, entre otras cosas, que sean desconocidos o que el sistema reconozca como potencialmente peligrosos [15]. Esto significa que las herramientas deben proveer información acerca de los factores que se reconocen como amenazas. El módulo Cortex integra un grupo de analizadores [10] que son programas que toman el factor a observar y datos de configuración como entrada, analizan el factor en cuestión y proporcionan información del mismo.

Para poder integrar McAfee TIE Server con Cortex se propuso crear un analizador de archivos que, usando McAfee OpenDXL como mecanismo de comunicación, permita obtener información del archivo en cuestión. Para el desarrollo del mismo, se utilizó el lenguaje de programación Python y la librería cortexutils, la cual facilita el desarrollo de los analizadores y también proporciona métodos para darle el formato esperado por The Hive a la salida. Para poder cumplir dicho objetivo se tomó como referencia el analizador llamado VirusTotal, el cual brinda dos enfoques diferentes. Por un

lado, VirusTotal [14] tiene la capacidad de analizar un archivo, hash, dominio o dirección IP a través de una URL y devolver los resultados de dicho análisis, pero también nos permite obtener el último reporte de un análisis que se hizo previamente.

La ventaja que ofrece una integración con McAfee TIE Server frente al resto de los analizadores es que no solo brinda información y la reputación del archivo, sino que también nos proporciona información sobre el contexto en el que se ejecutó el archivo dentro de la organización. De esta manera se logra proveer al analista acceso a la información proporcionada por el ecosistema de los productos McAfee.

Arquitectura de la Solución

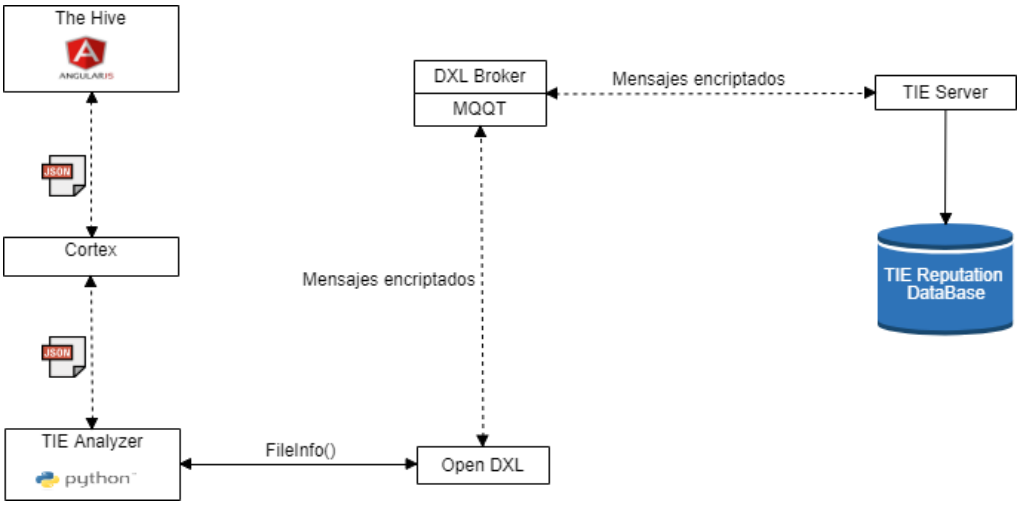

Fig. 2. Diagrama de arquitectura de la solución propuesta

Cortex ejecuta el programa central que hace a la funcionalidad del analizador, es decir el programa que se encarga de ejecutar las acciones necesarias para obtener información del factor que se está analizando. Para indicarle al analizador cual es el factor que se desea observar, Cortex le proporciona como entrada una estructura JSON con diferentes porciones de información.

Para poder comunicarse con McAfee TIE Server el analizador va a usar el contrato de McAfee Data Exchange Layer (DXL) [5]. Este último es un servicio de mensajería segura y rápida entre aplicaciones que es utilizado para establecer las bases de comunicación entre los productos McAfee. En este caso el módulo de McAfee DXL es el que permite al analizador solicitar la información del archivo de forma segura a McAfee TIE Server.

Finalmente, la salida de los analizadores consiste en una estructura JSON con un formato estandarizado.

Cortex devuelve estos resultados a The Hive. Esta última cuenta con un motor de plantilla de informes que permite adaptar la salida que Cortex le proporciona y mostrarla de forma más elegante. A la hora de crear un nuevo analizador The Hive permite agregar plantillas HTML para los reportes, de esta manera los analistas pueden observar la salida del analizador en cuestión en un formato que es más fácil de leer.

3 Conclusión y próximos pasos

Al finalizar este informe se pudo demostrar que tanto Cortex y The Hive son sumamente útiles para los analistas de seguridad del SOC, ya que el primero integra un conjunto de analizadores que le permiten a los miembros del SOC obtener información de algún factor que está provocando un incidente. Mientras que el segundo proporciona herramientas para la gestión de las actividades que debe llevar a cabo un analista de seguridad ante un determinado incidente.

Sin embargo, como se ha planteado, integrar estas tecnologías con McAfee TIE Server potencia las capacidades de la plataforma, ya que permite acceder a la información captada por todos los productos McAfee, generando un ecosistema que se retroalimenta con información tanto interna de la organización como externa de herramientas de código abierto.

Además, también se demostró que es posible cambiar la dinámica de la seguridad de una organización integrando productos McAfee externos a la organización permitiendo un análisis de seguridad colaborativo.

Esta integración entre McAfee TIE Server, la plataforma de The Hive y Cortex es simplemente una pequeña parte de lo que se puede hacer usando estas tecnologías. En un futuro se podría integrar el sistema SIEM con The Hive, logrando que cuando el primero detecte posibles riesgos dentro de la red le envié alertas a la plataforma de The Hive y a través de esta última y a partir de dichas alertas, generar casos de investigación.

4 Referencias

1. C. Onwubiko, *"Security operations center: Situation awareness, threat intelligence and cybercrime"* 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), London, 2017, pp. 1-6
2. N. Miloslavskaya, *"Security Operations Centers for Information Security Incident Management"* 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, 2016, pp. 131-136.
3. Abe Chin-Ching Lin, Hsing-Kuo Wong and Tzong-Chen Wu, *"Enhancing interoperability of security operation center to heterogeneous intrusion detection systems"* Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology, 2005, pp. 216-221.
4. McAfee LLC, *"McAfee Threat Intelligence Exchange"* [en línea]. Recuperado de: https://www.mcafee.com/es/products/threat-intelligence-exchange.aspx
5. McAfee LLC, *"Data Exchange Layer"* [en línea]. Recuperado de: https://www.mcafee.com/es/solutions/data-exchange-layer.aspx
6. McAfee LLC, *"Introduction to OpenDXL"* [en línea]. Recuperado de: "https://www.opendxl.com/index.php?article/11-introduction-to-opendxl/"
7. The Hive Project (2018), *"The Hive"* [en línea]. Recuperado de: https://www.github.com/TheHive-Project/TheHive
8. The Hive Project (2018), *"Cortex"* [en línea]. Recuperado de: https://www.github.com/TheHive-Project/Cortex
9. The Hive Project (2018), *"How to Write and Submit an Analyzer"* [en línea]. Recuperado de: https://www.github.com/TheHive-Project/CortexDocs/blob/master/api/how-to-create-an-analyzer.md
10. The Hive Project (2018), "Cortex Analyzers" [en línea]. Recuperado de: https://github.com/TheHive-Project/Cortex-Analyzers
11. Wikipedia (2018), *"Security information and event management"* [en línea]. Recuperado de: https://www.wikipedia.org/wiki/Security_information_and_event_management
12. Zhang Ellen (2017), *"What is a security analyst? Responsibilities, qualifications, and more"* [en línea]. Recuperado de: https://digitalguardian.com/blog/what-security-analyst-responsibilities-qualifications-and-more
13. P. A. Legg, *"Visualizing the insider threat: challenges and tools for identifying malicious user activity"* 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), Chicago, IL, 2015, pp. 1-7.
14. VirusTotal (2018), *"Advanced features & tools"* [en línea]. Recuperado de: https://www.virustotal.com/es-ar/
15. OWASP (2017), *"The Ten Most Critical Web Application Security Risks"*