**Infocyte Partners we współpracy z Check Point Software Technologies**

**Infocyte, firma zajmująca się bezpieczeństwem cybernetycznym, skoncentrowana na proaktywnym wykrywaniu zagrożeń i reagowaniu na incydenty oraz Check Point Software Technologies rozpoczęli współpracę, by zapewnić szybsze wykrywanie zagrożeń oraz sposoby reagowania na incydenty bezpieczeństwa. Jako część partnerskiej platformy Infocyte, Infocyte HUNT zostanie zintegrowany z pakietem zaawansowanych usług Check Pointa. Obie firmy będą wymieniać się informacjami o zagrożeniach, aby usprawnić wykrywanie zagrożeń i możliwości reagowania na incydenty.**

Najnowszy raport Check Pointa dotyczący trendów cybernetycznych podkreśla rosnący niepokój związany z zaawansowanymi zagrożeniami. Nowe formy złośliwego oprogramowania, kryptominerów, oprogramowania ransomware i innych cyberataków nadal wykazują alarmujące wskaźniki infekcji w sieciach chmurowych, zarówno tradycyjnych i hybrydowych. Wraz z ewolucją cyberataków stają się one lepsze w penetrowaniu sieci IT i ukrywaniu się przed tradycyjnymi technologiami wykrywania. Starając się z tym walczyć, firmy przyjmują proaktywne praktyki, takie jak wykrywanie zagrożeń po awarii i rozwiązania naprawcze, które uzupełniają istniejące mechanizmy bezpieczeństwa cybernetycznego.

- *Kiedy klienci kontaktują się z Check Point i naszą globalną siecią partnerską w celu uzyskania pomocy, oczekują natychmiastowych odpowiedzi* - powiedział Dan Wiley, dyrektor ds. Reagowania na incydenty w Check Point. - *Wdrożyliśmy Infocyte HUNT w wielu środowiskach klientów z ogromnym sukcesem. Zintegrowanie funkcji bezpieczeństwa Check Point i funkcji oceny urządzeń końcowych Infocyte HUNT znacznie poprawia nasz czas reakcji. Dodatkowo, rozwiązanie „Compromise Assessment” pozwala nam świadczyć te usługi klientom w proaktywnej i chmurowej platformie.*

Jednym z najtrudniejszych aspektów ustanawiania linii bazowej i wykrywania zagrożeń cybernetycznych w dowolnym środowisku IT jest poleganie na istniejących narzędziach zabezpieczeń, danych i dziennikach. Infocyte HUNT został tak zaprojektowany, aby być niezależnym i opierać się zagrożeniom dla tradycyjnych rozwiązań, które są podatne na pewne typy ataków. Możliwość rozmieszczania na hostach fizycznych lub wirtualnych, stacjonarnie lub w chmurze, umożliwia Infocyte HUNT dostarczanie decydujących wyników - szybciej i dokładniej.

*- To, co zaczęło się jako spowolnienie sieci, przerodziło się w pełnoprawny atak* - powiedział Erik Pufahl, wiceprezes działu IT w Linden Bulk Transportation. - *Infocyte HUNT zapewnił natychmiastową widoczność ruchu całej naszej sieci, co umożliwiło nam szybkie odizolowanie i wyeliminowanie zagrożeń. Posiadamy teraz rozwiązania Check Pointa zapewniające ochronę oraz Infocyte HUNT do proaktywnego wykrywania i reagowania, co pozwala nam na bieżąco wykrywać i badać nowe potencjalne zagrożenia.*

Połączenie Infocyte HUNT z rozwiązaniami Check Point Cloudguard i Sandblast zapewnia specjalistom ds. bezpieczeństwa możliwość wykrywania wyrafinowanych ataków i zagrożeń w środowiskach chmurowych, centrach danych i sieciach hybrydowych.

- *Cieszymy się, że możemy współpracować z Check Point i ich sieciami partnerskimi oraz zapewnić najlepsze na rynku możliwości wykrywania zagrożeń i reagowania na incydenty -* dodaje Curtis Hutcheson, dyrektor generalny Infocyte. *- Dzięki naszej współpracy możemy pomóc większej liczbie organizacji aktywnie wykrywać zagrożenia, naprawiać je i szybciej odzyskiwać sprawność.*