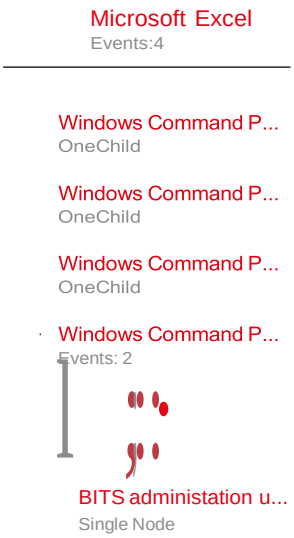
SentinelOne Active EDR

Autonomiczna ochrona punktów końcowych, która pomaga zaoszczędzić czas

PROBLEM

Dotychczasowe systemy antywirusowe oraz narzędzia do ochrony punktów końcowych (endpoint protection - EPP)i narzędzia do wykrywania i zwalczania zagrożeń w punktach końcowych (endpoint detection and response - EDR) nie rozwiązują problemów przedsiębiorstw z cyberbezpieczeństwem. Niektóre firmy używają dodatkowych usług, aby wypełnić tę lukę. Jednak korzystanie z chmury przedłuża cały proces. Obecnie nie można być zależnym od łączności z chmurą, ponieważ szkodliwemu oprogramowaniu wystarczy kilka sekund, aby zainfekować punkt końcowy, poczynić szkody, a następnie zatrzeć ślady. Ta zależność od łączności sprawia, że obecne narzędzia EDR są pasywne, ponieważ opierają się na reakcji operatorów i usług wtedy, gdy jest już za późno.

Platforma SentinelOne Endpoint Protection ujednolica proces zapobiegania, wykrywania i zwalczania zagrożeń na jednym agencie stworzonym specjalnie w tym celu, opartym na uczeniu maszynowym i automatyzacji. Zapewnia on zapobieganie wszystkim głównym typom ataków i ich wykrywanie, szybką eliminację zagrożeń za pomocą w pełni zautomatyzowanych funkcji reagowania opartych na regułach, a także pełną widoczność punktów końcowych i analizę śledczą uwzględniającą pełny kontekst w czasie rzeczywistym.



ROZWIĄZANIE - ACTIVE EDR

Architektura rozwiązania ActiveEDR składa się z jednego agenta SentinelOne, jednej bazy kodu i jednej konsoli. Rozwiązanie ActiveEDR, oparte na opatentowanej technologii TrueContext firmy SentinelOne, wychodzi poza tradycyjne rozwiązania antywirusowe i rozwiązania EDR. Pozwala ono Działom Bezpieczeństwa szybko zrozumieć historię i przyczynę zagrożeń oraz autonomicznie na nie zareagować, bez polegania na zasobach chmurowych. TrueContext koreluje wszystkie zdarzenia należące do grupy procesów i służy jako ich unikalny identyfikator.

Za pomocą ActiveEDR wszyscy, od doświadczonych analityków SOC po nowicjuszy w zakresie bezpieczeństwa, mogą zrozumieć przebieg ataku bez poświęcania wielu godzin na jego ręczne odtwarzanie. Agent SentinelOne jest również w stanie automatycznie reagować na zagrożenia i je neutralizować - wystarczy nacisnąć jeden przycisk. Dzięki tej technologii działy zabezpieczeń mogą skupić się na istotnych alarmach oraz wykorzystywać technologię w obszarach, które dotychczas były ograniczone do działań człowieka.

ROZWIĄZANIE WYRÓŻNIAJĄCE SIĘ POD KAŻDYM WZGLĘDEM

Obszerne dane z analizy śledczej pozwalają automatycznie reagować na zagrożenia, co obejmuje ograniczanie ich skutków, a nawet przywracanie ich do stanu sprzed szyfrowania.

ROZSZERZONE PRZECHOWYWANIE DANYCH

Dane Deep Visibility są przesyłane do chmury i domyślnie przechowywane przez 14 dni. Klienci mogą wykupić przedłużone przechowywanie, aby spełnić wymagania prawne dotyczące przechowywania danych nawet przez wiele lat.

ZWALCZANIE ZAGROŻEŃ I PRZYWRACANIE DO BEZPIECZNEGO STANU

Rozwiązanie zapewnia szczegółowy wgląd w każdą operację na agencie, w tym możliwość szukania danych historycznych oraz przywracania plików i kluczy rejestru do znanego bezpiecznego stanu.

INTEGRACJE

SentinelOne udostępnia interfejsy RESTful API i wbudowane integracje z różnymi aplikacjami i usługami korporacyjnymi, takim jak Splunk, QRadar, Slack, ServiceNow, Joe Sandbox, Reversing Labs Threat Intel,

KONTEKSTOWE INFORMACJE I IDENTYFIKACJA ZAGROŻEŃ W CZASIE RZECZYWISTYM

Technologia TrueContext ogranicza czynności wykonywane ręcznie i automatycznie łączy powiązane ze sobą zdarzenia w historię ataku.

WYKRYWANIE ZAGROŻEŃ ZTRUECONTEXT

Umożliwia monitorowanie plików, wskaźników włamań (IOC) i aktywności w sieci oraz otrzymywanie powiadomień o dostępie lub zmianach.

IMPORT/EKSPORT

Dla klientów przeprowadzających migrację z innych rozwiązań EDR SentinelOne może zaimportować dotychczasowe zapytania do języka zapytań SentinelOne Query Language (S1QL). Ponadto SentinelOne zapewnia strumień eksportowy oparty na środowisku Kafka (Hermes) klientom, którzy chcą przechowywać/ analizować swoje dane EDR w swoich własnych repozytoriach danych.

SentinelOne

sales@cc.com.pl | www.cc.com..pl