**Cisco ogłasza kolejne innowacje w ramach Cisco Security Cloud**

*Po premierze Cisco Hypershield i przejęciu Splunk, Cisco idzie za ciosem i redefiniuje cyberbezpieczeństwo w skali AI*

**Najważniejsze informacje**:

* Cisco i Splunk pomagają klientom przyspieszyć transformację w kierunku Security Operations Center (SOC) przyszłości dzięki potężnej integracji zaledwie dwa miesiące po przejęciu Splunk przez Cisco.
* Dzięki pierwszej w branży architekturze bezpieczeństwa opartej na sztucznej inteligencji, klienci będą mogli chronić się zarówno przed znanymi, jak i nieznanymi atakami za pomocą Cisco Hypershield.
* Cisco Identity Intelligence jest teraz dostępne w Cisco Duo, aby umożliwić nieprzerwaną ochronę tożsamości (Continuous Identity Security) w celu ochrony organizacji przed gwałtownym wzrostem liczby ataków opartych na tożsamości.

**Warszawa, 14 maja 2024 r.** - Cisco ogłosiło innowacje w Cisco Security Cloud, aby zarówno wspierać, jak i chronić rewolucję AI w firmach. Nowe możliwości ujednoliconej, opartej na sztucznej inteligencji, wielodomenowej platformy bezpieczeństwa Cisco pomagają organizacjom lepiej chronić aplikacje, urządzenia, użytkowników i dane, a także szybciej wykrywać, reagować oraz odzyskiwać dane po naruszeniach cyberbezpieczeństwa.

Zabezpieczanie złożonych systemów nie może już odbywać się na poziomie rozumianym przez człowieka, ponieważ cyberataki stają się coraz bardziej wyrafinowane. Zgodnie z badaniem Cisco Cybersecurity Readiness Index 2024, prawie 90 procent firm na całym świecie twierdzi, że niedobór kadr w dziedzinie cyberbezpieczeństwa jest dla nich znaczącym problemem. Organizacje muszą na nowo opracować strategie bezpieczeństwa, budując systemy z wykorzystaniem sztucznej inteligencji i kwestionując długo utrzymywane przekonania, aby przechylić przewagę na korzyść zespołów ds. cyberbezpieczeństwa.

"Podczas zeszłorocznej konferencji RSA daliśmy klientom większą skuteczność dzięki Cisco Security Cloud. Minimalizując rozwiązania punktowe, klienci uzyskali lepszą widoczność, odkryli praktyczną inteligencję i automatyzację dzięki sztucznej inteligencji oraz uprościli zarządzanie dzięki ujednoliconej infrastrukturze bezpieczeństwa Cisco" - powiedział Jeetu Patel, wiceprezes i dyrektor generalny ds. bezpieczeństwa i współpracy w Cisco. "Od tego czasu nasz rozwój w zakresie bezpieczeństwa nadal przyspiesza. Dzięki innowacjom takim jak Cisco Hypershield i strategicznym przejęciom, takim jak Splunk i Isovalent, moc platformy bezpieczeństwa Cisco jest niezrównana".

Cisco pomaga klientom bronić się przed całym łańcuchem ataków - od wykrywania i blokowania luk w zabezpieczeniach za pomocą Cisco Hypershield, po powstrzymywanie rosnącej liczby ataków na tożsamość za pomocą Cisco Duo i reorganizację centrum operacji bezpieczeństwa (SOC) za pomocą Splunk, aby analitycy mogli działać szybciej i podejmować bardziej świadome decyzje dzięki kontekstowym danym i zautomatyzowanym przepływom pracy.

**Rozwój wizji SOC przyszłości**

Połączenie Cisco i Splunk to najbardziej kompleksowe rozwiązanie bezpieczeństwa do zapobiegania zagrożeniom, wykrywania, badania i reagowania na nie dla organizacji dowolnej wielkości, wykorzystujące chmurę, ruch w punktach końcowych - wraz z niezrównanym zasięgiem sieci Cisco - w celu zapewnienia najlepszej widoczności. W miarę jak Cisco i Splunk łączą te platformy, istnieje wiele możliwości usprawnienia operacji związanych z bezpieczeństwem, w tym:

* **Integracja Cisco Extended Detection & Response (XDR) z Splunk Enterprise Security (ES)**: Płynne przesyłanie wysokiej jakości alertów i spostrzeżeń z Cisco XDR, stworzonych specjalnie do wykrywania najczęstszych ataków, takich jak ransomware, do Splunk ES w celu przyspieszenia dochodzenia i naprawy. Integracja pozwala organizacjom wykorzystać siłę każdego z rozwiązań do stworzenia bardziej kompleksowej strategii obrony, która poprawi odporność cyfrową.
* **Splunk Asset and Risk Intelligence**: Krytyczne rozwiązanie dla SOC, zaprojektowane w celu zrewolucjonizowania proaktywnego ograniczania ryzyka. Osiągnięte to zostanie poprzez ciągłe wykrywanie zasobów i monitorowanie zgodności. Jest to odpowiedź na potrzebę zespołów ds. bezpieczeństwa, ponieważ nie mogą one chronić tego, czego nie widzą.
* **Cisco AI Assistant for Security w XDR**: Asystent AI Cisco dla zespołów bezpieczeństwa jest teraz dostępny w Cisco XDR - rok po tym, jak Cisco podzieliło się swoją wizją zmiany analityki bezpieczeństwa za pomocą sztucznej inteligencji na scenie RSAC 2023. Asystent AI w XDR umożliwia analitykom bezpieczeństwa podejmowanie szybszych i bardziej świadomych decyzji dotyczących zagrożeń, oferując kontekstowe spostrzeżenia, odpowiedzi, zalecenia i automatyzację procesów.
* **Nowe możliwości wykrywania i reagowania w chmurze**: platforma ochrony aplikacji w chmurze Cisco Panoptica (CNAPP) wykorzystuje teraz sztuczną inteligencję oraz uczenie maszynowe do wykrywania i ostrzegania zespołów bezpieczeństwa o pojawiających się zagrożeniach w aplikacjach w chmurze w czasie rzeczywistym, podczas gdy GenAI Dynamic Remediation umożliwia zespołom szybkie rozwiązywanie problemów poprzez dostarczanie wskazówek. Funkcja Search Graph Query umożliwia zapytania i wizualizacje wykresów w środowiskach wielochmurowych, aby umożliwić głębsze badanie stanu bezpieczeństwa chmury w celu zmniejszenia ryzyka.

"Rynek XDR jest szeroki i obejmuje wiele firm, które obiecują zapewnić pełniejszy obraz stosu zabezpieczeń poza punktem końcowym. W ten sposób XDR ma na celu wykrywanie zagrożeń cyberbezpieczeństwa w wielu domenach" - powiedział Will Townsend, wiceprezes i główny analityk w Moor Insights. "Obserwowalność jest kluczowa, a dzięki udanemu przejęciu Splunk, Cisco jest w stanie ulepszyć swoje rozwiązanie XDR uruchomione rok temu, dodając teraz sztuczną inteligencję, ujednolicone wykrywanie zagrożeń, badanie, reagowanie i transformację mające na celu usprawnienie operacji bezpieczeństwa".

"W Optiv zapewniamy naszym klientom niezbędną wiedzę i rozwiązania w zakresie bezpieczeństwa, których potrzebują, dzięki zintegrowanemu podejściu, które obejmuje całą ich drogę w zakresie cyberbezpieczeństwa, a wszystko to z naciskiem na przyspieszenie wyników biznesowych" - powiedział John Hurley, Chief Revenue Officer, Optiv. "Zintegrowana platforma Cisco Security Cloud oparta na sztucznej inteligencji, to rozwiązanie, które pomaga zmniejszyć złożoność. Integracja Cisco XDR i Splunk Enterprise Security umożliwi naszym klientom wydajne działanie przy jednoczesnym podejmowaniu świadomych decyzji dotyczących wzmocnienia ich cyberodporności w dzisiejszym ewoluującym krajobrazie zagrożeń".

**Ochrona przed nieznanymi ryzykami dzięki Cisco Hypershield**

W dzisiejszym krajobrazie ataków czas od wykrycia podatności do przygotowania exploita przez cyberprzestępców kurczy się - a obrona przed coraz bardziej wyrafinowanymi, złożonymi zagrożeniami w centrach danych wykracza poza skalę, którą jest w stanie pojąć ludzki umysł.

Bazując na wprowadzonym w zeszłym miesiącu Cisco Hypershield z Distributed Exploit Protection chroniącym przed znanymi niebezpieczeństwami (np. CVE), Cisco wprowadza teraz możliwości wykrywania i blokowania ataków wynikających z nieznanych luk w środowiskach aktywnych obciążeń. Ponadto podejrzane procesy mogą być izolowane w celu ograniczenia promienia rażenia podatności.

Cisco Hypershield to nowe, radykalne podejście do zabezpieczania centrów danych i chmur w odpowiedzi na rosnące wymagania, jakie rewolucja AI stawia przed infrastrukturą IT. Cisco Hypershield chroni aplikacje, urządzenia oraz informacje w publicznych i prywatnych centrach danych, chmurach i lokalizacjach fizycznych - wszędzie tam, gdzie potrzebują tego klienci. Zaprojektowany i zbudowany z myślą o sztucznej inteligencji od samego początku, Hypershield umożliwia organizacjom osiągnięcie wyników w zakresie bezpieczeństwa wykraczających poza to, co było możliwe przy użyciu samych ludzi.

**Płynna ochrona użytkowników dzięki nieprzerwanej ochronie tożsamości**

Wraz ze wzrostem liczby ataków opartych na kradzieży tożsamości, rozwiązania bezpieczeństwa muszą odejść od pytania "czy" użytkownik może uzyskać dostęp do aplikacji. Zamiast tego muszą stale oceniać, czy użytkownik "powinien" być w stanie robić to, co robi - i weryfikować to bez powodowania tarć dla użytkownika. Idąc za ciosem po uruchomieniu Cisco Identity Intelligence, Cisco łączy w rozwiązaniu Duo funkcje odporne na phishing, aby zrealizować swoją wizję nieprzerwanej ochrony tożsamości (Continuous Identity Security) - powstrzymując ataki na prywatność, jednocześnie zapewniając prostsze, bardziej płynne wrażenia użytkownika.

* **Eliminacja wyczerpującego uwierzytelniania dzięki Duo Passport**: Pozwala ograniczyć powtarzające się żądania uwierzytelnienia, aby zapewnić nieprzerwany dostęp do wszystkiego, czego potrzebują pracownicy. Dzięki Duo Passport odbywa się to bez uszczerbku na komforcie pracy użytkownika.
* **Cisco Identity Intelligence w Duo**: Pozwala wykorzystać potężną analitykę opartą na sztucznej inteligencji, aby wzmocnić w całej infrastrukturze rozpoznawalność pracowników, ocenić i zareagować na ryzyko kradzieży tożsamości przed, w trakcie i po zalogowaniu. Obecnie w ograniczonej dostępności, dodatek ten umożliwia klientom wdrożenie Continuous Identity Security (nieprzerwanej ochrony tożsamości), co zmniejsza luki w zabezpieczeniach i eliminuje najczęstsze obecnie zagrożenia cybernetyczne.

"Cisco Duo wykracza poza swoje podstawowe funkcje zarządzania dostępem, włączając wzbogacanie tożsamości z Cisco Identity Intelligence i wprowadzając usprawniony dostęp dzięki Duo Passport" - powiedział Todd Thiemann, starszy analityk w Enterprise Strategy Group. "Ta ewolucja prowadzi do bezpieczeństwa opartego na identyfikacji, w którym dostęp dostosowuje się w czasie rzeczywistym do powiązanego ryzyka, co ma kluczowe znaczenie w dzisiejszym krajobrazie zagrożeń, w którym ataki oparte na tożsamości rosną. Zaangażowanie Cisco Duo w dynamiczną reakcję na ryzyko, w połączeniu z naciskiem na płynną obsługę użytkownika, jest nie tylko na czasie - jest przełomowe".

**Materiały dodatkowe**

* Informacja: [Splunk Unveils Asset and Risk Intelligence to Revolutionize Proactive Risk Mitigation](https://www.splunk.com/en_us/newsroom/press-releases/2024/splunk-unveils-asset-and-risk-intelligence-to-revolutionize-proactive-risk-mitigation.html)
* Wpis na blogu: [Cisco & Splunk: A Complete SOC Platform Purpose-Built for the AI-Driven Future](https://blogs.cisco.com/security/cisco-splunk-a-complete-soc-platform-purpose-built-for-the-ai-driven-future)
* Wpis na blogu: [Cisco Hypershield - Our Vision to Combat Unknown Vulnerabilities](https://blogs.cisco.com/security/cisco-hypershield-our-vision-to-combat-unknown-vulnerabilities)
* Wpis na blogu: [Authentication Alone is Failing: Introducing Continuous Identity Security](https://duo.com/blog/introducing-continuous-identity-security)
* Wpis na blogu: [Outshift Leads the Way with AI at RSA Conference 2024](https://blogs.cisco.com/news/outshift-leads-the-way-with-AI-at-RSA-conference-2024)

.:|:.:|:.

**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 lub globalnym 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. Wymienione znaki towarowe innych firm są własnością ich odpowiednich właścicieli. Użycie słowa partner nie oznacza relacji partnerskiej między Cisco a jakąkolwiek inną firmą.