accenture

VOCÊ SABE O QUE É O CYBERWAR GAME?

Segurança Cibernética é uma área que está em constante preparação. A gente estuda, investiga, melhora constantemente as defesas e protocolos. Mas para alguns tipos de ameaça, o único jeito de se preparar é através de simulação.

Um ataque cibernético é uma preocupação na indústria, hoje em dia. O ambiente industrial é quase um paciente na UTI. Ele tem que estar no hipercuidado. Principalmente pelos impactos que podem ser causados ao meio ambiente, ao processo produtivo e até perda de vidas. Para se precaver, você precisa simular, testar esses eventos em um ambiente controlado. O Cyber War game consiste em uma simulação entre ataque e defesa utilizando a plataforma hiper-realista do SIMOC.

Os atacantes estão sempre um passo à frente. A grande maioria das empresas é uma peneira e você tem que tapar cada furinho. E para um atacante não. Para um atacante, basta um furinho e ele vai conseguir o acesso e vai fazer o que ele quiser.

Existem uma série de ferramentas no mercado com o objetivo de colocar a empresa um passo à frente de um ataque cibernético, para que tenha uma chance de defesa um pouco maior. Os ataques, quando ocorrem, eles são imediatos, bem financiados e muito bem coordenados. Por isso, é importante ter uma equipe de prontidão para atuar em incidente cibernético.

Hoje, atendemos diversas empresas: infraestrutura, telecomunicações, instituições financeiras, recurso naturais.

A gente traz para essas simulações a nossa experiência como time de defesa de empresas de grande porte em diversas indústrias críticas do país.

Existe esse mundo, um mundo que as pessoas não têm muita noção, mas no cerca e cada vez quanto mais tecnológicos nós formos, mais expostos nós seremos a esse tipo de ataque.

A simulação traz esses componentes de desconforto, mas um desconforto positivo, para que a pessoa se sinta preocupada a focar naquele ponto quando ela volta para dentro da organização e ela entende que ela precisa desenvolver em um pouco mais ou de conteúdo de processo. Ou até de investimento em tecnologia, até de equipe, para poder atender aquele ponto que percebeu dentro do jogo.

Nenhuma ferramenta é capaz de substituir uma equipe de prontidão para atuar na defesa de um ataque cibernético.