BlackBerry | Cyberbezpieczeństwo

CylanceOPTICS

Łagodzenie Incydentów w Milisekundach: Wykrywanie i reagowanie w punktach końcowych oparte na sztucznej inteligencji

INFORMACJE O ROZWIĄZANIU

WPROWADZENIE

Czasy, gdy organizacja mogła umocnić granice swojej sieci, aby zmniejszyć ryzyko cybernetyczne, minęły. Szybki wzrost liczby urządzeń mobilnych i IoT, które udostępniają dane i łączą się z wieloma sieciami, stworzyło wykładniczo rosnącą powierzchnię ataku.

W tym nowym środowisku zagrożeń priorytetem jest uniemożliwienie przeciwnikom zainfekowania tych odległych urządzeń złośliwym oprogramowaniem. Oferowana przez BlackBerry® platforma ochrony punktów końcowych, CylancePROTECT®, osiąga to dzięki sztucznej inteligencji (AI) i technologiom uczenia maszynowego (ML), które zapobiegają detonacji zarówno znanych, jak i nieznanych form złośliwego oprogramowania.

Jak jednak zauważyła firma Verizon[1], „odnotowuje się stały i konsekwentny spadek procentowego udziału złośliwego oprogramowania w naruszeniach w ciągu ostatnich pięciu lat." Nie oznacza to, że złośliwe oprogramowanie zanika jako wektor ataku, a jedynie, że przeciwnicy coraz częściej wykorzystują taktyki, techniki i procedury (TTP), które nie wymagają użycia przenośnych plików wykonywalnych w celu naruszenia punktu końcowego. Na przykład stosują phishing do kradzieży danych uwierzytelniających użytkowników, wykorzystują powszechnie znane luki w zewnętrznych usługach sieciowych, takich jak RDP, i osadzają backdoory w powszechnie używanych aplikacjach, jak w przypadku ataków SolarWinds.

Taktyki te często obejmują sekwencję pozornie łagodnych działań, które dopiero w połączeniu ujawniają ich złośliwe intencje. Pojedynczy punkt danych może być istotny tylko w oparciu o kontekst, w którym się pojawia i jego korelację z innymi zdarzeniami związanymi z naruszeniem bezpieczeństwa. Ten rodzaj analizy kontekstowej dobrze nadaje się do rozwiązań wykrywania

i reagowania w punktach końcowych (EDR).

W związku z tym EDR może odegrać dwie kluczowe role w cyberobronie. Po pierwsze, może ostrzegać analityków z centrum operacji bezpieczeństwa (SOC), gdy wykryje wczesne oznaki naruszenia bezpieczeństwa, dzięki czemu reagowanie ograniczające może zostać zainicjowane wystarczająco szybko, aby zminimalizować szkody. Skrócenie czasu reakcji jest nie tylko niezbędne dla odporności operacyjnej, ale także przynosi korzyści finansowe. Organizacje, które rozwiązują incydenty w czasie krótszym niż 200 dni, oszczędzają średnio 1,12 miliona dolarów[2].

Drugą rolą jest uzbrojenie analityków w dane, których potrzebują do proaktywnego poszukiwania zagrożeń i przeprowadzania analizy przyczyn źródłowych po incydencie. Jednak biorąc pod uwagę szybki wzrost liczby urządzeń końcowych oraz ogromne ilości danych telemetrycznych i danych o zdarzeniach, które generują, w jaki sposób analityk ma odróżnić subtelny sygnał zagrożenia od losowego szumu rutynowej aktywności?

W tych informacjach dotyczących rozwiązania rozważymy, w jaki sposób rozwiązanie EDR oparte na sztucznej inteligencji BlackBerry, CylanceOPTICS®, potrafi lepiej niż inne narzędzia pomóc klientom w osiągnięciu obu tych celów. Na przykład, po wdrożeniu CylancePROTECT i CylanceOPTICS, jeden klient[3]:

- **Zredukował stratę czasu o 95%** dzięki szybszemu badaniu i usuwaniu usterek: Mniej użytkowników końcowych było narażonych. Przyspieszone badanie zagrożeń i ich usuwanie pozwoliło użytkownikom końcowym szybko wznowić efektywną pracę.
- **Zredukował ponowne obrazowanie maszyn o 97%:** Umożliwiło to klientowi realokację zasobów IT do bardziej produktywnych projektów.
- **Oszczędził 8,4 miliona dolarów** (wartość bieżąca netto) dzięki wycofaniu starszych rozwiązań w zakresie zabezpieczania punktów końcowych firmy.

PODEJŚCIE BLACKBERRY DO EDR

Stosowane przez BlackBerry podejście nowej generacji do EDR opiera się na trzech filarach:

- **Architektura oparta na chmurze**: CylanceOPTICS stosuje całą logikę wykrywania i reagowania w punkcie końcowym i przechowuje wynikowe dane telemetryczne, alerty i dane śledcze w chmurze do analizy offline.
- **Inteligentna praktyka Edge AI**: Oparte na sztucznej inteligencji i kontekstowe reguły wykrywania zagrożeń identyfikują naruszenia bezpieczeństwa i uruchamiają zautomatyzowane reagowanie, które skraca średni czas do wykrycia (MTTD) i średni czas do naprawy (MTTR).
- **Wnikliwa analiza:** CylanceOPTICS ułatwia wyszukiwanie zagrożeń i analizę przyczyn źródłowych, zapewniając analitykom skonsolidowany, skorelowany, oparty na sztucznej inteligencji i obejmujący całe przedsiębiorstwo widok historii aktywności punktów końcowych.

ARCHITEKTURA OPARTA NA CHMURZE

W przeciwieństwie do innych produktów EDR, CylanceOPTICS wdraża całą logikę wykrywania i reagowania na zagrożenia w punkcie końcowym. W efekcie każdy punkt końcowy działa jako samodzielne SOC, wykrywając i reagując na zagrożenia w czasie zbliżonym do rzeczywistego, bez konieczności korzystania z łączności w chmurze. Eliminuje to opóźnienia w reakcji, w wyniku których drobne zdarzenie związane z naruszeniem bezpieczeństwa może eskalować do poważnego incydentu bezpieczeństwa.

Dane alertów, zdarzeń i telemetrii wszystkich chronionych punktów końcowych są automatycznie gromadzone, korelowane i przechowywane w chmurze do analizy offline. Po rozpakowaniu klienci otrzymują 30 dni przestrzeni dyskowej w chmurze. BlackBerry oferuje również opcje 90-dniowych i 365-dniowych pakietów retencyjnych dla klientów z branż podlegających ścisłym

regulacjom, którzy potrzebują dodatkowych danych historycznych w celu wykazania zgodności z przepisami. To hybrydowe podejście do chmury eliminuje ograniczenia fizycznej pamięci masowej na punkcie końcowym, zapewniając jednocześnie maksymalną elastyczność w zakresie wykrywania zagrożeń i analizy po incydencie.

EDGE AI

Termin Edge AI odnosi się do praktyki BlackBerry polegającej na wdrażaniu zaawansowanych technologii AI i ML w punkcie końcowym w celu zmniejszenia ryzyka cybernetycznego. Praktyki Edge AI są wykorzystywane w rozwiązaniach CylancePROTECT, CylanceOPTICS i CylancePERSONA™.

Wykrywanie zagrożeń za pomocą silnika analizy kontekstowej

Silnik CylanceOPTICS Context Analysis Engine (CAE) jest wbudowany w każdy punkt końcowy, monitorując zdarzenia z prędkością maszyny w celu identyfikacji złośliwych i podejrzanych działań. CAE jest dostarczany z gotowym zestawem logiki wykrywania stworzonej przez BlackBerry, która może wyzwalać niezliczone losowe i zautomatyzowane reakcje. CAE zawiera reguły:

- Oparte na informacjach o zagrożeniach w branży i raportach zarządzania.
- Pochodzące z rzeczywistych ataków zbadanych i rozwiązanych w terenie przez zespoły reagowania na incydenty BlackBerry oraz zagrożeń zdekonstruowanych i udokumentowanych przez badaczy BlackBerry. Na przykład zespół BlackBerry Research and Intelligence opracował niestandardowe reguły, które chronią klientów przed atakami HAFNIUM na podatne serwery Microsoft Exchange, a także inne, które oznaczają i łagodzą warianty złośliwego oprogramowania ransomware Ryuk.
- Utworzone przez analityków SOC, które odzwierciedlają zasady bezpieczeństwa specyficzne dla środowiska. Na przykład analityk może zdefiniować regułę, która wyzwala alert i gromadzenie danych śledczych za każdym razem, gdy użytkownik końcowy próbuje uzyskać dostęp do ograniczonego zasobu lub eskalować swoje uprawnienia do konta.
- Odwzorowane w Strukturze MITRE ATT&CK®, globalnej bazie wiedzy o taktykach i technikach aktorów zagrożeń pochodzących z rzeczywistych cyberataków.
- Wykorzystujące unikalną telemetrię procesora z technologii Intel® Threat Detection Technology do wykrywania i łagodzenia skutków cryptojackingu w systemach operacyjnych Windows® 10. Reguły cryptojackingu można łatwo skonfigurować i nie mają one praktycznie żadnego wpływu na procesor chronionych systemów.

Chociaż reguły wykrywania są niezbędne, nie mogą modelować każdego rodzaju zachowania ataku. Dlatego CylanceOPTICS zawiera również moduły wykrywania zagrożeń ML opracowane przez zespół BlackBerry Data Science, które stale analizują aktywność punktów końcowych w celu wykrywania ataków zero-day i zaawansowanych trwałych zagrożeń (APT).

Reagowanie na zagrożenia za pomocą pakietów na żądanie i zautomatyzowanych podręczników

CylanceOPTICS zapewnia zarówno reagowanie na żądanie, jak i automatyczne reagowanie za każdym razem, gdy uruchamiana jest reguła wykrywania CAE lub ML. Oba pakiety są niezbędne do zminimalizowania czasu oczekiwania i zmniejszenia kosztów, ryzyka i długoterminowych skutków wynikających z rozległego incydentu związanego z naruszeniem bezpieczeństwa.

- **Reagowanie na żądanie z zastosowaniem pakietów:** Analitycy mogą wykorzystać zaawansowany silnik skryptowy w CylanceOPTICS do tworzenia i wdrażania pakietów. Są to zbiory skryptów wykonywanych na punkcie końcowym w celu uruchamiania aplikacji, zbierania danych śledczych, przełączania systemów w tryb offline oraz wykonywania innych funkcji dochodzeniowych i naprawczych. Rozwiązanie CylanceOPTICS jest dostarczane z domyślnym zestawem pakietów do wykonywania wielu rutynowych zadań. Pakiety mogą być wdrażane na żądanie i na dużą skalę na pojedynczym urządzeniu, wielu urządzeniach, w wybranych strefach bezpieczeństwa lub w całym przedsiębiorstwie.

- **Zautomatyzowane reagowanie z zastosowaniem podręczników:** Pakiety mogą być również łączone i konfigurowane jako podręczniki, złożone zbiory akcji reagowania, które są uruchamiane automatycznie za każdym razem, gdy wyzwolone zostanie wykrycie CAE lub ML. Analityk może na przykład utworzyć podręcznik gromadzenia danych śledczych, który będzie wykonywany za każdym razem, gdy punkt końcowy uruchomi polecenie programu PowerShell w celu pobrania pliku. Gdy reguła zostanie uruchomiona, podręcznik może automatycznie zbierać logi PowerShell, pliki historii przeglądarki i dane ze zrzutu pamięci, zapewniając w ten sposób analitykowi kontekstowe informacje śledcze bez konieczności przyciskania jakiegokolwiek klawisza.

WNIKLIWA ANALIZA

Po wykryciu incydentu należy go dokładnie zbadać, aby upewnić się, że wszystkie etapy łańcucha zabójstw są zrozumiałe i uwzględnione podczas późniejszych działań związanych z ograniczaniem i odzyskiwaniem. Termin Wnikliwa Analiza (Deep Insight) odnosi się do obszernego zestawu ręcznych i zautomatyzowanych narzędzi do badania incydentów i wyszukiwania zagrożeń, które zapewniają analitykom płynny dostęp do danych punktów końcowych.

Poszukiwanie wskaźników narażenia za pomocą wyszukiwania InstaQuery

Łowcy zagrożeń wykorzystują zarówno dane wywiadowcze, jak i procesy oparte na metodologii, aby identyfikować nietypowe zdarzenia związane z bezpieczeństwem i wzorce aktywności, które łącznie wskazują, że może być przeprowadzany atak. Tradycyjnie wymagało to elitarnych analityków o specjalistycznych umiejętnościach i dużym doświadczeniu. Na szczęście CylanceOPTICS umożliwia analitykom na każdym poziomie umiejętności łatwe i wydajne wyszukiwanie zagrożeń.

CylanceOPTICS upraszcza proces wyszukiwania zagrożeń, umożliwiając zespołom bezpieczeństwa gromadzenie i analizowanie danych za pomocą zaawansowanych wyszukiwaŒ InstaQuery (IQ). IQ to lekkie narzędzie, które zbiera i agreguje odpowiednie dane punktów końcowych i prezentuje je w formacie, który umożliwia zarówno kontekstową, jak i intuicyjną analizę. Wyszukiwania IQ mogą gromadzić artefakty związane z plikami, kluczami rejestru, procesami, połączeniami sieciowymi i wieloma innymi elementami. Dzięki temu analitycy mogą udzielać odpowiedzi na pytania, takie jak:

- Czy ta wartość skrótu lub rozszerzenie pliku pojawiły się kiedykolwiek na jednym z moich punktów końcowych?
- Czy ten wiersz polecenia został kiedykolwiek wykonany na jednym z moich systemów?

Konsultanci BlackBerry Incident Response niedawno wykorzystali IQ, aby pom· c duŨemu przedsiňbiorstwu w zbadaniu i zaradzeniu epidemii ransomware. W ciŃgu kilku sekund zesp· ğustaliğ Ũe gğ wny wskaŦnik naraŨenia, rozszerzenie pliku ransomware, wystňpowağ tylko w Stanach Zjednoczonych. UmoŨiwiğo to zespoğom klienta i BlackBerry skoncentrowanie na tym obszarze dziağaŒ dochodzeniowych, naprawczych i porzŃdkowych, zamiast spňdzania bezproduktywnych godzin na ocenie Ŝrodowisk operacyjnych klienta w Europie, Azji i na poğudniowym Pacyfiku. Konsultanci BlackBerry pomogli r· wnieŨ klientowi w zapobieganiu dalszym infekcjom poprzez tworzenie i dystrybucjň niestandardowych reguğ kt· re zapewniğy natychmiastowe wykrycie i poddanie kwarantannie oprogramowania ransomware.

Optymalizacje dla środowisk Linux

CylanceOPTICS oferuje również ulepszoną ochronę dla systemów pracujących w systemie operacyjnym Linux®, w tym RHEL, Ubuntu, CentOS i SUSE. Ochrona systemów Linux jest niezbędna, ponieważ grupy APT coraz częściej postrzegają system Linux jako atrakcyjny cel. W niedawnym raporcie zespół BlackBerry Research and Intelligence zauważył, że większość firm zajmujących się bezpieczeństwem koncentruje swoją uwagę inżynieryjną i marketingową na produktach zaprojektowanych z myślą o systemach front office, a nie szafie serwerowej. Defensywna ochrona systemu Linux jest często rozproszona i niedojrzała. CylanceOPTICS rozwiązuje te braki w zabezpieczeniach dzięki funkcjom specyficznym dla systemu Linux, takim jak:

- **Architektura bez sterowników**, która zwiększa bezpieczeństwo poprzez wyeliminowanie zależności na poziomie jądra systemu.
- **Reguły CAE dla systemu Linux**, które automatycznie wykrywają złośliwe oprogramowanie i złośliwe zdarzenia..
- **Funkcja Refract dla systemu Linux**, która automatycznie naprawia złośliwe oprogramowanie i złośliwe zdarzenia.
- **Blokada urządzeń**, która ułatwia usuwanie skutków incydentów i odzyskiwanie danych poprzez izolowanie zainfekowanych punktów końcowych w celu powstrzymania rozprzestrzeniania się złośliwego oprogramowania.

Funkcje te umożliwiają administratorom wykrywanie i powstrzymywanie zagrożeń atakujących serwery centrów danych, urządzenia w punktach sprzedaży (POS), terminale bankomatów (ATM) i urządzenia o stałej funkcji oparte na systemie Linux. Linux jest również wszechobecny na serwerach internetowych, superkomputerach, w głównych witrynach internetowych i u dostawcach usług w chmurze, takich jak Google, Yahoo i Amazon.

SPODZIEWANE KORZYŚCI

Oparte na sztucznej inteligencji podejście BlackBerry do EDR pomaga organizacjom zmniejszyć ryzyko cybernetyczne poprzez:

- **Zwalczanie zagrożeń za pomocą zautomatyzowanego reagowania.** Obejmuje to izolowanie urządzeń, kończenie procesów i podejmowanie innych odpowiednich działań, które uniemożliwiają aktorom zagrożenia kradzież danych uwierzytelniających, eskalację uprawnień, poruszanie się po sieci lub realizowanie swoich celów w inny sposób
- **Usuwanie zagrożeń poprzez przywracanie dotkniętych nimi systemów do pierwotnego, idealnego stanu.** Obejmuje to wyeliminowanie wszystkich śladów ataku, wraz z jego mechanizmami trwałości i artefaktami śledczymi.
- **Pomaganie analitykom w identyfikowaniu sygnałów ataku** ukrytych w ogromnych ilościach historycznych danych telemetrycznych punktów końcowych i metadanych przechowywanych w chmurze. Obejmuje to każdy utworzony plik, każdy uruchomiony proces, każdą zmianę kluczy rejestru, każde połączenie sieciowe itp. CylanceOPTICS osiąga to dzięki zautomatyzowanym regułom wykrywania opartym na sztucznej inteligencji i analizie kontekstowej.
- Usprawnienie procesu śledzenia ataków i identyfikowania luk w zabezpieczeniach poprzez zapewnienie analitykom natychmiastowego dostępu do kontekstowych danych, których potrzebują do skutecznego wyszukiwania zagrożeń i analizy przyczyn źródłowych.

WIĘCEJ INFORMACJI

Dowiedz się więcej o CylanceOPTICS i BlackBerry® Cyber Suite.

[1] Raport z badań w sprawie naruszeń ochrony danych w 2020 r.
[2] Raport IBM Security dotyczący kosztów naruszenia ochrony danych w 2020 r.
[3] Badanie Forrester Total Economic Impact™

BlackBerry. Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) zapewnia przedsiębiorstwom i rządom na całym świecie inteligentne oprogramowanie i usługi w zakresie bezpieczeństwa. Firma zabezpiecza ponad 500 milionów punktów końcowych, w tym ponad 195 milionów pojazdów. Firma z siedzibą w Waterloo, Ontario wykorzystuje uczenie SI i maszynowe do dostarczania innowacyjnych rozwiązań w dziedzinach cyberbezpieczeństwa, bezpieczeństwa i ochrony danych oraz jest liderem w dziedzinie bezpieczeństwa punktów końcowych, zarządzania punktami końcowymi, szyfrowania i systemów wbudowanych. Wizja BlackBerry jest jasna — zapewnić skomunikowaną przyszłość, której można ufać.

BlackBerry. Intelligent Security. Everywhere.

Aby uzyskać więcej informacji, odwiedź witrynę BlackBerry.com i obserwuj @BlackBerry.

BB23 | 220412