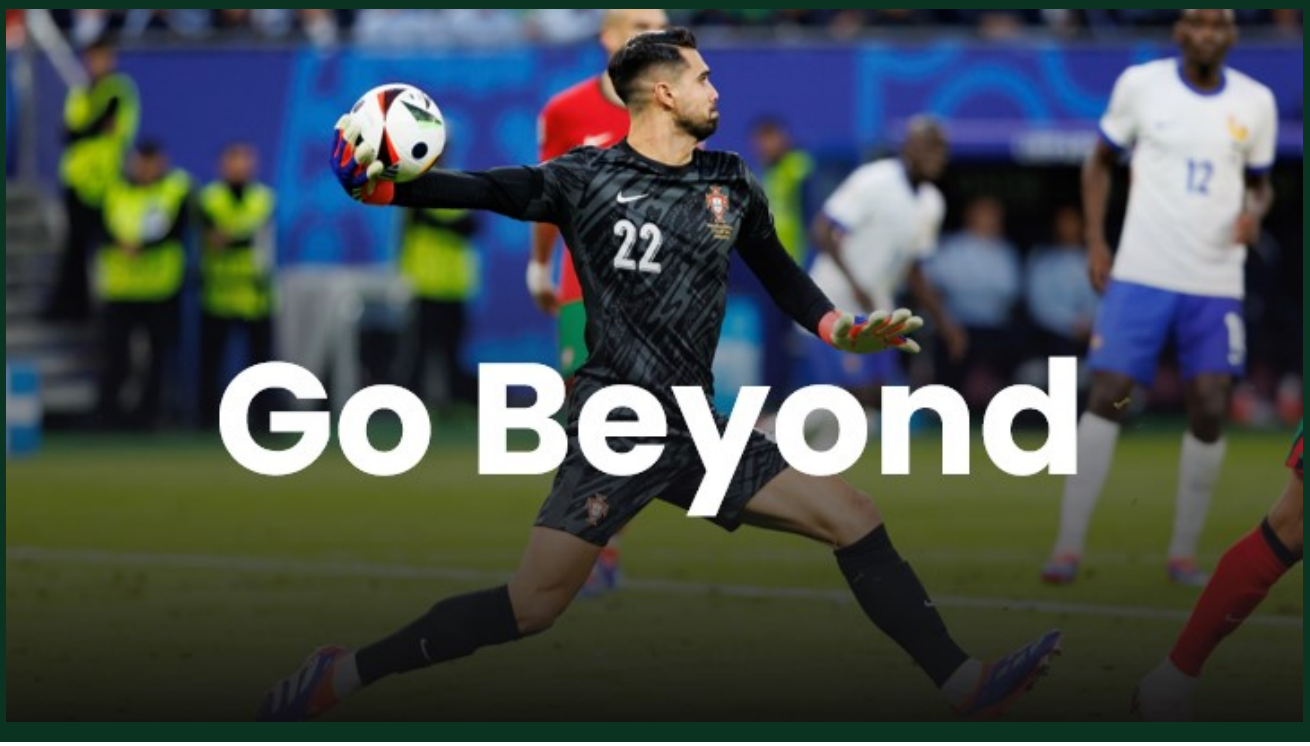

SUMÁRIO EXECUTIVO
De Sensibilização a Prontidão em Cibersegurança

Principais ideias da palestra apresentada no evento no Auditório 2:

From Awareness to Readiness:

Building Training Instincts for the Human Firewall

O desafio atual

A cibersegurança deixou de ser apenas uma questão tecnológica. Hoje, as pessoas são uma parte crítica da defesa das organizações — e muitas vezes a última linha de defesa.

- A questão já não é se a organização será atacada, mas quando;
- Cerca de 95% dos ataques começam pela manipulação de pessoas;
- Os atacantes exploram emoções humanas como medo, urgência, curiosidade e tentação.

Os atacantes não procuram a organização mais fraca. Procuram o comportamento mais previsível.

Porque a sensibilização tradicional não chega

Muitas organizações continuam a depender de ações pontuais de sensibilização. Embora importantes para transmitir conhecimento, estas iniciativas raramente criam os reflexos necessários para responder a ataques reais.

- Evento pontual não cria instinto;
- Conhecimento teórico não garante comportamento seguro;
- Cumprir o mínimo protege da auditoria, mas não protege do ataque.

O que fazem as organizações mais resilientes

- Programas contínuos de treino e simulações;
- Medição regular de comportamentos e resultados;
- Melhoria contínua baseada em dados.

Tal como no futebol e desporto de alto nível, a preparação eficaz exige treino regular, repetição e capacidade de decisão sob pressão.

Três comportamentos que reduzem drasticamente o risco

- Reconhecer ataques de engenharia social (phishing, smishing, vishing);
- Nunca partilhar credenciais ou dados sensíveis;
- Manter software e aplicações atualizados.

As organizações que evoluem de Sensibilização para **Preparação Contínua** conseguem reduzir significativamente o risco humano em cibersegurança e aumentar a sua resiliência.