**Check Point wprowadza nowy system Infinity SOC, wykorzystujący sztuczną inteligencję w celu szybkiego i dokładnego zapobiegania cyberatakom.**

**Check Point Infinity SOC to scentralizowane narzędzie w organizacji, które wykorzystując sztuczną inteligencję, stale monitoruje i analizuje działania ludzkie, procesy oraz technologie reagując i zapobiegając incydentom cyberbezpieczeństwa.**

Nowością Infinity SOC jest wykorzystanie – jako pierwszej w branży - sztucznej inteligencji (AI) w procesie wykrywania fałszywych alarmów i automatycznego wskazania i naprawy newralgicznych punktów struktury bezpieczeństwa firmy za pomocą jednego kliknięcia. System Infinity SOC wykorzystuje analizę incydentów do filtrowania milionów nieistotnych dzienników i alertów, pomagając zespołom ds. bezpieczeństwa w przedsiębiorstwach skutecznie i szybko odpierać zewnętrzne cyberataki.

*- Infinity SOC pozwala zespołom bezpieczeństwa opanować codzienne przeciążenie alertami o zdarzeniach i eliminuje martwe punkty w sieci, aby automatycznie wskazywać i blokować najbardziej wyrafinowane ataki, zanim spowodują szkody -* powiedział Itai Greenberg, wiceprezes ds. Zarządzania produktem w Check Point.  *- Zaawansowana analiza oparta na sztucznej inteligencji i zasobom wywiadowczym, pozwala na najszybszą i najbardziej ukierunkowaną odpowiedź. Żadne inne rozwiązanie nie oferuje takiego połączenia zautomatyzowanych funkcji zapobiegania, wykrywania, badania i naprawy w jednej platformie -* dodaje.

Dotychczas większość organizacji używała wielu produktów punktowych do identyfikacji zagrożeń zewnętrznego ataku. Takie działanie wiązało się z codzienna analiza i generowaniem milionów dzienników zdarzeń i alertów. W badaniu SOC\* 68% respondentów stwierdziło, że połowa analizowanych przez nich zdarzeń miała wyniki fałszywe. Stąd większość specjalistów ds. bezpieczeństwa IT uważa, że głównymi wyzwaniami operacyjnymi są prace związane z analizowaniem i usuwaniem incydentów (52% cytowanych), dokładne identyfikowanie najbardziej krytycznych zdarzeń (52%) oraz przeciążenie logów i alerty (51%). Check Point Infinity SOC rozwiązuje te problemy i pomaga przedsiębiorstwom chronić ich sieci, zapewniając:

1. **Dokładność**: automatycznie odsłania nawet najbardziej ukryte ataki z milionów dzienników i alertów, wykorzystując pierwszą w branży analizę incydentów AI. Infinity SOC automatycznie sortuje alerty, aby umożliwić szybszą reakcję na krytyczne ataki. Zapobiega również uruchamianiu kampanii phishingowych przeciwko użytkownikom przez usunięcie podobnych firmowych domen.

2. **Szybkie wykrywanie incydentów**: Infinity SOC jest zasilany przez ThreatCloud, największą na świecie sieć współpracy do walki z cyberprzestępczością, umożliwiającą zespołom wywiad na temat dowolnego typu ataku, w tym globalnego rozprzestrzeniania się, terminów i wzorów ataku czy DNA złośliwego oprogramowania. Obejmuje to również wyszukiwanie głębokiego linkowania w mediach społecznościowych i OSINT. Podejrzane pliki są szybko sprawdzane przy użyciu emulacji zagrożeń SandBlast, która ma najlepszy w branży wskaźnik wyłapywania złośliwego oprogramowania.

3. **Ujednolicony system:** Infinity SOC to pojedyncza, centralnie zarządzana platforma chmurowa, która poprawia wydajność operacyjną zespołów i obniża całkowity koszt działania. Wdraża się w kilka minut i pozwala uniknąć kosztownego przechowywania dzienników i problemów związanych z prywatnością dzięki unikalnej analizie zdarzeń w chmurze, która nie eksportuje i nie zapisuje dzienników zdarzeń. *- Kluczowe znaczenie miało dla nas znalezienie rozwiązania, które pomogłoby nam poradzić sobie z codziennym zalewem alertów i wydarzeń oraz znaleźć garść autentycznych, potencjalnie szkodliwych zagrożeń dla naszych sieci -* powiedział Soren Kristensen, inżynier ds. Bezpieczeństwa w firmie Terma A / S.