**Sztuczna inteligencja i automatyzacja sposobem na niedobór ekspertów cyberbezpieczeństwa**

**Wiele uwagi poświęcono ostatnio najlepszym sposobom ochrony sieci korporacyjnych przed zagrożeniami cybernetycznymi, przeciwdziałaniu atakom ukierunkowanym oraz całkowitym kosztom z tym związanym. Jednak szefowie działów bezpieczeństwa IT na całym świecie zmagają się z jeszcze poważniejszym problemem, który w dłuższej perspektywie ma ogromny wpływ na ich organizacje: coraz większym niedoborem wysokokwalifikowanych specjalistów w zakresie cyberbezpieczeństwa.**

Według ankiety przeprowadzonej przez Ponemon Institute we współpracy z DomainTools, 73% zespołów ds. bezpieczeństwa IT odczuwa brak rąk do pracy. Kadra kierownicza uważa jednak, że jest na to sposób. Niektórzy z szefów zespołów odpowiedzialnych za bezpieczeństwo ufają, iż systemy uczące się stanowią remedium na wszelkie wyzwania związane z cyberbezpieczeństwem. Specjaliści bezpieczeństwa z różnych sektorów gospodarki mocno stawiają obecnie na automatyzację i sztuczną inteligencję, z nadzieją na wypełnienie braków kompetencyjnych i sprostanie wymaganiom związanym z bezpieczeństwem IT.

- *Specjaliści cyberbezpieczeństwa ostrzegają, że choć istnieją dowody na ich skuteczność, sztuczna inteligencja i automatyzacja nie mogą zastąpić ludzi. Oczywiście, nie wszyscy specjaliści uważają, że ich praca jest zagrożona przez te technologie. Z wprowadzeniem nowych technologii wiązać się będzie zapotrzebowanie na większą liczbę zdolnych i dobrze wykształconych pracowników, co doprowadzi nawet do zwiększenia liczby miejsc pracy w branży* - **przewiduje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe**.

Dzięki oszczędności czasu i zasobów – trwonionych na pracochłonne zadania, takie jak analiza złośliwego oprogramowania – automatyzacja ma stać się głównym czynnikiem zwiększającym skuteczność i wydajność zabezpieczeń, twierdzą respondenci, przyznając jednocześnie, że nie wszystkie problemy zostaną w ten sposób rozwiązane. Połowa ankietowanych już zautomatyzowała tego typu zadania, a 56% planuje zrobić to w ciągu najbliższych trzech lat.

„*W ciągu zaledwie roku perspektywa wdrożenia zautomatyzowanych procesów została wśród specjalistów bezpieczeństwa znacząco skrócona*” – powiedział dr Larry Ponemon, prezes i założyciel Ponemon Institute.

„*Wbrew powszechnemu przekonaniu, że rozwój automatyzacji zagrozi rynkowi pracy, w odczuciu organizacji technologie te pomogą zwolnić z rutynowych zajęć wysokokwalifikowanych pracowników i dać im możliwość wykonywania pracy wymagającej najwyższych kompetencji, co przyczyni się do znaczącej poprawy bezpieczeństwa cybernetycznego*”.

Raport powstał w oparciu o 1400 opinii szefów działów IT i specjalistów bezpieczeństwa ze Stanów Zjednoczonych, Wielkiej Brytanii oraz Australii i Oceanii (APAC). Geografia odgrywa ważną rolę w postrzeganiu automatyzacji i sposobie jej wdrażania w organizacjach. Ze względu na większy niedobór specjalistów, profesjonaliści – dla przykładu – z USA (65%) i Wielkiej Brytanii (59%) częściej wykorzystywali sztuczną inteligencję jako narzędzie wspomagające pracę ich zespołów i pozwalające skupić się im na ważniejszych zadaniach, podczas gdy region APAC z większym sceptycyzmem podchodzi do możliwości i wydajności technologii AI wprzęgniętej w system ochrony bezpieczeństwa systemów IT.