Bitdefender
BUILT FOR RESILIENCE

GravityZone XDR

Extended Detection and Response

W ostatnim czasie częstotliwość i poziom zaawansowania cyberataków gwałtownie wzrosły. Bywało, że kliknięcie linku w e-mailu wystarczyło, aby strona internetowa firmy zniknęła z sieci. Zaawansowane trwałe zagrożenia (APT) mogą być niewykryte przez wiele miesięcy, wykradając dane firm, rozpowszechniając ransomware i usuwając pliki z krytycznych systemów. Dodatkowo upowszechnianie się modeli pracy zdalnej oraz hybrydowej przyczyniło się do powstania nowych wektorów cyberataku. Pomimo rozwoju technologii zapobiegania cyberprzestępczości eksperci z zakresu bezpieczeństwa przyznają, że nie da się w 100% zapobiec temu zjawisku, gdyż atakujący wciąż doskonalą taktyki, techniki i procedury. Toteż najlepszym narzędziem w rękach zespołów bezpieczeństwa są informacje – pozwalają one skrócić czas potrzebny na wykrycie zagrożenia, a docelowo zmniejszyć ryzyko szkód i poprawić cyberodporność.

Potrzeba gromadzenia i analizy rozproszonych danych na temat bezpieczeństwa była motorem ewolucji technologii EDR (endpoint detection and response) w kierunku XDR (extended detection and response). XDR ma na celu rozszerzenie możliwości EDR poprzez uwzględnienie dodatkowych źródeł danych, uzyskanie bardziej przejrzystego obrazu etapów ataku oraz określenie skuteczniejszych sposobów reagowania.

Rosnąca wielowektorowa złożoność cyberataków doprowadziła do opracowania technologii XDR. Skuteczny XDR musi posiadać następujące funkcje:

- gromadzenie danych ze źródeł, które mogą być miejscami podatnymi na cyberatak;
- zaawansowane mechanizmy uczenia maszynowego i sztucznej inteligencji w celu analizy danych na potrzeby dostarczania kontekstowych informacji;
- zapobieganie nadmiarowi alertów poprzez eliminację zbędnych sygnałów w procesie badania ataku;
- zapewnienie zespołom ds. bezpieczeństwa narzędzi do podejmowania natychmiastowych działań.

Jak XDR rozszerza wykrywanie i reagowanie poza punkt końcowy

GravityZone XDR łączy wielokrotnie nagradzane technologie Bitdefender w zakresie wykrywania i zapobiegania z zaawansowanymi sensorami obejmującymi systemy, aplikacje, chmurę, system zarządzania tożsamością i sieci. Dzięki GravityZone XDR zespoły bezpieczeństwa mają szerszy wgląd w cały cykl ataku – od miejsca jego rozpoczęcia poprzez rozprzestrzenianie się i dalsze etapy. GravityZone XDR zapewnia szczegółową analizę przyczyn i szerszą widoczność zagrożeń, która wykracza poza punkt końcowy. Dzięki funkcjonalności GravityZone XDR zespoły bezpieczeństwa mają natychmiastowy dostęp do skorelowanych źródeł informacji

W skrócie

GravityZone XDR zapewnia szybszą, bardziej precyzyjną analizę i detekcję ataków w całej infrastrukturze oraz aplikacjach organizacji. Pomaga zespołom bezpieczeństwa skupić się na kluczowych obszarach, które są celem cyberprzestępców, z uwzględnieniem systemów, aplikacji, chmury, zarządzania tożsamością i sieci. Zapewnia narzędzia analityczne i szeroki kontekst bezpieczeństwa, umożliwiając korelację alertów z różnych źródeł, szybką priorytetyzację incydentów oraz powstrzymywanie ataków poprzez automatyczne i kierowane reagowanie. Całość dostarczana jest w ramach jednej, intuicyjnej konsoli zarządzania, co jest istotne z punktu widzenia zapobiegania zmęczeniu alertami.

Kluczowe zalety

- Wykrywa cyberataki w systemach, aplikacjach, chmurze, systemie zarządzania tożsamością i sieciach.
- Zapewnia zespołom bezpieczeństwa wgląd w analizę przyczyn.
- Obrazuje cały łańcuch ataku w przystępnej formie, umożliwiającej identyfikację słabych stron łańcucha zabezpieczeń.
- Umożliwia szybką reakcję – usuwanie złośliwych wiadomości e-mail, izolowanie hostów, wyłączanie kont użytkowników itp.
- Udaremnia ataki zanim do nich dojdzie dzięki nagradzanym funkcjom

„GravityZone XDR doskonale radzi sobie z łączeniem i korelowaniem incydentów w czasie w zakresie wszystkich naszych operacji, co dało nam natychmiastowe korzyści. Nie sposób nie docenić zalet posiadania kompleksowego rozwiązania z wbudowanymi funkcjami wykrywania na potrzeby identyfikacji i badania znanych oraz nowych zagrożeń dostarczającego naszym analitykom wiedzy o tym, co i jak się zdarzyło, a także narzędzi reagowania."

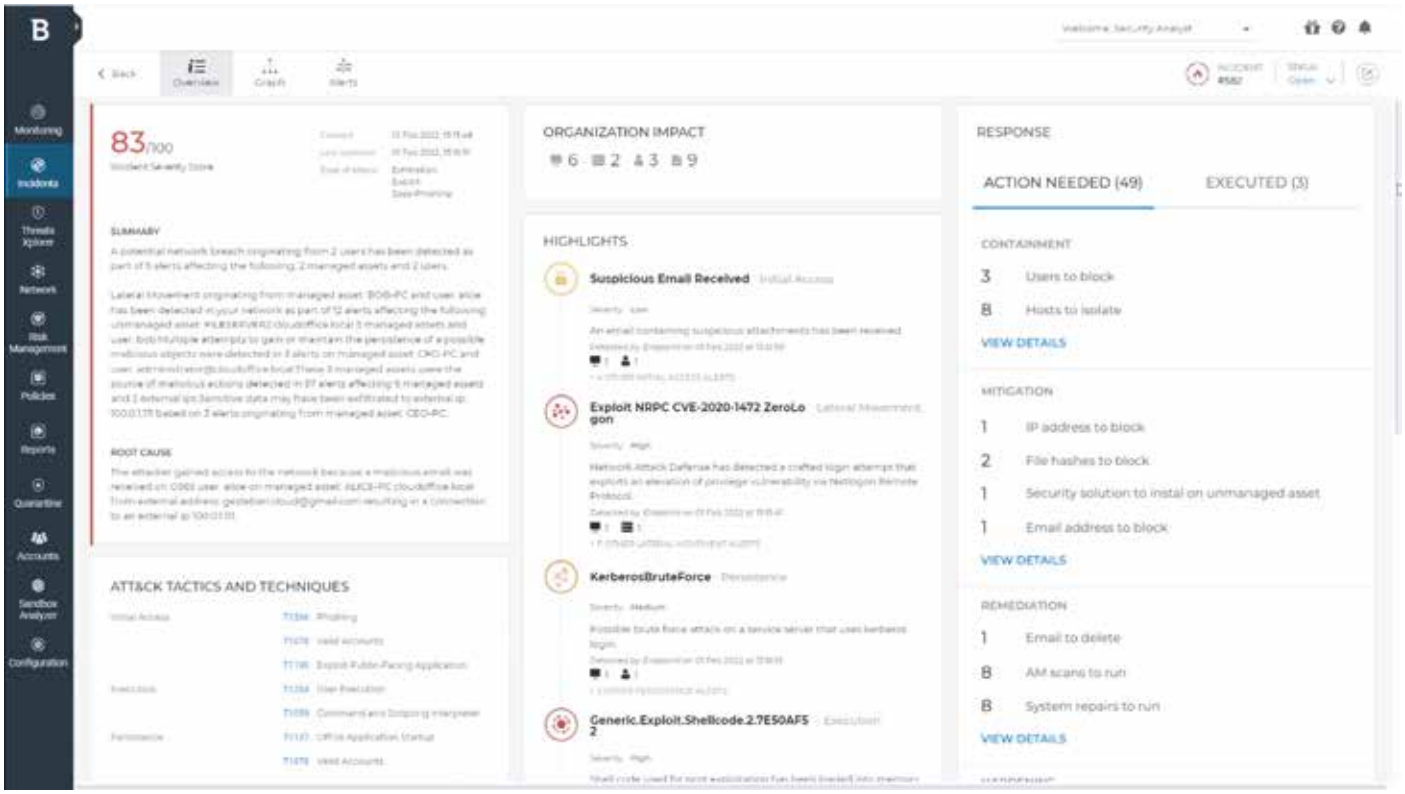
Mahmood Haq, chief information security officer (CISO), MyVest

o zdarzeniach, danych bazowych i szerokiego kontekstu, co pozwala na szybką identyfikację łańcucha działań związanych z cyberatakami w całym środowisku. Zaawansowane uczenie maszynowe i sztuczna inteligencja zapewniają zespołom bezpieczeństwa wgląd w schematy ataków, co umożliwia podejmowanie konkretnych działań. Technologia ta zmniejsza ryzyko wystąpienia fałszywych alarmów i ogranicza zjawisko zmęczenia alertami.

GravityZone XDR pobiera dane z kilku różnych systemów:

- punktów końcowych i serwerów w siedzibie firmy oraz w chmurze;
- aplikacji i poczty e-mail w usłudze Microsoft Office 365™;
- środowiska chmury;
- Microsoft® Active Directory® w zakresie zarządzania tożsamością;
- sieci.

Wszystkimi narzędziami bezpieczeństwa w powyższym zakresie można zarządzać z poziomu jednej, intuicyjnej konsoli GravityZone.



Rys. 1: GravityZone XDR zapewnia zespołom ds. bezpieczeństwa szczegółowe informacje na temat ataków. Umożliwia szybkie zrozumienie danych nt. zdarzeń i incydentów bezpieczeństwa, ich potencjalnego wpływu na organizację, możliwych przyczyn oraz zalecanych działań.

Jak XDR usprawnia wykrywanie i reagowanie

GravityZone XDR łączy zalety GravityZone Business Security Enterprise z jednym lub kilkoma sensorami XDR. GravityZone zapewnia wiodące technologie cyberbezpieczeństwa – ochronę punktów końcowych, wykrywanie i reagowanie na ich zdarzenia, analitykę ryzyka użytkowników oraz punktów końcowych, ochronę przed atakami sieciowymi, filtrowanie zawartości, dostosowalne uczenie maszynowe, analizę sandbox, elastyczne zarządzanie politykami, obszerne raportowanie, a także wiele innych – za pośrednictwem jednej, intuicyjnej konsoli zarządzania opartej na chmurze. Sensory XDR rozszerzają możliwości wykrywania Bitdefender poza punkt końcowy.

GravityZone XDR wspiera cztery dodatkowe typy sensorów. Sensory te przetwarzają dane z wielu źródeł i przekazują je do silników zaawansowanego uczenia maszynowego. GravityZone XDR analizuje przetworzone dane i kompiluje szczegółową oś czasu ataku, która jest widoczna w Doradcy Incydentów. Dzięki GravityZone EDR, zespoły ds. bezpieczeństwa mogą podejmować akcje takie jak izolowanie hostów, wysyłanie plików do Analizatora Sandbox GravityZone w celu dalszej analizy, zabijanie procesów, i otwieranie zdalnej sesji na stacjach roboczych. GravityZone XDR rozszerza te akcje dzięki dodatkowi każdego z opisanych poniżej sensorów.

Sensor aplikacji / Bitdefender XDR Productivity Sensor

Uważa się, że jednym z najważniejszych łupów cyberprzestępców są przechwycone konta Microsoft Office 365. W celu wyłudzenia danych logowania do Office 365 często wykorzystują oni ataki phishingowe. Wiedza o tego typu działaniach jest bezcenna dla zespołów bezpieczeństwa. GravityZone XDR wykrywa ataki, których celem lub źródłem są konta bądź poczta e-mail w usłudze Office 365.

Sensor aplikacji identyfikuje szczególne aspekty kont Office 365, które mogą wskazywać na aktywność cyberprzestępczą. Sensor wykrywa następujące działania:

- wyłączanie ochrony antyphishingowej w Office 365;
- podejrzane działanie dotyczące tworzenia użytkowników, np. wyłączenie nowo utworzonego użytkownika z wymogu uwierzytelniania wielopoziomowego;
- dodawanie dokumentów z podejrzanymi makrami do SharePoint i OneDrive;
- przesyłanie plików wykonywalnych do kont Office 365;
- podejrzane żądania dostępu, takie jak przyznanie użytkownikowi dostępu do wielu plików lub katalogów w różnych witrynach SharePoint w krótkim czasie.

Sensor wykrywa też anomalie w działaniach użytkowników, które odbiegają od normy. Potrafi on zidentyfikować, że użytkownik wykonał danego dnia nietypową liczbę działań administracyjnych lub operacji na dokumentach, np. odbiega to od typowych działań danego konta użytkownika.

Zakres wykrywania podejrzanych działań w Office 365 obejmuje też pocztę e-mail. Sensor aplikacji identyfikuje następującą potencjalnie niebezpieczną aktywność w ramach Microsoft Exchange Online™:

- Eksfiltracyjne wiadomości e-mail – ich celem jest pobranie przez odbiorcę plików ze skompromitowanego konta użytkownika.
- Wiadomości spear phishingowe – mają na celu wyłudzenie danych logowania do kont użytkowników.
- Podejrzane działania dotyczące uprawnień do skrzynek pocztowych; na przykład, gdy użytkownik uzyskuje w krótkim czasie dostęp do kilku różnych skrzynek pocztowych.
- Usuwanie przez użytkownika dużej liczby wiadomości e-mail ze skrzynki pocztowej, której użytkownik nie jest właścicielem.

GravityZone XDR nie tylko identyfikuje podejrzaną aktywność, lecz również pomaga zespołom bezpieczeństwa w podejmowaniu działań w celu ochrony firmy. Za sprawą sensora Office 365 zespoły bezpieczeństwa mogą usuwać wiadomości e-mail w organizacjach Office 365 i zawieszać konta Office 365 z poziomu pulpitu GravityZone.

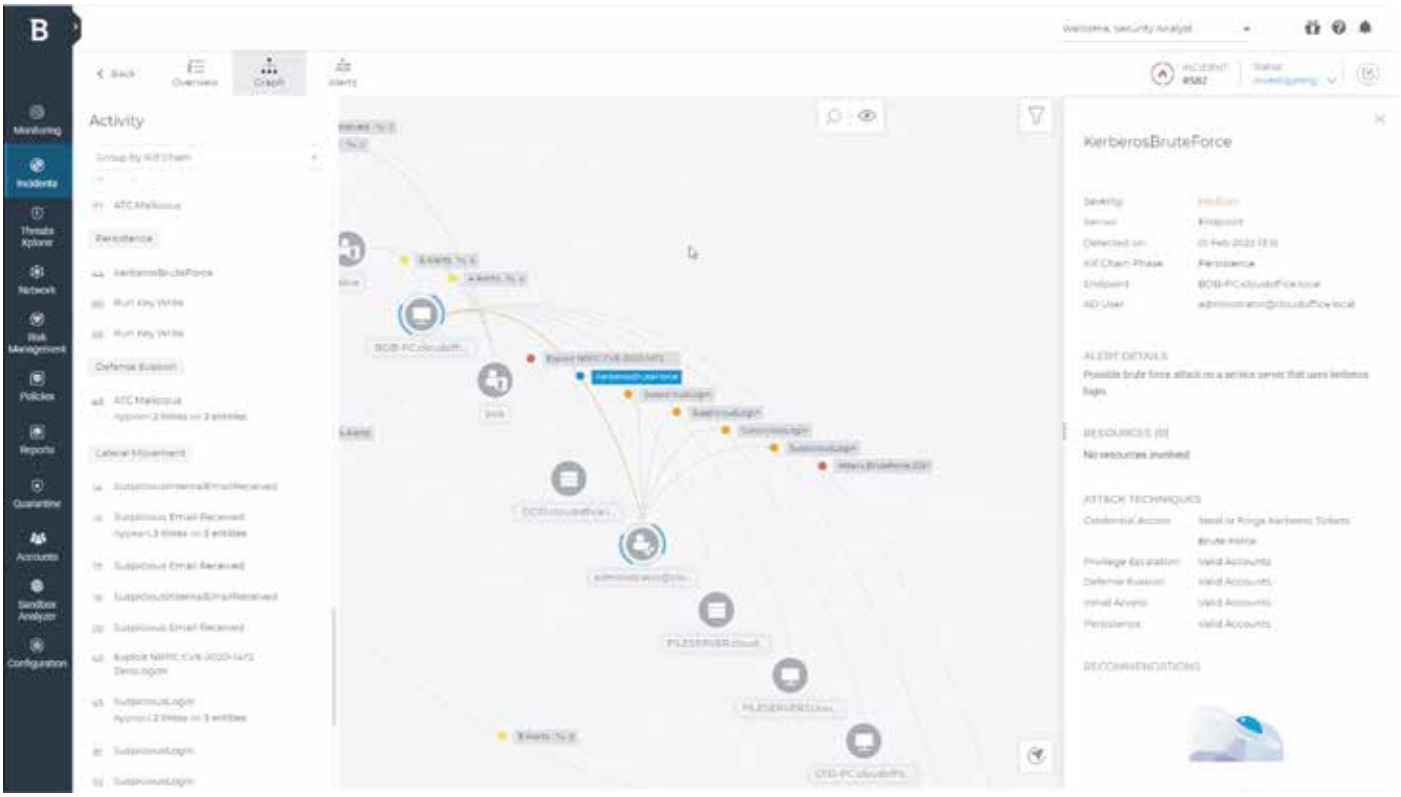
Sensor chmury / GravityZone XDR Cloud Sensor

Za pośrednictwem sensora chmury GravityZone XDR monitoruje aktywność, która może wskazywać na naruszenie bezpieczeństwa środowisk chmurowych, takich jak Amazon Web Services® (AWS). Monitorowanie uwzględnia szereg wskaźników ataku.

Sensor ten rozpoznaje anomalie, ustalając najpierw wzorzec typowego zachowania, a następnie identyfikując przypadki odbiegania wykrytych działań od wzorca. GravityZone wykrywa nietypowe działania użytkownika w przypadku przesłania pliku z podejrzanym rozszerzeniem, którego działanie odbiega od wzorca. Potrafi też wychwycić niestandardowe działanie funkcji w środowisku chmurowym oraz inne zagrożenia dla bezpieczeństwa chmury.

Ponadto sensor chmury identyfikuje podejrzane działania związane z wieloma granularnymi funkcjami usług w chmurze, takimi jak AWS Lambda®. Wykrywa on uruchomienie funkcji Lambda, która wywołuje podejrzane działanie. Potrafi na przykład wychwycić podejrzane automatyczne wykonanie kodu, takie jak użycie funkcji Lambda do utworzenia klucza dostępu dla użytkownika AWS Identity and Access Management (IAM) w celu uruchomienia backdoora. Innym przykładem jest użycie funkcji Lambda do aktualizacji grupy zabezpieczeń w celu zezwolenia na łączenie się przez dany port, które GravityZone XDR zidentyfikuje to jako manewr mogący umożliwić atakującemu dostęp do instancji chmury.

GravityZone XDR Cloud Sensor wykrywa również podejrzane działania innego typu, jak przypadki usunięcia przez nieznanego użytkownika lub hosta domyślnego szyfrowania tzw. wiadra (bucket) w usłudze AWS Simple Cloud Storage (S3). Atakujący ujawnia w ten sposób wszystkie zaszyfrowane obiekty (przy użyciu szyfrowania po stronie serwera) w danym wiadrze S3. XDR wykrywa, kiedy atakujący wyłącza lub usuwa usługi monitorowania, np. zatrzymuje usługę logowania Amazon, CloudTrail, bądź usuwa logi z usługi monitorowania AWS, CloudWatch. Identyfikuje również zdarzenia polegające na rozpoznaniu wiadra S3 przez atakującego. GravityZone XDR potrafi też wykryć jednoczesne logowanie użytkownika z wielu regionów, co jest typowym wskaźnikiem kompromitacji konta.



Rys. 2: Zespoły bezpieczeństwa mają wgląd w szczegółowe informacje na temat każdego aspektu ataku w widoku Rozszerzone incydenty. Nasze sensory monitorują i korelują aktywność w różnych źródłach danych, dostarczając szczegółowych informacji o każdym miejscu wystąpienia ataku w przystępnym formacie. Aktywność można sortować w zależności od preferencji według czasu lub łańcucha ataku.

Sensor tożsamości / Bitdefender XDR Identity Sensor

Bezpieczeństwo tożsamości jest kluczowym aspektem wzmacniania cyberodporności. Identyfikacja podejrzanych działań dotyczących uwierzytelniania w aplikacjach, narzędziach DevOps, bazach danych, systemach, środowiskach chmurowych i innych krytycznych zasobach pomaga zapobiegać lub ograniczać potencjalne szkody związane z cyberatakiem. Po połączeniu z usługą Active Directory sensor tożsamości wykrywa aktywność mającą związek z atakami polegającymi na próbie

posłużenia się skompromitowanymi kontami, tokenami i obiektami. Dotyczy to kont użytkowników, jak również kont systemowych oraz kont API.

Sensor tożsamości wykrywa ataki ukierunkowane na protokół uwierzytelniania sieciowego Kerberos. Potrafi między innymi wykryć przypadki użycia loginu Kerberos do przeprowadzania ataków typu brute-force na system. W trakcie ataku typu brute-force atakujący dąży do użycia szybko generowanych haseł lub kluczy szyfrujących, aby uzyskać dostęp do systemu. Sensor wykrywa też dodatkowe działania dotyczące protokołu Kerberos, w tym: wykorzystywanie skradzionych biletów Kerberos do przemieszczania się po sieci, żądanie biletów ze słabym szyfrowaniem – co jest częstą oznaką złośliwych zamiarów – oraz ataki typu replay attack. Te ostatnie polegają na kradzieży pakietów z sieci w celu przekazania ich do usługi lub aplikacji.

Sensor tożsamości rozpoznaje także podejrzane logowanie po wykryciu ataku typu brute-force. Identyfikuje on rejestrację fałszywego kontrolera domeny Active Directory przez atakującego i posługiwanie się nim w celu wstrzyknięcia złośliwych obiektów do innych kontrolerów domeny w ramach tej samej infrastruktury Active Directory. Rozpoznaje różnego rodzaju czynności wykonywane przez atakującego w obiekcie Active Directory i uwierzytelnianie w zdalnych systemach przy użyciu skradzionych danych uwierzytelniających.

Wszechstronny komponent GravityZone XDR, jakim jest sensor tożsamości, jest wspomagany działaniem funkcji, które umożliwiają zespołom bezpieczeństwa podejmowanie konkretnych działań. Mogą one przykładowo wyłączyć konto Active Directory lub wymusić reset hasła bezpośrednio z poziomu konsoli platformy GravityZone XDR.

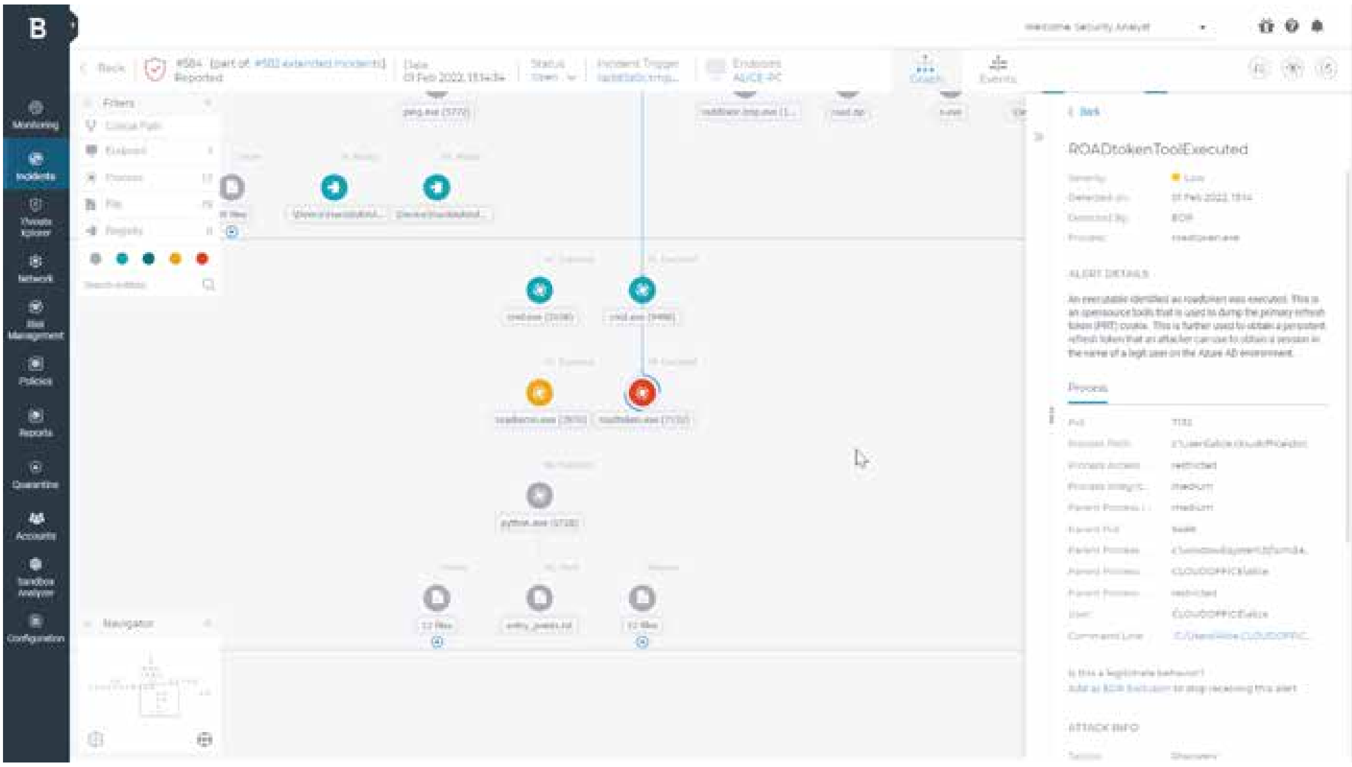
Sensor sieci / GravityZone XDR Network Sensor

GravityZone XDR Network Sensor ma postać wirtualnego urządzenia, które monitoruje ruch sieciowy pod kątem oznak ataku. Atakujący często dążą do rozszerzenia zakresu ataku, przemieszczając się w sieci firmowej z jednego systemu na drugi. Sensor pomaga zespołom bezpieczeństwa identyfikować próby poruszania się atakującego po sieci. Potrafi też określić, kiedy atakujący próbuje wyprowadzić dane poza organizację. Sensor sieciowy XDR wykrywa techniki skanowania portów oraz ataki sieciowe typu brute-force.

GravityZone XDR Network Sensor pomaga w udaremnianiu ataków sieciowych oraz zapewnia zespołom bezpieczeństwa wgląd w sytuację, co pozwala ograniczyć skutki cyberataków i skrócić czas potrzebny na ich usunięcie.

Światowej klasy zabezpieczenia wsparte wiedzą ekspercką

GravityZone XDR zapewnia firmom wszechstronną ochronę, która łączy nagradzaną technologię zapobiegania oraz zaawansowane funkcje wykrywania i reagowania na zagrożenia, dostarczając istotnych informacji w trakcie, jak i po cyberataku. Rozwiązanie GravityZone XDR wykrywa i przeciwdziała atakom na systemy, aplikacje, środowiska chmurowe, systemy zarządzania tożsamością i sieci, zatem cyberprzestępcy nie mają gdzie się ukryć. Firmom, które chciałyby poszerzyć swoje szeregi na potrzeby obsługi operacji bezpieczeństwa 24x7, Bitdefender oferuje usługi Managed Detection and Response (MDR) oparte na GravityZone XDR. Nasza kadra MDR to wysoce doświadczeni, certyfikowani specjaliści mający na swoim koncie łącznie ponad 100 lat doświadczenia z zakresu cyberbezpieczeństwa w firmach sektora prywatnego i rządowych instytucjach wywiadowczych. MDR jest najlepszym połączeniem funkcjonalności i wiedzy eksperckiej w zakresie bezpieczeństwa. Zapewnia najwyższą ochronę przed współczesnymi wielowektorowymi cyberzagrożeniami.



Rys. 2: GravityZone XDR zapewnia szczegółowe wizualizacje, ułatwiając zespołom bezpieczeństwa prześledzenie ścieżki krytycznej każdego ataku. Wgląd w kompleksową analizę każdego pliku użytego podczas ataku umożliwia szybkie reagowanie, np. umieszczenie pliku na czarnej liście, przesłanie go do GravityZone sandbox w celu dalszej analizy, odizolowanie hosta i inne.

Bitdefender®
BUILT FOR RESILIENCE

Centrala

Siedziba przedsiębiorstwa – Santa Clara, Kalifornia, USA
Centrala technologiczna – Bukareszt, Rumunia

Przedstawiciel marki Bitdefender w Polsce

Marken Systemy Antywirusowe
Tel: 58 667 49 49
E-mail: kontakt@marken.com.pl
www.bitdefender.pl

Bitdefender jest światowym liderem w dziedzinie cyberbezpieczeństwa, dostarczając najwyższej klasy rozwiązania do zapobiegania, wykrywania i reagowania na zagrożenia. Wybrany przez miliony konsumentów, firm i instytucji państwowych, Bitdefender jest jednym z najbardziej zaufanych ekspertów w branży w zakresie eliminacji zagrożeń, ochrony prywatności i danych oraz wzmacniania cyberodporności. Dzięki dużym nakładom na badania i rozwój, Bitdefender Labs co minutę odkrywa 400 nowych zagrożeń i sprawdza 40 miliardów zapytań o zagrożenia dziennie. Będąc pionierem przełomowych innowacji w dziedzinie zabezpieczeń, bezpieczeństwa IoT, analityki behawioralnej i sztucznej inteligencji, dostarcza licencji technologicznych ponad 150 najbardziej rozpoznawalnym firmom technologicznym na świecie. Założony w 2001 roku Bitdefender ma klientów w ponad 170 krajach i biura na całym świecie.

Więcej informacji na stronie https://www.bitdefender.com