

VisionWare: “A IA é mais uma ferramenta, não é uma silver bullet” (com vídeo)

| T itsecurity.pt/news/its-conference/visionware-a-ia-e-mais-uma-ferramenta-nao-e-uma-silver-bullet-com-video



No mundo atual, onde os ciberataques se tornaram uma constante, a Inteligência Artificial (IA) surge como uma aliada fundamental para os **Centros de Operações de Segurança (SOC)**. **Filipe Custódio**, **Partner e Board Member da VisionWare**, partilhou a sua visão sobre a aplicação da IA na cibersegurança, destacando tanto as vantagens como os desafios da sua integração.



Watch Video At: <https://youtu.be/CdbMSZ3Zw9c>

O papel da inteligência artificial no SOC

Segundo Filipe Custódio, o SOC é uma estrutura relativamente recente, mas essencial devido à crescente necessidade de defesa contra ataques que afetam gravemente as empresas. *“Existem tecnologias de IA que estão a ser usadas para potenciar estes centros de segurança a poderem tratar mais eventos, tratar mais incidentes de segurança, mais ataques com o mesmo número de pessoas”*, afirmou.

A IA atua como *“acelerador e automatizador”* de tarefas repetitivas, filtrando dados para que os analistas se foquem nos incidentes críticos, ajudando a gerir grandes volumes de dados. Contudo, Filipe Custódio ressaltou que *“a decisão final deve estar do lado dos humanos”*, tornando a IA uma ferramenta complementar, mas não substituta das equipas humanas.

Identificação de padrões e aprendizagem automática

A IA, especialmente através da aprendizagem automática, destaca-se pela sua capacidade de identificar padrões em grandes volumes de dados e de detetar comportamentos suspeitos. Filipe Custódio exemplificou esta aplicação, referindo que, na rede de clientes da empresa, têm *“cerca de alguns milhares de dispositivos detetados que geram bilhões de eventos por dia (...) não é possível um ser humano conseguir olhar para bilhões de eventos e tomar decisões informadas”*.

Com esta tecnologia, o sistema aprende com incidentes anteriores, descartando automaticamente falsos positivos e reconhecendo eventos similares a ataques reais. Desta forma, a IA acelera a análise e a resposta, reduzindo o tempo que os analistas humanos necessitariam para agir.

Resposta Automatizada a Incidentes

É precisamente no processo de resposta a incidentes, que inclui desde a identificação até à contenção e recuperação, que Filipe Custódio se referiu à importância do SOAR (Security Orchestration, Automation and Response), uma vez que é uma ferramenta que permite respostas automatizadas. *“Se a ação do analista é pegar naquele IP e pôr numa blacklist, essa ação pode ser automatizada. E é automatizada para todo esse tipo de eventos”*, o que permite aliviar a carga dos analistas humanos e acelerar a contenção de ameaças. Com o auxílio da IA, os SOC conseguem responder de forma mais rápida e eficiente, um fator crucial na cibersegurança moderna.

Desafios da integração da IA nos SOC

A integração da IA em operações de segurança enfrenta desafios importantes, com a escassez de profissionais qualificados entre os principais obstáculos. O Partner e Board Member da VisionWare apontou *“uma escassez muito grande de recursos humanos em cibersegurança e, igualmente, em inteligência artificial”*, com a formação e programas curriculares que desenvolvam competências nestas áreas. Além disso, o investimento financeiro para manter infraestruturas de IA robustas é essencial.

Na VisionWare, que gere cerca de meio petabyte de dados anuais, a IA é aplicada no SOC para proteger redes de clientes. *“Estamos também em projetos de inovação (...) que preveem modelos preditivos para combater ransomware via phishing”*, referiu o orador.

Para as organizações que pretendem integrar a IA e machine learning nos seus SOC, Filipe Custódio deixou claro que *“a IA é mais uma ferramenta, não é uma silver bullet”*, sendo fundamental que as empresas tenham objetivos claros para a aplicação da IA e que evitem automatizar processos ineficientes.

