**Cisco prezentuje nowe rozwiązanie do szybkiego wykrywania zaawansowanych cyberzagrożeń**

**i automatyzacji reakcji na incydenty bezpieczeństwa**

**Najważniejsze informacje:**

* Dzięki niezrównanej widoczności w całej sieci i punktach końcowych, Cisco Extended Detection and Response (XDR) upraszcza operacje bezpieczeństwa we współczesnym hybrydowym środowisku wielu dostawców i stale zmieniającym się krajobrazie zagrożeń.
* Cisco XDR pozwala szybciej wykrywać incydenty bezpieczeństwa, wykorzystując automatyzację opartą na danych.
* W celu ochrony przed atakami na uwierzytelnianie wieloskładnikowe (MFA), Cisco oferuje zaawansowane funkcje bezpieczeństwa we wszystkich edycjach Duo. Jest to najbardziej opłacalne, najprostsze w obsłudze i najbezpieczniejsze na rynku narzędzie do zarządzania dostępem.

**RSA CONFERENCE 2023, SAN FRANCISCO, 25 kwietnia 2023** - Firma Cisco zaprezentowała postępy w realizacji swojej wizji Cisco Security Cloud, ujednoliconej, napędzanej sztuczną inteligencją, platformy bezpieczeństwa działającej w środowisku hybrydowym. Nowe rozwiązanie Cisco XDR oraz udostępnienie zaawansowanych funkcji dla Cisco Duo pomoże organizacjom lepiej chronić integralność całego ekosystemu IT.

**Wykrywanie i reagowanie na zagrożenia**

Strategia Cisco dotycząca XDR łączy wiedzę z widocznością w sieci oraz punktach końcowych w jednym rozwiązaniu opartym na analizie ryzyka. Cisco XDR upraszcza weryfikowanie incydentów i umożliwia zespołom Security Operations Center (SOC) natychmiastowe usuwanie skutków zagrożeń. Rozwiązanie oparte na chmurze stosuje analitykę w celu nadawania priorytetów wykrywanym incydentom i przenosi punkt ciężkości z niekończących się dochodzeń na naprawianie incydentów o najwyższym priorytecie za pomocą automatyzacji popartej dowodami.

"Krajobraz zagrożeń jest bardzo złożony i ciągle ewoluuje. Wykrywanie bez reagowania jest niewystarczające, natomiast reagowanie bez wykrywania jest niemożliwe. Dzięki Cisco XDR zespoły mogą reagować na zagrożenia i likwidować je, zanim te będą miały szansę wyrządzić znaczne szkody" - powiedział Jeetu Patel, wiceprezes i dyrektor generalny ds. bezpieczeństwa i współpracy w Cisco. "Mamy wyjątkową pozycję, aby dostarczać zintegrowane rozwiązania, które upraszczają zabezpieczanie dzisiejszych, coraz bardziej złożonych, hybrydowych środowisk wielochmurowych, bez uszczerbku dla wygody użytkowników."

Podczas gdy tradycyjna technologia Security Information and Event Management (SIEM) zapewnia zarządzanie danymi skoncentrowanymi na logach i mierzy wyniki przez kilka dni, Cisco XDR koncentruje się na danych telemetrycznych i dostarcza wyniki w ciągu minut. W sposób naturalny analizuje i łączy dane z sześciu źródeł, które zdaniem operatorów Security Operations Center (SOC) są kluczowe dla rozwiązania XDR: punkt końcowy, sieć, zapora sieciowa, poczta elektroniczna, tożsamość i DNS. W odniesieniu do punktów końcowych, Cisco XDR wykorzystuje wgląd z 200 milionów punktów końcowych korzystających z rozwiązania Cisco Secure Client, dawniej AnyConnect, aby zapewnić widoczność na poziomie procesu, gdzie punkt końcowy spotyka się z siecią.

„Prawdziwą miarą skuteczności XDR jest jego zdolność do zapewnienia rzeczywistych wyników w zakresie bezpieczeństwa, realnych i wymiernych korzyści dla organizacji - wczesnego wykrywania, nadawania priorytetów oraz skutecznego i efektywnego reagowania" - powiedział Frank Dickson, wiceprezes IDC ds. Bezpieczeństwa i Zaufania. "Prawdziwe wyniki muszą być policzalne, a nie tylko jakościowo opisane słowami. Cisco XDR dostarcza przejrzystych ram umożliwiających organizacjom osiąganie takich wymiernych rezultatów."

Oprócz natywnej telemetrii, Cisco XDR integruje się z rozwiązaniami innych wiodących dostawców w celu współdzielenia telemetrii, zwiększenia interoperacyjności i dostarczania spójnych wyników niezależnie od dostawcy lub technologii. Wstępny zestaw integracji out-of-the-box obejmuje:

* **Endpoint Detection and Response (EDR)**: CrowdStrike Falcon Insight XDR, Cybereason Endpoint Detection and Response, Microsoft Defender for Endpoint, Palo Alto Networks Cortex XDR, Trend Vision One, SentinelOne Singularity
* **Email Threat Defense:** Microsoft Defender for Office, Proofpoint Email Protection
* **Next-Generation Firewall (NGFW):** Check Point Quantum, Palo Alto Networks Next-Generation Firewall
* **Network Detection and Response (NDR):** Darktrace DETECT™ and Darktrace RESPOND™, ExtraHop Reveal(x)
* **Security Information and Event Management (SIEM):** Microsoft Sentinel

**Zero Trust i zarządzanie dostępem**

Cisco na nowo definiuje, co jest niezbędne w zarządzaniu dostępem, ponieważ napastnicy coraz częściej celują w luki w słabszych wdrożeniach uwierzytelniania wieloskładnikowego (MFA). Każda firma potrzebuje trzech kluczowych filarów dla swojej strategii zarządzania dostępem: egzekwowania silnego uwierzytelniania, weryfikacji urządzeń i zmniejszenia liczby używanych haseł. Właśnie dlatego, począwszy od 1 maja, Cisco dodaje Trusted Endpoints do wszystkich swoich płatnych wersji Duo. Wcześniej dostępne tylko w najwyższej wersji Duo, Trusted Endpoints pozwala na dostęp do zasobów tylko zarejestrowanym lub zarządzanym urządzeniom. Dostarczając Trusted Endpoints obok Single Sign On, MFA, Passwordless i Verified Push w ramach podstawowej edycji Duo Essentials, Cisco dostarcza najbardziej opłacalne, przyjazne dla użytkownika i najbezpieczniejsze na rynku rozwiązanie do zarządzania dostępem.

**Materiały dodatkowe:**

* Dowiedz się więcej o rozwiązaniach Cisco pod adresem: <http://cisco.com/go/security>
* Blog Cisco: [XDR and the Importance of Cross-Domain Correlated Telemetry](https://blogs.cisco.com/security/xdr-importance-of-cross-domain-correlated-telemetry)

### Blog Cisco: [Simplify Your Security Operations with Cisco XDR, Launching at RSAC](https://blogs.cisco.com/security/simplify-your-security-operations-with-cisco-xdr)

### Blog Cisco: [Raising the Bar: Duo Redefines What is Essential for Access Management](https://duo.com/blog/duo-redefines-what-is-essential-for-access-management)

.:|:.:|:.

**O Cisco:**

Cisco (NASDAQ: CSCO) jest światowym liderem w dziedzinie technologii tworzących Internet, które zmieniają oblicze aplikacji, zabezpieczają dane, przekształcają infrastrukturę i łączą zespoły pracowników na całym świecie. Dowiedz się więcej na [www.newsroom.cisco.com](https://newsroom.cisco.com/). Cisco i logo Cisco to zastrzeżone znaki towarowe należące do Cisco i/lub jego podmiotów zależnych w U.S.A i innych krajach. Pełna lista znaków towarowych Cisco dostępna jest pod adresem: [www.cisco.com/go/trademarks](file:///C:\Users\ldabrows\Downloads\www.cisco.com\go\trademarks). Znaki towarowe firm trzecich są ich własnością.