RUI SHANTILAL
Managing Partner, Devoteam Cyber Trust

1 Em 2024, o setor de cibersegurança enfrentará desafios significativos, mas também apresentará oportunidades consideráveis. A antecipação e a gestão das ameaças cibernéticas sofisticadas será um desafio constante, assim como a educação de utilizadores sobre práticas seguras.
A segurança de dispositivos IoT e a integração eficaz da Inteligência Artificial na segurança cibernética são outras áreas desafiantes. Por outro lado, a crescente procura por soluções robustas de cibersegurança abre portas para inovações, como frameworks integrados que simplificam a gestão da segurança cibernética com integração e participação de todos os intervenientes - caso da Alert Readiness Framework recentemente lançada pela Devoteam.
A colaboração entre diferentes setores e a partilha de conhecimento sobre ameaças emergentes também representam oportunidades. Além disso, o desenvolvimento de soluções inteligentes baseadas em IA para automação de segurança, detecção, bloqueio e resposta de ameaças e análise de vulnerabilidades é uma tendência crescente.
O mercado de cibersegurança está projetado para crescer significativamente, refletindo uma maior consciencialização sobre a importância da segurança digital. Adaptarmo-nos rapidamente às mudanças, investir em tecnologias emergentes e fomentar uma cultura de segurança são chaves para o sucesso neste setor.

2 Para o próximo ano, as principais tendências tecnológicas em cibersegurança refletem uma mistura de inovação contínua e resposta a desafios persistentes. Primeiramente, a segurança de terceiros ganha destaque, pois as cadeias de fornecimento e os ecossistemas de negócios estão cada vez mais interconectados. A avaliação e gestão rigorosa dos riscos associados a fornecedores e parceiros tornam-se essenciais.
Além disso, a conformidade regulatória, especialmente em relação à NIS2 e DORA na União Europeia, será uma prioridade. As organizações precisarão alinhar as suas práticas de segurança com esses novos requisitos para evitar penalidades e garantir a proteção eficaz dos dados.
Outra área em foco será a resiliência cibernética. Diante de ataques cada vez mais sofisticados, as empresas irão procurar estratégias robustas para recuperarem rapidamente de incidentes e manter a continuidade dos negócios.
Quanto à Inteligência Artificial e machine learning em pentesting, embora haja um potencial significativo para futuras inovações, esta área ainda está a desenvolver-se. Portanto, é mais uma direção provável do que uma tendência estabelecida.
Por último, a crescente necessidade de talentos especializados em cibersegurança continua a ser um desafio. As organizações investirão mais em formação e desenvolvimento de competências internas, além de recorrerem a serviços geridos especializados para enfrentar a complexidade da cibersegurança.
Estas tendências refletem um setor em constante evolução, onde a adaptação e a inovação contínuas são cruciais para enfrentar os desafios de um ambiente digital cada vez mais complexo.