Dobierz licencję SentinelOne do swoich potrzeb

Wymagania stawiane przed działami IT w różnych organizacjach w zakresie bezpieczeństwa sprzętów i systemów IT mogą być bardzo zróżnicowane. Wynika to z rodzaju posiadanych zasobów, a także samej charakterystyki organizacji – jej wielkości, sektora działalności, a także regulacji prawnych, którym podlega.

Przed takimi dylematami organizacja może również stanąć w momencie dokonywania decyzji o wyborze rozwiązania typu EDR (Endpoint Detection and Response) i licencji odpowiadającej jej potrzebom. SentinelOne pozwala na dostosowanie funkcjonalności do potrzeb organizacji w ramach trzech rodzajów licencji: **CORE, CONTROL** oraz **COMPLETE**.

1. SENTINELONE CORE

Wersja CORE zapewnia podstawowe funkcje EDR – detekcję zagrożeń i ochronę stacji poprzez blokadę złośliwych skryptów czy procesów. W tym wariancie produktu mamy dostęp do pełnej **analityki detekcyjnej**, w skład której wchodzą:

- **statyczny silnik AI**, zaimplementowany wprost w agencie pracującym na stacji końcowej,
- oraz **dynamiczny silnik AI**, który dokonuje dodatkowej analizy procesów, które nie zostały jednoznacznie zidentyfikowane przez statyczne AI.

Wariant CORE umożliwia podejmowanie szeregu czynności w ramach **modułu reakcyjnego** – sieciową kwarantannę dla zainfekowanego hosta, cofnięcie niepożądanych zmian na stacji roboczej, a w przypadku ataku typu ransomware, także rollback hosta i przywrócenie plików w formie sprzed ataku (o ile OS wspiera tą funkcjonalność).

SentinelOne do detekcji zagrożeń używa zaawansowanych algorytmów, które z wykorzystaniem uczenia maszynowego korelują procesy pracujące na danej stacji i na podstawie analizy behawiorystycznej, potrafią zidentyfikować potencjalne zagrożenia.

Co najważniejsze, ta metoda jest skuteczna nawet w przypadku ataków typu 0-day czy wykorzystujących podatności zaszyte w hardware danego rozwiązania.

SentinelOne do detekcji zagrożeń używa zaawansowanych algorytmów, które z wykorzystaniem uczenia maszynowego korelują procesy pracujące na danej stacji i na podstawie analizy behawiorystycznej, potrafią zidentyfikować potencjalne zagrożenia. Co najważniejsze, ta metoda jest skuteczna nawet w przypadku ataków typu 0-day czy wykorzystujących podatności zaszyte w hardware danego rozwiązania.

GŁÓWNE ZALETY LICENCJI CORE:

- **Pełna ochrona stacji roboczej za pomocą pojedynczego agenta,**
- **Detekcja zagrożeń oparta o Machine Learning oraz modele behawiorystyczne,**
- **Wykorzystywanie Cloud Engine do dynamicznego wykrywania zagrożeń, niesklasyfikowanych przez statyczne AI,**
- **Automatyzacja odpowiedzi na zagrożenia dzięki elastycznym politykom dostosowanym do chronionych procesów.**

2. SENTINELONE CONTROL

Wariant CONTROL stanowi rozwinięcie CORE o nowe moduły. Licencja ta umożliwia administratorom łatwą inwentaryzację aplikacji stosowanych przez ich użytkowników końcowych, z uwzględnieniem zarządzania ich podatnościami oraz automatyzacją w zakresie usuwania tychże zagrożeń. Oprócz modułu **Vulnerability Management**, licencja CONTROL wprowadza funkcjonalności zarządzania podłączonymi urządzeniami do stacji roboczej, niezależnie, czy jest podłączona za pomocą interfejsu USB, czy bezprzewodowo poprzez Bluetooth. Wariant CONTROL daje możliwość zarządzania regułami firewall na stacjach końcowych, również w sposób proaktywny poprzez zmiany, które są uwarunkowane stworzonymi politykami dla danej grupy oraz pojawiającymi się zagrożeniami w środowisku IT.

GŁÓWNE ZALETY LICENCJI CONTROL:

- **Pełny dostęp do modułów i funkcjonalności dostarczanych w licencji CORE**
- **Kontrola urządzeń podłączanych do stacji roboczych (USB / Bluetooth)**
  - **Możliwości tworzenia czarnych/białych list urządzeń,**
  - **Możliwości blokowania specyficznych procesów, np. kopiowanie wideo na pamięć zewnętrzną**
  - **Możliwość granularnego tworzenia polityk, biorących pod uwagę m. in. MAC ID urządzenia, wersję używanego protokołu, producenta sprzętu, klasy urządzenia etc.**
- **Kontrola reguł firewall na chronionych stacjach:**
  - **Kontrola ruchu sieciowego,**
  - **Zezwalanie / blokowanie ruchu pochodzącej od konkretnej aplikacji końcowej,**
  - **Adaptacja reguł do wykrytych zagrożeń na podstawie wdrożonych polityk,**
- **Zarządzanie podatnościami aplikacji (Vulnerability Management)**
  - **Inwentaryzacja aplikacji,**
  - **Detekcja podatności, ze wskazaniem sposobu ich usuwania,**
  - **Kontrola wersji oprogramowania, alarmowanie nieaktualnych wersji software na stacjach końcowych.**

3. SENTINELONE COMPLETE

Wersja COMPLETE oferuje wszystkie moduły i funkcjonalności zaimplementowane w systemie SentinelOne i dedykowana jest dla organizacji o najwyższym poziomie wymagań w zakresie cyberbezpieczeństwa. Licencja COMPLETE oprócz kompleksowej ochrony i kontroli nad stacjami roboczymi, wprowadza moduł dedykowany procesowi Threat Hunting. Jest to niezbędne narzędzie do przeprowadzania szybkiej i trafnej analizy po zdarzeniowej, która dla wielu organizacji stała się już wymogiem prawnym w wypadku wystąpienia jakichkolwiek incydentów cyberbezpieczeństwa. Wykorzystanie Cloud Engine - Deep Visibility, pozwala na niespotykany dotąd sposób, wejrzeć w głąb całego środowiska i skorelować ze sobą dane z setek, a nawet tysięcy stacji końcowych, co znacząco upraszcza proces określenia, w jaki sposób został przeprowadzony atak, jakiego spectrum hostów z naszego środowiska dotyczył i jakie podatności wykorzystywał podczas penetrowania naszego środowiska.

GŁÓWNE ZALETY LICENCJI COMPLETE:

- **Pełny dostęp do modułów i funkcjonalności dostarczanych w licencjach CORE i CONTROL**
- **Silnik Deep Visibility umożliwiający zaawansowaną analizę próbek pochodzących z hostów z całego środowiska, niezależnie od zastosowanego OS na hoście, stosowanych aplikacji czy grupy urządzeń, do której został dany host dopisany. Silnik Deep Visibility pozwala na wzajemną korelację tych danych, co pozwala na wgląd w całe środowisko i zdecydowanie ułatwia analizę po zdarzeniową oraz przywracanie pełnej ochrony i funkcjonalności zaatakowanemu środowisku.**
- **Moduł Threat Hunting, który, z wykorzystaniem silnika Deep Visibility, umożliwia rozłożenie ataku na czynniki pierwsze. Umożliwia graficzną reprezentację ataku/zdarzeń w postaci drzewa wzajemnie skorelowanych ze sobą procesów i wgląd użytkownika w:**
  - **Miejsce, w którym rozpoczęła się penetracja środowiska,**
  - **Jakie procesy zostawały powoływane przez atak,**
  - **W jaki sposób procesy próbowały zdobyć informację z środowiska,**
  - **W jaki sposób cyberprzestępcy chcieli wyprowadzić informację ze środowiska (data leak) i gdzie chcieli je wysłać.**