EL SOC "AUTÓNOMO": INTELIGENCIA ARTIFICIAL PARA LA NUEVA CIBERSEGURIDAD

THE "AUTONOMOUS SOC": ARTIFICIAL INTELLIGENCE FOR THE NEW CYBERSECURITY

Autores:

Tomas Serna Navarro. Junta de Comunidades de Castilla-La Mancha. tserna@jccm.es

Antonio Gonzalez Guerrero. Junta de Comunidades de Castilla-La Mancha. agonzalezg@jccm.es

Resumen:

En el marco del Esquema Nacional de Seguridad, se presenta la estrategia de seguridad de la información de la Administración Regional de Castilla-La Mancha cuyos ejes son: el refuerzo del sistema de seguridad, el desarrollo de una cultura de seguridad y la modernización de nuevos servicios de ciberseguridad, destacando la aplicación de la Inteligencia Artificial orientada a la evolución hacia un "SOC autónomo".

Abstract:

The information security strategy of the Regional Administration of Castilla-La Mancha is presented within the framework of the National Security Scheme. The axes of this strategy are: the reinforcement of the security system, the development of a security culture and the modernization of new cybersecurity services, highlighting the application of Artificial Intelligence oriented to the evolution towards an "autonomous SOC".

Palabras clave:

Centro de operaciones de seguridad; Ciberseguridad; Seguridad de la información

Keywords:

Security Operations Center; Cibersecurity; Information Security

INTRODUCCIÓN

Las Administraciones Públicas deben crear las condiciones necesarias de confianza en el uso de los medios electrónicos a través de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, permitiendo a la ciudadanía y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Hoy día la Administración se encuentra inmersa en un proceso de transformación digital que además de la aplicación y el uso de tecnologías emergentes está empujando a un cambio organizacional y cultural.

Este proceso de transformación digital proporciona innumerables oportunidades de futuro, oportunidades que a su vez están ligadas a determinados desafíos ante los que las Administraciones no pueden permanecer ajenas.

Uno de estos desafíos es el de la seguridad tal y como se recoge en la actual Estrategia de Seguridad Nacional, donde junto con el contexto geopolítico, el entorno socioeconómico y la transición ecológica, la transformación digital figura como uno de los principales vectores de transformación.

Las sociedades hiperconectadas, las tecnologías disruptivas, el dato como recurso estratégico de primer orden, así como la soberanía digital son realidades que conllevan que determinados riesgos se vean amplificados.

Esto hace necesario incrementar las capacidades tecnológicas, humanas y económicas dirigidas a la prevención, detección, respuesta, recuperación, investigación y defensa activa para garantizar el uso seguro y fiable del ciberespacio.

La ciberseguridad es un factor crítico en la generación de confianza digital y en el aseguramiento de las operaciones digitales, por lo que se configura como un eje imprescindible para la transición digital.

Los ciberincidentes se incrementan de forma exponencial y son cada vez más complejos y sofisticados. En un entorno interconectado y global, en el que los organismos públicos están cada vez más digitalizados, la correcta gestión de riesgos y la estrategia en ciberseguridad se convierten en elementos cruciales de cara al futuro.

En este trabajo se presenta la interconectividad y la automatización del conocimiento de inteligencia de ciberseguridad aumentado con *machine learning* y análisis de *big data*, para convertir el conocimiento de la inteligencia de ciberseguridad en una estrategia de ciberdefensa predecible y proactiva como una opción realista y de futuro para la seguridad en las organizaciones.

ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN

La línea estratégica de seguridad de la información de toda Administración Pública debe sustentarse en la plena adopción del Esquema Nacional de Seguridad que está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados, para asegurar el acceso, confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen las administraciones públicas en el ejercicio de sus competencias.

El Esquema Nacional de Seguridad concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, con frecuencia, este punto es la coordinación entre medidas individualmente adecuadas, pero deficientemente acopladas.

Destacan entre sus objetivos, crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, promover la gestión continuada de la seguridad, promover la prevención detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques, promover un tratamiento homogéneo de la seguridad que

facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades y servir de modelo de buenas prácticas.

ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN REGIONAL DE CASTILLA-LA MANCHA

La estrategia de seguridad de la información de la Administración Regional de Castilla-La Mancha se define en su Plan Director de Seguridad y se fundamenta en los siguientes tres ejes principales:

- **Refuerzo del sistema de gestión de seguridad de la información.**
  Se apuesta por potenciar y ampliar el sistema de gestión de seguridad de la información implantado en la actualidad ya que proporciona un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de la organización. Este sistema de gestión de seguridad de la información se encuentra certificado en el Esquema Nacional de Seguridad y en la Norma UNE-EN ISO/IEC 27001:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.

- **Desarrollo de cultura de seguridad.**
  Los esfuerzos asociados a este eje están encaminados a mejorar la concienciación, formación y capacitación del personal en seguridad de la información con el objetivo de desarrollar una correcta cultura de ciberseguridad que permeabilice en toda la organización.

- **Modernización e impulso de nuevos servicios de ciberseguridad.**
  Adopción de nuevos servicios de ciberseguridad que permitan mejorar la capacidad de prevención, detección, respuesta, recuperación y resiliencia a los posibles incidentes de seguridad.

Es dentro de estos nuevos servicios donde se encuentra la aplicación de la Inteligencia Artificial en la ciberseguridad.

INTELIGENCIA ARTIFICIAL EN LA ESTRATEGIA DE CIBERSEGURIDAD

La implicación de la IA en la ciberseguridad tiene cuatro objetivos básicos:

1. **Gestión masiva de información:** priorizando qué situaciones y ataques tienen prioridad de gestión y cuáles son falsas amenazas, desbloqueando la carga de trabajo de los sistemas y analistas.

2. **Respuesta en tiempo real:** la IA permite tomar acción inmediata como respuesta a los ataques para minimizar riesgos, basándose en infinidad de datos y de contexto.

3. **Automatización:** automatización de respuesta a muchas de las amenazas, minimizando su coste en cuanto a detección y respuesta (SOAR).

4. **Predicción:** la IA ayuda a un mejor análisis forense de ataques previos, lo que se traduce en una mejora de las defensas.

Para implementar IA en la estrategia de ciberseguridad, se debe disponer de un plan que debe contar con las siguientes etapas:

1) **Creación de una plataforma de datos**: identificar fuentes de datos y crear plataformas para poner en funcionamiento la IA (*Data Lake*).

2) **Selección de casos de uso de alto impacto:** seleccionar un conjunto de casos de uso relevantes para acelerar y maximizar los beneficios.

3) **Mejora de la inteligencia de amenazas**: colaborar con partners estratégicos para mejorar la inteligencia de amenazas.

4) **Implementación de SOAR:** implementar orquestación de seguridad, automatización y respuesta para mejorar la gestión de la seguridad.

5) **Formación a ciberanalistas**: capacitar a los analistas cibernéticos para que dominen la IA.

6) **Gobernanza eficaz:** establecer un modelo de administración de la IA en ciberseguridad para ofrecer mejoras a largo plazo de forma transparente y ética.

Como puntos relevantes nos centraremos en el aporte del aprendizaje automático a la ciberseguridad, el marco tecnológico necesario para su implantación y su aplicación a un SOC (Security Operations Center) “autónomo”.

APLICACIÓN DEL APRENDIZAJE AUTOMÁTICO A LA CIBERSEGURIDAD

Entre los casos de uso de ML (Machine Learnig) más valiosos en ciberseguridad podemos destacar:

— **Predicción de nuevos patrones de Indicadores de Compromiso (IoC)**: descubrir nuevos IoC aplicando modelos de aprendizaje profundo sobre grandes conjuntos de datos. Estos modelos pueden aprender las características de los patrones maliciosos (por ejemplo, firmas de *malware*, URL incorrectas y patrones de detección de intrusiones). Cuantos más datos haya disponibles, mejor será la capacidad de detección de IoC con el tiempo. Por ejemplo, al proporcionar miles de ejemplos de URL maliciosas y no maliciosas conocidas, usando algoritmos de inteligencia artificial se puede extraer características clave de estas URL para construir modelos que puedan discernir posibles URL maliciosas frente a no maliciosas.

— **Detección de intrusiones mediante UEBA**: al emplear inteligencia artificial, las desviaciones del comportamiento normal se pueden extraer en tiempo real y evaluar mediante algoritmos de aprendizaje automático. Los algoritmos de UEBA comparan el comportamiento actual con el estándar, detectan anomalías aplicando algunas reglas (por ejemplo, día de la semana inusual, hora del día, volumen o país para un usuario), ensamblan anomalías y agregan el riesgo de todas las anomalías detectadas (agregación de riesgo de entidad). Los algoritmos de UEBA reducen los falsos positivos, priorizan las alertas de seguridad y mejoran la eficiencia del SOC.

— **Descubrimiento de nuevos TTP (Técnicas, Tácticas y Procedimientos de ataques)**: proporcionar información sobre los perfiles de los grupos de ataque inspeccionando los patrones históricos y predecir posibles actividades futuras.

La idea es abordar los desafíos de seguridad modernos prediciendo o reaccionando a las amenazas a la seguridad en tiempo real o casi real y produciendo una predicción de riesgo cibernético para priorizar los recursos para abordarlo. Esto se puede lograr utilizando el aprendizaje automático (ML), el análisis de macrodatos y los *playbooks* de respuestas automatizadas.

MARCO TECNOLÓGICO DE LA ESTRATEGIA DE CIBERSEGURIDAD

Como base fundamental del marco tecnológico de ciberseguridad se encuentra el *data lake* corporativo. El *data lake* ingiere datos de seguridad y no seguridad procedentes de diferentes fuentes internas o externas. Cuantos más datos se dispongan de diferentes fuentes mejor predicción de seguridad e información sobre las amenazas emergentes dentro y fuera del organismo. Los datos pueden adoptar la forma de alertas, registros, información de incidentes, registros de acceso a aplicaciones, procesos de *endpoint*…

Se debe enriquecer continuamente los conocimientos de inteligencia de amenazas de la organización interconectándose con fuentes de amenazas externas o internas aumentadas con capacidades de respuesta predictiva y automatizada. Impulsado por el análisis de *Machine Learnig* y *big data* sobre los grandes conjuntos de datos ingeridos en la capa de agregación de datos, el objetivo principal es actualizar continuamente las tácticas, técnicas y procedimientos (TTP), así como los indicadores de compromiso (IoC) en tiempo real o como resultado de un procesamiento por lotes. Por lo tanto, el conocimiento de la inteligencia de amenazas corporativa se enriquece continuamente con amenazas emergentes descubiertas, ataques en curso, nuevos IoC y TTP, nuevos algoritmos de detección de amenazas y *playbooks* de operaciones de seguridad actualizados.

La capa superior del marco es la capa SOAR. Impulsado por el conocimiento predictivo

e interconectado de inteligencia de amenazas de la capa anterior, permite a la organización orquestar y automatizar las operaciones de seguridad basadas en *workflows* (flujos de trabajo) y *playbooks*. La detección de amenazas de seguridad desde la capa de inteligencia de amenazas activa flujos de trabajo que involucran a los equipos *SecOps* del SOC y proporciona respuestas automatizadas o semiautomatizadas u orquestadas a eventos de seguridad.

LA NECESARIA EVOLUCIÓN DEL SOC HACIA LA AUTOMATIZACIÓN: SOC "AUTÓNOMO"

Cualquier organización actual de tamaño medio cuenta con miles de activos TI dispersos entre sus sedes y usuarios, los *data centers on-premise* y la nube pública. Y para la gestión de su seguridad despliega varias docenas de herramientas especializadas, cada una con su correspondiente consola, curva de aprendizaje y carga de gestión, que recae sobre los equipos de operación del SOC (SecOps). De media, cada SOC recibe 11.000 alertas diarias, de las cuales solamente el 17% están automatizadas, y la investigación de cada una requiere la consulta de 10 categorías de herramientas diferentes (Fuente: *Forrester Study: The 2020 State of Security Operations*).

No se trata de un problema reciente, el mercado de la *ciberseguridad* ya se dió cuenta hace tiempo y trató de resolverlo añadiendo una nueva herramienta a la pila, los SIEM (Security Information and Event Management), que prometían integrar y correlacionar las alertas de distintas fuentes, con el fin de facilitar por fin la gestión de los incidentes.

Sin embargo, pasados unos años ya desde su aparición, podría pensarse que no han cumplido sus objetivos ya que el problema no ha hecho más que acrecentarse conforme los volúmenes de datos y de alertas también se incrementan. De hecho, el tiempo medio de investigación de un incidente avanzado de seguridad es de más de 4 días.

¿Por qué? Porque los SIEM no consiguen simplificar las tareas de gestión y se han convertido, en la mayoría de los casos, en simples *ingestores* de *logs* desde múltiples fuentes, con poca o ninguna automatización, lo que hace que los equipos de seguridad

se sientan perdidos entre multitud de eventos de baja fidelidad e ignoren amenazas que sí son reales. De hecho, el citado informe de Forrester pone de manifiesto que el 28% de las alertas son ignoradas porque los equipos no son capaces de atenderlas al requerir una gran carga de intervención manual. Como consecuencia, el 79% de las organizaciones estudiadas sufrieron al menos una brecha de seguridad conocida durante el último año. Aun así, el mayor riesgo que han de afrontar los CISOs no son las propias brechas, sino el coste humano asociado al hartazgo de los equipos de *SecOps* debido a la fatiga por la gestión de demasiadas alertas y la realización de tareas rutinarias que, en general, son poco interesantes para un perfil de expertos de alto nivel, lo que se conoce como el síndrome de la silla giratoria.

Además de diversos problemas de salud, esta forma de trabajo bajo mucha presión y stress provoca que exista una gran rotación de este tipo de personal: el 25% de los ingenieros de *SecOps* cambia de trabajo en menos de dos años y el 67% lo hace al tercer año (Fuente: *The State of SOAR Report, 2018*):

Teniendo en cuenta que el 53% de los incidentes de respuesta (IR), se originan en el SIEM, es necesario incorporar procesos de automatización en estas herramientas que permitan liberar el tiempo de los valiosos recursos humanos de *SecOps*, para que realicen las tareas en las que aportan más valor y con las que se sienten más satisfechos principalmente *threat hunting* e implementación de procesos de mejora.

Por tanto, es lógico pensar en modificar el modo en el que opera un SOC para que sea capaz de partir de información de más valor para la ciberseguridad de la que ofrece un SIEM y automatizar la respuesta a incidentes, evolucionando a lo que denominamos SOC “autónomo”.

Desde el punto de vista tecnológico, el SOC autónomo se compone de dos piezas fundamentales: una herramienta XDR (detección y respuesta extendida) y una herramienta SOAR, que deben integrarse de manera nativa. De hecho, y de manera ideal, debería tratarse de una única herramienta, con una misma consola de gestión, que

simplifique las tareas de despliegue, integración y administración que han de realizar los equipos de *SecOps*.

La pieza XDR es la encargada de recoger todos los eventos de seguridad provenientes de la red, la nube y los *endpoints*, sobre los que aplica técnicas de analítica e inteligencia artificial al menos durante 30 días, para identificar de manera automática las amenazas que debe agregar sobre incidentes para que sea más sencillo su tratamiento. La pieza SOAR consume los incidentes que genera XDR y automatiza las tareas de enriquecimiento y respuesta en base a la utilización de *playbooks* (obtención de inteligencia de diversas fuentes, validación del incidente, *scoring*, *ticketing* y acciones de respuesta).

Múltiples áreas de IR y *SecOps* están cosechando los beneficios de SOAR, quizás debido a la capacidad de SOAR para automatizar *SecOps*. Como dice *Gartner*, "Las tecnologías SOAR emergentes prometen llevar la automatización, la consistencia y la eficiencia a los centros de operaciones de seguridad más allá de lo que es posible en SIEM hoy en día" (Fuente: *Top Security and Risk Management Trends, Gartner, February 27, 2020*).

Entre los encuestados que han usado SOAR durante al menos dos años, el 54% compartió que SOAR les ha ahorrado tiempo al tomar medidas sobre incidentes. Otras mejoras incluyen la reducción del tiempo de mitigación (51%), la reducción del tiempo promedio de extremo a extremo en un incidente (47%) y la reducción del tiempo de clasificación (44%). Otro 37% dijo que SOAR ayudó a reducir la cantidad de pasos necesarios para dar respuesta a los incidentes. (Fuente: *The State of SOAR Report, 2020*).

CONCLUSIONES

Conscientes de la necesidad de concebir la seguridad como una actividad integral huyendo de actuaciones puntuales o tratamientos coyunturales, y que los ataques a la seguridad de las organizaciones son cada vez más interconectados y coordinados mejor a escala global, se propone una nueva generación de inteligencia de ciberseguridad

interconectada, predictiva y automatizada, de forma que las nuevas amenazas puedan abordarse utilizando un nuevo conjunto de tecnologías: *machine learning* y análisis de macrodatos.

Para ello es necesario establecer un marco tecnológico innovador de ciberdefensa, el cual permita hacer uso de una inteligencia de ciberseguridad interconectada, automatizable y previsible que alimente un SOC "autónomo".

Este SOC permitirá a las organizaciones partir de información de más valor para la ciberseguridad de la que ofrecen otras herramientas similares con la ventaja añadida de poder automatizar la respuesta a los incidentes que ocurran, mejorando los tiempos de respuesta y la eficacia de las acciones realizadas frente a dichos ataques.