Mejorando las capacidades de respuesta a incidente de las EPS mediante el uso de SOAR

Juan Pablo Daza Pinzón y Juan Sebastian Rodriguez Peña

Escuela Colombiana de Ingeniería Julio Garavito

Actualmente la ciberseguridad de las EPS es un tema en auge, se han realizados varios ataques que han dejado ver la facilidad y lo vulnerables que son los sistemas de estas entidades en Colombia, los recientes ataques a diferentes entidades dejan ver que existe una falta de reconocimiento en la importancia de la ciberseguridad y su buena implementación. Para fortalecer el sistema de las EPS queremos demostrar el funcionamiento de un buen SOAR (Security Orchestation, Automation and Response) y los beneficios que brindaría a las EPS para mantener los datos de los usuarios seguros y disponibles para su consulta.

I. Introducción

La ciberseguridad es un aspecto clave para garantizar la protección de la información y la continuidad de los servicios de las entidades prestadoras de salud (EPS) en Colombia. Sin embargo, el sector salud ha sido blanco de numerosos ataques cibernéticos que han afectado la confidencialidad, integridad y disponibilidad de los datos de los usuarios, así como el funcionamiento de los sistemas informáticos. Ante este escenario, se hace necesario adoptar medidas que permitan prevenir, detectar y responder a las amenazas cibernéticas de forma eficiente y efectiva. En este sentido, el SOAR es una solución que integra herramientas, procesos y equipos de seguridad para automatizar y orquestar las acciones de defensa cibernética, reduciendo el tiempo de respuesta y mejorando la capacidad de reacción. El objetivo de este trabajo es demostrar el funcionamiento de un buen SOAR y los beneficios que brindaría a las EPS para fortalecer su sistema de ciberseguridad. [1]

II. Estado del arte

i. Historia del SOAR

El SOAR nace como una respuesta a la sobrecarga de los SIEM (Security Information and Event Manager), estos se veían con demasiados eventos o alertas, complejidad y duplicación de herramientas y así, los mismos fabricantes se pusieron en la labor de desarrollar herramientas para automatizar tareas con el objetivo de facilitar la gestión de incidentes.

El termino SOAR nace en 2017 cuando la empresa Gartner, la cual es una empresa consultora y de investigación de TI que presta servicios de gestión de la información, entre otros, empezó a describir una nueva categoría emergente de plataformas para la respuesta a incidentes, la automatización de la seguridad, la gestión de casos y otras herramientas de seguridad. [2]

Estas plataformas denominadas SOAR se crearon para ayudar a los equipos de seguridad a administrar y responder a las amenazas con la ayuda de la automatización.

ii. Definición de SOAR

El SOAR hace referencia a tres funciones clave del software, la gestión de los casos y flujos de trabajo; la automatización de las tareas; y un método centralizado para acceder a la información sobre las amenazas. [3]

El principal objetivo de un SOAR es la optimización de los flujos de trabajo dentro y fuera del centro de operaciones de seguridad (SOC), lo que permite a los analistas centrar sus

esfuerzos en proteger el ecosistema de su organización.

iii. Beneficios de la implementación de un SOAR

Los ciberataques son mas comunes que nunca, y cada vez son mas sofisticados que nunca, esto está causando que muchas organizaciones destinen más recursos a la ciberseguridad de sus negocios.

Aunque exista mas presupuesto para proteger los activos, no ha sido suficiente ante las contantes amenazas que existen hoy en día. Se generan demasiadas alertas de seguridad ralentizando los SOC (Security Operations Center) y responder a todas estas alertas es una tarea laboriosa y conlleva mucho tiempo y aquí es donde entran los SOAR.

La tecnología SOAR ofrece un sistema que logra identificar automáticamente las vulnerabilidades y responde a ellas sin necesidad de intervención humana. Además, cada organización puede definir y establecer como desea reaccionar a un evento, lo que permite liberar tiempo y presupuesto para centrarse en proyectos más prioritarios. [4]

iv. Empresas lideres

Las grandes empresas de software destinan muchos recursos al desarrollo de herramientas destinadas a la ciberseguridad, por ejemplo:

- Microsoft: Tiene a su disposición SIEM y XDR [5]
- IBM: Presta su servicio con IBM Security QRadar SOAR [6]
- Red Hat: Utiliza un software opensource llamado Red Hat Ansible Automation Platform [3]
- Amazon: Dentro de sus módulos ofrece Amazon GuardDuty [7]

III. Situación de las EPS

El sistema de salud en nuestra nación se ha convertido en un tema de gran controversia, especialmente debido a las extensas esperas para obtener citas médicas y las largas filas para obtener documentos esenciales. Agravando aún más esta situación, se encuentra la problemática que detallamos en este documento: nuestros servicios de salud han caído víctimas de ciberataques.

Un ejemplo de este más relevante es el ataque que fue realizado a la EPS Sanitas [8] en Colombia. En el cual el grupo Ransomhouse, logro vulnerar el sistema impuesto por el grupo Keralty, el cual es contratado por sanitas para alojar sus datos digitalmente, este ciberataque dio paso en noviembre del 2022 [9] y dio como resultado la filtración de datos personales de pacientes y empresas con las cuales sanitas hizo negociaciones, entre los datos que se filtraron se pueden encontrar documentos personales, historial médico, entre otros. Esta situación da lugar a que las personas tengan que soportar aún más demoras para acceder a los servicios que la EPS ofrece, y obligo a que muchos profesionales de la salud, que en el pasado habían optado por la digitalización de su trabajo, a volver a métodos antiguos, como el uso del papel [8].

Esto representa un problema multifacético porque involucra datos sensibles, la continuidad en la atención medica e incluso la atención en los centros médicos, por lo cual se debe abordar para así garantizar a los usuarios integridad, confidencialidad y disponibilidad de la información de la salud en el país.

IV. Implementación del SOAR para la seguridad de la información

Vamos a simular la infraestructura de una EPS e implementar el modelo SOAR, para mejorar la seguridad, la información y la capacidad de respuesta ante los incidentes de seguridad.

Desarrollaremos esta infraestructura en amazon e implementaremos Amazon GuardDuty.

Utilizaremos un WAF para proteger la aplicación de las peticiones HTTP maliciosas y su respectivo control para no permitir su acceso al servidor principal que va a mantener la página web principal. Es necesario el uso de un servidor como fachada para mostrar a los usuarios diferentes servicios que ofrezca la organización con la finalidad de separar los ambientes donde entraran cualquier usuario y otro donde los usuarios necesitaran pasar por una autenticación para poder acceder a los servicios de cada usuario.

Utilizaremos funciones Lambda con la finalidad de agilizar el proceso de recibir las peticiones que quieran ingresar al portal de los usuarios y definir que se hace con estas, toda petición pasara por IAM para poder identificar a cada usuario, y a su vez GuardDuty se encargara de registrar el ingreso. En caso de que se requiera GuardDuty podrá poner en una lista negra las IP de donde provengan peticiones maliciosas o un gran numero de peticiones, con la finalidad de minimizar la perdida de disponibilidad e integración de los servicios.

Por último, una vez el usuario acceda de manera correcta a su portal entonces podrá realizar la búsqueda de su información en la base de datos, como restricción cada usuario solo podrá buscar su propia información y no consultar la de otros.

V. Pruebas de concepto

Como primera intención queremos intentar probar si GuardDuty puede responder a ataques de tipo inundación, por lo tanto, enviaremos muchas peticiones de conexión con la finalidad de que GuardDuty ponga la IP en la lista negra e informe al WAF de que no reciba más peticiones desde esa IP.

VI. Conclusiones

- El SOAR es una solución que permite mejorar la gestión de la seguridad cibernética en las EPS, al integrar las diferentes fuentes de información, automatizar las tareas repetitivas y orquestar las acciones de respuesta a incidentes.

- Con el uso del SOAR se logra optimizar los recursos humanos y técnicos disponibles, al reducir la carga de trabajo manual y aumentar la productividad y la eficiencia de los analistas de seguridad.

- Con la implementación de mejora la protección de los datos de los usuarios y la continuidad de los servicios de salud, al disminuir el impacto y la duración de los ataques cibernéticos, así como el riesgo de pérdida o filtración de información sensible.

- Es una inversión rentable para las EPS, ya que genera un retorno positivo al reducir los costos asociados a los incidentes de seguridad, mejorar la reputación y la confianza de los usuarios y aumentar la competitividad y el valor agregado del sector salud.

Referencias

[1] IBM, "IBM," [Online]. Available: https://www.ibm.com/mx-es/topics/security-orchestration-

automation-response. [Accessed 8 Septiembre 2023].

[2] A. d. P. Medina, "Universitat Oberta de Catalunya," junio 2021. [Online]. Available: https://openaccess.uoc.edu/bitstream/10609/132128/7/adelpinomeTFM0621memoria.pdf. [Accessed 15 septiembre 2023].

[3] "Red Hat," 11 Mayo 2022. [Online]. Available: https://www.redhat.com/es/topics/security/what-is-soar. [Accessed 15 Septiembre 2023].

[4] "Microsoft," [Online]. Available: https://www.microsoft.com/es-co/security/business/security-101/what-is-soar#:~:text=La%20tecnología%20SOAR%20(orquestación%2C%20automatización,procesos%20relacionados%20con%20la%20seguridad.. [Accessed 15 Septiembre 2023].

[5] "Microsoft," [Online]. Available: https://www.microsoft.com/es-co/security/business/solutions/siem-xdr-threat-protection. [Accessed 15 Septiembre 2023].

[6] "IBM," [Online]. Available: https://www.ibm.com/es-es/products/qradar-soar. [Accessed 15 Septiembre 2023].

[7] "Amazon," [Online]. Available: https://aws.amazon.com/es/guardduty/. [Accessed 15 Septiembre 2023].

[8] infobae, "Infobae," Noticias, 21 12 2022. [Online]. Available: https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/#:~:text=Sanitas%20sufrió%20un%20ataque%20cibernético,Promotora%20de%20Salud%20(EPS).. [Accessed 15 09 2023].

[9] L. Benito, "Infobae," Noticias, 14 03 2023. [Online]. Available: https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/. [Accessed 15 09 2023].

[10] Wikipedia, "Wikipedia," 12 enero 2023. [Online]. Available: https://es.wikipedia.org/wiki/Gartner_(empresa). [Accessed 15 septiembre 2023].

[11] "elastic," [Online]. Available: https://www.elastic.co/es/what-is/soar. [Accessed 15 Septiembre 2023].