DOCUMENTOS
Nº 32 – 2021

Ciberprotección consistente, integrada y resiliente

Microsoft

Pablo Vera
Sr Sales Manager
Cybersecurity Solutions
Microsoft

"Zero Trust: un enfoque holístico con capacidades únicas"

Microsoft: ADN de ciberseguridad para contar con una protección anticipativa

Seguridad en la nube:
Swift security to the left

Gestión del riesgo y cumplimiento inteligente

Modern SOC

ENTREVISTA

Alberto Pinedo
National Technology Officer (NTO) de Microsoft

Microsoft

Su apuesta por la IA, el principio de seguridad por defecto, 3.500 especialistas y una inversión millonaria convierten a la compañía en un gran referente mundial

Microsoft: ADN de ciberseguridad para contar con una protección anticipativa

La ciberseguridad forma parte del ADN de Microsoft. Con una inversión de más 1.000 millones de dólares al año en ella, su reto es ofrecer protección basada en el principio de 'Confianza Cero' y un enfoque holístico a través de la gestión de identidades y de accesos, la detección proactiva y avanzada de amenazas, la protección del dato y la monitorización unificada, una apuesta que le ha llevado a facturar globalmente en estos segmentos más de 10.000 millones de dólares en su último ejercicio.

La seguridad está en el ADN de **Microsoft** desde que hace más de dieciséis años **Bill Gates** formulara la 'Trustworthy Computing Initiative', por la que la seguridad se promueve por diseño. Ahora, con más de 3.500 profesionales dedicados a la protección de sus productos, sus servicios y la de sus clientes y una inversión de más de 1.000 millones de dólares (840 millones de euros) cada año, apuesta por una aproximación holística, integrando la ciberseguridad como servicio horizontal en todos sus productos y servicios para ayudar a "simplificar y reforzar la protección de las organizaciones".

Para conseguirlo cuenta con equipos de expertos especializados en diferentes ámbitos de la ciberseguridad, entre los que están desde su **Digital Crimes Unit (DCU)** hasta el **Microsoft Threat Intelligence Center (MSTIC),** especializado en el seguimiento de adversarios avanzados, su **Detection and Response Team (DART)** centrado en la Respuesta a Incidentes y, por supuesto, su centro de operaciones, el **Microsoft Cyber Defense Operation Center (CDOC),** desde el que monitoriza toda la actividad 24x7. Gracias a ellos, se analizan ocho billones de 'señales' diarias a través de una red de monitorización mundial que otorga a la compañía una posición privilegiada para detectar y remediar amenazas.

Para apoyar la seguridad proactiva, la compañía ha apostado por la IA, que permite tener a punto sistemas de alerta temprana muy efectivos para enfrentarse a los crecientes riesgos de ciberseguridad que, en 2022, supondrán un coste de más de ocho billones de dólares a escala mundial. "La IA hace posible que los profesionales de ciberseguridad se centren en tareas que aporten el máximo valor, reduciendo labores administrativas y repetitivas para ayudarles a procesar grandes cantidades de alarmas, detectar anomalías y responder en el menor tiempo posible". Además, la compañía con sede en Redmond destaca por la combinación de uno de los mayores repositorios de inteligencia de seguridad del mundo (Microsoft Intelligence Security Graph) con sus capacidades en IA y el contexto humano, proporcionado por los expertos de DCU, MSTIC, DART y el CDOC para adaptar los modelos predictivos de *Machine Learning* a los cambios en el entorno de amenazas.

Cuatro pilares

Así, su apuesta es lograr una protección de 360º a través de cuatro grandes pilares: la gestión de identidades y autenticación, la detección proactiva y avanzada de amenazas, la protección del dato y la monitorización unificada, todo un reto en el que juega un papel destacado su Plataforma XDR que integra, de forma nativa, controles de seguridad para los sistemas, la colaboración en Microsoft 365 y la nube de Azure (con más de 60 regiones y utilizada por el 95% del Fortune 500), tanto para IaaS, PaaS y SaaS, extendiendo su cobertura a múltiples plataformas y con un enfoque *multicloud.* A sus capacidades se suma que es una plataforma abierta a la integración de soluciones de terceros, fruto de su colaboración con los más de 200 socios de la **Microsoft Intelligent Security Association**.

Cumplimiento

Su objetivo es que, a través de ella, los clientes de Microsoft puedan desarrollar una estrategia Zero Trust basada en asumir que pueden sufrir un incidente de seguridad en cualquier momento.

Dado que la privacidad es de forma creciente un imperativo de negocio, la multinacional también ha apostado por ofrecer una nube segura y preparada para la adaptación continua al marco regulatorio, facilitando el cumplimiento de normas internacionales tan exigentes como el RGPD, la ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2 o, en España, la certificación con el Nivel Alto del Esquema Nacional de Seguridad (ENS). ●

Microsoft posee uno de los mayores repositorios de inteligencia de seguridad del mundo (Microsoft Intelligence Security Graph), que combinado con sus grandes capacidades en IA y el contexto humano proporcionado por sus expertos en diferentes áreas, es capaz de adaptar los modelos predictivos de *Machine Learning* a los cambios en el entorno de amenazas.

Zero Trust: un enfoque holístico con capacidades únicas

La transformación digital y las nuevas formas de trabajo remoto híbrido, que van a formar parte de nuestra realidad presente y futura, están forzando a las organizaciones a cambiar el concepto de seguridad tradicional a un modelo de desconfianza total, en la que todos los accesos desde todas las ubicaciones no deben ser confiables por defecto. Unimos a esta situación que los adversarios cada vez buscan más usar identidades comprometidas para entrar en los sistemas, haciéndose pasar por usuarios legítimos, lo que nos obliga a poner en la identidad el nuevo plano de control de la seguridad. Es precisamente la identidad uno de los pilares fundamentales de la propuesta Zero Trust de Microsoft.

Zero Trust es, en términos prácticos, una transición de la confianza implícita —suponiendo que todo dentro de una red corporativa es seguro— al modelo que asume la brecha y verifica explícitamente el estado de seguridad de la identidad, el dispositivo utilizado, la red y otros recursos en función del análisis de todas las señales y datos disponibles. Pero para establecer una estrategia sólida de Zero Trust se debe adoptar un enfoque holístico que tenga en cuenta todos los aspectos que consideramos fundamentales: identidades, dispositivos, redes, infraestructura, aplicaciones y datos.

Cada uno de estos seis elementos principales sirve como fuente de señales para la detección y el análisis de anomalías, establece un plano de control para su aplicación y constituye un recurso crítico a defender.

La Plataforma de Seguridad XDR de Microsoft, Microsoft Defender, proporciona controles nativos, integrados, multiplataforma y *multicloud* para todos estos elementos, simplificando la aplicación efectiva de la estrategia Zero Trust, reduciendo los tiempos de implementación, los riesgos y la complejidad de las operaciones de seguridad.

La aproximación Zero Trust de Microsoft se basa en tres principios:

1. Nunca confiar, verificar siempre. Independientemente de dónde se origine la solicitud o a qué recurso se acceda, Zero Trust nos enseña a "nunca confiar y verificar siempre". Saber quién está solicitando acceso es esencial. Antes de concederlo, cada solicitud debe autenticarse fuertemente, autorizarse dentro de las restricciones de las directivas y monitorizarse en tiempo real en busca de anomalías. El proceso, basado en *Machine Learning,* comprueba todo el contexto y otorga una puntuación de riesgo a cada conexión, desde la identidad del usuario, su ubicación, el estado del dispositivo desde el que se accede y su postura de seguridad, el comportamiento de la aplicación, las directivas organizativas, la clasificación de la información accedida hasta el entorno de hospedaje de la aplicación para evitar una infracción. A partir de ese veredicto, se desencadenan una serie de procesos: dar el acceso, concederlo limitado, bloquearlo completamente, solicitar una autenticación multifactor (MFA) o pedir al usuario que restablezca sus credenciales y vuelva a solicitar el acceso. Todo ello, realizado de forma automática o de forma autónoma por el usuario, reduciendo la carga de trabajo sobre los equipos del *Help Desk.*

2. Privilegios mínimos para los usuarios. Otro principio fundamental de Zero Trust, el acceso con privilegios mínimos, otorga acceso a los usuarios sólo cuando lo necesitan, por el tiempo que lo precisan y para la tarea específica en cuestión. El control de acceso utiliza políticas adaptativas basadas en el riesgo de cada conexión protegiendo los datos, sin comprometer la productividad del usuario.

Microsoft proporciona herramientas para la verificación de los accesos para limitar, al mínimo, el número de usuarios privilegiados, estableciendo un modo de trabajo basado en solicitudes de escalada de privilegios temporales. Igualmente, dispone de herramientas integradas para la gestión de las identidades privilegiadas (PIM), de los accesos privilegiados (PAM) y para la implementación de máquinas específicas para accesos privilegiados (PAW), que facilitan una gestión de los accesos privilegiados completa y robusta.

La utilización de un modelo de identidad moderno basado en la nube, como Azure Active Directory (Azure AD), es más sencillo y seguro que usar mecanismos de federación con las identidades locales. No solo es más fácil de mantener (al tener menos elementos que los atacantes puedan explotar), sino que además el modelo basado en la nube permite recopilar una gran cantidad de señales que, junto con procesos de análisis avanzados, hace posible la detección de anomalías muy sutiles y sólo detectables en conjuntos de datos muy grandes.

3. Asumir el incidente de seguridad. Zero Trust también significa que se debe asumir que se podrían producir incidentes de seguridad en cualquier momento, incluso que podríamos estar sufriendo una situación crítica ahora mismo. Una mentalidad siempre vigilante ayuda a tener un comportamiento proactivo que permita minimizar y prevenir los movimientos laterales. También, deben utilizarse técnicas como microsegmentación, cifrado fuerte y análisis de la telemetría para detectar más rápido las posibles brechas. Siguiendo este comportamiento, además de mejorar las capacidades de detección y respuesta, también se reducirá el impacto cuando se produzcan los incidentes. La preparación para la respuesta a un incidente es una tarea fundamental. Desde Microsoft disponemos de servicios profesionales específicamente diseñados para ayudar a nuestros clientes a identificar donde están sus áreas de mejora, en cuanto a herramientas, procedimientos y necesidades formativas de sus equipos de respuesta. Mediante la realización de ejercicios prácticos de simulación usando ejemplos de situaciones de crisis reales, el cliente pone a prueba a sus equipos y sus procesos, verificando qué elementos funcionan bien y cuáles necesitan ajustes de mejora. Las empresas que operan bajo el modelo Zero Trust de Microsoft son más resilientes, consistentes y reaccionan mejor y más rápido ante nuevos ataques.

Para facilitar a nuestros clientes el inicio de este camino disponemos de guías de implementación de Zero Trust, de acceso público, a través del portal https://docs.microsoft.com/en-us/security/zero-trust

Pablo Vera
Sr Sales Manager
Cybersecurity Solutions
Microsoft

Alberto Pinedo,

National Technology Officer (NTO) de Microsoft

Desde hace casi dos décadas en Microsoft es uno de los referentes en tecnología y, también, en ciberseguridad. De hecho, ha sido el responsable en la compañía de llevar a cabo grandes proyectos en sectores tan diversos como *retail*, finanzas... Además, ha liderado la renovación del Esquema Nacional de Seguridad para Azure, Microsoft 365 / Microsoft 365 Education y Dynamics 365. Especializado en IA, Datos, Computación en la Nube, Identidad Digital, Innovación y Transformación Digital, Alberto Pinedo explica las claves que han llevado a Microsoft a tener la ciberprotección como un pilar fundamental en sus productos y servicios, además de colaborar con gobiernos en la lucha contra el cibercrimen.

"El camino hacia la resiliencia en la automatización de los negocios lo marcan la adopción del modelo Zero Trust y la aplicación de Inteligencia Artificial"

– ¿Qué lema resumiría mejor la estrategia de Microsoft en ciberseguridad?

– Nuestra estrategia es única en la industria, por un lado, con un enfoque integrado y, por otro, aprovechando la Inteligencia Artificial y la automatización. Además, contamos con una aproximación holística sobre aspectos fundamentales de la ciberprotección como la seguridad de la identidad y la administración de acceso; los puntos de acceso, el correo electrónico y la seguridad de las aplicaciones; la prevención de la pérdida de datos y la seguridad en la nube y nuestras soluciones de SIEM/SOAR hacen que nuestro enfoque sea de extremo a extremo.

– ¿Qué capacidades de ciberseguridad les demandan sus clientes en España?

– Contamos con clientes a los que proporcionamos servicios de defensa proactiva en todos los sectores. Ninguna empresa debe bajar la guardia y, en consecuencia, tomar medidas para minimizar su área de exposición. Entre las capacidades más demandadas en el último año están las relacionadas con las plataformas de trabajo confiables, debido a que el perímetro de seguridad de las empresas se ha ampliado. Por ello, es más necesario que nunca adoptar el modelo Zero Trust, para el que contamos con una evaluación *online*, que permite a las empresas determinar en qué etapa de madurez están y cómo mejorar.

– En los últimos años han firmado acuerdos relevantes con entidades como el CCN...

– Son una prueba fehaciente de la apuesta de Microsoft por la seguridad en todos sus servicios y garantiza a las empresas los máximos estándares a la hora de adoptar nuestras soluciones. Microsoft cumple con un amplio abanico de normas internacionales tan exigentes como el RGPD o la norma ISO/IEC 27001, entre otras muchas. En el caso concreto del Centro Criptológico Nacional, fuimos el primer gran proveedor de soluciones *cloud* en obtener el certificado de conformidad con el ENS, con categoría ALTA, en 2018. Actualmente, hemos renovado los certificados para Microsoft Cloud (Microsoft 365, Dynamics 365 y Microsoft Azure) con categoría ALTA en todos nuestros servicios. Además, también colaboramos con este organismo, a través de su ecosistema de *partners,* en la elaboración conjunta de guías de seguridad alineadas con el cumplimiento del ENS.

– ¿A qué nuevas amenazas se están enfrentando las empresas?

Las actividades de los ciberdelincuentes se han vuelto más oportunistas, es un modelo de negocio en sí. El volumen y la complejidad de los

ciberataques ha crecido de forma notable en los últimos tiempos. En este contexto, es necesario tener una estrategia sólida y confiar en proveedores que ofrezcan una ventaja competitiva para afrontar los riesgos cíber. Entre otras capacidades, el Microsoft Cyber Defense Operation Center (CDOC) nos permite monitorizar la actividad mundial 24x7, analizando billones de señales diarias. A ello hay que sumar la combinación de uno de los mayores repositorios de inteligencia de seguridad del mundo, con nuestra tecnología de IA y la adaptación de los modelos predictivos de *machine learning* a los cambios en el entorno de amenazas.

– Su compañía apuesta hoy por adoptar un modelo Zero Trust…

Sí; y lo hacemos en cada uno de los cuatro grandes frentes que permiten la protección de 360 grados de nuestros servicios: gestión de identidades y autenticación, detección proactiva y avanzada de amenazas, protección del dato y monitorización unificada. Además, nuestra propuesta de soluciones de seguridad se basa en una plataforma XDR (Extended Detection & Response), que integra de forma nativa controles para todos los sistemas y que está abierta a la integración con soluciones de seguridad de terceros, gracias al trabajo de la Microsoft Intelligent Security Association, que cuenta con más de 200 socios.

– ¿Qué aporta Microsoft a un CISO que quiere tener un nivel aceptable de riesgo de ciberseguridad en sus entornos multinube?

– Una base tecnológica que cumple con los estándares más exigentes de la industria, manuales para su despliegue elaborados en colaboración con el CCN, una filosofía DevSecOps para proteger todo el ciclo de vida de desarrollo de software y una red de monitorización global para actuar proactivamente ante los riesgos. A ello se suma una red de *partners* especializados que proponen las soluciones más adecuadas a cada situación. En entornos *multicloud* es necesario obtener una vista holística para correlacionar las amenazas y evaluar cómo una amenaza puede afectar a otro recurso. Soluciones como Microsoft Cloud App Security brindan herramientas para detectar aplicaciones en la nube y supervisarlas y protegerlas, mientras que con Azure Sentinel recopilamos y analizamos datos en todas las instalaciones y en varias nubes.

“Soluciones como Microsoft Cloud App Security brindan herramientas para detectar aplicaciones en la nube, supervisarlas y protegerlas, mientras que con Azure Sentinel podemos recopilar y analizar datos en todas las instalaciones y en varias nubes”

– ¿Cuál es la tecnología de protección digital de Microsoft más desconocida por los clientes corporativos?

– Es difícil apostar por una, pero sí destacaría Microsoft Intelligent Security Graph API, que permite conectar productos y servicios de seguridad Microsoft, así como de nuestros *partners* para optimizar las operaciones de seguridad y mejorar la protección, detección y respuesta ante ciberamenazas. Es una gran aproximación y da excelentes resultados.

– El ‘Modern SOC’ se basa en una combinación de herramientas SIEM nativas de la nube, con IA y aprendizaje automático… ¿Qué marca la diferencia con otras aproximaciones?

– La misión principal del SOC es identificar rápidamente situaciones de compromiso y responder a los incidentes. En medio de un ataque, los minutos importan. En este contexto, en un SOC moderno la IA y el aprendizaje automático juegan un papel clave y su uso permite a los expertos reducir el ‘ruido’ y centrarse en las cuestiones relevantes. De este modo, se cuenta con una importante ventaja competitiva. Es nuestro caso, con Azure Sentinel, donde la IA y el *machine learning* analizan cantidades masivas de datos para detectar con mayor precisión los modelos de comportamiento que indican un riesgo.

– Ataques contra la cadena de suministro han evidenciado la necesidad de incrementar los esfuerzos en esta área, ¿Cómo aborda el problema Microsoft?

– Es una de las tres amenazas más importantes a las que nos enfrentamos, no sólo como compañía, sino también como sociedad, tal y como lo reflejó nuestro presidente, Brad Smith, pidiendo una respuesta fuerte y global en materia de ciberseguridad. Los ataques-nación se han vuelto más sofisticados y de una mayor determinación. En nuestro caso, disponemos de un programa denominado ‘Government Security Program’ con el que damos información a más de 45 países, entre ellos España, sobre vulnerabilidades, código fuente de nuestros productos y amenazas. Adicionalmente, mantenemos línea directa con los equipos que investigan dichos ataques a escala mundial. El objetivo es ofrecer la mayor información posible, de forma transparente y con una comunicación proactiva, a los responsables de ciberseguridad a nivel nacional.

– ¿Cuál diría usted que es la gran novedad en materia de ciberseguridad de Microsoft en lo que llevamos de 2021?

– Uno de los grandes anuncios en Microsoft Ignite, nuestro evento anual para Profesionales de TI y desarrolladores, fue el lanzamiento de la autenticación sin contraseñas en Azure Active Directory. Las organizaciones ya pueden hacer uso de esta funcionalidad y beneficiarse de una mayor seguridad y simplicidad apoyándose en tecnologías como Windows Hello, la aplicación Microsoft Authenticator y llaves FIDO2.

De hecho, ya contamos con más de 200 millones de usuarios que se autentican sin contraseña en nuestros servicios de consumo y empresa. En 2021, esperamos que el *passwordless* se convierta en una tendencia. ●

Microsoft

SEGURIDAD EN LA NUBE: SWIFT SECURITY TO THE LEFT

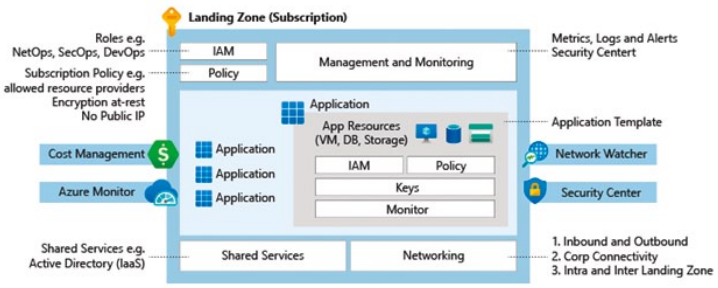
Dictar las normas ya no es suficiente: de las políticas como documentación a las políticas como código

Comparar la ciberseguridad con el sistema inmunológico no es novedoso, pero no por ello deja de ser fascinante. Se trata de un punto de vista que plantea la ciberprotección como un proceso evolutivo, de resiliencia y, también, de adaptabilidad.

Un claro ejemplo son las citoquinas, uno de los métodos usados por las células y el sistema inmunitario para comunicar que están siendo atacadas y, tras recibir esta señal, activar en el organismo el 'modo protegido', deshabilitando comportamientos no vitales o reforzando medidas de protección. Esto ha inspirado a Microsoft para diseñar sus aplicaciones para que, en caso de verse comprometidas, detecten que son incapaces de cumplir sus indicadores de confidencialidad, integridad o disponibilidad, alertando de la situación y activando un proceso que supone suprimir capacidades no imprescindibles e implementar medidas adicionales.

Sin duda, la nube proporciona una gran plataforma sobre la que desarrollar aplicaciones con las características esperadas sin necesidad de controlarlas individualmente. Se trata de una apuesta por implementar en la nube de Microsoft, Azure, un principio fundamental como es el uso de los llamados Blueprints, que definen políticas y roles, así como la existencia (o ausencia) de ciertos componentes en todo despliegue.

Estas políticas pueden ser utilizadas para múltiples propósitos entre los que están desde mejorar la ciberseguridad, hasta el gobierno y, también, el cumplimiento. Gracias a ello, Microsoft logra que todo disco esté cifrado, que cada servicio envíe su telemetría a un sistema central, que ningún componente desplegado tenga IP pública o prohibir desplegar en ciertos países, entre otros aspectos determinantes. Además, como componente básico también se apuesta por una arquitectura en la que toda aplicación tenga asociada una 'caja fuerte' donde guardar secretos, se cuente con un WAF protegiendo la salida a Internet, se habilite un espacio donde se hagan copias de seguridad, etc. De esta forma, la multinacional consigue dotar a cada una de las aplicaciones de una inmunidad innata frente a amenazas.



Valor diferencial

El valor para la seguridad de la aproximación DevOps en la nube emerge usando repositorios de código como única fuente de verdad, así como *pipelines* continuos automatizados de testeo y despliegue en todos los entornos, desde desarrollo a producción. Eso sí, para garantizar su eficacia este modelo debe usarse tanto para el desarrollo de las aplicaciones como en la definición de la infraestructura general. Así, Microsoft no solo se adapta mejor a las nuevas amenazas, sino que permite recuperarse de cualquier incidente con solo pulsar el botón de 'Redesplegar todo'.

Gestión del riesgo y cumplimiento inteligente frente a un entorno normativo dinámico global

La gestión y protección del dato se ha convertido en uno de los grandes retos para las empresas, especialmente cuando se trata de garantizar el cumplimiento, con un marco normativo tan cambiante como el actual. Solo en 2020 se registraron más de 215 actualizaciones de regulaciones al día, de más de 1.000 organismos en todo el mundo, según el informe 'Coste del cumplimiento 2020. Actualización de la Covid-19', de Thomson Reuters. A ello, se le suma el hecho de que los datos no son estáticos. Tienen un ciclo de vida desde el momento en que se crean, comparten y almacenan en un amplio abanico de plataformas y servicios, tanto en la nube, como en las instalaciones o en entornos híbridos.

En la mayoría de los casos, las organizaciones disponen de recursos y herramientas limitados para identificar y mitigar los riesgos derivados de su falta de seguimiento y control en toda la empresa, al tiempo que se tiene que cumplir con los estándares de privacidad del usuario. Por ello más de la mitad de las compañías (54%) reconocen estar preocupadas por la falta de visibilidad de su ecosistema digital.

Ante estos desafíos, Microsoft ofrece un portafolio de soluciones de cumplimiento inteligente y gestión de riesgos que proporcionan capacidades integradas en cuatro áreas clave:

1.-Gobierno y protección de los datos donde quiera que se encuentren. Los clientes disponen de la flexibilidad necesaria para implementar los controles precisos para cumplir con los requisitos de cumplimiento y seguridad internos y externos, enriquecidos por una plataforma inteligente.

2. Identificación de los riesgos internos críticos y aplicación de medidas sobre ellos. Microsoft ha potenciado su solución Insider Risk Management para aprovechar el repositorio Microsoft Graph, entre otros servicios, y poder obtener señales de terceros y nativas en tiempo real para identificar los riesgos internos, controlar el anonimato y permitir la colaboración entre TI, RR.HH. y legal.

3. Investigación y reacción con datos relevantes. Microsoft ha llevado a cabo un gran esfuerzo para desarrollar su solución de eDiscovery Avanzado, que proporciona un flujo de trabajo de extremo a extremo para preservar, recopilar, analizar, revisar y exportar contenido para asuntos legales o investigaciones internas de una organización.

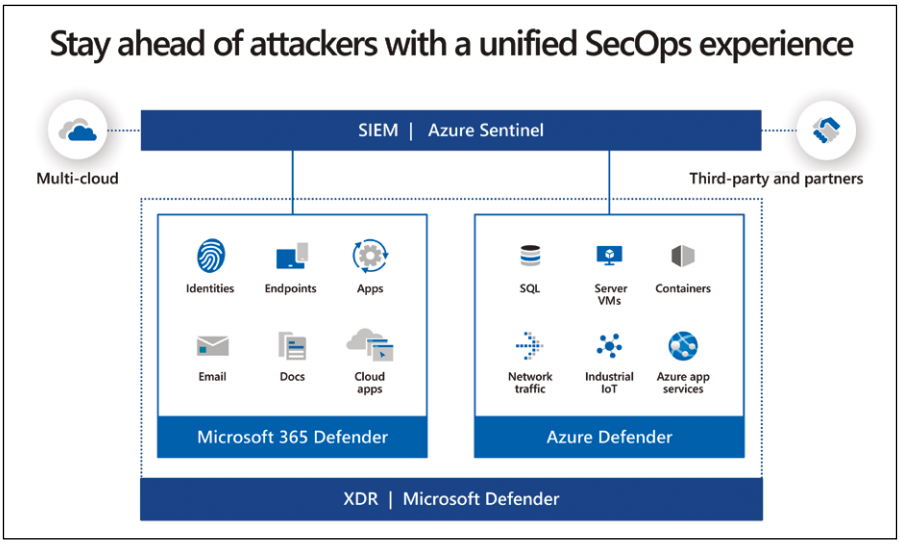
4. Simplificar el cumplimiento. La compañía cuenta con su Compliance Manager, que permite evaluar y monitorizar los controles de protección de datos, con la capacidad de puntuación de cumplimiento para reducir los riesgos. Además, ofrece más de 150 plantillas personalizables, para cumplir con las normativas internacionales, locales y sectoriales. En todas ellas, la compañía aplica su experiencia en IA y aprendizaje automático. Se trata de que las organizaciones puedan, incluso, escalar estos procesos y flujos de trabajo, reduciendo, en gran medida, el riesgo.

Modern SOC: aplicando la teoría de la gravedad de los datos para protegerlo todo

Los equipos de seguridad aún están viviendo en 2021 el impacto del repentino cambio al teletrabajo. A la par, las amenazas son constantes y los adversarios han incrementado rápidamente su sofisticación, usando técnicas que dificultan su detección y que ponen en peligro, incluso, a las empresas e instituciones mejor preparadas.
Y una vez que los atacantes están dentro, los daños pueden escalar rápidamente.

Modern SOC

El escenario descrito es un gran reto al que se suma el hecho de que se está redefiniendo el modelo de seguridad hacia a un enfoque Zero Trust. Los principios de Zero Trust obligan a tener una profunda visibilidad de todo el entorno para contar con el mayor contexto posible, analizar una ingente cantidad de señales y automatizar la respuesta. Sin embargo, el SOC tradicional no está preparado para la ingesta y análisis de grandes volúmenes de datos de los actuales escenarios (Cloud, IoT, Zero Trust). A mayor número de señales, más ruido, mayor tiempo de respuesta y, también, mayor dificultad para atender todas las alertas.
Por ello, Microsoft propone implementar un nuevo modelo de SOC (*"cloud ready"*, *"IoT ready"* y *"Zero Trust ready"*) apoyado en las capacidades que la nube ofrece para manejar grandes volúmenes de datos, aplicar analítica avanzada y automatizar procesos.
Precisamente, cuando se habla de analizar grandes volúmenes de señales, se tiende a pensar en traerlas todas al SIEM del SOC y aplicar allí la analítica. Una aproximación que Microsoft ve como "poco adecuada" por lo costoso de mover e 'ingestar' todos los datos (o en su defecto renunciar a traer todas las señales perdiendo el valioso contexto), y por la latencia introducida en el proceso, que va en contra de una detección y respuesta rápida. Por ello, la multinacional propone apostar por el concepto de la 'gravedad de los datos' ('*data gravity*'), acuñado por **Dave McCrory,** en 2010. Se basa en considerar que a medida que los conjuntos de datos crecen, son cada vez más difíciles de mover por lo que se quedan estáticos. Frente a esta situación es la gravedad lo que atrae aplicaciones y servicios donde está el dato.
¿Cómo se debe construir un SOC moderno? Pues respetando la 'ley de *data gravity*'. Si se puede aplicar la analítica cerca de dónde ya está el dato, se puede incrementar la velocidad de detección y respuesta. Esto no supone el fin de la agregación. Un SOC moderno realiza una aproximación híbrida, aplicando la analítica tan cerca del dato como sea posible, para luego extender la visibilidad y el conocimiento, en un repositorio central del SOC para el análisis y el conocimiento adicional a lo largo de otros centros de gravedad. Además, hay que incorporar analítica avanzada (ML & UEBA) para permitir a los SOCs modernos detectar peligros que antes pasaban desapercibidos y automatizar la detección y la respuesta de amenazas *commodity* (autocuración), permitiendo a los analistas centrarse en las tareas de más valor, como el *hunting* de amenazas avanzadas, sólo realizables por humanos.



La propuesta de valor de Microsoft

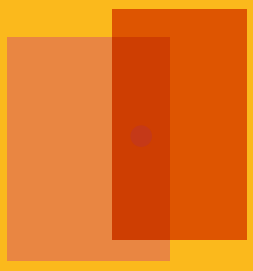
Partiendo de este planteamiento, Microsoft ofrece una aproximación para modernizar las Operaciones de Seguridad única en la industria a través de una plataforma integrada, apoyada en las potentes capacidades AI/ML que ofrece Azure, y alimentadas por un ingente y diverso número de señales de seguridad de sus plataformas y servicios (*Intelligence Security Graph*).
Así, sus equipos de seguridad definen los modelos analíticos avanzados en base a su conocimiento de los adversarios, modelos que son entrenados y refinados en el *Intelligence Security Graph*. Además, esta analítica avanzada se embebe en cada una de las herramientas de detección y respuesta, y es aplicada cerca del dato o servicio que monitorizan, proporcionado profundidad en la detección, análisis y respuesta a lo largo de múltiples dominios.
Al contrario que otras aproximaciones, estas herramientas no trabajan en silos, sino que están ya integradas en la plataforma XDR Microsoft Defender, que cubre dominios como el punto final, la identidad, aplicaciones de colaboración, aplicaciones *cloud* e infraestructura (almacenamiento, contenedores, redes, VMs, etc.) sea *on-premise* o multinube.
Adicionalmente Azure Sentinel (SIEM nativo-cloud, SOAR, UEBA & Threat Intelligence Hub) proporciona amplitud en la detección, análisis y respuesta, habilitando un nivel superior de agregación de alertas y señales para mayor contexto, no solo de la plataforma XDR Microsoft Defender sino también de fuentes de terceros y otras nubes, mejorando la fiabilidad de las alertas.
En definitiva, Microsoft ofrece una solución integrada XDR + SIEM (+SOAR, UEBA, TI Hub) que brinda una experiencia de operaciones de seguridad unificada, y proporciona:
Efectividad, reduciendo drásticamente los tiempos de resolución al eliminar tareas manuales y maximizando el uso de ML y automatización.
Eficiencia, haciendo un mejor uso del presupuesto de seguridad, consolidando herramientas, reduciendo tiempos de despliegue y optimizando los costes de operación.
Agilidad, a la hora de monitorizar el modelo *Zero Trust* y los entornos modernos que el negocio está fomentando.
Esta solución integrada no sólo cubre su plataforma, sino que abarca múltiples sistemas operativos y otras nubes, ofreciendo a sus clientes una solución completa a lo largo de todo su 'estado digital'.

Microsoft

Seguridad inteligente
que mejora tu organización.

Desbloquea la innovación
de manera segura

Transforma los servicios
al ciudadano de manera
segura



Tecnología segura que
mejora los servicios al
paciente.

Para más información accede a: https://www.microsoft.com/es-es/security/