Mantenga el control con IBM QRadar on Cloud

QRadar

IBM Security

Contenido

SIEM inteligente como servicio

Asegurar los datos y las redes de forma local y en la nube es una tarea titánica para cualquier organización de grandes proporciones. Nuevas vulnerabilidades son descubiertas casi a diario; se desarrollan nuevas cadenas de malware en cuanto se escribe una guía de detección para las anteriores, y los cibercriminales pueden comprar en la red oscura kits de exploits preconfigurados , con respaldo de equipos de soporte profesionales. Como analista de seguridad, usted necesita más que unas pocas soluciones puntuales diseñadas para defender el perímetro de la red. Usted necesita visibilidad, perspectiva y un sentido innato de cuando las cosas no parecen estar bien.

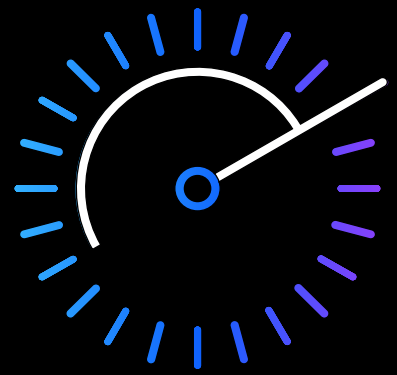
IBM® QRadar® on Cloud se supera en todas estas tareas. Con información de seguridad sólida y capacidades de gestión de eventos (SIEM), la solución ayuda a resguardar los datos y las redes con una amplia gama de capacidades que pueden mostrarle quién está haciendo qué, cuándo y dónde. Usa paneles de control y visualizaciones avanzadas, comprimiendo miles o millones de incidentes discretos en simples indicaciones de sospechas de problemas y conserva registros detallados de cualquier actividad sospechosa para análisis futuros. Al mismo tiempo, sus capacidades avanzadas de registro y sus herramientas de generación de informes le ayudan a cumplir rápidamente con requisitos básicos, tales como obligaciones de informes regulatorios.

Obtenga más información sobre IBM QRadar on Cloud →

QRadar on Cloud puede procesar más de

500.000

eventos por segundo.[1]



Beneficios clave de IBM QRadar on Cloud

"Los CIO deben cambiar su pregunta de si '**La nube es segura**' a '**¿Estoy usando la nube de forma segura?**'"

Gartner
Gartner.com

Explore los beneficios →

Cumpla con las exigencias regulatorias y de seguridad al mismo tiempo.

Es probable que haya implementado medidas básicas de seguridad en el perímetro de su red para prevenir ataques simples, pero que la mayoría de sus terminales tengan fallas de seguridad y que algunos de los usuarios simplemente no puedan evitar hacer clic en enlaces inseguros. Los dispositivos y las credenciales también se suelen ver comprometidas, abriendo las puertas para la pérdida de datos y posibles interrupciones comerciales.

Implementar un sistema de informes de recolección y conformidad de datos es bastante fácil, pero dejar felices a los auditores y proteger los datos críticos de su organización puede ser de todo menos fácil. Mientras más avanzado el sistema más prolijamente le preparará para gestionar actividades rutinarias y brechas poco frecuentes en la red, que requieran investigación y respuesta a incidentes.

Obtenga más insights sobre las amenazas empresariales actuales de IBM X-Force Threat Intelligence® →

Vea y descubra más sobre amenazas persistentes avanzadas →

"El procesamiento y correlación de datos no estructurados usando capacidades cognitivas nos dará más contexto para ofrecer recomendaciones más precisas y realizables, al tiempo que facilitará la vida de los analistas de seguridad en el día a día".

Christophe Bianco
Gestor asociado y
Director de tecnología
de Excellium Services

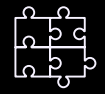
Lea el caso de estudio →

Lo que ofrece QRadar en Cloud:

Cambie de un modelo CAPEX a OPEX

Aborda la brecha de habilidades

Alta visibilidad, conformidad y seguridad



Más de 500 integraciones listas para usar

Insights impulsados por datos usando IA

Flexibilidad y escalabilidad

Obtenga insights profundos para proteger sus activos críticos en la nube

Es importante detectar y erradicar malware, así como establecer reglas de firewall para resguardar subredes. Es por lo que tal vez usted haya invertido en seguridad perimetral. Pero el software de analítica de seguridad se basa en el concepto fundamental de que ningún perímetro conectado a la internet es realmente seguro y que las organizaciones deben ser capaces de detectar cambios de comportamiento y anormalidades.

Con el modelo de nube, su organización puede implementar puertas de enlace de datos seguras y enviar sus datos de seguridad a un entorno de nube gestionado e implementado inteligentemente con información operacional mensual predecible. El modelo de nube le da a usted el control, al tiempo que permite que su personal dedique la mayoría de su tiempo a supervisar el entorno, afinando las reglas de detección de amenazas y personalizando los informes regulatorios o de gestión, en vez de aplicando parches y realizando copias de seguridad de datos.

Manténgase al día con la conformidad y las reglamentaciones →

Un tomador de decisiones de TI pasa casi

2 horas por día buscando datos relevantes.[2]

69 % de las empresas

ve mandatos de conformidad impulsando sus gastos.[3]

Haga que su organización esté en conformidad

La solución QRadar on Cloud cumple con una función primordial impulsada por el negocio. Al proteger los datos y preservar un registro de eventos y prácticas de seguridad listo para auditoría que habilita la protección, ayuda a las organizaciones a cumplir con las reglamentaciones gubernamentales y de la industria. De ser ignorados, los mandatos pueden perjudicar una organización con penalidades, así como el malware puede perjudicarla con pérdida de datos.

Una gran cantidad de requisitos y de estándares de mejores prácticas, diseñados para proteger la información personal y financiera de los clientes, así como aumentar la transparencia corporativa, controlan la forma en que los datos de los clientes y de la organización se recolectan, almacenan y resguardan. La ley Sarbanes-Oxley (SOX), el Estándar de seguridad de datos industriales de tarjetas de pago (PCI DSS), la ley de Portabilidad y responsabilidad de los seguros de salud (HIPAA), la Reglamentación general de protección de datos de la Unión Europea (RGPD) y otras reglamentaciones significan que las empresas pueden enfrentar penalidades criminales, prohibiciones en el uso de tarjetas de pago y otros riesgos que pueden conllevar devastadoras interrupciones comerciales por prácticas de no conformidad.

Vea la extensión de contenido de IBM QRadar para RGPD →

Las violaciones a la HIPAA pueden acarrear penas criminales, así como multas de hasta USD 50.000 por cada violación, con un máximo anual de

USD 1,5 millones.[4]

88 % de las empresas

gastó más de USD 1 millón para prepararse para la RGPD.[3]

Ayude a priorizar amenazas

Algunas amenazas de seguridad pueden abordarse de forma táctica, usando herramientas especializadas para cubrir aspectos individuales de seguridad. Estas herramientas pueden ser útiles para cubrir amenazas definidas y problemas conocidos, así como también pueden generar respuestas tan simples como bloquear nuevos puertos, eliminar una instancia de malware o colocar un parche a un activo vulnerable identificado.

Pero el software QRadar es mucho más valioso que soluciones puntuales porque recolecta un conjunto más amplio de datos de seguridad que se comparte básicamente entre todos los módulos de inteligencia seguridad. Una vez que observa y calcula los límites para las normas de flujo de datos en su red, percibe automáticamente los eventos que violan estos límites y alerta a su equipo de seguridad. Las reglas de límite, normalmente, pueden detectar transferencias salientes de datos, uso de ancho de banda, cambios en aplicaciones o un número sospechosamente alto de intentos de acceso desde una dirección de Protocolo de internet (IP) inesperada. QRadar también vigila los eventos conectados, por ejemplo, comparando las identidades de los usuarios, la fuente y el destino de direcciones IP, así como ubicaciones geográficas en las que se originan las actividades. Examina estos eventos relacionados buscando un contexto para distinguir mejor los verdaderos ataques de las instancias únicas de nuevos comportamientos.

Lea más sobre las predicciones de seguridad de IBM X-Force para 2020 →

La ciberseguridad se está volviendo cada vez más compleja. En 2019, el tiempo promedio para identificar y contener una fuga era de

279 días

con un costo global promedio de pérdida de datos estimado en

USD 3,9 millones.[5]

El cuidado de la salud es la industria más costosa en pérdidas de datos, que cuestan a las organizaciones

USD 429 por cada registro perdido o robado.[5]

Adopte un nuevo modelo de gastos con software de seguridad basado en la nube

El software puede ser crítico para permitir las operaciones de TI y empresariales, pero para la mayoría de las organizaciones, mantener el software de seguridad localmente agrega una carga de trabajo extra que puede realmente atravesarse en el camino de sus tareas centrales de seguridad. Reducir y simplificando la mezcla de roles que el personal de seguridad necesita ejercer, y esos pueden ser motivos significativos para adoptar una alternativa basada en la nube.

Lograr una mejor seguridad siempre requerirá algún nivel de recursos humanos y técnicos, pero con una solución alojada, basada en la nube, el tiempo y los gastos asociados que el personal de seguridad ocupa en deberes de rutina pueden redistribuirse en análisis y planificación.

Lea este documento para saber más sobre QRadar on Cloud, una solución SaaS flexible y altamente escalable →

Comparación de costos

On premises versus en la nube

Costos iniciales	En premises	SaaS
Personalización	●	●
Hardware	●	
Implementación	●	●
Personal de TI	●	
Gestión de ciclo de vida	●	
Mantenimiento	●	
Licencias de software	●	
Capacitación	●	●
Costos recurrentes		
Costos constantes de TI	●	
Mantenimiento constante	●	
Parches y arreglos	●	
Actualizaciones	●	
Tasa de suscripción		●

"Nuestro costo total promedio creció, pero no vemos este amento como algo necesariamente malo. Estamos invirtiendo en protección de datos a largo plazo porque sabemos que las fugas de datos no están va a desaparecer."[6]

Estudio " An IT Supervisor/South Africa/ Industrial in 2018 Cost of Data breach ", del Instituto Ponemon.

Lea el estudio →

Amplíe QRadar con otras herramientas de seguridad

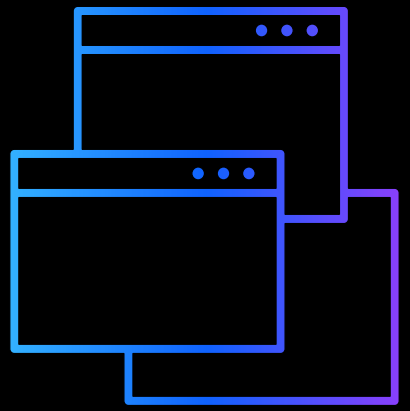
QRadar on Cloud hereda más de 500 integraciones existentes desarrolladas a lo largo de la última década, respondiendo a solicitudes de clientes on premises y alineándonos con soluciones de terceros que complementan la plataforma de inteligencia de seguridad. Los profesionales con experiencia que realizan la implementación de su nube raramente tendrán que desarrollar nuevos módulos de soporte para empezar a aceptar datos de sus activos y aplicaciones. La mayoría de los clientes empezará a obtener valor a los pocos días de haber completado un acuerdo.

Usted puede descargar e instalar nuevas extensiones o aplicaciones desde IBM Security App Exchange, lo que ampliará sus capacidades de supervisión sobre la red y su equipo de mantenimiento de IBM CloudTM podrá brindar soporte a la extensión tecnológica. Ya existen decenas de estas extensiones compatibles, incluyendo nuevas visualizaciones, integraciones, parches, reglas personalizadas y nuevas aplicaciones completas, como la aplicación IBM QRadar User Behavior Analytics. Todo el contenido del sitio web es revisado por IBM Security por medio de su proceso de validación Ready for IBM Security Intelligence.

Más información sobre plug-in y extensiones de QRadar por medio del IBM Knowledge Center →

QRadar puede recolectar eventos de acceso o flujos de red desde

500+ aplicaciones y dispositivos.[7]



Aborde la brecha de habilidades con IA

En años recientes ha habido un marcado aumento en la brecha de habilidades en ciberseguridad. IBM QRadar Watson Advisor App está diseñado para ayudar a su organización a detectar amenazas más rápidamente.

La aplicación usa la inteligencia artificial (IA) para ayudar a usuarios en el análisis de incidentes y de riesgos, clasificación y respuesta, así como también habilita a los equipos de operaciones de seguridad para hacer más con mayor precisión. ¿El resultado? Una drástica reducción del tiempo utilizado para investigar incidentes, de días y semanas a horas.

Además, los equipos de seguridad pasarán menos tiempo trabajando en tareas rutinarias de centros de operaciones de seguridad (SOC) y más tiempo en otras prioridades estratégicas.

Vea cómo QRadar Advisor con Watson puede ayudar a su equipo SOC a hacer más con mayor precisión. Vea el video →

Descubra QRadar Advisor con Watson Versión 2.5.0 →

Se espera que los puestos sin cubrir de ciberseguridad alcancen los

1,8 millones

en 2022.[8]

De acuerdo con un estudio reciente, la fuerza de trabajo global en ciberseguridad necesita

crecer en un 145 %

para cerrar la brecha de habilidades. En los EE.UU. necesita crecer un 62 %.[9]

"Cargills Bank pudo superar estas limitaciones usando IBM QRadar SIEM y QRadar Advisor con Watson para recibir alertas prioritarias en tiempo real. El portafolio de seguridad cognitiva de primera línea de IBM nos ayudará a anticipar el cambio de hilos y mitigar riesgos, reforzando, así, nuestra posición como un banco digital líder".

Rohan Muttiah
Director general de operaciones, Cargills Bank

Lea el caso de estudio →

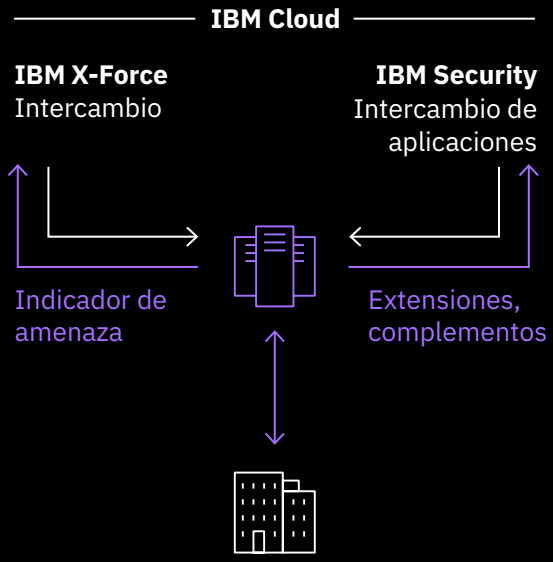
Logre más flexibilidad y escalabilidad

Comprar software como un servicio (SaaS) ofrece ventajas en escalabilidad y flexibilidad porque significa que los cambios en la capacidad no están atados a una infraestructura local y son mucho menos dependientes de la disponibilidad del personal interno. Las empresas pueden cambiar muy rápidamente en esta economía. Ya sean picos ocasionales de tráfico o cambios permanentes en las cargas de trabajo debido a fusiones e incorporaciones, con la solución QRadar en Cloud, pueden escalar su poder computacional según su necesidad. Como la infraestructura vive en la nube y está diseñada pensando en los cambios de capacidad, no hay necesidad de cambiar el software de forma local. La capacidad puede ampliarse o reducirse en poco tiempo y con un mínimo de necesidad de participación del cliente.

Destacados de la oferta QRadar on Cloud

- Actualizaciones elásticas; rápida rentabilidad
- DevOps dedicados
- Supervisión de salud, 24 horas, 7 días a la semana
- Gestión de sistema: actualizaciones, parches
- Soporte para 450+ integraciones de seguridad y de TI
- Detección avanzada de amenazas
- Paneles de SOC y de gestión configurables
- Cobertura global del punto de presencia
- Soporte para modelo multiusuario para proveedores de servicios

IBM QRadar on Cloud



Activos del cliente on premises o en la nube

- Dispositivos de seguridad
- Recursos de servidores y de la nube
- Red y actividad virtual
- Actividad de datos
- Actividad de aplicaciones
- Vulnerabilidades y amenazas
- Usuarios e identidades

"Antes, siempre sentíamos que estábamos atrasados con relación a la seguridad, pero ahora somos mucho más proactivos".

Michael Warrer
CIO, NRGi

Lea el caso de estudio →

Obtenga acceso a servicios gestionados

Para organizaciones que necesitan ayuda más allá de las capacidades, el tiempo o la experiencia que su equipo de seguridad pueda proporcionar, también hay opciones de servicios disponibles de gestión adicionales. QRadar on Cloud ofrece integración con IBM Managed Security Services, ofreciendo servicios totalmente gestionados, con supervisión activa y respuesta a amenazas de seguridad las 24 horas, 7 días a la semana. Opcionalmente, las organizaciones pueden tercerizar sus operaciones de seguridad con un Proveedor de servicios de seguridad (MSSP) asociado a IBM. Los MSSP ofrecen soluciones amplias de supervisión y gestión de seguridad, así como un amplio rango de servicios complementarios de supervisión de amenazas para cubrir casos de uso esenciales y avanzados.

IBM ha sido nuevamente seleccionada en el Cuadrante mágico Gartner 2019 por Servicios de Seguridad Gestionados, mundialmente.

Descargue el informe Forrester →

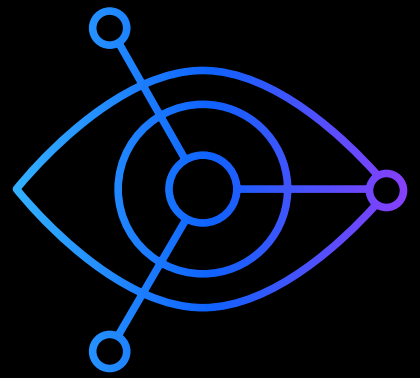
IBM ofrece seguridad gestionada a escala global con capacidades locales de entrega para ayudar a asegurar sus entornos de nube híbrida y multinube.

Obtenga más información sobre IBM Managed Security Services →

La infraestructura de QRadar on Cloud es

monitoreada: 24 horas, 7 días a la semana

por profesionales de IBM de confianza.[10]



Migre a un modelo de gastos operativos basado en la nube

IBM QRadar on Cloud aplica la experiencia obtenida en miles de implementaciones on premises de QRadar para suplir las necesidades de su entorno.

No hay necesidad de mantener o retocar software de seguridad local. Con actualizaciones de software automáticas y escalabilidad a pedido, QRadar on Cloud ayuda a simplificar la vida del equipo de seguridad de TI, migrando de un modelo de grandes gastos de capital (CAPEX) a un modelo más flexible basado en gastos operativos (OPEX).

El sistema es capaz de realizar análisis de nivel empresarial, con capacidades de incluyen:

- Recolección de datos y capacidades de correlación e informes para lograr la conformidad regulatoria
- Grandes máximos de eventos por segundo (EPS), cubriendo las necesidades de clientes con cientos de locales al rededor del mundo
- Configuración de sistema altamente disponible con niveles de servicio comprometidos y garantías de tiempo de funcionamiento
- Aplicaciones, complementos y extensiones por medio de IBM Security App Exchange
- Alertas enriquecidas con información de X-Force Threat Intelligence

¿Qué sigue?
Haga esta prueba de uso de 14 días de la solución QRadar on Cloud y conozca sus sofisticadas capacidades de detección.

Iniciar mi prueba sin costo →

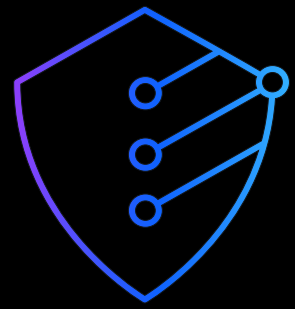
¿Por qué IBM?

IBM Security ofrece uno de los portafolios de productos y servicios de seguridad empresarial más avanzados e integrados. El portafolio, con el respaldo del mundialmente famoso X-Force Research, proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger holísticamente sus infraestructuras, datos y aplicaciones. Ofrece soluciones para la gestión de acceso e identidades, seguridad de base de datos, desarrollo de aplicaciones, gestión de riesgo, gestión de terminales, seguridad de la red y mucho más.

Estas soluciones permiten que las organizaciones gestionen efectivamente los riesgos e implementen seguridad integrada para arquitecturas móviles, en la nube, de redes sociales y otras arquitecturas comerciales empresariales. IBM opera una de las mayores organizaciones de investigación, desarrollo y entrega de seguridad del mundo, supervisa 15 mil millones de eventos de seguridad diarios en más de 130 países y posee más de 3.000 patentes de seguridad.

Además, IBM Global Financing ofrece diversas formas de pago para ayudarle a adquirir la tecnología que necesita para hacer crecer su empresa. IBM ofrece la gestión completa del ciclo de vida de los productos y servicios de TI, desde su adquisición hasta su desecho. Para obtener más información, visite ibm.com/financing.

Para saber más sobre IBM QRadar Security Intelligence Platform en la nube, póngase en contacto con su representante de IBM, Asociado de negocios de IBM o visite ibm.com/software/products/en/qradar-on-cloud.



IBM Corporation
New Orchard
Road Armonk, NY 10504

Producido en los Estados Unidos de América
febrero de 2020.

Este documento se actualizó por última vez en la fecha de su publicación y puede ser modificado por IBM en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Los ejemplos de cliente y datos de rendimiento mencionados fueron presentados solamente para propósitos ilustrativos. Los resultados de rendimiento reales pueden variar dependiendo de configuraciones específicas y condiciones de operación. LA INFORMACIÓN EN ESTE DOCUMENTO SE PROPORCIONA "TAL CUAL", SIN NINGUNA GARANTÍA, EXPRESA O IMPLÍCITA, SIN CUALQUIER GARANTÍA O COMERCIABILIDAD, ADECUACIÓN PARA UN PROPÓSITO PARTICULAR Y CUALQUIER GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. Los productos de IBM están garantizados de conformidad con los términos y condiciones de los contratos en virtud de los cuales se suministran.

El cliente es responsable de garantizar la conformidad con las leyes y los reglamentos aplicables. IBM no proporciona asesoría legal, ni representa ni garantiza que sus servicios o productos aseguren que el cliente cumple con cualquier ley o regulación.

Declaración de buenas prácticas de seguridad: La seguridad de los sistemas de TI implica proteger los sistemas y la información mediante prevención, detección y respuesta al acceso indebido dentro y fuera de su empresa. El acceso inadecuado puede causar alteración, destrucción, apropiación indebida o mal uso de la información o puede resultar en daño o uso indebido de sus sistemas, incluyendo el uso para atacar a otros. Ningún producto o sistema de TI deberá considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente eficaz en la prevención de la utilización o el acceso indebidos. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un enfoque de seguridad legal e integral, el cual necesariamente involucrará procedimientos operativos adicionales y puede requerir otros sistemas, productos o servicios para contar con el máximo de eficacia. IBM NO GARANTIZA QUE NINGÚN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE, HAGA A SU EMPRESA INMUNE, A LA CONDUCTA MALINTENCIONADA O ILEGAL DE CUALQUIER TERCERO.

1 IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_siem_vrt_ap_ov.html

2 "Data management challenges are having a severe impact on profitability." Help Net Security, 13 de marzo de 2019. https://www.helpnetsecurity.com/2019/03/13/data-management-challenges/

3 Josh Fruhlinger. "Top cybersecurity facts, figures and statistics for 2018." CSO, 10 de octubre de 2018. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics. html

4 "HIPAA Violations and Enforcement, American Medical Association. Consultado en diciembre de 2019. https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

5 2019 Cost of a Data Breach Report: https://www.ibm.com/security/data-breach

6 2018 Cost of a Data Breach Study: Global Overview. Realizado por el Instituto Ponemon. https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf

7 QRadar On Cloud Overview. YouTube. https://www.youtube.com/watch?time_continue=53&v=dCTnR_hHToU&feature=emb_logo

8 Marten Mickos, "The Cybersecurity Skills Gap Won't Be Solved in a Classroom." Forbes, junio de 2019. https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#353d37bd1c30

9 "Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap", SECURITY, noviembre de 2019, https://www.securitymagazine.com/articles/91224-cybersecurity-workforce-needs-to-grow-145-to-close-skills-gap

10 IBM Managed Services - https://www.ibm.com/security/services/managed-security-services

WGW03245-USEN-02