BDO

Guardians of digital trust
Cybersecurity Awareness Month

Colmatar a lacuna de profissionais de Cibersegurança

Reforçar o esforço humano com IA

Colmatar a lacuna de profissionais de Cibersegurança: *reforçar o esforço humano com IA*

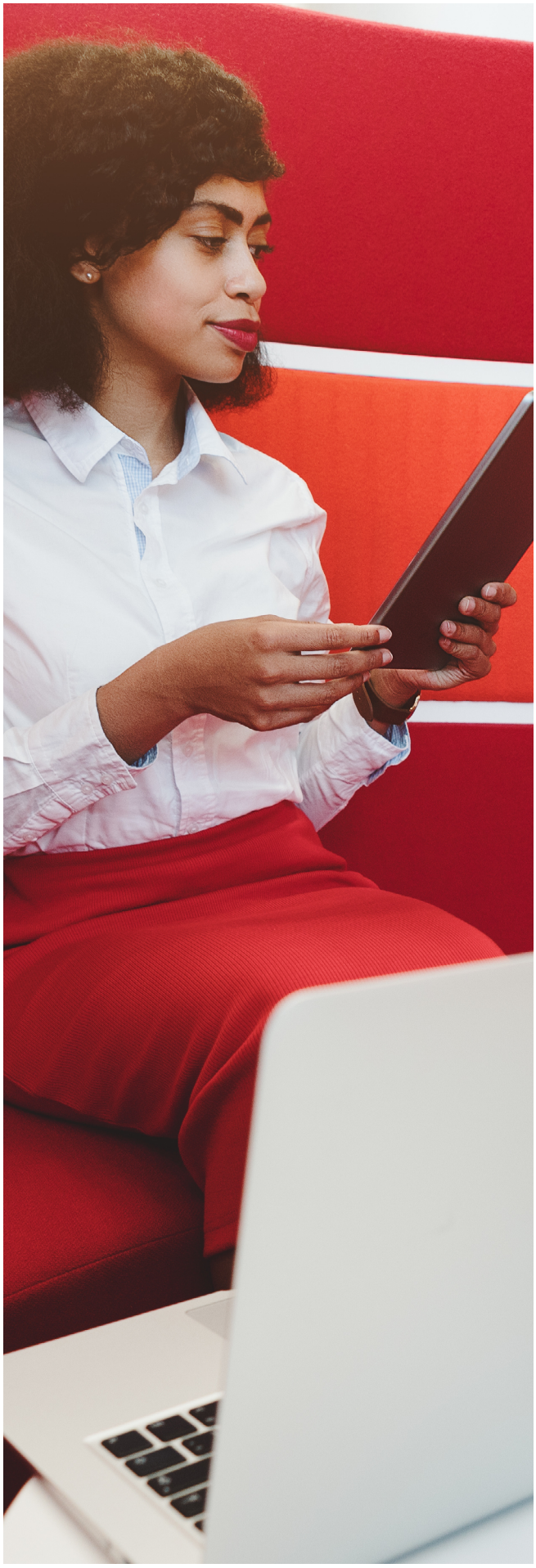
Numa era em que a transformação digital está a remodelar indústrias, enfrentamos um desafio significativo: uma crescente divisão entre organizações que estão em extremos opostos do espectro de resiliência cibernética. Um contributo significativo para esta divisão crescente é a crescente escassez de profissionais qualificados em cibersegurança e, à medida que as ameaças cibernéticas continuam a crescer em volume, velocidade e sofisticação, as organizações têm dificuldade em proteger eficazmente a sua pegada digital em rápida expansão. A escassez de talentos em cibersegurança, a adoção acelerada de novas tecnologias e o cenário de ameaças em constante evolução representam um risco substancial para todas as organizações que utilizam tecnologia globalmente.

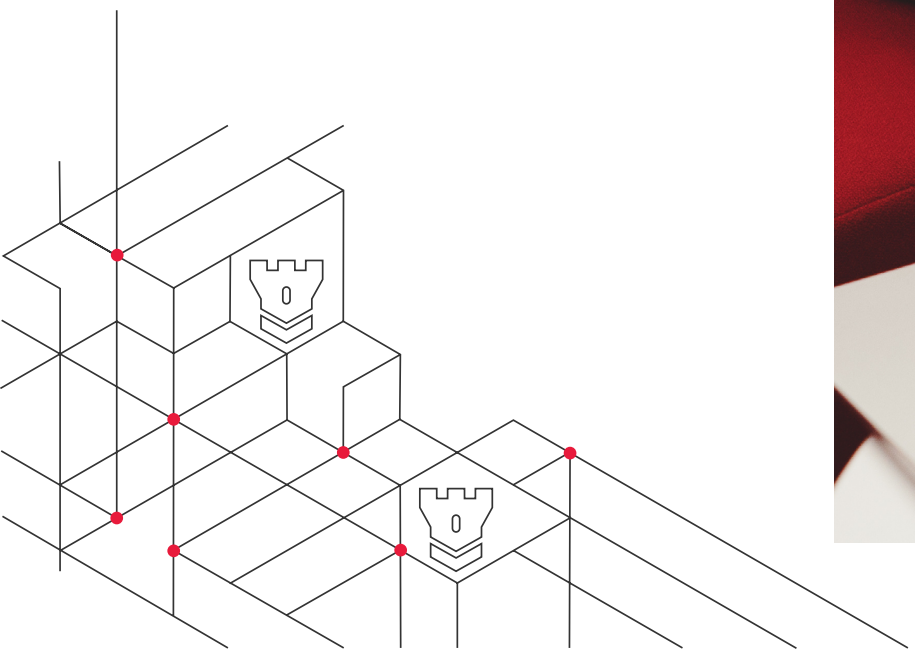
Em setembro de 2024, o International Information System Security Certification Consortium (ISC)² conduziu um estudo que destaca a crescente lacuna na força de trabalho em cibersegurança. O estudo revelou uma carência global de 4,8 milhões de profissionais de cibersegurança necessários para proteger eficazmente as organizações. O ISC² indica que a lacuna cresceu significativamente, estimando um aumento de 19% ano após ano.

"O Estudo da Força de Trabalho em Cibersegurança do ISC² destaca uma perceção preocupante entre os profissionais de cibersegurança. Após dois anos de investimento decrescente na contratação e nas oportunidades de desenvolvimento profissional, as organizações estão agora a enfrentar uma escassez significativa de competências e pessoal – um problema que os profissionais alertam estar a aumentar o risco geral", disse Andy Woolnough, Vice-Presidente Executivo de Assuntos Corporativos do ISC². "Num momento em que a instabilidade global e tecnologias emergentes como a IA estão a aumentar rapidamente o cenário de ameaças, o investimento no desenvolvimento de competências e na próxima geração da força de trabalho em cibersegurança

Descubra o nosso segundo artigo da série: a crescente divisão entre organizações resilientes em cibersegurança e não resilientes.

O défice de talentos em cibersegurança é resultado da falta de formação e educação de qualidade, da falta de investimento em pessoal por parte das organizações, dos desafios orçamentais e, muitas vezes, da dificuldade em reter pessoal qualificado devido ao papel desafiante e, por vezes, ingrato de um profissional de cibersegurança. A perspetiva parece sombria e, se não for corrigida, levará a consequências a longo prazo para empresas e organizações de todos os tamanhos. Existem duas áreas em que devemos focar-nos. A primeira e mais óbvia é desenvolver o talento que já temos nas nossas organizações, proporcionando-lhes a experiência e a capacidade de que precisam para nos ajudar a defender os nossos ativos. Precisamos de nos concentrar no desenvolvimento contínuo de competências, bem como na retenção destes indivíduos no campo. A segunda é aproveitar as capacidades tecnológicas mais recentes e avançadas para apoiar estes indivíduos a acompanhar o aumento do volume, focando a sua atenção em tarefas complexas/de alto valor, enquanto utilizamos a tecnologia para lidar com funções rotineiras/de baixo valor. À medida que lutamos com a escassez de talentos, soluções modernas como a inteligência artificial (IA) e a automação estão a emergir como facilitadores chave para fechar esta lacuna e proteger os nossos sistemas críticos.





A escala da escassez de talento em cibersegurança

A atual lacuna de competências em cibersegurança é um problema complexo de resolver, pois, no seu cerne, a questão é o ritmo da mudança tecnológica. A Indústria 4.0 proporcionou-nos novas formas de trabalhar, colaborar e automatizar que nunca pensámos ser possíveis. Com cada evolução do panorama tecnológico, surgem exponencialmente mais novos vetores de ataque, à medida que os atacantes procuram fraquezas nos sistemas e empregam táticas sofisticadas para ganhar acesso a estes patrimónios tecnológicos em constante mudança e expansão. A evolução constante requer uma força de trabalho em cibersegurança que seja habilidosa nos princípios de segurança tradicionais, mas que também seja capaz de se adaptar às novas tecnologias e aos métodos modernos de proteção dessas capacidades.

A velocidade dos negócios e da evolução tecnológica torna difícil para os profissionais de cibersegurança acompanhar, especialmente neste mercado onde a escassez de talentos é prevalente e os atacantes estão vários passos à frente. É aqui que a contínua educação, a aprendizagem contínua para profissionais no campo sobre métodos modernos e um foco na contratação de talentos com experiência académica e prática são fundamentais.

IA: Um multiplicador de força para a ciberdefesa

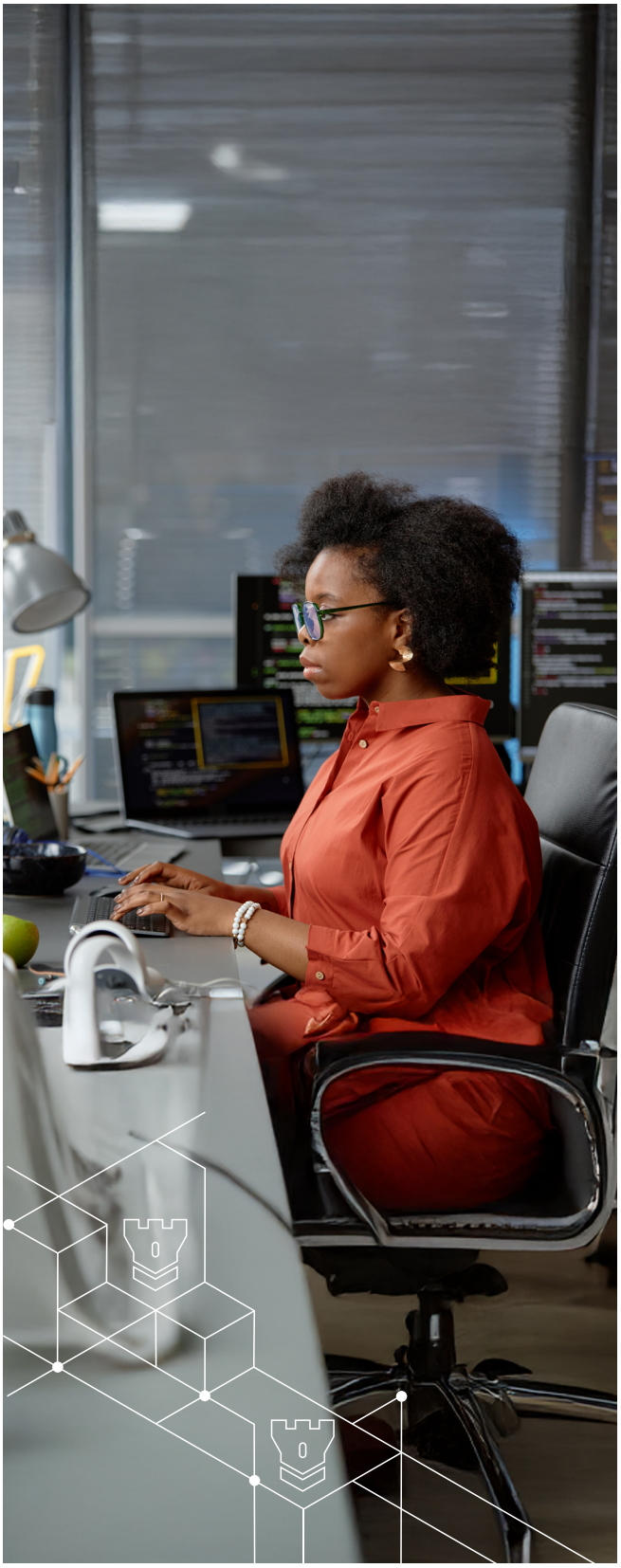
Os avanços na tecnologia também estão a alimentar oportunidades para as equipas de defesa cibernética. Como uma oportunidade para combater esta escassez de talentos, a inteligência artificial e a automação oferecem a oportunidade de um programa de cibersegurança mais sustentável e eficiente. A IA não substituirá a experiência humana, mas pode ser aproveitada como uma capacidade eficaz para aumentar os esforços humanos, permitir que os humanos acompanhem o ritmo e permitir que as organizações façam mais com menos recursos.

A IA e a machine learning com grandes modelos de linguagem analisam grandes quantidades de dados a uma alta velocidade, com a capacidade de encontrar padrões e sinalizar riscos em tempo quase real. Isto traz à superfície os maiores riscos para os recursos humanos, para que possam concentrar-se em atividades de investigação mais complexas. As ferramentas tradicionais de cibersegurança baseadas em regras dependem de assinaturas estáticas, muitas vezes lógica binária, e quase sempre criam ruído e distrações para os profissionais de cibersegurança. Os sistemas de IA podem aprender com dados, padrões, e estes sistemas adaptam-se para elevar aqueles sinais que são mais relevantes para os humanos analisarem. Quer sejam usados para identificar novos e incomuns padrões de comportamento, mapear comportamentos para técnicas conhecidas de maus atores ou identificar comportamentos desconhecidos que imitam comportamentos mais comuns com um ataque cibernético, estas tecnologias melhoram significativamente a capacidade de uma organização de responder a ameaças emergentes. Ameaças desta natureza passariam despercebidas por sistemas convencionais, ajudando o pessoal de cibersegurança a chegar à causa raiz mais rapidamente e a mitigar ameaças de forma quase imediata, com menos recursos humanos.

O benefício de ter a IA a lidar com tarefas repetitivas e pesadas em dados é uma forma eficaz de fazer mais com menos, mas o valor mais significativo está em como a IA aumentará e complementará a experiência humana. A IA não pode substituir os anos de experiência, o conhecimento institucional e contextual que os profissionais de cibersegurança fornecem. No entanto, uma colaboração entre inteligência humana e inteligência artificial resultará numa estratégia de defesa cibernética muito mais resiliente e numa organização mais resiliente.

Oportunidades de eficiência com IA

Existem muitas áreas na pilha de capacidades de cibersegurança onde os serviços de IA podem ser aproveitados para complementar as competências fornecidas pelo pessoal humano. Abaixo estão alguns exemplos de serviços de IA que podem ser considerados:



Threat Detection

A IA pode monitorizar a atividade da rede com incrível eficiência e precisão, usando heurísticas e machine learning para encontrar ameaças cibernéticas avançadas e identificar padrões de tráfego anormais. Estes serviços alimentados por IA podem assumir o "trabalho pesado" da análise de rede e da forense, permitindo a deteção de ameaças em tempo quase real e capacitando os analistas de segurança com dados correlacionados significativos.

Vulnerability Management

As plataformas de gestão de vulnerabilidades (VM) alimentadas por IA podem ser aproveitadas para fornecer dados e relatórios enriquecidos, permitindo uma visão precisa da postura de segurança da organização. Estas ferramentas aproveitam as capacidades para realmente testar a explorabilidade das vulnerabilidades, permitindo que a organização priorize os esforços de remediação com base no risco real, com controlos compensatórios considerados.

Incident Response

As ferramentas de resposta a incidentes (IR) alimentadas por IA podem lidar com as fases iniciais da resposta a incidentes através da identificação e contenção automática de ameaças identificadas. Aproveitar um ecossistema de segurança unificado pode permitir que uma plataforma de IR de IA aproveite várias capacidades de controlo dentro da pilha tecnológica para frustrar ataques cibernéticos. Isto reduz o tempo necessário para responder a ameaças e permite que as equipas de cibersegurança tenham mais largura de banda para se concentrar em atividades de remediação.

Conclusão: Fechando a lacuna com colaboração

A escassez global de talentos em cibersegurança é um desafio preocupante que ameaça a sustentabilidade dos nossos ecossistemas digitais. Aproveitando a IA, a automação e as técnicas modernas de educação, seremos bem-sucedidos em fortalecer o nosso talento em cibersegurança, bem como em aumentar a nossa força de trabalho existente para permitir que as organizações escalem os seus esforços de segurança de forma mais eficiente.

Embora a IA possa ajudar significativamente ao assumir tarefas rotineiras, os recursos humanos serão sempre necessários para fornecer contexto, criatividade e pensamento estratégico. Juntos, estes fatores ajudarão a fechar a lacuna.