Acelerando a segurança de OT para uma redução de riscos ágil

Protegendo ambientes de tecnologia operacional (OT) conforme eles se tornam cada vez mais digitalizados e conectados

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

As indústrias de petróleo e gás e outras organizações industriais estão enfrentando cada vez mais ameaças cibernéticas, não apenas em seus sistemas de tecnologia da informação (TI), mas também nos ambientes de tecnologia operacional (*operational technology* - OT). À medida que a OT se torna mais conectada, digitalizada e automatizada, o potencial para ataques cibernéticos que podem causar panes ou reversões perigosas aumenta simultaneamente. Acidentes e exposições não intencionais também têm causado incidentes da mesma proporção.

É por isso que é necessário assegurar que os ambientes de OT sejam seguros e que tenha as mesmas boas práticas que o domínio de TI. No ano passado, a lista de incidentes relacionados à OT cresceu. Isso inclui um ataque cibernético a duas distribuidoras alemãs de óleo e combustível[1] ocorrido em janeiro de 2022 que interrompeu as operações e o gerenciamento da cadeia de suprimentos, e um ataque em 2021 que obteve acesso remoto à estação de controle do sistema de água de Oldsmar, na Flórida (EUA)[2], na tentativa de interromper o abastecimento de água e elevar os níveis de hidróxido de sódio.

Pode-se dizer que eventos como esses são provavelmente apenas a ponta do iceberg. Seja por motivos financeiros, como instalar *ransomwares* para extorquir grandes pagamentos, seja simplesmente para causar pane e pôr em risco o desempenho e a segurança da infraestrutura básica, pode-se esperar mais ameaças desse tipo às empresas industriais no futuro.

Certamente, os invasores estão se tornando mais profissionalizados e organizados e têm ferramentas à sua disposição para atingir os sistemas de OT. Os *malwares* de TI e alguns de OT são facilmente encontrados na *dark web* e podem permitir que um *hacker* entre nos sistemas da organização. Com conhecimento e as habilidades certas, os invasores podem então aplicar outros *malwares* para se mover lateralmente e atingir o ambiente de OT.

Os invasores também farão a sua *due diligence*, pesquisando quais programas de *software* são utilizados pelos sistemas de controle industrial (*industrial control systems* - ICS) de uma organização e avaliando a quais *malwares* eles podem ser suscetíveis. Além disso, alguns programas de *software* geralmente utilizados nos ICSs têm vulnerabilidades potencialmente graves.

Nesse contexto, fortalecer a segurança da OT deve ser uma prioridade absoluta. Isso é algo que deve ser feito depressa, já que os invasores cibernéticos não vão esperar que as organizações tenham a oportunidade de se preparar primeiro.

[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.

Convergência entre OT e TI

A convergência entre OT e TI também é uma prioridade, porque a OT está convergindo cada vez mais para a TI conforme novas tecnologias são introduzidas para gerar eficiências, ganhos de produtividade e operações mais inteligentes. Há mais ou menos uma década, a OT era segregada e inacessível, mas agora está sendo conectada a outros sistemas.

Hoje em dia, uma OT autônoma, não conectada, simplesmente não atende às necessidades de desempenho, entre outras. Podemos fazer uma analogia com o setor de serviços financeiros. Há dez ou 15 anos atrás, os sistemas de *mainframe* dos bancos eram isolados, mas tiveram que ser reprojetados e digitalizados para atender a várias necessidades modernas, como o *open banking*, e a regulamentos, como o PSD2, o que exigiu novos protocolos de segurança e mais proteções.

A convergência entre OT e TI significa que as organizações devem aproximar as pessoas, os processos e os sistemas dos dois ambientes para criar uma rede mais inteligente e mais segura, com alta visibilidade para monitorá-los e controlá-los.

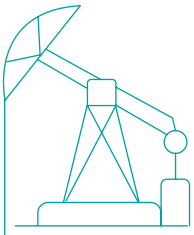
Isso nos leva a uma questão importante: até que ponto é útil distinguir OT de TI atualmente? À medida que os dois domínios se aproximam, essa distinção é mais sútil. Afinal, 80% das plantas industriais têm mais servidores e TI do que um banco de porte médio.

Talvez seja mais útil pensar simplesmente em termos de tecnologia, e provavelmente será mais necessário no futuro, uma vez que as operações têm se tornado cada vez mais digitais. Quer se pense em OT, quer se pense em TI, ambas se resumem à tecnologia. A opção de mantê-las como ambientes separados irá diminuir gradativamente.

Essa integração está se tornando mais visível de diferentes formas, tais como o crescimento da relevância do diretor de tecnologia (*Chief Technology Officer* - CTO) nas organizações industriais. Essa ainda é uma função recente, e suas responsabilidades variam de empresa para empresa.

Contudo, à medida que os conselhos priorizam cada vez mais a transformação digital, os CTOs têm sido procurados para liderar essa mudança, abrangendo TI e OT. O diretor de segurança da informação (*Chief Information Security Officer* - CISO) continua sendo uma função imprescindível para a segurança, já que a segurança da OT tem se tornado uma realidade e a função do cargo se estende para cobri-la também.

De certa forma, a função de CISO está mudando de proteção da TI (geralmente domínio do *Chief Information Officer* - CIO) para a proteção de toda a tecnologia da organização (domínio do CTO). Algumas empresas também podem ter um CISO específico de OT que se reporta ao CISO geral. Os padrões variam, pois se trata de um quadro em desenvolvimento, e será interessante observar o rumo dessa transformação.



Agora, a convergência de OT e TI significa que as organizações devem

preencher a lacuna

entre as pessoas, processos e sistemas dos dois ambientes para construir uma rede mais inteligente e segura, com alta visibilidade para realizar o seu monitoramento e controle. Agora, a convergência de OT e TI significa que as organizações devem preencher a lacuna entre as pessoas, processos e sistemas dos dois ambientes para construir uma rede mais inteligente e segura com alta visibilidade para monitorar e controlar ambos os ambientes.

Abordagens de cima para baixo e de baixo para cima

Qualquer que seja o caso, um componente essencial para a proteção da OT é ter uma estrutura de governança de cima para baixo para estabelecer funções, responsabilidades e linhas de relatórios, sem protelar a implementação de um mecanismo de detecção e defesa de baixo para cima.

A definição de OT pode ser muito ampla. Ela é encontrada em todas as operações de uma organização, o que significa que, geralmente, não há uma única pessoa responsável por todas as funções. Portanto, é essencial coordenar os esforços para tratar da segurança da OT. Isso requer uma estrutura de governança e um modelo operacional claros. Uma forte autoridade da liderança da empresa é um pré-requisito para tratar a segurança de OT como uma prioridade estratégica.

Além disso, uma abordagem de detecção e defesa de baixo para cima deve ocorrer quase em paralelo, pois os invasores não esperarão até que uma estrutura de governança seja estabelecida pela empresa. Enquanto o modelo de governança e de operação é orquestrado, tecnologias de detecção (idealmente integradas a um centro de operações de segurança [*Security Operations Center*, SOC]) devem ser implementadas, esquemas de respostas para cenários comuns devem ser definidos (por exemplo, *ransomwares*) e medidas básicas de limpeza cibernética devem ser adotadas.

Estruturas maduras de governança e modelo operacional devem produzir melhoras sustentáveis a longo prazo, ajudando também a blindar a organização no futuro, conforme surjam novas tecnologias e ameaças. No entanto, embora as organizações apreciem o valor e a importância dessas abordagens estruturais de cima para baixo, algumas questões são levantadas, como "*o que posso conectar hoje para fazer uma diferença imediata*?" ou "*o que posso fazer para obter uma redução rápida nos riscos de OT*?".

Essas perguntas são válidas e apontam para o fato de que existem algumas medidas de baixo para cima que devem ser tomadas com a estrutura de cima para baixo para fazer uma diferença rápida e significativa.

Em grande medida, talvez seja o caso de não reinventar a roda: importar as melhores práticas de segurança da TI para a OT e vice-versa, como a consciência da segurança, por exemplo. Assim, há três áreas que devem ser avaliadas e atendidas de imediato:

— Proteção de *endpoint* dos ativos de OT.

— *Firewalls* perimetrais em torno dos ativos de OT.

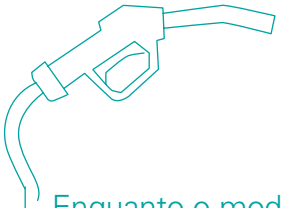
— Segmentação de rede dentro da OT e entre OT e TI.

Além disso, nos estágios iniciais de sua jornada de segurança de OT, as organizações devem implementar a visibilidade dessa rede. Existem algumas tecnologias que permitem a sua monitoração contra ameaças conhecidas ou comportamentos suspeitos.

O ideal é que essas tecnologias sejam integradas à estrutura existente de monitoramento e resposta da organização, o que normalmente inclui um SOC e uma equipe de resposta a incidentes de segurança em computadores.

Além disso, as empresas precisam lutar pelo gerenciamento dos ativos integrados, pelo menos os mais importantes. A maioria das empresas tem um grande número de ativos e vários sistemas de gerenciamento, desde bancos de dados de gerenciamento de configurações de TI até sistemas de gerenciamento de ativos específicos que as áreas de OT podem ter.

A capacidade de gerenciar esses ativos consiste em primeiro obter e depois manter a sua visibilidade, portanto, essa deve ser uma prioridade. Há uma série de ferramentas disponíveis no mercado que podem produzir visibilidade nos ativos.



Enquanto o modelo de governança e de operação é organizado, algumas ações precisam ser realizadas: a implementação da **detecção de tecnologias** (integradas em uma operação de segurança Cerisano [SOC]), o desenvolvimento de manuais de respostas para possíveis incidentes, como invasões por *ransomware*, e a adoção de medidas básicas de higiene cibernética.

Oito perguntas-chave

Para entender a situação atual e depois implementar controles e processos que possam fazer a diferença rapidamente, recomendamos a reflexão a respeito das oito perguntas a seguir:

1 Foram identificados os riscos cibernéticos aos quais a rede de controle está exposta e eles estão sendo ativamente trabalhados para sua redução?

Uma avaliação dos riscos de segurança de OT e uma avaliação da maturidade cibernética podem dar uma boa ideia do que será necessário considerar nos âmbitos técnico e de governança.

2 Há um inventário atualizado da rede de controle?

É fundamental saber o que precisa ser protegido no ambiente de produção. Há muitas soluções comerciais disponíveis para detecção automática de ativos que combinam recursos de descoberta e identificação de ameaças.

3 Qual é o nível de integração entre OT e a rede corporativa?

O *ransomware* se espalha geralmente pela rede que ele ataca. A segmentação pode limitar os movimentos, por exemplo, da rede corporativa para a OT e vice-versa. As ferramentas dos sistemas de detecção de intrusão industriais (*industrial intrusion detection systems* - IDS) têm recursos que podem auxiliar na modelagem de uma rede segregada.

4 Como o acesso remoto à rede é gerenciado?

O acesso remoto seguro é um tópico fundamental quando se trata da manutenção e reparo de ativos à distância, especialmente em um cenário durante e pós-pandemia. Os tipos de acesso remoto comuns incluem *remote desktop protocol* (RDP) e rede virtual privada (*virtual private network* - VPN). Os *softwares* de acesso remoto seguro atualmente estão disponíveis no mercado e devem ser considerados.

5 Há um mecanismo de backup robusto em vigor e a segurança é testada de maneira consistente?

Caso os ativos de OT sejam invadidos, as únicas opções podem ser pagar qualquer quantia de resgate exigida (hoje, as organizações têm feito seguro para *ransomware* cada vez mais) ou restaurar um *backup*. Os *backups* podem ser complexos e o meio em que eles são armazenados é crucial para evitar que sejam infectados também por *malware*.

6 Quais métodos são utilizados para aplicar patches de segurança?

Gerenciar os *patches* é essencial e pode ser difícil se um ativo estiver em uso 24 horas por dia, sete dias por semana. Os ativos críticos devem ser atualizados regularmente. Entretanto, para ativos de baixa criticidade, às vezes é possível aplicar um *patch* no próximo intervalo de manutenção programado.

7 Quais são as soluções *antimalware* atuais?

A detecção precoce é crucial, por exemplo, por meio das ferramentas de *Intrusion Detection System* (IDS). Essas ferramentas devem ser conectadas a um sistema de Gerenciamento de Incidentes e Eventos de Segurança (*Security Incident and Event Management* - SIEM), que deve registrar várias fontes, inclusive *firewalls*, ativos e ferramentas de acesso remoto para alertar as equipes sobre um possível ataque.

8 Há uma mentalidade de confiança zero (*zero trust*)?

Muitas organizações veem a OT como algo apartado da TI, totalmente confiável. Esse modelo mostrou-se falho: podemos citar o ataque do Stuxnet em 2010, quando um sistema verdadeiramente isolado foi violado por meio de um fornecedor comprometido.
Em vez disso, as organizações precisam adotar uma mentalidade e uma arquitetura de confiança zero (*zero trust*), em que não se presuma nada sobre os níveis de confiança e que envolva a coleta de contexto adicional dentro do tráfico da rede e, em seguida, a tomada de decisões sobre o que permitir ou negar com base nessas informações. Embora tenha suas raízes na TI, a zero trust pode ser adaptada para a OT.

Aproveitando as tecnologias emergentes

Uma vez criada uma base sólida de segurança, as tecnologias de inteligência artificial (IA) também têm um papel a desempenhar. Uma postura de segurança robusta exige "deslocar a segurança para a esquerda", isto é, ampliar os recursos de prevenção e detecção, evitando ameaças antes que elas se se transformem em incidentes danosos.

Uma postura de segurança robusta exige **"deslocar a segurança para a esquerda",** isto é, ampliar os recursos de prevenção e detecção, evitando ameaças antes que elas se se transformem em incidentes danosos.

Isso requer a identificação e caracterização dos ativos, a detecção precoce das ameaças e, se apropriado, uma resposta autônoma. Foram desenvolvidas tecnologias de IA que possibilitam às organizações aumentar esses recursos com aplicações em camadas de *machine learning*.

Ao observar passivamente e entender dinamicamente o comportamento contextual de todos os ativos, a IA de autoaprendizagem fornece um inventário de ativos continuamente atualizado, que possibilita às organizações ganhar total visibilidade em seus ambientes de TI, OT e TI-OT convergidas. Além disso, a compreensão das nuances que indicam um comportamento incomum permite que a IA de autoaprendizagem identifique a atividade ameaçadora em seus estágios iniciais, apresentando-a antes que ela possa se transformar em uma crise.

Acelerar as respostas por meio de *machine learning* também é particularmente útil na defesa contra *ransomwares*. As empresas têm que tomar medidas decisivas imediatas para interromper a propagação da ameaça, e o *machine learning* as capacita a realizar uma avaliação mais rapidamente.

Em ambientes industriais sujeitos a ameaças de *ransomware*, a capacidade da IA de autoaprendizagem de responder de forma autônoma – calculando matematicamente a maneira mais precisa de neutralizar uma ameaça sem afetar as operações normais – é muito valiosa, pois pode interromper as ameaças na TI muito antes que elas tenham a chance de se espalhar nos sistemas de OT.

Obtendo a abordagem correta das pessoas e equipes

Isso nos traz de volta à questão dos limites entre TI e OT – em muitos sentidos, o desafio das organizações é manter uma separação de segurança prudente entre as duas áreas e, ao mesmo tempo, fazê-las convergir operacionalmente.

A chave para o sucesso desse ato de equilíbrio são as pessoas. Ambas as funções devem aprender uma com a outra à medida que ficam mais próximas.

Por exemplo, um atributo que está absolutamente incorporado nos profissionais que trabalham em ambientes de OT é a cultura de segurança e desafio. Essas atitudes devem ser adotadas dentro da TI também. Agora que seu trabalho está mais diretamente integrado aos sistemas de fabricação ou produção e às pessoas que os operam fisicamente, os administradores de TI precisam reconhecer os altos riscos associados à segurança cibernética. A mudança cultural resultante dentro da área deve preparar melhor os seus processos e fluxos de trabalho para a convergência.

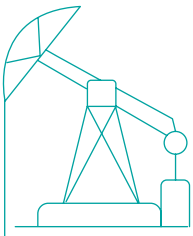
Por outro lado, os processos e fluxos de trabalho de OT devem ser adaptados para se ajustarem a um cronograma de atualizações mais regulares. Essa perspectiva é necessária para respaldar a segurança cibernética em um ambiente de convergência com mais dispositivos conectados e possíveis vulnerabilidades. Os administradores de TI estão familiarizados com essa abordagem e devem usar seu conhecimento ao planejar novos processos, sistemas e recursos de OT para apoiar a convergência.

Em síntese, há fatores que cada equipe pode aprender e ensinar umas às outras. Criar uma cultura comum e senso de equipe, ressaltando o fato de que, no fundo, todos têm os mesmos objetivos, é a chave para o sucesso.

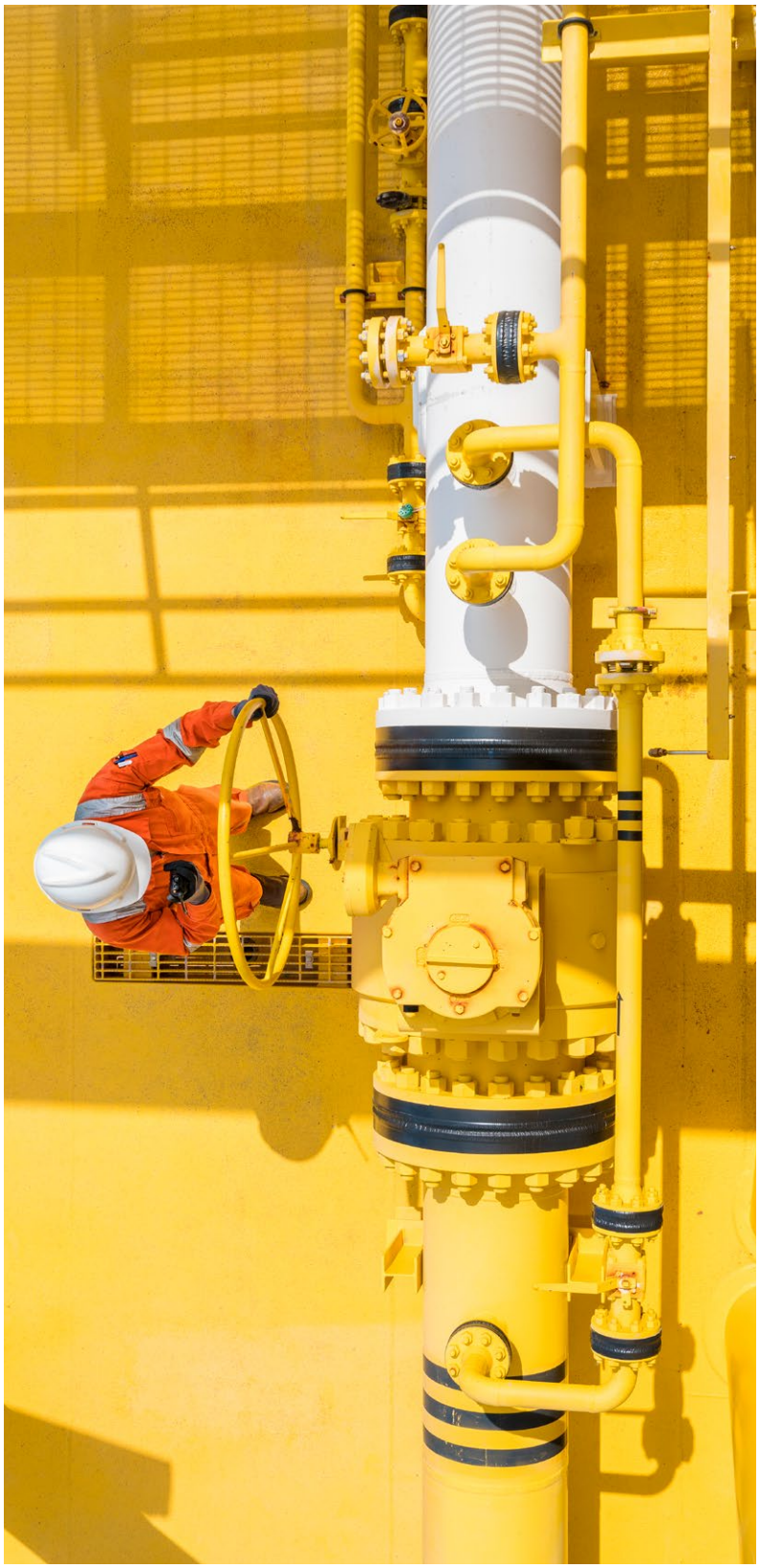
Muitas vezes, observamos a falta de colaboração entre as equipes de TI e OT, o que resulta em programas de segurança fracos e descoordenados e em financiamento insuficiente e pouca conscientização sobre os riscos. Isso precisa ser superado por meio de uma mentalidade colaborativa, que reconheça a centralização cada vez maior entre tecnologia e operações nos dias de hoje.

Ao mesmo tempo, pode haver escopo para a combinação de equipes ou de seus aspectos para maior clareza e simplicidade. Por exemplo, podem existir equipes gerenciando os *firewalls* em ambos os lados do muro entre OT e TI. Remover a duplicação de esforços aqui faz sentido para a empresa e também pode gerar economia de custos.

Pode estar um pouco distante, mas como as tarefas são cada vez mais executadas de forma remota, mesmo pelo pessoal de OT, que não precisa mais estar fisicamente no local para as atividades de rotina, não surpreenderia se, no futuro, as equipes de TI e OT fossem integradas, da mesma forma que as disciplinas dessas áreas poderão ser englobadas em um único conceito de tecnologia.



Criar uma cultura comum e um sentido de equipe – destacando o fato de que todos compartilham os mesmos objetivos — é a **chave para o sucesso.**



Quatro conclusões

Gerenciar a OT no ambiente de ataques cibernéticos agressivos dos dias de hoje é um desafio. É necessário agir rapidamente para reduzir os riscos enfrentados e encontrar abordagens que reconheçam a crescente convergência de OT com TI.

Isso pode ser feito, por isso, seguem algumas dicas prioritárias checagem e medição do progresso nesse desafio.

1 Estude as melhores práticas de TI

Conheça os processos que são comuns no ambiente de TI e aplique-os à OT. Por exemplo, o gerenciamento de *patches* pode ser feito, ou seja, não é algo que precise ser reinventado.

2 Consolide e combine

Quando possível, reduza o número de métodos de gerenciamento de produtos e ativos em uso. Simplificar torna a tarefa mais administrável. Combine grupos de OT e TI quando eles estiverem executando as mesmas tarefas, quando apropriado. Será necessário ter certeza de que não há prejuízo da qualidade e dos padrões do serviço ao fazê-lo.

3 Pense de forma estratégica, como se fosse o invasor

Concentre-se em seu programa de longo prazo, mas não perca de vista o momento atual. Quais são seus ativos de OT mais valiosos aos olhos de um criminoso cibernético, e como ele provavelmente vai tentar alcançá-los?

4 Não perca tempo tentando fazer o impossível

Concentre-se em seus ativos prioritários e os proteja. Se metade da sua base de ativos já está protegida por uma rede segregada, foque na outra metade. Não crie soluções para coisas que já estão dentro do padrão: mantenha o foco nas vulnerabilidades e ameaças.

Como a KPMG pode ajudar

A KPMG tem vasta experiência em ajudar as empresas industriais e de petróleo e gás a reduzir os riscos rapidamente em sua OT. Prestamos assessoria e implementamos as melhores práticas, a padronização efetiva e soluções de mercado disponíveis no setor.

Devido à nossa ampla gama de relacionamentos e trabalho no setor, conhecemos as duas áreas: OT e TI. Podemos ajudar você a fazer a ponte entre elas e gerar engajamento em todos os níveis da organização – da diretoria até a sala de controle operacional.

Entre em contato conosco para tratar de qualquer aspecto referente à aceleração da área de OT, mantendo-a modernizada e segura e fazendo-a se ajustar ao presente e ao futuro.

Fale com o nosso time

Rodrigo Milo
Sócio de Cyber Security & Privacy
da KPMG no Brasil
rodrigomilo@kpmg.com.br

Leandro Augusto
Sócio-líder de Cyber Security &
Privacy da KPMG no Brasil e
na América do Sul
lantonio@kpmg.com.br

Walter Risi
Sócio-líder global de Cyber Security
em IioT da KPMG na Argentina
wrisi@kpmg.com.ar