**Veeam wprowadza do Veeam Data Platform nowe narzędzia do proaktywnej analizy zagrożeń. Pozwoli to przeciwdziałać cyberatakom i ich twórcom oraz wzmocnić wiodące funkcje odporności danych dla przedsiębiorstw**

Nowe narzędzie Veeam Recon Scanner proaktywnie identyfikuje zagrożenia cybernetyczne przy użyciu technologii będącej w procesie patentowania oraz największej na świecie bazy danych dotyczących cyberincydentów.

**Seattle, Waszyngton, USA – 1 października 2024 –** [Veeam Software](https://www.veeam.com/?ad=in-text-link), lider pod względem udziału w rynku rozwiązań zapewniających odporność danych, ogłosił podczas konferencji [VeeamON Data Resilience Summit](https://www.veeam.com/veeamon-data-resilience-summit) wprowadzenie do platformy Veeam Data Platform (VDP) nowego narzędzia Veeam Recon Scanner. Ta przełomowa technologia, opracowana przez Coveware by Veeam, oparta jest na wieloletnim doświadczeniu firmy w zakresie reagowania na incydenty związane z cyberwyłudzeniami. Wykorzystuje także dane zgromadzone w największej na świecie bazie incydentów cybernetycznych. Celem Veeam Recon Scanner jest proaktywna identyfikacja i klasyfikacja incydentów oraz zapobieganie cyberatakom. Narzędzie to rewolucjonizuje proces oceny zagrożeń na rynku rozwiązań do ochrony danych.

— *Zabezpieczenie przedsiębiorstwa przed cyberatakiem wymaga skoordynowanej strategii. W jej zakres wchodzi obrona punktów dostępu do zasobów firmy, a także kompleksowa ochrona danych i kopii zapasowych. Jednak zawsze istnieje ryzyko, że przestępca przeniknie przez tę warstwę zabezpieczeń. Recon Scanner rozpoznaje taktykę oraz wykorzystywane przez przeciwnika techniki i procedury, zanim dojdzie do ataku* – mówi Dave Russell, starszy wiceprezes ds. strategii w Veeam. – *Dzięki funkcjom proaktywnej analizy danych nowe narzędzie jest w stanie identyfikować niespodziewane połączenia sieciowe, nietypowe zachowania użytkowników, podejrzaną aktywność w obrębie plików, próby wykradania danych, a nawet potencjalne ataki typu brute force. W tradycyjnym procesie wykrywania i neutralizacji zagrożeń wyzwaniem jest tzw. dwell time, czyli okres między naruszeniem dostępu do firmy a samym atakiem. Dzięki proaktywnym funkcjom oceny zagrożeń zintegrowanym z Veeam Data Platform nasi klienci mogą wykrywać i przeciwdziałać atakom zanim wpłyną one na ich biznes. Wzmacniają tym samym odporność danych i chronią kluczowe zasoby*.

Cyberataki, w tym zagrożenia ransomware, stają się coraz bardziej powszechne i biorą na celownik zarówno środowiska produkcyjne, jak i kopie zapasowe. Odzyskiwanie danych po takich incydentach jest coraz trudniejsze i wskazuje potrzebę posiadania kompleksowych rozwiązań do ochrony danych. Będący częścią Veeam Data Platform Premium Recon Scanner oferuje klientom możliwość identyfikowania zagrożeń zanim wyrządzą one szkody. Poprzez regularne skanowanie narzędzie to rozpoznaje podejrzaną aktywność oraz TTPs (Taktyki, Techniki i Procedury), umożliwiając firmom podjęcie wyprzedzających działań obronnych i łagodzenie skutków. Wraz z pierwszym w branży proaktywnym podejściem Veeam jako jedyny dostawca platformy danych zapewnia użytkownikom VDP Premium tak zaawansowaną technologię oceny zagrożeń bez dodatkowych kosztów.

Recon Scanner oferuje unikatową technologię proaktywnej oceny zagrożeń, bazującą na szerokim doświadczeniu Coveware w zarządzaniu tysiącami incydentów związanych z oprogramowaniem ransomware. Narzędzie to łączy funkcje zautomatyzowanego skanowania, alertów w czasie rzeczywistym oraz analizy danych, umożliwiając zespołom ds. bezpieczeństwa podejmowanie działań zapobiegawczych oraz poprawę ogólnego bezpieczeństwa przedsiębiorstwa.

Wspierane przez Recon Scanner rozwiązanie Veeam Data Platform v12.2 jest dowodem zaangażowania firmy Veeam w podnoszenie poziomu odporności, zarządzania i bezpieczeństwa danych. Platforma zapewnia przedsiębiorstwom możliwość ochrony, odzyskiwania i bezpiecznego administrowania danymi w ich hybrydowych środowiskach. Będąc zgodnym z zasadami ZeroTrust Data Resilience oraz Secure By Design opracowanymi przez amerykańską agencję ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (ang. *Cybersecurity and Infrastructure Security Agency, CISA*), Veeam kontynuuje przestrzeganie najlepszych praktyk w zakresie bezpieczeństwa, pozwalając klientom na prowadzenie działalności biznesowej z poczuciem, że ich cenne dane są bezpieczne.

Aplikacja Veeam Recon Scanner będzie dostępna do pobrania od listopada. Więcej informacji na temat Veeam Data Platform z Recon Scanner dostępnych jest na stronie <https://www.veeam.com>.

**O firmie Veeam Software**

Veeam® jest wiodącym globalnym dostawcą rozwiązań w dziedzinie odporności danych. Firma wierzy, że każde przedsiębiorstwo powinno być w stanie swobodnie przywracać działalność po wystąpieniu zakłóceń i w pełni kontrolować dane w każdym momencie i w dowolnym miejscu. Veeam nazywa to podejście maksymalną odpornością i z zaangażowaniem tworzy innowacyjne sposoby pozwalające klientom ją osiągnąć. Rozwiązania firmy zostały zaprojektowane z myślą o zwiększaniu odporności danych poprzez tworzenie kopii zapasowych, odzyskiwanie danych i ich niezależność, a także bezpieczeństwo danych i działania z zakresu data intelligence. Dzięki temu kierownicy działów IT i bezpieczeństwa mają pewność, że ich aplikacje i dane są chronione oraz zawsze dostępne w środowiskach chmurowych, wirtualnych, fizycznych, SaaS i Kubernetes. Firma Veeam, z siedzibą w Seattle w stanie Waszyngton i biurami w ponad 30 krajach, chroni ponad 550 tys. klientów na całym świecie, w tym 74% firm z listy Global 2000, które ufają, że Veeam zapewni ciągłość działania ich firm. Maksymalna odporność zaczyna się od Veeam. Więcej informacji można znaleźć na stronie [https://www.veeam.com](https://www.veeam.com/) lub profilach Veeam w serwisach LinkedIn [@veeam-software](https://nam10.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.linkedin.com%2Fcompany%2Fveeam-software&data=05%7C02%7CHeidi.Kroft%40veeam.com%7Ca34876b5cfae45e6182308dc9af3f018%7Cba07baab431b49edadd7cbc3542f5140%7C1%7C0%7C638555619703514662%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=3MAm4Yul%2FpfhWOnUxOGAbeaYjbugX21%2B87LuxUUgpM0%3D&reserved=0) i X [@veeam](https://nam10.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FVeeam&data=05%7C02%7CHeidi.Kroft%40veeam.com%7Ca34876b5cfae45e6182308dc9af3f018%7Cba07baab431b49edadd7cbc3542f5140%7C1%7C0%7C638555619703524801%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=Op4qacBPb7en%2FNpSdxqllhSSyfkY0fPKc0qDnHtaWkU%3D&reserved=0).