

Devoteam Cyber Trust debate Tendências de Cibersegurança para 2026

Lisboa, 28 de janeiro de 2026 - A **Devoteam Cyber Trust** realizou hoje o evento “**Tendências de Cibersegurança 2026: Viabilizar a Inovação Transversal**”, um encontro que reuniu vários decisores e especialistas da empresa e **Pedro Mendonça, Coordenador do Departamento de Desenvolvimento e Inovação do Centro Nacional de Cibersegurança (CNCS)**, para refletir sobre os principais desafios e prioridades da cibersegurança, num contexto marcado pela aceleração da inteligência artificial, da cloud e da transformação digital.

Na sessão de abertura, **Hugo Mestre, Executive Director & Head of Cyber Trust na Devoteam Portugal**, sublinhou a relevância estratégica do evento para o ecossistema empresarial afirmando que **“este encontro reflete a necessidade crescente de criar espaços de reflexão estratégica onde tecnologia, risco e negócio convergem. Falar de cibersegurança em 2026 é falar de confiança digital, de governação da IA e da capacidade das organizações se adaptarem a um ambiente de ameaça em permanente evolução”**.

Segundo **Hugo Mestre**, **“a IA está no centro da agenda estratégica, sendo reconhecida por 94% dos líderes como o principal motor de mudança nas organizações”**. Neste contexto, a cibersegurança assume um papel crítico e indissociável do sucesso do negócio, uma vez que influencia diretamente todas as decisões estratégicas e operacionais. Este avanço expõe desafios relevantes, nomeadamente um gap de competências que afeta 85% das organizações: investir em resiliência digital não deve ser visto como um custo, mas como um investimento para garantir crescimento sustentável, confiança e continuidade do negócio.

Por sua vez, **Pedro Mendonça** destacou a mais recente edição do **Relatório de Cibersegurança, tema Riscos & Conflitos, de 2025, desenvolvido pelo Observatório de Cibersegurança do CNCS**, que oferece uma análise aprofundada das ameaças atuais no ciberespaço e do impacto potencial sobre organizações e infraestruturas críticas. O documento identificou o *phishing*, o *smishing* e outras formas de engenharia social como as ciberameaças mais frequentes, bem como o *ransomware* e o DDoS como as que têm mais impacto, e evidenciou o aumento da exposição de Portugal ao contexto político e geoestratégico, que introduz novas ameaças, tendo como principais agentes os cibercriminosos, os atores estatais e os hacktivistas. **“Entre as principais tendências observadas, destacam-se o aumento de ataques dirigidos a infraestruturas cloud, a proliferação de infostealers e a comercialização de credenciais online, a exploração de vulnerabilidades resultante do crescimento da superfície de ataque, a**

utilização de IA generativa para potenciar ciberataques e a persistência de ameaças que exploram o fator humano”, refere **Pedro Mendonça**.

Seguiu-se a sessão “**AI Chaos Management**”, apresentada por **Rui Shantilal, VP of Devoteam | Cyber Trust** onde foram analisados os desafios da gestão da IA num contexto de rápida evolução tecnológica: à medida que esta se torna cada vez mais autónoma, a imprevisibilidade deixa de ser um defeito e passa a ser uma característica intrínseca, tornando a questão central não como usamos a IA, mas sim como a gerimos.

Durante a apresentação, **Rui Shantilal** fez uma analogia entre a confiança digital e a mente humana. “**Embora o potencial da IA seja inegável, impõe-se uma questão: o que acontece quando a tecnologia falha num processo crítico?**” Além dos riscos inerentes, uma falha deste tipo pode traduzir-se em impactos financeiros significativos. Neste enquadramento, a IA deve ser integrada nas organizações com o mesmo rigor aplicado ao recrutamento de pessoas, incluindo um processo estruturado de onboarding. ““**Num ambiente marcado pela incerteza, a estratégia não é eliminar o caos, mas garantir que ele é gerido — e não deixado à solta dentro da nossa organização**”, concluiu, concluiu **Rui Shantilal**.

A governação e a conformidade em ambientes cada vez mais automatizados estiveram em destaque na sessão “**AI Governance and Compliance**”, conduzida por **Aurélio Maia**, que reforçou o calendário de implementação do **AI Act** referindo que as empresas devem estar preparadas para o cumprimento destas obrigações para uma adequada conformidade e gestão estratégica. **Bruno Morisson** apresentou uma visão sobre a evolução dos testes de intrusão com a sessão “**The Rise of the Autonomous Pentester**”, evidenciando o papel crescente da automação e da inteligência artificial ofensiva, reforçando a importância de uma abordagem integrada entre a IA e a visão humana, onde a automação é aplicada às tarefas repetitivas e operacionais, enquanto as atividades de maior valor acrescentado, estratégicas, criativas e de decisão, devem permanecer sob responsabilidade humana, potenciando uma otimização global dos resultados.

A agenda incluiu ainda a sessão “**Cyber Tech for Cloud Security**”, apresentada por **Herman Duarte**, dedicada aos desafios da proteção de ambientes multicloud, tendo ficado claro que falar em IA é, também, falar de cloud, uma vez que não existe uma IA segura, sem uma infraestrutura de cloud segura. **Herman Duarte** destacou a integração da segurança na cloud como uma componente estratégica na jornada de cada cliente, reconhecendo que cada organização apresenta necessidades e desafios distintos, o que exige respostas personalizadas e adaptadas a cada contexto específico.

O evento “**Tendências de Cibersegurança 2026: Viabilizar a Inovação Transversal**” terminou com um **momento de networking** e reafirmou a posição

da Devoteam Cyber Trust como referência estratégica na promoção da confiança digital em Portugal. Ao reunir especialistas, decisores e entidades-chave num espaço de debate qualificado, a iniciativa evidencia o compromisso da empresa em capacitar o mercado, antecipar riscos emergentes e reforçar a resiliência cibernética das organizações, num cenário cada vez mais complexo e interdependente.

Sobre a Devoteam Cyber Trust

A Devoteam Cyber Trust é a unidade especializada em cibersegurança do Grupo Devoteam. Com mais de 800 especialistas localizados na região EMEA, o nosso objetivo é estabelecer a cibersegurança como um facilitador do sucesso dos negócios, em vez de um obstáculo. Utilizamos uma abordagem abrangente de Resiliência Cibernética, Segurança Aplicada e Gestão de Serviços de Segurança para proteger a jornada tecnológica de empresas de grande e média dimensão de todos os setores e indústrias.

Desde 2009, anteriormente com a denominação INTEGRITY, a nossa equipa sediada em Portugal é especializada em fornecer Serviços Geridos de Segurança de ponta, que combina a sua expertise e tecnologia proprietária para reduzir de forma consistente e eficaz o risco cibernético dos nossos clientes. A ampla gama de serviços abrange Testes Persistentes de Intrusão, ISO 27001, PCI-DSS, Consultoria e Soluções de GRC e Gestão de Riscos de Terceiras Partes. Certificados em ISO 27001 (Segurança da Informação), ISO 27701 (Gestão de Informação Privada) e ISO 9001 (Qualidade), PCI-QSA e membros da CREST e do CIS - Centro de Segurança na Internet. Também somos acreditados pela Iniciativa Europeia de Pagamentos (EPI) para realizar avaliações de segurança do Wero, a carteira digital móvel. Com uma base considerável de clientes, operamos em mais de 20 países.

Contactos

BE Ideas | Boutique PR Agency

Sofia Alcobia

sofia.alcobia@beideas.pt

T: + 351 962 615 717

Magda Carvalho

magda.carvalho@beideas.pt

T: + 351 966 015 450