BLACKBERRY OPTICS.

Inteligentne rozwiązanie EDR napędzane sztuczną inteligencją.
Oparte na chmurze, lecz od niej niezależne.

Gdyby istniał idealny świat, urządzenia końcowe byłyby nie do zdobycia, użytkownicy byliby odporni na phishing, a podatne systemy byłyby zawsze szybko poprawiane. Jednak w prawdziwym świecie świadome organizacje przygotowują się na niemal pewne ryzyko naruszenia i dlatego wdrażają **EDR nowej generacji - BlackBerry® Optics** (część BlackBerry® Cyber Suite).

BlackBerry Optics umożliwia analitykom centrum operacji bezpieczeństwa (SOC) wykrycie wczesnych oznak włamania, dzięki czemu można szybko rozpocząć działania mające na celu zminimalizowanie szkód. Skrócenie czasu reakcji jest istotne nie tylko dla odporności operacyjnej, ale również przynosi korzyści finansowe. Organizacje, które rozwiązują problemy w czasie krótszym niż 200 dni, oszczędzają średnio 1,12 miliona dolarów. Ponadto **BlackBerry Optics wyposaża analityków w narzędzia do wyszukiwania zagrożeń i analizy ich źródłowych przyczyn**, dzięki czemu można odróżnić zazwyczaj niezauważalne objawy zagrożenia od przypadkowego szumu wynikającego z codziennej pracy przedsiębiorstwa.

NOWATORSKIE PODEJŚCIE BLACKBERRY DO EDR

Podejście BlackBerry do technologii EDR opiera się na trzech filarach:

- Architektura oparta na chmurze: BlackBerry Optics stosuje całą logikę wykrywania i reagowania na zagrożenia na końcówce i przechowuje uzyskane w ten sposób dane telemetryczne, alertowe i dowodowe w chmurze dla celów analizy offline.
- Inteligentne Edge AI: Sztuczna inteligencja (AI), uczenie maszynowe (ML) i kontekstowe reguły wykrywania zagrożeń identyfikują naruszenia bezpieczeństwa i uruchamiają automatyczne działania, które skracają średni czas do wykrycia (MTTD) i usunięcia skutków (MTTR).
- Pełny wgląd: BlackBerry Optics ułatwia wyszukiwanie zagrożeń i analizę przyczyn źródłowych dzięki zapewnieniu analitykom bezproblemowego dostępu do skorelowanych danych z urządzeń końcowych.

ARCHITEKTURA OPARTA NA CHMURZE

W przeciwieństwie do innych produktów EDR, BlackBerry Optics wdraża całą logikę wykrywania i reagowania na zagrożenia bezpośrednio na urządzeniu końcowym. Alerty, zdarzenia i dane telemetryczne chronionych urządzeń są automatycznie zbierane, porównywane i przechowywane w chmurze w celu analizy offline. Użytkownicy otrzymują 30-dniowy okres przechowywania danych, ale BlackBerry oferuje również 90-dniowe i 365-dniowe pakiety retencyjne dla klientów z branż podlegających ścisłym regulacjom prawnym, którzy potrzebują dodatkowych danych historycznych do wykazania zgodności z przepisami.

WYKRYWANIE ZAGROŻEŃ ZA POMOCĄ EDGE AI I ANALIZY KONTEKSTOWEJ

BlackBerry Optics Context Analysis Engine (CAE) monitoruje zdarzenia na punktach końcowych w mgnieniu oka w celu identyfikacji złośliwych i podejrzanych działań. CAE jest dostarczany z gotowym zestawem zaprojektowanych przez BlackBerry logik wykrywania, które mogą uruchamiać szereg doraźnych i zautomatyzowanych reakcji.

CAE zawiera reguły:

• oparte na raportach zarządczych i branżowych źródłach informacji dotyczących zagrożeń,

• pochodzące z rzeczywistych ataków analizowanych i rozwiązywanych na bieżąco przez zespoły reagowania firmy BlackBerry oraz przez analityków zagrożeń,

• zmapowane do MITRE ATT&CK® Framework,

• wykorzystujące unikalną telemetrię CPU z Intel® Threat Detection Technology do wykrywania i łagodzenia skutków cryptojackingu w systemach operacyjnych Windows®10.

BlackBerry Optics posiada również mechanizmy wykrywania zagrożeń oparte o Machine Learning opracowane przez BlackBerry, które stale analizują aktywność urządzeń końcowych w celu wykrycia ataków zero-day oraz ataków APT-Advanced persistent threat. Analitycy SOC mogą również tworzyć niestandardowe reguły, które uwzględniają politykę bezpieczeństwa specyficzną dla środowiska ich organizacji.

OCHRONA NOWEJ GENERACJI

BlackBerry Optics wykorzystuje AI, Machine Learning i analizę kontekstową dla:

• wykrywania zagrożeń,

• analizy przyczyn źródłowych,

• uruchamiania zautomatyzowanych działań ograniczających i naprawczych.

KORZYŚCI:

- Wykorzystuje wiele technik do wykrywania ataków we wczesnym stadium.
- Wdraża logikę wykrywania i reagowania bezpośrednio na urządzeniu końcowym w celu minimalizowania opóźnień reakcji. Eliminuje zależność od wyszukiwania w chmurze i połączenia z nią.
- W wersji standardowej zapewnia 30-dniowe przechowywanie danych z urządzeń końcowych w chmurze. Dostępne są dłuższe pakiety retencyjne.
- Zautomatyzowane schematy postępowania przyspieszają reakcję na incydenty, usuwanie skutków i odzyskiwanie danych.
- Zaawansowane wyszukiwania InstaQuery ułatwiają wykrywanie zagrożeń i analizę pierwotnych przyczyn.
- Szerokie wsparcie dla różnych platform, w tym Linux®.

REAGOWANIE NA ZAGROŻENIA ZA POMOCĄ PAKIETÓW ON-DEMAND I ZAUTOMATYZOWANYCH PLAYBOOKÓW

Reagowanie na żądanie za pomocą pakietów:

Analitycy mogą wykorzystywać zaawansowany silnik skryptowy w BlackBerry Optics do tworzenia i wdrażania pakietów. Są to zbiory skryptów, które zostają aktywowane na urządzeniu końcowym w celu uruchomienia aplikacji, zebrania danych dowodowych, wyłączenia systemów i wykonania innych funkcji dochodzeniowych i naprawczych. Pakiety mogą być wdrażane we własnym zakresie na pojedynczym urządzeniu, wielu urządzeniach, wybranych strefach bezpieczeństwa lub w całym przedsiębiorstwie.

Zautomatyzowane reagowanie za pomocą playbooków:

Pakiety mogą być również łączone i konfigurowane jako playbooki, które uruchamiają się automatycznie za każdym razem, gdy zostanie wyzwolona reguła wykrywania. Na przykład, analityk może stworzyć playbook, który automatycznie zbierze logi PowerShell, pliki historii przeglądarki i dane zrzutu pamięci za każdym razem, gdy urządzenie końcowe wykona polecenie PowerShell pobierające plik.

WYKRYWANIE WSKAŹNIKÓW ZAGROŻEŃ ZA POMOCĄ ZAAWANSOWANEGO WYSZUKIWANIA INSTAQUERY

BlackBerry Optics usprawnia poszukiwanie zagrożeń, umożliwiając zespołom bezpieczeństwa zbieranie i analizowanie danych za pomocą zaawansowanych wyszukiwań InstaQuery (IQ). Jest to lekkie narzędzie, które zbiera i agreguje istotne dane z urządzeń końcowych i prezentuje je w formacie, który jest zarówno kontekstowy, jak i intuicyjny do analizy.

Pozwala analitykom odpowiedzieć na takie pytania jak:

• Czy skrót lub rozszerzenie pliku było już kiedyś widziane na jednym z moich punktów końcowych?

• Czy ta komenda była kiedykolwiek wykonywana na którymś z moich systemów?

TYPOWE PRZYKŁADY UŻYCIA BLACKBERRY OPTICS

BlackBerry Optics jest odpowiednim rozwiązaniem dla organizacji, które chcą:

• zmniejszyć wskaźniki MTTD i MTTR poprzez powstrzymywanie zagrożeń za pomocą pakietów On-Demand i zautomatyzowanych playbooków,

• eliminować zagrożenia poprzez szybkie przywracanie narażonych systemów do ich prawidłowego stanu,

• przeszukiwać dane urządzeń końcowych takie jak pliki, programy wykonywalne, obiekty MITRE ATT&CK i inne wskaźniki kompromitacji systemów,

• chronić punkty końcowe bez narzucania ograniczeń wydajności,

• szybko identyfikować sygnały ataku ukryte w ogromnej ilości innych danych z urządzeń końcowych,

• zwiększyć odporność poprzez usprawnienie procesu wyszukiwania zagrożeń i analizy pierwotnych przyczyn.

SKONTAKTUJ SIĘ Z NAMI:

www.bakotech.pl

blackberry@bakotech.pl

+48 12 340 90 30

bako tech®

in @bakotechpl

f @bakotechpl

Bakotech Poland&CEE