Krótki przegląd
Materiały ogólnodostępne Cisco

Cisco Stealthwatch

Skalowane rozwiązania w celu wglądu w informacje o sieci i narzędzia do analizy zabezpieczeń

Czy bezpieczeństwo Twojej sieci zostało naruszone? Skąd możesz o tym wiedzieć?

Twoja firma dokonała znacznych inwestycji w infrastrukturę IT i zabezpieczenia. Tym niemniej ataki nie ustały, a nieznani sprawcy bezkarnie działają wewnątrz firmy. Co więcej, wykrywanie zagrożeń zajmuje całe miesiące, a nawet lata[1]. Brak wglądu w zagrożenia to efekt coraz większej złożoności rozwijającej się sieci, a także coraz bardziej rozbudowanych ataków. Ponadto pracownicy ds. zabezpieczeń dysponują małymi zasobami i zestawami oddzielnych narzędzi, przez co ich możliwości są ograniczone. Skąd możesz wiedzieć, czy bieżące funkcje zabezpieczeń są prawidłowo skonfigurowane, zarządzane i że działają jak należy? Które z narzędzi faktycznie spełniają funkcje, jakich potrzebuje firma?

Rozwiązanie: sieć i system zabezpieczeń

Metadane pakietów sieciowych zapewniają wgląd w informacje o tym, kto łączy się z firmową siecią i jakie ma zamiary. Taki wgląd obejmuje zarówno główną siedzibę, jak i oddziały firmy, publiczną chmurę, prywatne centra danych, użytkowników w ramach roamingu, a nawet Internet rzeczy (IoT). Analiza tych danych pomaga wykrywać zagrożenia i luki w istniejących systemach, zanim powstaną większe szkody. Pozwala również rozpoznawać podejrzane zachowania napastników działających od wewnątrz. Warto podkreślić, że właściwie funkcjonujący system analiz odciąża pracowników ds. zabezpieczeń, pozwalając im skupić się na zagrożeniach o większym prawdopodobieństwie. Takie podejście do wykrywania zaawansowanych zagrożeń pozwala na:

integrację
z istniejącą infrastrukturą

rozwiązanie bez agentów
ani konieczności rozmieszczania czujników we wszystkich miejscach

elastyczność
w zakresie opcji wdrażania i użytkowania: lokalnie lub w chmurze, sprzęt lub maszyny wirtualne, oprogramowanie jako usługa

Zyskaj pewność, że Twoje systemy zabezpieczeń są skuteczne

Cisco Stealthwatch zapewnia wgląd w informacje na wszystkich poziomach firmy, od sieci prywatnych po chmurę publiczną. Zaawansowany system analizy zabezpieczeń pozwala wykrywać i reagować na zagrożenia w czasie rzeczywistym. Rozwiązanie stale analizuje aktywność w sieci, tworząc podstawy dopuszczalnego zachowania, aby wykorzystać te informacje wraz z zaawansowanymi algorytmami uczenia maszynowego do wykrywania nieprawidłowości. Warto jednak pamiętać, że nie wszystkie *podejrzane* zachowania są złośliwymi atakami. Rozwiązanie Stealthwatch umożliwia szybką i zdecydowaną korelację nieprawidłowości z zagrożeniami takimi jak ataki C&C, oprogramowanie ransomware, ataki DDoS, cryptomining, nieznane złośliwe programy i zagrożenia od wewnątrz. Jednolite rozwiązanie bez agentów to kompleksowe monitorowanie zagrożeń w całym centrum danych, oddziale firmy, w punktach końcowych i w chmurze, niezależnie od systemu szyfrowania sieciowego.

Korzyści:

znać każdego hosta, widzieć wszystkie rozmowy, określać dopuszczalne zachowania, być wyczulonym na zmiany, szybko reagować.

- **Stały monitoring i wykrywanie** zaawansowanych zagrożeń, które pokonały istniejące zabezpieczenia lub pochodzą od wewnątrz
- **Skupienie się na kluczowych zdarzeniach, a nie na informacyjnym szumie** za sprawą precyzyjnych alarmów kontekstowych, sortowanych według stopnia zagrożenia
- **Szybka i skuteczna reakcja** dzięki pełnej wiedzy o zagrożeniach, ścieżki audytu sieci pozwalające przeprowadzać dochodzenia, a także integracja z istniejącym systemem zabezpieczeń
- **Wykorzystanie bieżącej inwestycji** w infrastrukturę IT i kompleksowej telemetrii sieci, aby zwiększyć poziom bezpieczeństwa
- **Skalowanie systemu zabezpieczeń wraz z rosnącymi potrzebami firmy,** od nowych oddziałów czy centrów danych, po przenoszenie obciążeń do chmury, czy po prostu zwiększanie liczby podłączonych urządzeń
- **Zapewnianie zgodności z przepisami** za sprawą alarmów dla przypadków naruszenia regulaminu, które można dostosować do mechanizmów działania firmy

1. Według raportu Ponemon z 2018 r. średni czas wykrycia naruszenia bezpieczeństwa wynosi 197 dni.

„Rozwiązanie Cisco Stealthwatch zwiększyło o 100% nasz wgląd w informacje o ruchu wewnętrznym, co umożliwiło identyfikację zagrożeń, które wcześniej były wyjątkowo trudne do wykrycia”.

Projektant infrastruktury IT, duże przedsiębiorstwo
Firma zajmująca się produkcją przemysłową

Kolejne kroki

Aby poznać szczegółowe informacje, odwiedź stronę https://www.cisco.com/c/pl_pl/products/collateral/security/stealthwatch/datasheet-c78-739398.html lub skontaktuj się z lokalnym przedstawicielem firmy Cisco.

C45-736510-05 11/18

Kontekstowy wgląd w informacje o całej sieci

Rozwiązanie Stealthwatch zapewnia **wgląd w informacje dla całej firmy** zarówno na miejscu, jak również we wszystkich środowiskach chmury publicznej. Wiedząc kto korzysta z sieci i co w niej robi, firmy mogą łatwiej wdrażać **inteligentne rozwiązania segmentacji**, dostosowane do mechanizmów działania firmy. To również **praktyczne informacje**, wzbogacone o kontekst w postaci np. nazwy użytkownika, urządzenia, lokalizacji, czasu, aplikacji itp.

Prognostyczna analiza zagrożeń

Rozwiązanie Stealthwatch wykorzystuje szereg technik analitycznych, aby wykrywać zaawansowane zagrożenia zanim dojdzie do ataku. Użycie **analizy zachowania sieci** pozwala wskazać anomalie, które są poddawane dalszej analizie, z wykorzystaniem **uczenia maszynowego (z nadzorem i bez),** co przekłada się na precyzyjne wykrywanie zagrożeń. Dzięki temu pracownicy ds. systemu zabezpieczeń mogą skupić się na najważniejszych zagrożeniach. Mechanizm systemu analizy zabezpieczeń Stealthwatch używa również renomowanego **systemu informowania o zagrożeniach w ramach grupy Cisco Talos.** To najnowsze informacje o korelacji zagrożeń globalnych i lokalnych.

System automatycznego wykrywania i reagowania

Połączenie kontekstowego wglądu w całą firmę i stosowania zaawansowanych technik analitycznych pomaga organizacjom wykrywać zagrożenia takie jak **nieznane lub szyfrowane programy malware, zagrożenia od wewnątrz, naruszenia regulaminów** i wszystko, „co zostanie wykryte w sieci”. Zespoły ds. zabezpieczeń mogą przeglądać **alarmy posiadające priorytet wg stopnia zagrożenia** i posiadają dodatkowe informacje, które pozwolą szybko podjąć działania. Rozwiązanie Stealthwatch to także możliwość przechowywania telemetrii zależnie od skali firmy oraz funkcja ścieżki audytu sieci do **przeprowadzania dochodzeń** w zakresie przeszłych zdarzeń. To również możliwość monitorowania **zgodności z przepisami.** System pozwala na integrację z bieżącym systemem zabezpieczeń, tak aby reagować na zagrożenia bez przestojów w firmie.

Większe bezpieczeństwo dzięki analizie ruchu szyfrowanych danych

Gwałtowny wzrost ruchu szyfrowanych danych wpływa na zmianę stosowanych ataków. Szyfrowanie to funkcja przydatna w ochronie prywatności i systemach zabezpieczeń, ale również narzędzie do ukrywania złośliwego oprogramowania i unikania wykrycia. Firma Gartner przewiduje, że do 2019 roku 80% całego ruchu internetowego będzie szyfrowane, a 70% ataków będzie korzystać z funkcji szyfrowania. Deszyfrowanie i analiza ruchu sieciowego są mało wydajne, a wraz z nadejściem protokołu TLS 1.3 staną się niemożliwe. Firma Cisco wprowadziła rewolucyjną technologię o nazwie **Encrypted Traffic Analytics (ETA),** która jest aktywna w sieci Cisco nowej generacji i w rozwiązaniu Stealthwatch. Pozwala ona analizować ruch szyfrowany bez wykonywania operacji deszyfrowania. Dzięki temu organizacje mogą 1) wykrywać zagrożenia w ruchu szyfrowanym i 2) wykonywać testy zgodności kryptograficznej, aby mieć wgląd w to ile danych cyfrowych firmy wykorzystuje silne szyfrowanie. To również mechanizm kontroli w przypadku naruszeń regulaminów. Aby dowiedzieć się więcej, odwiedź stronę https://www.cisco.com/go/eta