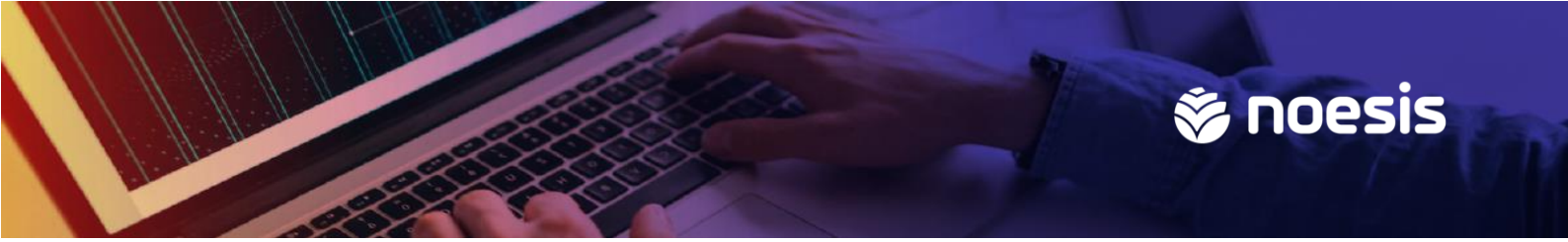


Inteligência artificial na Cibersegurança?

A inteligência é um dos temas "sexy" no panorama tecnológico, já a cibersegurança uma temática antiga em constante evolução. A junção de ambas é inevitável, mas para quando? **Para hoje**!

Atualmente existem no mercado ferramentas e equipas especializadas, capazes de implementar sistemas de cibersegurança baseados em IA para a deteção e resolução de ameaças cibernéticas. Da parte técnica a resposta está a ser dada, o principal desafio está na capacidade de decisão das organizações e na relevância que dão ao tema.

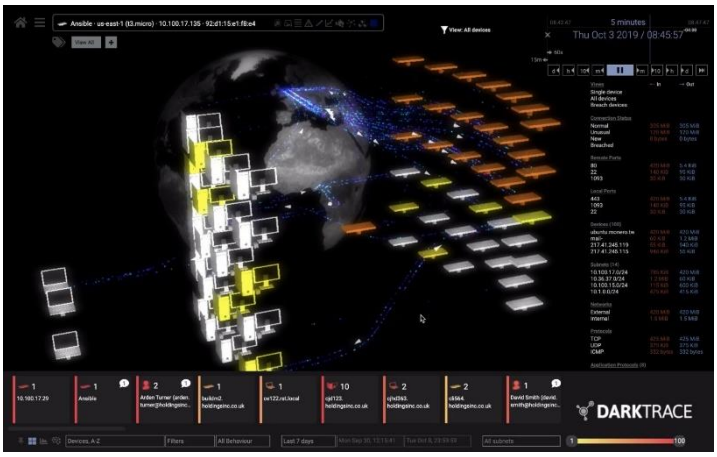
Hoje em dia, é inegável que o **número de dispositivos conectados vai continuar a aumentar**, os avanços das interfaces cloud também e, por consequência, novos ataques remotos e até com base em IA vão surgir em maior escala. Este panorama cria dificuldades às organizações, que focadas nos seus negócios têm cada vez menos capacidade de resposta às ameaças crescentes. A capacidade de resposta das organizações relaciona-se em tudo com o peso que a cibersegurança assume nos departamentos de IT, as organizações não são especialistas (nem o devem ser!), e a preocupação principal destes departamentos está focada no seu core business.

Inteligência assistida ao serviço da Cibersegurança

A Inteligência Artificial entra neste campo como um facilitador, não implica custos, mas sim um investimento na segurança e até nas próprias equipas de IT, retirando grande parte do esforço de análise e permitindo um maior foco no que é importante, o negócio e os objetivos da organização.

É neste ponto que surge a visão de **inteligência assistida**, isto é, recorrer a mecanismos de inteligência artificial para analisar informações e eventuais anomalias e permitir que os departamentos de TI, com o menor esforço possível, possam ter a visibilidade completa das suas redes e atuar em real-time sobre as ameaças que as suas organizações estão a ser alvo, sejam elas externas ou internas. É esta assistência que o mercado exige, inteligência artificial entregue de forma simples e eficaz.

Uma das tecnologias que mais tem surpreendido o mercado é a da Darktrace, fundada por matemáticos de Cambridge em parceria com as melhores agências de Inteligência, recorre a algoritmos de IA e Machine Learning para definir padrões de comportamento em qualquer rede, dispositivo ou utilizador numa organização, tenha esta 12 dispositivos ou mais de um milhão! Esta tecnologia disponibiliza duas grandes soluções, o Entreprise/Industrial Immune System e o Antigena. Na sua abordagem, a Darktrace recorre a uma metáfora com o sistema imunitário do ser humano, a solução Immune System tem por finalidade a deteção de todo e qualquer comportamento da rede, aprende o que é normal e alerta para o que é anormal. Esta é uma importante ferramenta de assistência para os departamentos de TI, através da visualização topológica, os técnicos conseguem acompanhar em tempo real o comportamento da rede e dos seus dispositivos.



Visualização topológica da rede

Tal como no corpo humano, quando o sistema imunitário deteta uma anomalia são lançados os anticorpos, neste caso o Antigena, uma solução para organizações em estados de maturidade superior. Com base na monitorização do Immune System, o Antigena permite lançar respostas automáticas às ameaças numa questão de segundos! Estas ações conseguem evitar até os ataques mais cirúrgicos e silenciosos a que as organizações estão expostas.

Ver para querer!

Em todas as implementações desta tecnologia que temos feito, o mais extraordinário é a capacidade de resposta e a incredulidade dos clientes ao perceber as suas vulnerabilidades e as ameaças a que estão expostos.

Com um trial de 4 semanas completamente gratuito e instalação da solução em apenas uma hora a tecnologia é possível iniciar os processos inteligentes de aprendizagem na sua rede.

Ao fim de muito pouco tempo, os primeiros relatórios começam a evidenciar e a expor as debilidades da organização. Mesmo em organizações com elevados investimentos em cibersegurança o resultado destes “trials” têm sido surpreendentes. Como refere o claim da Darktrace – “Nós vemos o que os outros não veem”.

As ameaças estão onde menos se espera.

Um dos use cases mais populares da Darktrace reflete bem e de forma prática que as ameaças estão onde menos esperamos. Nos Estado Unidos, um Casino instalou um aquário gigante como nova atração, com sensores avançados que regulavam automaticamente a temperatura, a salinidade e os horários de alimentação. Para garantir que essas comunicações permanecessem separadas da rede comercial, o casino configurou os sensores através de VPN individual para isolar os dados. Assim que o Proof-of-Value foi realizado, foram identificadas transferências de dados anómalas do aquário para um destino externo. As transferências externas de dados foram consideradas altamente incomuns pelos algoritmos de IA da tecnologia. Os dados estavam efetivamente a ser transferidos para um dispositivo na Finlândia, onde um hacker conseguiu obter o controlo total sobre o aquário.

Este é apenas um exemplo que demonstra a necessidade de ter visibilidade completa sobre todos os utilizadores e dispositivos, ate mesmo daquele que estamos menos à espera.

Tudo isto é surpreendente, não?