**Cisco wprowadza nowy poziom cyfrowej ochrony dzięki wykorzystaniu**

**sztucznej inteligencji w całym portfolio rozwiązań bezpieczeństwa**

**Najważniejsze informacje:**

* Asystent *AI for Security* zmieni sposób, w jaki organizacje myślą o wynikach analiz cyberbezpieczeństwa i przechyli szalę na korzyść osób odpowiedzialnych za ochronę, pomagając w podejmowaniu świadomych decyzji, rozszerzając istniejące możliwości i automatyzując złożone zadania.
* Dzięki niezrównanej widoczności w całej architekturze sieci i bezpieczeństwa jaką ma Cisco, asystent AI Cisco jest szkolony na jednym z największych na świecie zestawów danych dotyczących cyberbezpieczeństwa, który analizuje ponad 550 miliardów zdarzeń związanych z bezpieczeństwem każdego dnia.

**CISCO LIVE, MELBOURNE, 7 grudnia 2023 r. -** W trakcie odbywającej się w Melbourne konferencji Cisco Live, firmazaprezentowała Cisco AI Assistant for Security. Jest to ważny krok w kierunku uczynienia sztucznej inteligencji (AI) wszechobecną w Security Cloud, ujednoliconej, opartej właśnie na AI, wielodomenowej platformie bezpieczeństwa Cisco. Asystent AI pomoże klientom podejmować świadome decyzje, rozszerzy możliwości ich narzędzi i zautomatyzuje złożone zadania.

"Aby stawiać na sztuczną inteligencję, firma musi opierać się na danych. Dzięki naszej rozległej natywnej telemetrii, Cisco ma wyjątkową pozycję, aby dostarczać rozwiązania z zakresu cyberbezpieczeństwa, które dzięki wykorzystaniu uczenia maszynowego i sztucznej inteligencji rozszerzają możliwości firmowych zespołów IT i bezpieczeństwa" - powiedział Jeetu Patel, wiceprezes i dyrektor generalny Cisco Security and Collaboration. "Dzisiejsze ogłoszenie to ogromny krok naprzód. Pomoże przechylić szalę na korzyść osób i organizacji odpowiedzialnych za cyberbezpieczeństwo, wzmacniając pozycję klientów dzięki sztucznej inteligencji wbudowanej wszechobecnie w Cisco Security Cloud".

Ponieważ cyberataki wciąż ewoluują, mechanizmy obronne organizacji muszą za nimi nadążać. Według nowego raportu [Cisco Talos 2023 Year in Review](https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/), ataki typu ransomware utrzymują się na stałym, wysokim poziomie, stanowiąc 20 procent tegorocznych interwencji zespołu Cisco Talos Incident Response. Talos zaobserwował również wzrost liczby wyrafinowanych ataków na urządzenia sieciowe w ubiegłym roku, szczególnie ze strony podmiotów sponsorowanych przez państwo. Zwiększona inteligencja złośliwych podmiotów wymaga więc zastosowania zabezpieczeń na o wiele większą skalę.

Dzięki niezrównanej widoczności jaką ma Cisco w całej architekturze sieci i bezpieczeństwa, firma pracuje z większą ilością telemetrii i na większą skalę niż większość w branży. Nowy Cisco AI Assistant for Security jest szkolony na jednym z największych na świecie zestawów danych dotyczących bezpieczeństwa, który analizuje ponad 550 miliardów zdarzeń bezpieczeństwa każdego dnia w Internecie, poczcie e-mail, punktach końcowych, sieciach i aplikacjach. Potrafi on ocenić wagę zdarzeń, ich wpływ i zakres, przeprowadzić analizę przyczyn źródłowych i zaprojektować zasady dalszego postępowania. Mając te informacje, Asystent AI ma za zadanie wypełnienie luki między intencjami cyberbezpieczeństwa a wynikami. Wszystkie możliwości sztucznej inteligencji Cisco są tworzone w sposób bezpieczny i zgodny z zasadami [Cisco Responsible AI Framework](https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-responsible-artificial-intelligence-framework.pdf).

**Kontynuując wprowadzanie innowacji w obszarze AI i cyberbezpieczeństwa, Cisco zaprezentowało następujące rozwiązania:**

* **Asystenta AI dla polityki zapór sieciowych**: Cisco AI Assistant for Security w pierwszej kolejności będzie wprowadzony do chmurowych rozwiązań Cisco Firewall Management Center i Cisco Defense Orchestrator, aby rozwiązać duże wyzwanie związane z ustawianiem i utrzymywaniem złożonych zasad i reguł zapór sieciowych. Administratorzy mogą teraz używać języka naturalnego do znajdowania polityk i uzyskiwania zaleceń dotyczących reguł, eliminując duplikaty, błędnie skonfigurowane zasady i złożone przepływy pracy przy jednocześnie zwiększonej widoczności. Przyspiesza to rozwiązywanie problemów i zadania konfiguracyjne.
* **Silnik widoczności ruchu szyfrowanego oparty na sztucznej inteligencji dla wszystkich modeli zapór sieciowych:** większość ruchu w centrach danych jest obecnie szyfrowana, a brak możliwości inspekcji zaszyfrowanego ruchu jest kluczowym problemem w zakresie bezpieczeństwa. Odszyfrowywanie ruchu w celu jego inspekcji wymaga dużych zasobów i jest obarczone kwestiami operacyjnymi, prywatności i zgodności. Dzięki systemowi operacyjnemu 7.4.1 dostępnemu teraz w całej rodzinie Cisco Secure Firewall, klienci widzą, że sztuczna inteligencja pozwoli im tu na dużo więcej dzięki zastosowaniu silnika widoczności ruchu szyfrowanego (Encrypted Visibility Engine). Wykorzystuje on miliardy próbek, w tym złośliwego oprogramowania w izolacji, aby określić, czy w zaszyfrowanym ruchu znajduje się złośliwe oprogramowanie. Rozwiązanie określa, z jakiego systemu operacyjnego pochodzi ruch i jaka aplikacja kliencka go generuje - wszystko to bez konieczności odszyfrowywania.

"Zdolność sztucznej inteligencji do przekształcania naszego codziennego życia i krajobrazu zawodowego jest ogromna. Jako wieloletni partner Cisco, jesteśmy podekscytowani Cisco AI Assistant for Security i tym, w jaki sposób umożliwi to naszym klientom wydajność opartą na sztucznej inteligencji" - powiedział Graham Robinson, dyrektor ds. technologii w Data#3. "Wprowadzenie AI Assistant do Cisco Firewall Management Center pomoże naszym klientom szybko i łatwo skonfigurować zmiany polityk. W połączeniu z nowymi funkcjami w wersji oprogramowania 7.4.1 i Encrypted Visibility Engine, oferuje to naprawdę atrakcyjne ogólne wrażenia".

Więcej informacji jest dostępne na stronie [cisco.com/go/security](http://cisco.com/go/security).

**Materiały dodatkowe:**

* Blog: [How We’re Making AI Pervasive in the Cisco Security Cloud](https://blogs.cisco.com/news/how-were-making-ai-pervasive-in-the-cisco-security-cloud)
* Blog: [Give your firewall admins superpowers with Cisco AI Assistant for Security](https://blogs.cisco.com/security/give-your-firewall-admins-superpowers-with-cisco-ai-assistant-for-security)
* Raport: [Cisco Talos 2023 Year in Review](https://blog.talosintelligence.com/cisco-talos-2023-year-in-review)

.:|:.:|:.

**O Cisco:**

Cisco (NASDAQ: CSCO) jest światowym liderem technologicznym, który bezpiecznie łączy wszystko ze światem. Naszym celem jest zapewnienie inkluzywnej przyszłości dla każdego i pomaganie naszym klientom w tworzeniu nowych aplikacji, umożliwianiu pracy hybrydowej, transformacji i zabezpieczaniu ich infrastruktury oraz osiąganiu celów zrównoważonego rozwoju. Dowiedz się więcej na [polskim](https://news-blogs.cisco.com/emea/pl/) lub [globalnym](https://newsroom.cisco.com/c/r/newsroom/en/us/index.html) biurze prasowym.

Cisco i logo Cisco są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Cisco i/lub jej podmiotów stowarzyszonych w Stanach Zjednoczonych i innych krajach. Listę znaków towarowych Cisco można znaleźć na stronie [www.cisco.com/go/trademarks](file:///C%3A%5CUsers%5CAdamMaj%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CTK4DW2DH%5Cwww.cisco.com%5Cgo%5Ctrademarks). Wymienione znaki towarowe innych firm są własnością ich odpowiednich właścicieli. Użycie słowa partner nie oznacza relacji partnerskiej między Cisco a jakąkolwiek inną firmą.