**Check Point prezentuje ThreatCloud Graph, wielowymiarową perspektywę cyberbezpieczeństwa opartą o AI**

**W obliczu złożonych i wyrafinowanych zagrożeń cybernetycznych przedsiębiorstwa mają coraz większe trudności z utrzymaniem swojego bezpieczeństwa. Chcąc odpowiedzieć na to wyzwanie, Check Point Software wprowadził ThreatCloud Graph, skupiający się na proaktywnym zapobieganiu pojawiającym się zagrożeniom. Ta przełomowa funkcja w ThreatCloud AI, mózgu wszystkich produktów Check Point, oferuje nowatorskie podejście do bezpieczeństwa cybernetycznego.**

Check Point Software Technologies w szerokim zakresie wykorzystuje technologię sztucznej inteligencji w swoich rozwiązaniach z zakresu bezpieczeństwa cybernetycznego. ThreatCloud AI, szkielet infrastruktury bezpieczeństwa Check Point, wykorzystuje ponad 40 silników AI do przetwarzania i analizowania ogromnych ilości danych. Takie podejście zapewnia dynamiczną analizę bezpieczeństwa w czasie rzeczywistym, umożliwiając identyfikację i zapobieganie złożonym i wyrafinowanym cyberatakom. Integrując sztuczną inteligencję ze swoim wielowarstwowym systemem bezpieczeństwa, Check Point zapewnia kompleksową i proaktywną ochronę, dotrzymując kroku zmieniającej się naturze zagrożeń.

**To podejście oparte na sztucznej inteligencji ma kluczowe znaczenie dla skuteczności funkcji takich jak ThreatCloud Graph, zwiększając ich zdolność do ochrony przedsiębiorstw przed pojawiającymi się wyzwaniami w zakresie cyberbezpieczeństwa.**

ThreatCloud Graph umożliwia analizę złożonej sieci relacji między podmiotami cyfrowymi, oferując wielowymiarowe spojrzenie na cyberzagrożenia. Jest dostosowany do potrzeb przedsiębiorstw i uwzględnia rosnącą złożoność oraz wyrafinowanie cyberataków. Oferuje m.in.:

l **Holistyczne zapobieganie zagrożeniom:** analizowanie relacji między adresami URL, adresami IP i domenami w celu przewidywania potencjalnych zagrożeń. To kompleksowe podejście zapewnia pełne zrozumienie krajobrazu zagrożeń, ze szczególnym uwzględnieniem zapobiegania zagrożeniom.

l **Wzorce wykresów i wgląd w ataki:** rozszyfrowanie złożonych wzorców ataków, w tym zaawansowanych zagrożeń, takich jak „zatruwanie DNS”. Funkcja umożliwia głębszy wgląd w potencjalne strategie ataków, ulepszając mechanizmy proaktywnego zapobiegania.

l **Proaktywne zapobieganie zagrożeniom zero-day:** wykorzystanie wiedzy ThreatCloud AI do identyfikowania i łagodzenia pojawiających się zagrożeń. System ocenia reputację podmiotów cyfrowych, takich jak adresy URL, domeny i adresy IP, na podstawie ich powiązań z wcześniej znanymi złośliwymi artefaktami, takimi jak popularne adresy IP, rejestratory i serwery nazw, zapewniając kluczowe zabezpieczenie zapobiegawcze przed nowymi, nieudokumentowanymi zagrożeniami.

**Odsłonięcie perspektywy wielowymiarowej**

Innowacja Check Pointa umożliwia zmianę paradygmatu w wykrywaniu zagrożeń, wykraczając poza tradycyjną analizę samodzielnych elementów, takich jak adresy URL, adresy IP i nazwy domen. ThreatCloud Graph zagłębia się w połączoną sieć powiązań między tymi podmiotami, odsłaniając wielowymiarowe spojrzenie na zagrożenia cybernetyczne.

Tradycyjnie zagrożenia identyfikowano na podstawie złośliwej zawartości wykrywanej przez silniki zaprojektowane do identyfikowania określonych typów zagrożeń. Jednak ThreatCloud Graph zdaje sobie sprawę, że zagrożenia nigdy nie działają w izolacji: są częścią większych sieci i kampanii, często identyfikowalnych z podmiotami takimi jak serwery nazw i rejestratorzy. Podkreślając relacje między adresami URL, adresami IP, serwerami nazw i innymi elementami, ThreatCloud Graph identyfikuje wzorce i łączy wspólne podmioty, umożliwiając zapobieganie zagrożeniom typu „zero-day” nawet w przypadku braku wykrytej złośliwej zawartości.

**Holistyczne spojrzenie na wskaźniki zagrożenia**

Jedną z kluczowych funkcji ThreatCloud Graph jest możliwość przechowywania i indeksowania całego krajobrazu zagrożeń w postaci graficznej bazy danych. Została ona zaprojektowana do obsługi wysoce połączonych danych, dzięki czemu idealnie nadaje się do zastosowań obejmujących złożone relacje. Elastyczność i skalowalność infrastruktury ThreatCloud Graph pozwala na łatwą rozbudowę w celu uwzględnienia dodatkowych relacji i różnych typów ataków.

ThreatCloud Graph wprowadza całościowe spojrzenie na wskaźniki zagrożeń, przechodząc od pojedynczego wskaźnika naruszenia (IOC) do wielowymiarowego widoku opartego na wzorcach ataków. Wykorzystując potężną wiedzę ThreatCloud AI na temat wzorców ataków, ThreatCloud Graph ma na celu zapobieganie IOC typu „zero-day”, takim jak adresy URL, domeny i adresy IP, poprzez ustalanie ich reputacji na podstawie powiązań z wcześniej znanymi złośliwymi artefaktami. Osiąga się to poprzez podobieństwa w adresach IP, rejestratorach i serwerach nazw.

Mechanizm działania ThreatCloud Graph polega na analizie relacji adresów URL z hostami domen. ThreatCloud Graph może identyfikować potencjalne zagrożenia, badając wspólne relacje znanych złośliwych domen. Dalsza analiza gwarantuje, że te relacje są unikalne dla złośliwych podmiotów i nie są udostępniane przez legalne domeny, ostatecznie identyfikując określone adresy URL jako złośliwe.

ThreatCloud Graph jest idealnym rozwiązaniem dla przedsiębiorstw ze względu na wielowymiarowe podejście do cyberbezpieczeństwa. Wykracza poza analizę pojedynczych zagrożeń, zamiast tego bada relacje między podmiotami cyfrowymi, takimi jak adresy URL, adresy IP oraz nazwy domen. Ta holistyczna perspektywa umożliwia przedsiębiorstwom skuteczniejsze przewidywanie i neutralizowanie wyrafinowanych zagrożeń cybernetycznych. Dodatkowo jego integracja z obszerną bazą wiedzy ThreatCloud AI pozwala na proaktywne zapobieganie pojawiającym się zagrożeniom, w tym atakom typu „zero-day”. To sprawia, że ThreatCloud Graph jest potężnym narzędziem w arsenale cyberbezpieczeństwa przedsiębiorstwa, oferującym zaawansowaną ochronę opartą na sztucznej inteligencji w coraz bardziej złożonym krajobrazie zagrożeń.