**Inteligentna ochrona tożsamości od Cisco zabezpiecza przed najbardziej uporczywymi cyberzagrożeniami**

*Sztuczna inteligencja staje się coraz bardziej znaczącym składnikiem platformy Cisco Security Cloud*

**Najważniejsze informacje:**

* Innowacje napędzają rozwój Security Cloud - ujednoliconej, opartej na sztucznej inteligencji, międzydomenowej platformy bezpieczeństwa Cisco.
* Firma wprowadza pierwszą w swoim rodzaju technologię Identity Intelligence, która pomaga chronić przed atakami opartymi na kradzieżach tożsamości.
* Dzięki nowym możliwościom sztucznej inteligencji Cisco pozwala firmom przejąć inicjatywę w walce o swoje bezpieczeństwo, pomagając podejmować świadome decyzje, rozszerzając istniejące możliwości i automatyzując złożone zadania.

**AMSTERDAM, 13 lutego 2024 r.** – Cisco zaprezentowało nowe funkcje platformy Security Cloud. Pierwsze w swoim rodzaju narzędzie Cisco Identity Intelligence i innowacje w zakresie sztucznej inteligencji to najnowsze osiągnięcia na rzecz ujednoliconej, opartej na AI, wielodomenowej platformy bezpieczeństwa.

Cisco, jako pierwsze w branży, realizuje podejście, które łączy tożsamość, sieć i bezpieczeństwo, aby lepiej chronić złożony stos tożsamości w organizacjach przed coraz bardziej wyrafinowanymi technikami ataku.

Obecne rozwiązania uwierzytelniania i dostępu są w powszechnej opinii uważane za zaufane, mimo iż cyberprzestępcy skutecznie atakują za ich pośrednictwem nawet największe firmy na świecie. W rzeczywistości, ponad 26% wszystkich czynności podejmowanych przez zespół Cisco Talos Incident Response było związanych ze skradzionymi danymi uwierzytelniania i uzyskiwaniem w ten sposób dostępu do prawdziwych kont użytkowników.

Użytkownik jest często przypisany do wielu cyfrowych tożsamości i kont - drastycznie zwiększając liczbę możliwych punktów wejścia dla atakujących i możliwość równoległego przemieszczania się "między" kontami. Często przestarzałe uprawnienia nie są usuwane, a zespołom ds. bezpieczeństwa brakuje kluczowego kontekstu dotyczącego przeszłych zachowań, działań w systemach i bieżących poziomów ryzyka, które są potrzebne do podejmowania decyzji dotyczących zaufanego dostępu.

Cisco Identity Intelligence działa w oparciu o istniejące bazy tożsamości klientów i zapewnia ujednoliconą widoczność, a także analitykę opartą na sztucznej inteligencji. Klienci mogą sprawdzać całą swoją bazę tożsamości, usuwać podatne konta, eliminować nieużywane i ryzykowne uprawnienia, wykrywać anomalie zachowania i blokować próby dostępu wysokiego ryzyka - bez niszczenia i zastępowania obecnych rozwiązań.

Podczas gdy uwierzytelnianie wieloskładnikowe (MFA) pozostaje krytyczną pierwszą linią obrony przed atakami opartymi na naruszeniach tożsamości, cyberprzestępcy wykorzystują nowe i kreatywne sposoby kradzieży danych uwierzytelniających. Według raportu Duo Trusted Access Report z 2024 r., Cisco Duo przetworzyło 16 miliardów uwierzytelnień w 2023 r., co stanowi wzrost o 41% rocznie, a użycie słabszych form uwierzytelniania wieloskładnikowego, takich jak SMS-y i połączenia telefoniczne, spadło do najniższego w historii poziomu 5%. Mimo tego, liczba ataków na tożsamość jest wyższa niż kiedykolwiek.

“Tożsamość łączy ludzi, urządzenia i aplikacje w miejscu pracy i stała się łatwym celem współczesnych cyberataków. Organizacje muszą przyjąć podejście do bezpieczeństwa stawiające tożsamość na pierwszym miejscu, zgodnie z którym zamiast pytać, czy użytkownik *może* uzyskać dostęp do systemu, należy ciągle weryfikować czy uwierzytelniony użytkownik *powinien* móc robić to, co robi" - powiedział Jeetu Patel, wiceprezes i dyrektor generalny ds. rozwiązań bezpieczeństwa i współpracy w Cisco. “Analizując całą powierzchnię ataków na użytkowników, urządzenia, usługi, aplikacje i dane w ramach organizacji, Cisco Identity Intelligence wypełnia przestrzeń między uwierzytelnianiem, a dostępem. Jesteśmy pierwszym dostawcą łączącym tożsamość, sieć i bezpieczeństwo w kompletne rozwiązanie, aby sprostać największemu wyzwaniu cybernetycznemu współczesnych czasów".

Cisco Identity Intelligence opiera się na potężnej bazie tożsamości, która pobiera dane z wielu istniejących źródeł zewnętrznych klientów, zarządzających tożsamością i dostępem. Dzięki analityce behawioralnej opartej na sztucznej inteligencji i niezrównanemu zasięgowi Cisco w sieci, organizacje mogą odpowiednio zareagować, np. poddać tożsamość kwarantannie, zakończyć aktywne sesje lub odizolować sieć za pomocą Cisco Identity Services Engine (ISE). Klienci Cisco zyskają wgląd w te krytyczne informacje dzięki istniejącym rozwiązaniom, takim jak:

* **Inteligentne uwierzytelnianie z Cisco Duo**: wykrywanie nietypowych wzorców w oparciu o zachowanie i informacje innych firm.
* **Smart Access z Cisco Secure Access:** weryfikacja decyzji o uwierzytelnieniu i blokowanie nietypowych lub wysoce ryzykownych zachowań.
* **Inteligentne wykrywanie zagrożeń dzięki Cisco XDR:** korelacja sygnałów tożsamości w celu dostarczenia informacji, których brakuje tradycyjnym rozwiązaniom do ochrony punktów końcowych i sieci.

Cisco Identity Intelligence będzie dostępne w lipcu 2024 roku. Dzięki dodaniu Identity Intelligence do Cisco Security Cloud klienci uzyskają jeszcze większą wartość z istniejących inwestycji.

**Ciągły rozwój sztucznej inteligencji**

Cisco kontynuuje wdrażanie sztucznej inteligencji w ramach platformy Cisco Security Cloud, aby pomóc firmom przejąć inicjatywę w walce o swoje bezpieczeństwo. Ma to zostać osiągnięte również dzięki niedawno zaprezentowanemu narzędziu Cisco AI Assistant for Security, które pomaga klientom podejmować świadome decyzje, rozszerzać możliwości narzędzi i automatyzować złożone zadania. Po uruchomieniu Asystenta AI dla zapory sieciowej szybkie tempo innowacji Cisco jest dziś widoczne dzięki kolejnym przełomowym możliwościom AI:

* **Asystent AI w bezpiecznym dostępie:** klienci, wykorzystując moc generatywnej sztucznej inteligencji, mogą tworzyć bezpieczne zasady dostępu za pomocą podpowiedzi w języku naturalnym w ramach rozwiązania Cisco Secure Services Edge (SSE).
* **Zabezpieczanie AI**: nowe możliwości w Secure Access będą również automatycznie wykrywać i chronić własność intelektualną, gdy będzie ona wpływać i wypływać z systemów AI.
* **Wykrywanie zagrożeń e-mail oparte na sztucznej inteligencji**: Cisco Email Threat Defense wykorzystuje teraz sztuczną inteligencję do jednoczesnej oceny różnych części przychodzącej wiadomości e-mail pod kątem markerów złośliwych intencji.

**Bezpieczna łączność**

Cisco integruje swoje bogate możliwości sieciowe z Cisco Secure Access. Narzędzie Experience Insights, obsługiwane przez Cisco ThousandEyes, zwiększa produktywność pracowników hybrydowych, szybko ujawniając problemy z łącznością i aplikacjami oraz sprzyjając szybszemu rozwiązywaniu problemów. Ta funkcja nie wiąże się z żadnymi dodatkowymi kosztami, ponieważ jest ona zawarta we wszystkich licencjach Secure Access. Cisco Secure Access zawiera teraz również system Catalyst SD-WAN, zapewniając kompletną ofertę Secure Access Service Edge (SASE).

Cisco chroni 100% firm z listy Fortune 100. Aby dowiedzieć się więcej, odwiedź <http://cisco.com/go/security>.

**Dodatkowe informacje:**

* Blog: [Cisco Puts Identity at the Heart of Its Security Strategy & Uses AI to Simplify Operations](https://blogs.cisco.com/security/cisco-puts-identity-at-heart-of-security-strategy)
* Blog: [Announcing Identity Intelligence with Duo](https://duo.com/blog/announcing-identity-intelligence-with-duo)
* Blog: [The 2024 Duo Trusted Access Report — Navigating Complexity](https://duo.com/blog/2024-duo-trusted-access-report-navigating-complexity)
* Blog: [How are user credentials stolen and used by threat actors?](http://blog.talosintelligence.com/how-are-user-credentials-stolen-and-used-by-threat-actors)
* Blog: [Connect, Secure, Assess Every Digital Experience Everywhere](https://blogs.cisco.com/security/connect-secure-assure-every-digital-experience-everywhere)

.:|:.:|:.

**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:/Users/AdamMaj/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/TK4DW2DH/www.cisco.com/go/trademarks). Wymienione znaki towarowe innych firm są własnością ich odpowiednich właścicieli. Użycie słowa partner nie oznacza relacji partnerskiej między Cisco a jakąkolwiek inną firmą.