Acelerar la seguridad OT para reducir los riesgos con rapidez

La seguridad de los entornos tecnológicos operativos a medida que se digitalizan y conectan cada vez más.

Por: Serdar Cabuk, Jayne Goble, Ronald Heil, and Walter Risi

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Las organizaciones del sector del petróleo y el gas y otras organizaciones industriales se enfrentan a amenazas cibernéticas cada vez más frecuentes, no sólo para sus sistemas de tecnología de la información (TI), sino también para sus entornos de tecnología operativa (OT). A medida que la tecnología operativa está más conectada, digitalizada y automatizada, aumenta el potencial de los ciberatacantes para entrar y causar peligrosas alteraciones o anulaciones. Los accidentes y las exposiciones involuntarias también han causado incidentes importantes.

Por este motivo, hay que centrarse cada vez más en garantizar que los entornos de OT sean seguros y estén sujetos al mismo tipo de garantías de buenas prácticas que en el ámbito de las TI. Sólo en el último año, la lista de incidentes relacionados con las OT ha aumentado. Esto incluye un ciberataque a dos distribuidores alemanes de combustible y aceite[1] a finales de enero de 2022, que interrumpió las operaciones y la gestión de la cadena de suministro, y un ataque en 2021 que intentó interrumpir el suministro de agua en Oldsmar, Florida[2], obteniendo acceso remoto a la estación de control del sistema e intentando aumentar los niveles de hidróxido de sodio.

Cabe decir que sucesos como estos no son más que la punta del iceberg. Tanto si el motivo es financiero (instalar ransomware para exigir grandes pagos) o simplemente para causar alteraciones y poner en peligro el rendimiento y la seguridad de las infraestructuras esenciales, es de esperar que veamos más amenazas de este tipo para las empresas industriales en el futuro.

Sin duda, los atacantes están cada vez más profesionalizados y organizados, y tienen las herramientas a su disposición para llegar a los sistemas OT. El malware de TI y algunos programas maliciosos de OT son fácilmente accesibles en la dark web que pueden permitir a un hacker atravesar la "puerta principal" y entrar en los sistemas de una organización. Con las habilidades y conocimientos adecuados, los atacantes pueden aplicar otro malware para moverse de forma lateral y llegar al entorno OT. Los atacantes también harán su debida diligencia, investigando qué software utilizan los sistemas de control industrial (ICS) de una organización y evaluando a qué malware pueden ser susceptibles. Según nuestra experiencia, algunos de los programas informáticos que se utilizan con frecuencia para el funcionamiento de los sistemas de control industrial presentan vulnerabilidades potencialmente graves.

En este contexto, el refuerzo de la seguridad OT debe ser una prioridad absoluta. Y es algo que debe abordarse con rapidez: los ciberataques no esperarán a que las organizaciones puedan prepararse primero.

[1] BBC, Cyber-attack strikes German fuel supplies (2022)

[2] CNN, Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says (2021)

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

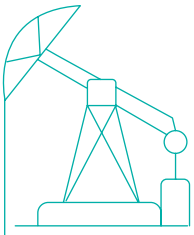
La convergencia de OT e IT

También es un imprescindible porque la OT está convergiendo cada vez más con la TI a medida que se introducen nuevas tecnologías para lograr eficiencias, ganancias de productividad y operaciones más inteligentes. Mientras que hace más o menos una década, la OT estaba segregada y era inaccesible, ahora se está conectando a otros sistemas. La OT independiente y no conectada no satisface las necesidades actuales de rendimiento y de otra índole. Una analogía sería con el sector de los servicios financieros: hace 10 o 15 años, los sistemas mainframe de los bancos estaban bloqueados, pero han tenido que rediseñarlos y digitalizarlos para satisfacer diversas necesidades modernas, como el Open Banking y normativas como la PSD2, que exigen nuevos protocolos y protecciones de seguridad.

Ahora, la convergencia de la OT y la TI significa que las organizaciones deben reducir la brecha entre las personas, los procesos y los sistemas de los dos entornos para construir una red más inteligente y segura con alta visibilidad para supervisar y controlar a ambos.

Esto nos lleva a un aspecto importante: ¿hasta qué punto es útil seguir distinguiendo la OT de la TI? A medida que los dos ámbitos se van acercando, gran parte de la OT es IT. Después de todo, el 80% de las plantas industriales tienen más servidores y TI que un banco promedio. Tal vez sea más útil (y probablemente será más necesario en el futuro, ya que las operaciones son cada vez más digitales) pensar simplemente en términos de tecnología. Tanto si se considera la OT como la TI, ambas se reducen a la tecnología. La opción de mantenerlos como entornos separados disminuirá cada vez más.

Esta combinación se está haciendo más visible de algunas formas interesantes, como el aumento en las organizaciones industriales de los Directores de Tecnología (CTO). En muchos sentidos, se trata de una función emergente: según nuestra experiencia, las responsabilidades de un CTO varían de una empresa a otra. Pero a medida que los directorios dan mayor prioridad a la transformación digital, es a los CTO a quienes se les pide que lideren el cambio, abarcando tanto las TI como las OT. El Director de Seguridad de la Información (CISO) sigue siendo una función clave para la seguridad, y a medida que la seguridad de OT se convierte en una prioridad, se está ampliando para abarcarla también. En cierto modo, el CISO está pasando de proteger la TI (normalmente, el dominio del CIO) a proteger toda la tecnología de la organización (el dominio del CTO). Por otra parte, algunas empresas tienen un CISO de OT específico que depende del CISO general. Los patrones varían (es un panorama en desarrollo) y será fascinante ver cómo se desenvuelve todo esto.



Ahora, la convergencia de la OT y la TI significa que las organizaciones deben **reducir la brecha** entre las personas, los procesos y los sistemas de los dos entornos para construir una red más inteligente y segura con alta visibilidad para supervisar y controlar a ambos.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Enfoques descendentes y ascendentes

Sea cual sea el caso, está claro que un componente esencial para asegurar la OT es contar con un marco de gobernanza descendente que establezca las funciones, las responsabilidades y las líneas de información, sin aplazar la aplicación de un mecanismo de detección y defensa ascendente. La definición de OT puede ser muy amplia, y se encuentra en todas las operaciones de una organización, lo que significa que normalmente no existe una única persona con responsabilidad para todo ello. Por lo tanto, es esencial coordinar los esfuerzos para abordar la seguridad de la OT. Esto requiere una estructura de gobernanza y un modelo operativo claros. Un mandato firme de la cúpula de la empresa es también un requisito previo, para impulsar la seguridad de la OT como una prioridad estratégica. Dicho esto, un enfoque de detección y defensa ascendente debe proceder casi en paralelo, ya que los actores de las amenazas no esperarán hasta que se establezca un marco de gobernanza. Mientras se instrumentan la gobernanza y el modelo operativo, deben implementarse las tecnologías de detección (idealmente, integradas en un Centro de Operaciones de Seguridad (SOC)), deben definirse las guías de respuesta para escenarios comunes (por ejemplo, ransomware) y deben tomarse medidas básicas de ciberhigiene.

Las estructuras maduras de gobernanza y modelo operativo están orientadas a ofrecer mejoras sostenibles a largo plazo, ayudando también a que la organización esté preparada para el futuro a medida que surjan nuevas tecnologías (y amenazas). Pero es un hecho simple que, mientras las organizaciones aprecian el valor y la importancia de estos enfoques estructurales descendentes, al mismo tiempo lo que casi siempre nos preguntan es: "¿Qué puedo aplicar hoy para marcar una diferencia inmediata? ¿Qué puedo hacer para reducir rápidamente los riesgos de la OT?".

Estas preguntas son válidas y apuntan al hecho de que hay una serie de medidas ascendentes que pueden tomarse junto con el marco descendente para marcar una diferencia rápida y significativa.

En muchos sentidos, se trata de un simple caso de no volver a inventar la rueda: importar las mejores prácticas de la seguridad de las TI a las OT (al igual que las TI pueden importar las mejores prácticas de las OT en otros aspectos, como la conciencia de seguridad). Así, hay tres áreas inmediatas que deberían evaluarse y abordarse:

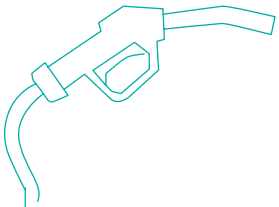
— Protección del terminal de los activos de OT

— Firewalls perimetrales alrededor de los activos de OT

— Segmentación de la red, dentro de OT y entre OT/IT

Junto a esto, las organizaciones deben implementar la visibilidad de la red OT en las primeras etapas de su proceso de seguridad OT. Hay una serie de tecnologías que permiten supervisar la red OT para detectar amenazas conocidas o comportamientos sospechosos. Lo ideal es que estas tecnologías se integren en el marco de supervisión y respuesta existente en la organización (que suele incluir un SOC y un equipo de respuesta a incidentes de seguridad informática).

Además, las organizaciones deben esforzarse por lograr una gestión de activos integrada, al menos para los activos más críticos. La mayoría de las empresas tienen un gran número de activos y varios sistemas de gestión de activos, desde la base de datos de gestión de la configuración de TI hasta los sistemas específicos de gestión de activos que puedan tener las áreas de OT. La capacidad de gestionar estos activos significa, en primer lugar, obtener y luego mantener la visibilidad de los mismos, por lo que debería ser una prioridad. Hay una serie de herramientas disponibles en el mercado que pueden infundir visibilidad a los activos.



Mientras se instrumentan la gobernanza y el modelo operativo, deben implementarse las **las tecnologías de detección** (idealmente, integradas en un Centro de Operaciones de Seguridad (SOC)), deben definirse las guías de respuesta para escenarios comunes (por ejemplo, ransomware) y deben tomarse medidas básicas de ciberhigiene.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Ocho preguntas clave

Para comprender el estado actual y, a continuación, implantar controles y procesos que puedan marcar una rápida diferencia, recomendamos hacerse estas ocho preguntas:

1 ¿Ha identificado los riesgos cibernéticos a los que está expuesta su red de control y está trabajando de forma activa para mitigarlos?

Una evaluación de los riesgos para la seguridad OT y una evaluación de la madurez cibernética pueden proporcionarle una visión de alto nivel de lo que debe abordarse tanto a nivel técnico como de gobernanza.

2 ¿Existe un inventario actualizado de su red de control?

Es vital saber qué necesita protección dentro de su entorno de producción. Existen muchas soluciones comerciales para la detección automática de activos que combinan capacidades de descubrimiento y detección de amenazas.

3 ¿Cuál es el nivel de integración entre la OT y la red corporativa?

El ransomware suele propagarse a través de la red que ataca. La segmentación puede limitar su movimiento, por ejemplo, de la red corporativa a la OT y viceversa. Las herramientas de los sistemas industriales de detección de intrusiones (IDS) tienen funciones que pueden ayudar a modelar una red segregada.

4 ¿Cómo se gestiona el acceso remoto a la red?

El acceso remoto seguro es un tema vital cuando se trata de mantener y reparar activos a distancia, especialmente en el mundo COVID y post-COVID. Los tipos de acceso remoto más comunes son el Protocolo de Escritorio Remoto (RDP) y la red privada virtual (VPN). Los softwares de acceso remoto seguro ya están disponibles en el mercado y deben ser considerados.

5 ¿Existe un mecanismo sólido de respaldo que se somete a pruebas de seguridad constantes?

Si se infiltran los activos de OT, las únicas opciones pueden ser o bien pagar el rescate que se pida (es cada vez más común que las organizaciones contraten un seguro contra el ransomware) o bien restaurar una copia de seguridad. Las copias de seguridad pueden ser complejas y el medio en el que se almacenan es fundamental para evitar que también se infecten con malware.

6 ¿Qué métodos se utilizan para aplicar los parches de seguridad?

La gestión de parches es esencial, y puede ser difícil si un activo está en uso 24/7. Los activos críticos deben actualizarse regularmente. Sin embargo, en el caso de los activos de baja criticidad, puede ser posible aplicar un parche en el siguiente intervalo de mantenimiento programado.

7 ¿Cuáles son sus soluciones antimalware actuales?

La detección temprana es crucial, por ejemplo, mediante herramientas IDS. Las herramientas de detección deben estar conectadas a un sistema de gestión de incidentes y eventos de seguridad (SIEM) que debe registrar múltiples fuentes, incluidos los firewalls, los activos y las herramientas de acceso remoto, para que pueda alertar a los equipos de un posible ataque.

8 ¿Tiene una mentalidad de confianza cero?

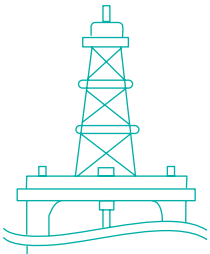
Muchas organizaciones consideran que la OT es una zona amurallada de la TI, y que todo lo que está detrás de ese muro es de confianza. Este modelo ha demostrado ser defectuoso: podemos remontarnos al ataque Stuxnet de 2010, cuando un sistema con medidas de seguridad Air Gap fue vulnerado a través de un proveedor afectado. En su lugar, las organizaciones deben empezar a adoptar una mentalidad y una arquitectura de confianza cero que no asuma nada sobre los niveles de confianza, sino que implique la recopilación de un contexto adicional dentro del tráfico de la red y, a continuación, la toma de decisiones sobre qué permitir o denegar en función de esta información. Aunque tiene sus raíces en las TI, la confianza cero puede adaptarse a las OT.

KPMG

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Aprovechar las tecnologías emergentes

Una vez establecida una base de seguridad sólida, las tecnologías de IA también pueden desempeñar su papel. Una postura de seguridad sólida exige "desplazar la seguridad hacia la izquierda", es decir, ampliar las capacidades de prevención y detección, evitando las amenazas antes de que se conviertan en incidentes perjudiciales. Esto requiere la identificación y caracterización de los activos, la detección de amenazas en una fase temprana y, en su caso, la respuesta autónoma. Se han desarrollado tecnologías de IA que pueden ofrecer a las organizaciones una forma de aumentar estas capacidades con aplicaciones de aprendizaje automático por capas.



Una postura de seguridad sólida exige **"desplazar la seguridad hacia la izquierda",** es decir, ampliar las capacidades de prevención y detección, evitando las amenazas antes de que se conviertan en incidentes perjudiciales.

Al observar de forma pasiva y comprender en forma dinámica el comportamiento contextual de todos los activos, la IA de autoaprendizaje proporciona un inventario de activos continuamente actualizado que permite a las organizaciones obtener una visibilidad completa de sus entornos convergentes de TI, OT y TI-OT. Además, la comprensión de la IA de autoaprendizaje de los matices que sustentan el comportamiento inusual le permite identificar la actividad amenazante en sus primeras etapas, presentando las amenazas para ser tratadas antes de que puedan escalar en una crisis.

La aceleración de las respuestas mediante el aprendizaje automático también es muy útil para defenderse del ransomware. Las empresas deben tomar medidas decisivas en el momento para detener la propagación, y el aprendizaje automático les permite evaluar la amenaza más rápido.

En el caso del ransomware que amenaza los entornos industriales, la capacidad de la IA de autoaprendizaje para responder de forma autónoma (calculando matemáticamente la forma más precisa de neutralizar una amenaza sin afectar a las operaciones normales) es muy valiosa, ya que puede interrumpir las amenazas en TI mucho antes de que tengan la oportunidad de propagarse a los sistemas de OT.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Conseguir un buen enfoque de personas y equipos

Esto nos lleva de nuevo a la cuestión de los límites entre las TI y las OT: en muchos sentidos, el reto para las organizaciones es mantener una separación prudente de la seguridad entre ambas y, al mismo tiempo, hacerlas converger operativamente.

La clave del éxito para este acto de equilibrio son las personas. Ambas funciones deben aprender la una de la otra a medida que se acercan.

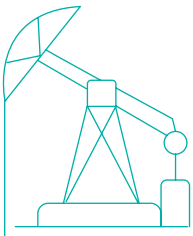
Por ejemplo, uno de los rasgos distintivos que está absolutamente incorporado a las personas que trabajan en entornos de OT es la cultura de la seguridad y el desafío. Estas actitudes deberían adoptarse dentro de las TI. Ahora que su trabajo está más integrado con los sistemas de fabricación o producción (y con las personas que los manejan físicamente), los administradores de TI deben reconocer los elevados riesgos asociados a la ciberseguridad. El cambio cultural resultante dentro de TI debería preparar mejor los procesos y flujos de trabajo del área para la convergencia.

Por otra parte, los procesos y flujos de trabajo de OT deben adaptarse a un calendario de actualizaciones más regular. Este enfoque es necesario para apoyar la ciberseguridad en un entorno convergente que contiene más dispositivos conectados y posibles vulnerabilidades. Los administradores de TI están familiarizados con este enfoque y su experiencia debe ser utilizada al diseñar nuevos procesos, sistemas y capacidades de OT para apoyar la convergencia.

En resumen, hay cosas que las personas de cada equipo pueden tomar de los demás y enseñarse mutuamente. La creación de una cultura común y un sentido de equipo (que subraye el hecho de que todos comparten, en última instancia, los mismos objetivos) es la clave del éxito. A menudo existe una falta de colaboración entre los equipos de TI y OT, lo que conduce a programas de seguridad débiles y descoordinados, así como a una financiación deficiente y a una escasa concienciación sobre los riesgos. Esto debe superarse mediante una mentalidad de colaboración que reconozca la creciente convergencia actual de la tecnología y las operaciones.

Al mismo tiempo, puede haber margen para combinar equipos o aspectos de equipos para lograr una mayor claridad y simplicidad. Por ejemplo, puede haber equipos que gestionen firewalls a ambos lados del muro de OT/IT: eliminar la duplicación de esfuerzos en este caso tiene sentido desde el punto de vista empresarial y también podría suponer un ahorro de costos.

Puede que sea algo lejano en el futuro, pero como las tareas se realizan cada vez más a distancia (incluso por parte del personal de OT que ya no necesita estar in situ para las actividades rutinarias), no sería sorprendente que, con el tiempo, los equipos de IT y OT se convirtieran en uno solo. Al igual que las disciplinas de TI y OT pueden quedar englobadas en el concepto único de tecnología.



La creación de una cultura común y un sentido de equipo (que subraye el hecho de que todos comparten, en última instancia, los mismos objetivos) **es la clave del éxito.**

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Cuatro puntos a tener en cuenta

La gestión de la OT en el agresivo entorno actual de ciberataques es un desafío. Exige una acción rápida para reducir los riesgos y encontrar enfoques que reconozcan la creciente convergencia de la OT con la TI.

BPero se puede hacer, y aquí hay algunos consejos prioritarios para medir su progreso.

1 **Tomar las mejores prácticas de las TI**
Tomar los procesos que son comunes en el entorno de las TI y aplicarlos a las OT. Por ejemplo, la gestión de parches se puede trasladar, no es algo que haya que reinventar.

2 **Consolidar y combinar** Reduzca el número de productos y enfoques de gestión de activos en uso, siempre que pueda. Simplificar hace que la tarea sea más manejable. Combine los grupos de OT e IT cuando realicen las mismas tareas, siempre que sea posible. Por supuesto, hay que asegurarse de no perjudicar la calidad y los estándares del servicio al hacerlo.

3 **Piense estratégicamente, pero también como un atacante**
Concéntrese en su programa a largo plazo, pero no pierda de vista el aquí y el ahora. ¿Cuáles son sus activos OT más valiosos a los ojos de un ciberdelincuente y cómo es probable que intente llegar a ellos?

4 **No intente lo imposible**
Céntrese en sus activos prioritarios y protéjalos. Si la mitad de su base de activos ya está detrás de una red segregada, céntrese en la otra mitad. No cree soluciones para cosas que ya son estándar: concéntrese en las vulnerabilidades y amenazas.

KPMG
© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Cómo puede ayudar KPMG

Las firmas de KPMG tienen una amplia experiencia en ayudar a las organizaciones industriales y de petróleo y gas a reducir rápidamente los riesgos de su OT. Podemos asesorar e implementar las mejores prácticas de la industria, la estandarización efectiva y las soluciones disponibles en el mercado. Gracias a nuestra amplia gama de relaciones y trabajos en el sector, "hablamos ambos idiomas": ¡hablamos con fluidez tanto de OT como de TI! Podemos ayudarle a reducir la brecha entre ambos, así como a crear un compromiso en todos los niveles de la organización, desde el directorio hasta la sala de control operativo.

Estaremos encantados de hablar con usted sobre cualquier aspecto de la aceleración de su OT: mantenerla modernizada, segura y protegida, y hacerla apta tanto para el presente como para el futuro.

About the authors

Dr Serdar Cabuk
Partner, Cyber and Technology Risk
KPMG in the UK
E: serdar.cabuk@kpmg.co.uk

Serdar is a partner in the Corporates Consulting practice at KPMG focusing on cyber and tech transformation in energy and consumer sectors. Previously he was the managing partner for a big four cyber practice in the Nordics and IBM's European leader for cyber risk services before that. He brings 20 years' of cyber, cloud and digital transformation experience also having led major response and recovery operations with global energy firms during several major incidents.

Jayne Goble
Director, Cyber Security
KPMG in the UK
E: jayne.goble@kpmg.co.uk

Jayne Goble, PhD leads KPMG's UK OT and IoT team and has over fifteen years' experience working with a range of global clients to oversee and deliver a variety of capital projects, ranging from responding to critical security failures of national infrastructure, to deployment of interception and intelligence platforms.

Ronald Heil
Global Cyber Security Leader for Energy and Natural Resources, KPMG International and Partner, KPMG in the Netherlands
E: heil.ronald@kpmg.nl

Ronald is a partner at KPMG in The Netherlands and is the Global Cyber Lead for the Energy and Natural Resources sector for KPMG International. He has extensive experience helping international companies connect their products and devices to the Internet of Things and providing information security and ICS/SCADA advice.

Walter Risi
Global IoT Lead and Partner
KPMG Argentina
E: wrisi@kpmg.com.ar

Walter is the Global IOT Lead and the Technology and Cyber Security Consulting leader at KPMG in Argentina. During his 20-year career, he has assisted companies in the application of technology management best practices, cybersecurity, transformation and software engineering. He's led both technology consulting teams and software development factories and is currently focused on the convergence of agility and cybersecurity in Digital Transformation.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Acknowledgments

This magazine would not be possible without the collaboration from colleagues around the world who generously contributed their support, knowledge and insights into the planning, analysis, writing and production of this report. Thank you to Tzouliano Chotza, Lyndie Dragomir, Nicole Duke, Mark Hamilton, Carmen Millet and Richard Turitz.

Contacts

Regina Mayor
Global Head of Energy
KPMG International
E: rmayor@kpmg.com

Valerie Besson
Regional Energy & Natural Resources Leader for Europe/Middle East/Africa (EMA) and National Sector Leader, Energy and Utilities
KPMG in France
E: valeriebesson@kpmg.fr

Manuel Fernandes
Regional Energy & Natural Resources Co-Leader for Americas and National Oil & Gas Leader
KPMG in Brazil
E: mfernandes@kpmg.com.br

Ronald Heil
Global Cyber Security Leader for Energy and Natural Resources
KPMG in the Netherlands
E: heil.ronald@kpmg.nl

Angela Gildea
Regional Energy & Natural Resources Co-Leader for Americas and National Sector Leader, Energy, Natural Resources and Chemicals
KPMG in the US
E: angelagildea@kpmg.com

Jonathon Peacock
Regional Energy & Natural Resources Leader for Asia Pacific (ASPAC) and Oil & Gas Leader
KPMG Australia
E: jjpeacock@kpmg.com.au

home.kpmg/drillingdown

home.kpmg/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Throughout this document, "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Designed by Evalueserve.
Publication name:Drillng Down
Publication number: 138002-G
Publication date: April 2022