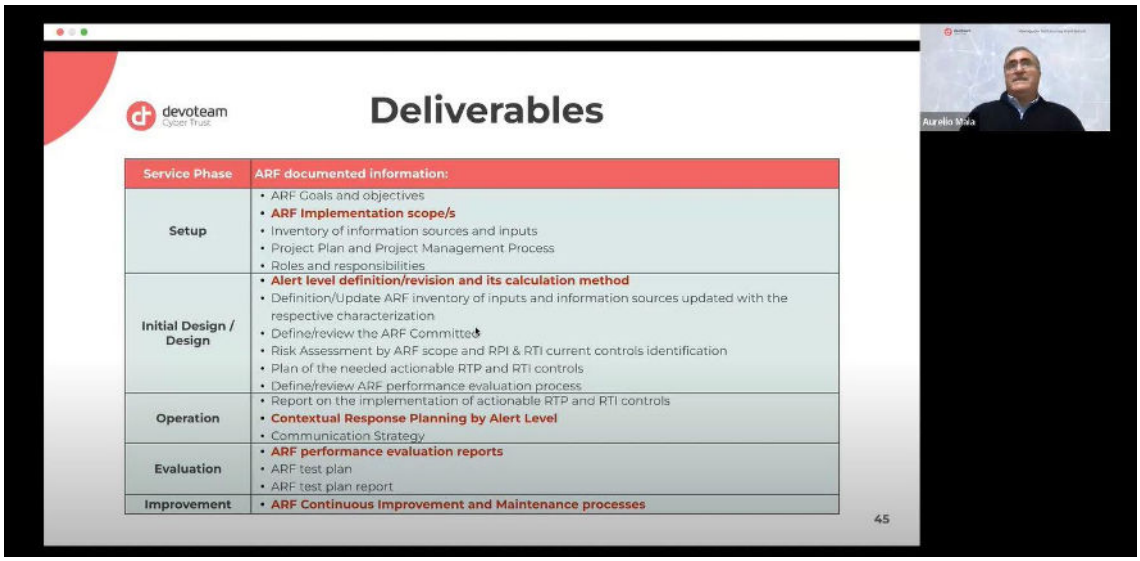
IT2TA de janeiro: Alert Readiness Framework na integração de cibersegurança ao nível empresarial



No dia 25 de janeiro realizou-se mais um It's Time To Talk About. Para abrirmos 2024, recebemos Rui Shantilal, Managing Partner da Devoteam Cyber Trust, e Aurélio Maia, Consulting Services Director, da Devoteam Cyber Trust, numa hora de análise da ferramenta Alert Readiness Framework para a integração eficiente de cibersegurança nas operações empresariais. A Devoteam Cyber Trust opera atualmente em 18 países e tem mais de 850 profissionais dedicados à cibersegurança.

No enquadramento foi referido que na atualidade um CISO tem de se preocupar com as ameaças, fazer uma gestão de risco adequada, estar preparado para responder a incidentes, consciencialização, conformidade e regulações. Tudo enquanto suporta o negócio e gere parceiros, identidade e acessos dos utilizadores.

As métricas de cibersegurança têm de acompanhar as tecnologias emergentes, como a IA, de forma integrada com a gestão e os inputs de negócio. Todavia, os ataques sucedem-se e são todos os dias mais sofisticados e elaborados. O impacto do cibercrime duplicou em dois anos e a fonte principal é quase sempre o elemento humano. Existem grupos organizados para promover os ciberataques, estão tão organizados que chegam a ter o "funcionário do mês".

A Alert Readiness Framework é um complemento às *frameworks* já existentes, dado que existe uma grande pressão das entidades regulatórias para forçar a implementação de medidas adequadas.

Nas organizações identificam-se dois estados: o normal, sem nenhum incidente crítico. Ao passar-se para um incidente crítico entra-se no cenário de alerta e resposta à incidente e modelo de continuidade de negócio nos casos mais graves. Mais de 80% das vulnerabilidades ainda têm origem num comportamento errado do utilizador.

Entre o estado de estar tudo bem e o estado de alerta devia haver estados intermédios, entende Rui Shantilal. Todos têm de entender o seu papel dentro da organização. Para se implementar este *mindset*. É aí que entra a Alert Readiness Framework (que não é um conceito, mas sim uma *framework* disponível num e-book gratuitamente), inspirada no sistema Defcon do Exército dos Estados Unidos com cinco níveis distintos de alerta desde o estado normal e controlado até ao nível máximo de alerta que indica perigo com consequências massivas.

De acordo com a ARF existem dois tipos de controlos que devem ser definidos por cada nível intermédio de alerta (RTP – o sistema ABS de um carro e RTI - o airbag, por analogia à linguagem automobilística). A *framework* foi construída com o contributo de colaboradores da Devoteam Cyber Trust um pouco por todo o mundo.

Rui Shantital sublinha as vantagens da ferramenta:

- Gamifica a Segurança;

- É proativa;

- Estende a prática da cibersegurança para o nível do negócio;

- Permite unificar a cibersegurança.

Aurélio Maia, Consulting Services Director, reforça que a ARF ajuda a colocar as perguntas certas para obter as respostas certas. Em primeiro lugar é cumprida uma etapa de *setup* e implementação. Segue-se o estágio de operação, avaliação e eventual melhoria contínua e manutenção da própria *framework*. Deste modo**, é criada uma linguagem comum dentro de toda a organização também entendida por todos os intervenientes. A melhor resposta a incidentes, conclui, é a prevenção.**

A 29 de janeiro o itSMF Portugal realiza mais um It’s Time To Talk About, desta vez sobre o DORA - Digital Operational Resilience Act.