**Check Point CloudGuard Log.ic - zabezpieczenie usług w chmurze dzięki nowym możliwościom analizy bezpieczeństwa**

**Firma Check Point ogłosiła dzisiaj premierę CloudGuard Log.ic, oprogramowania, które umożliwia natywną dla chmury ochronę przed zagrożeniami i analizę bezpieczeństwa. Dzięki CloudGuard Log.ic, klienci mogą teraz zobaczyć każdy przepływ danych oraz każdą akcję w elastycznych środowiskach chmurowych, przyspieszając w ten sposób procesy dochodzeniowe.**

CloudGuard Log.ic efektywnie wykrywa nieprawidłowości w chmurze, blokuje zagrożenia i włamania oraz zapewnia bogatą w detale wizualizację, która umożliwia dogłębne audyty incydentów bezpieczeństwa w publicznych infrastrukturach chmurowych takich jak AWS. Log.ic dołącza do rodziny oprogramowania dotyczącego bezpieczeństwa w chmurze firmy Check Point, CloudGuard.

Ankieta dotycząca bezpieczeństwa w chmurze, przeprowadzona dla Check Point przez CyberSecurity Insiders wykazała, że największymi bolączkami organizacji IT dotyczącymi bezpieczeństwa w chmurze są zgodność (34%) oraz brak wglądu w bezpieczeństwo infrastruktury (33%). Podczas gdy większość organizacji powiedziała, że ich instancje chmurowe nie zostały zhakowane (54%), niepokojące 25% nie wiedziało czy doszło do włamania, czy nie. 15% organizacji potwierdziło, że miało do czynienia przynajmniej z jednym incydentem bezpieczeństwa w chmurze.

W sercu CloudGuard Log.ic znajduje się silnik wzbogacający, który zestawia dane z różnorodnych źródeł, między innymi z logów procesów VPC oraz AWS CloudTrail, aby zbudować kontekstualną świadomość bezpieczeństwa publicznych środowisk chmurowych. Zespoły bezpieczeństwa i DevOps mogą używać tego gotowego rozwiązania celem skrócenia czasu reakcji na incydenty, śledzenia zagrożeń oraz przeglądania strategii bezpieczeństwa i wdrażania ich dla wielu kont naraz. CloudGuard Log.ic może również integrować się z rozwiązaniami SIEM innych firm, takimi jak Splunk czy ArcSight.

“Jedną z głównych różnic w środowiskach chmurowych jest ulotna natura ich elementów” - podkreśla Fernando Montenegro z firmy analizy rynku, 451 Research. - “Instancje maszyn wirtualnych, kontenery czy funkcje bezserwerowe wykorzystują dane, które kiedyś były uznawane za statyczne, jak na przykład adresy IP, a dziś nie mogą być uznawane za zaufane. Zdecydowanie dostrzegamy potrzebę nowszego zestawu narzędzi bezpieczeństwa, który rozumie nowe koncepty w natywny sposób i łączy informacje z logów procesów, load balancerów czy innych komponentów charakterystycznych dla chmury. Dzięki niemu, zespoły IT otrzymują szerszy pogląd na zdarzenia, co pozwala na lepsze zrozumienie środowiska i dokładniejsze egzekwowanie reguł bezpieczeństwa.”

Niektóre z funkcjonalności CloudGuard Log.ic to:

l Zaawansowana ochrona przed zagrożeniami dzięki wiodącym danym pochodzącym z ThreatCloud firmy Check Point bazujących na podejrzanych adresach IP.

l Łatwe tworzenie konfigurowalnych alertów uruchamianych przez podejrzaną aktywność sieciową i użytkowników, złamanie zasad zgodności i niepoprawne konfiguracje bezpieczeństwa.

l Przypisania użytkowników, grup i ról są analizowane celem śledzenia nawet zdarzeń delegowanych, ponieważ zmiany konfiguracji są śledzone i skorelowane z osobą lub rolą.

l Możliwość skonfigurowania bezpośredniej wysyłki raportów dotyczących istotnych wydarzeń, statystyk i ruchu sieciowego emailem oraz przy pomocy różnych narzędzi ITMS, takich jak ServiceNow, PagerDuty, Jira itp.

l Funkcje automatycznego reagowania na CloudBoty mogą zostać wykorzystane do automatycznego działania w przypadku wystąpienia specyficznych alertów lub podejrzanej działalności, a także do automatyzacji dalszych kroków, takich jak kwarantanna czy oznaczanie w celu późniejszej analizy.

“CloudGuard Log.ic dostarcza naszym klientom korporacyjnym potężne możliwości analizowania wszelkiej aktywności wewnątrz swoich środowisk chmurowych, połączonej z mechanizmami, które identyfikują złośliwą aktywność, oraz wykrywaniem włamań celem zapobieżenia cyberatakom piątej generacji” - powiedział Itai Greenberg, wicedyrektor działu zarządzania produktami i marketingu firmy Check Point Software Technologies. - “Dzięki wdrożeniu CloudGuard Log.ic, Check Point kontynuuje swoją misję polegającą na dostarczaniu swoim klientom najnowszych narzędzi bezpieczeństwa w celu wykrywania i zapobiegania zaawansowanym zagrożeniom w chmurze.”