

GravityZone Risk Management

Opis zagadnienia

Zagrożenia związane z bezpieczeństwem mogą potencjalnie narazić każdą firmę na destrukcyjne cyberataki. Wśród nich można wymienić: błędnie skonfigurowane ustawienia reguł w systemie operacyjnym, niezaszyfrowane hasła, słabe ustawienia zabezpieczeń przeglądarki, luki w oprogramowaniu i wiele innych. Co więcej na bezpieczeństwo organizacji mogą wpływać także błędy w zabezpieczeniach spowodowane ludzkim zachowaniem! Tego rodzaju zdarzenia są w stanie doprowadzić do wycieku poufnych danych narażając sieć na włamania i kradzieże danych, a nawet zniszczenie zasobów organizacji.

Zespoły zajmujące się cyberbezpieczeństwem potrzebują pełnego wglądu w takie incydenty w odpowiednim czasie, aby zapobiec naruszeniu bezpieczeństwa i udaremnić cyberatak. Do największych wyzwań i problemów specjalistów ds. cyberbezpieczeństwa należy to, że:

- Zarządzanie dużą liczbą użytkowników, w tym pracowników pracujących zdalnie, wymaga ogromnych zasobów.
- Utrzymywanie wglądu w programy i aplikacje podatne na ataki bez właściwych narzędzi jest trudne.
- Stałe nadzorowanie aktualizacji dla systemu i programów jest uciążliwe.
- Ciągła priorytetyzacja wysiłków to czasochłonne zadanie, które niesie z sobą spore ryzyko.

Wyzwania te są zdecydowanie trudniejsze dla dostawców usług zarządzanych (Managed Service Providers – MSP) oraz dostawców usług zarządzanych w zakresie bezpieczeństwa (Managed Security Service Providers – MSSP), do których obowiązków należy nadzorowanie środowisk w różnych firmach.

Przegląd funkcji wykrywania zagrożeń

GravityZone Risk Management umożliwia zespołom zajmującym się cyberbezpieczeństwem identyfikację ryzyka oraz skanowanie systemów i sieci w poszukiwaniu zagrożeń związanych z nieprawidłowymi konfiguracjami w systemie Windows, programami podatnymi na ataki oraz zachowaniami użytkowników, które mogą stanowić lukę w ochronie. Identyfikacja potencjalnego ryzyka to funkcja skrojona na miarę danej organizacji. Dzięki możliwości ustawienia opcji rutynowego skanowania, administratorzy mogą codziennie otrzymywać informacje o zagrożeniach w zakresie bezpieczeństwa, do których uzyskują następnie wgląd za pomocą wszechstronnego pulpitu do zarządzania ryzykiem.

W skrócie

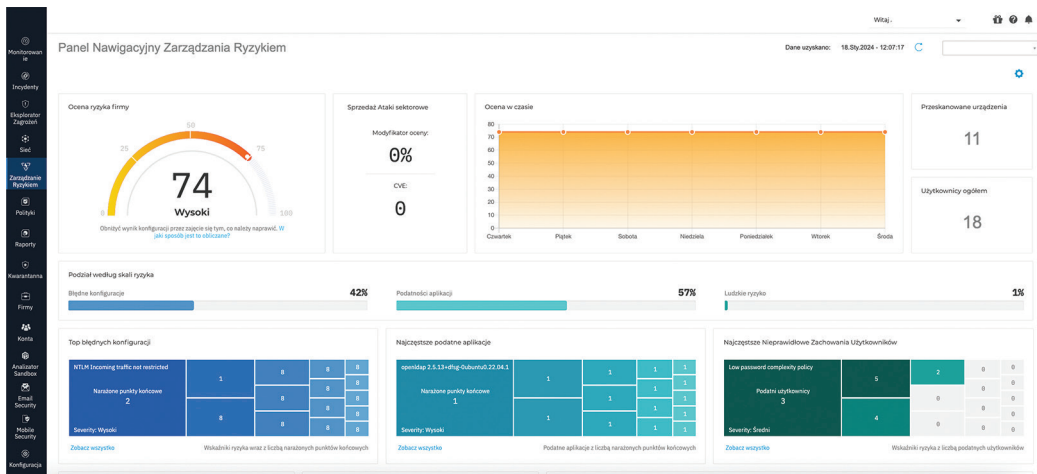
Zaawansowana ocena ryzyka związanego z punktami końcowymi i użytkownikami, dostępna w rozwiązaniu GravityZone dla systemów operacyjnych Windows i Linux, pomaga zminimalizować ryzyko związane z cyberbezpieczeństwem, poprzez analizę, raportowanie i działania zaradcze.

Kluczowe zalety

- **Pełny wgląd w dane dotyczące ryzyka dla bezpieczeństwa** – skanowanie zagrożeń związanych z nieprawidłowymi konfiguracjami systemów operacyjnych, podatnością aplikacji na ataki i zachowaniami użytkowników, które mogą narazić firmę na straty.
- **Wszechstronny pulpit nawigacyjny** – umożliwia zespołom zajmującym się cyberbezpieczeństwem szybką identyfikację i przegląd potencjalnie niebezpiecznych zachowań użytkowników i urządzeń, jednocześnie eliminując frustrację i zamieszanie związane z zarządzaniem ryzykiem w zakresie bezpieczeństwa.
- **Harmonogram skanowania pod kątem ryzyka** – pozwala zespołom zajmującym się cyberbezpieczeństwem na bieżąco śledzić pojawiające się zagrożenia. Podczas identyfikacji niebezpiecznych zdarzeń, członkowie takich zespołów mogą nie tylko trzymać rękę na pulsie, ale również szybko podejmować działania zaradcze.
- **Usuwanie zagrożeń bezpośrednio z konsoli GravityZone** – wiele nieprawidłowych konfiguracji systemu operacyjnego można łatwo poprawić bezpośrednio z pulpitu zarządzania ryzykiem. Dodatkowy moduł GravityZone Patch Management pozwala z kolei zespołom zajmującym się cyberbezpieczeństwem łączyć luki w zabezpieczeniach aplikacji podatnych na ataki za pomocą jednego kliknięcia w zakresie wszystkich systemów, których dana sytuacja dotyczy.

„Teraz mamy wgląd we wszystkie dane, dotyczące stanu bezpieczeństwa, za pomocą jednej konsoli. Nasz zespół uważa, że narzędzie GravityZone jest znacznie dużo prostsze w obsłudze, niż rozwiązania z zakresu bezpieczeństwa od innych dostawców.”

*Josh Gilliland, Security Team Lead,
GEHA*



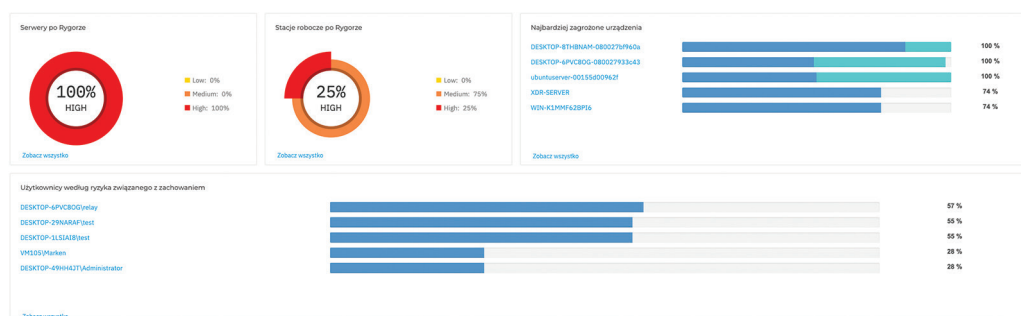
Rys. 1.1: Pulpit GravityZone Risk Management oferuje pełen wgląd w zagrożenia dla bezpieczeństwa, umożliwiając administratorom łatwiejsze śledzenie ryzykownych zdarzeń o wysokim priorytecie za pomocą kompleksowego systemu punktacji i kategoryzacji.

Pulpit Risk Management oferuje informacje na temat oceny ryzyka, podane w zrozumiały sposób. Pozwala to administratorom szybciej wyłowić systemy i użytkowników, narażonych na niebezpieczeństwo. Wynik zmienia się w zależności od liczby incydentów zidentyfikowanych podczas skanowania, ich wagi oraz tego, czy podjęte zostały skuteczne środki zaradcze. Na podstawie oceny ryzyka zagrożenia są przydzielane do określonych kategorii, które omówimy w kolejnym rozdziale. Kategorie te to „Server and Workstation Security Risks” (zagrożenia bezpieczeństwa związane z serwerami i stanowiskami pracy), „Top Devices at Risk” (urządzenia, najbardziej podatne na ryzyko), „Top Users at Risk” (użytkownicy, najbardziej podatni na ryzyko). Pozwala to zespołom zajmującym się cyberbezpieczeństwem błyskawicznie określić, które firmy, systemy i użytkownicy wymagają uwagi w pierwszej kolejności. Ta funkcja pomaga uniknąć wielu nieporozumień i trudności związanych z koniecznością zarządzania ryzykiem zarówno w jednej firmie, jak i w wielu organizacjach.

Dzięki analizie szczegółów zagrożeń, dostępnej z poziomu pulpitu nawigacyjnego, wyraźnie widać, na czym polega ryzyko, oraz jakie działania naprawcze należy podjąć, aby wyeliminować dane zagrożenie. Zespoły zajmujące się cyberbezpieczeństwem mogą także zainstalować aktualizacje bezpośrednio z pulpitu Risk Management przy pomocy narzędzia **Bitdefender GravityZone Patch Management**.

Przegląd informacji na temat funkcji reagowania na incydenty

Analizując systemy pod kątem różnych wskaźników ryzyka, **GravityZone Risk Management** pomaga zidentyfikować potencjalne słabe punkty w zakresie bezpieczeństwa, wynikające z nieprawidłowej konfiguracji systemów operacyjnych, aplikacji podatnych na ataki i niebezpiecznych zachowań użytkowników oraz ograniczyć ich wpływ na organizację. Zadanie Skanowanie Ryzyka można uruchomić samodzielnie na dowolnym systemie za pomocą konsoli GravityZone lub skonfigurować cykliczne skanowanie poprzez politykę. Kiedy skanowanie w poszukiwaniu zagrożeń dobiegnie końca, użytkownik otrzyma ogólną ocenę ryzyka, opracowaną na podstawie zidentyfikowanych zagrożeń oraz wybranych zmiennych Health Industry Modifier. Dzięki temu zespoły zajmujące się cyberbezpieczeństwem będą w stanie błyskawicznie określić, które systemy i którzy użytkownicy są najbardziej narażeni na niebezpieczeństwo.



Rys. 2.1: Konsola Risk Management sprawia, że priorytetyzacja urządzeń i użytkowników, podlegających największemu ryzyku, jest naprawdę prosta. Wiele niebezpieczeństw można zażegnać bezpośrednio z poziomu pulpitu Bitdefender Risk Management, co przekłada się na szybsze i bardziej efektywne ograniczanie zagrożeń.

Zarządzanie ryzykiem w przypadku wielu użytkowników

Dostawcy usług zarządzających, również w zakresie cyberbezpieczeństwa, zarządzający środowiskami w wielu firmach, mogą skorzystać z widoku „Companies” (Firmy), aby szybko określić, które z obsługiwanych organizacji narażone są na największe ryzyko i natychmiast zacząć rozwiązywanie problemów o najwyższym priorytecie.

Zagrożenia Bezpieczeństwa						
Błędne konfiguracje Podatności aplikacji Zachowanie Użytkowników Urządzenia Użytkownicy						
Napraw zagrożenia		Zignoruj zagrożenia				
Błędne konfiguracje	Nasilenie	Zainfekowane Urządzenia	Typ	Typ Ograniczenia	Status	
☐ Usługa telefoniczna	Niski (10%)	8	Bezpieczeństwo systemu operacyjnego	Ręczne	Aktywne	
☐ Usługa mikrofonu	Niski (10%)	1	Bezpieczeństwo systemu operacyjnego	Ręczne	Aktywne	
☐ Przechowywanie danych w nietypowych miejscach	Niski (10%)	8	Bezpieczeństwo systemu operacyjnego	Automatyczne	Aktywne	
☐ Niebezpieczne logowanie gościa	Średni (40%)	8	Ścieżka i Policie	Ręczne	Aktywne	
☐ Klient podpisuje oprogramowanie	Średni (40%)	8	Ścieżka i Policie	Automatyczne	Aktywne	
☐ Serwer podpisuje oprogramowanie	Średni (40%)	6	Ścieżka i Policie	Automatyczne	Aktywne	
☐ Wyłączenie autodoładzania	Średni (40%)	8	Bezpieczeństwo systemu operacyjnego	Automatyczne	Aktywne	
☐ Zapisać dane w pamięci podręcznej	Średni (30%)	6	Bezpieczeństwo systemu operacyjnego	Ręczne	Aktywne	
☐ Microsoft Consumer Experiences	Niski (5%)	6	Bezpieczeństwo systemu operacyjnego	Ręczne	Aktywne	
☐ Połączenia sieciowe inne niż domowe	Średni (40%)	6	Ścieżka i Policie	Automatyczne	Aktywne	
☐ Delegacja poleceń	Średni (30%)	8	Ścieżka i Policie	Ręczne	Aktywne	
☐ Instalacja urządzeń według ID	Średni (30%)	6	Bezpieczeństwo systemu operacyjnego	Ręczne	Aktywne	
☐ Instalacja urządzeń według klasy instalacji	Średni (30%)	6	Bezpieczeństwo systemu operacyjnego	Ręczne	Aktywne	
☐ Stwierdzenie naruszenia	Średni (30%)	8	Bezpieczeństwo systemu operacyjnego	Ręczne	Aktywne	

Rys. 3.1: Zespoły zajmujące się cyberbezpieczeństwem mogą błyskawicznie zażegnać niebezpieczeństwa, wynikające z nieprawidłowej konfiguracji, za pomocą jednego przycisku, dostępnego na pulpicie GravityZone Risk Management Dashboard. Zestawienie wyników oceny ryzyka zapewnia przegląd najważniejszych zidentyfikowanych zagrożeń w trzech oddzielnych kategoriach:

Nieodpowiednie konfiguracje

Identyfikuje niebezpieczeństwo związane z systemem operacyjnym Windows, w tym problemy z regułami lokalnymi i grupowymi, usługi podatne na ataki, ustawienia komputera i inne.

Podatności Aplikacji

Zapewnia wgląd w aplikacje zainstalowane na zarządzanych punktach końcowych, które zostały zidentyfikowane jako narażone na niebezpieczeństwo związane z systemem Common Vulnerabilities and Exposures (CVE).

Zachowanie Użytkowników

Śledzi aktywność użytkowników, która stanowi potencjalne ryzyko dla bezpieczeństwa firmy. Moduł do śledzenia użytkowników można wyłączyć w razie potrzeby, jeśli dany zespół zajmujący się cyberbezpieczeństwem nie chce z niego korzystać.

Rozwiązanie **GravityZone Risk Management** wyszukuje aplikacje zainstalowane na zarządzanych punktach końcowych, które są podatne na ataki, a ich bezpieczeństwo łatwo naruszyć metodą exploit. Funkcja pozwala zespołom zajmującym się cyberbezpieczeństwem namierzać w pierwszej kolejności te programy, które stanowią największe zagrożenie. Używając dodatku GravityZone Patch Management, odpowiedzialne osoby mogą jednym kliknięciem, szybko i łatwo zaktualizować niechronione aplikacje.

Można także zignorować zagrożenie, wyświetlić listę urządzeń, na których zainstalowana jest niebezpieczna aplikacja oraz dokładnie przejrzeć treść CVE, aby lepiej zrozumieć ryzyko.

Identyfikacja niebezpiecznych zachowań użytkowników

Przegląd ryzykownych zachowań użytkowników pozwala zespołom zajmującym się cyberbezpieczeństwem namierzyć osoby, zachowujące się w sposób, stanowiący potencjalne zagrożenie. Pulpit dostarcza szczegółowych informacji na temat przyczyn uznania danego zachowania za niebezpieczne, na których podstawie zespoły zajmujące się cyberbezpieczeństwem mogą albo bez zwłoki podjąć stosowne działania zaradcze albo zignorować zagrożenie. Zespoły zajmujące się cyberbezpieczeństwem, które zdecydują się włączyć tę funkcję, uzyskają unikalny wgląd w kilka wskaźników ryzyka, takich jak: użytkownicy posiadający mało skomplikowane hasła lub używający tego samego hasła w wielu witrynach, połączenia firm z sektora małych i średnich przedsiębiorstw z uwierzytelnianiem zwykłym tekstem, identyfikacja użytkowników, którzy korzystali z zainfekowanych zewnętrznych urządzeń pamięci masowej i nie tylko.

Security Risks

Misconfigurations
App Vulnerabilities
User Behavior Risks
Devices
Users

	Users	Severity	No. of Risks	Title
☐	Search..... Choose.....			
☒	RR [redacted]	● Medium (54%)	4	N/A
☐	LM [redacted] Michael	● Medium (57%)	4	N/A
☐	NN [redacted] Neil	● Medium (57%)	5	N/A
☐	DZ DANNY [redacted]	● Medium (57%)	4	N/A
☐	LG [redacted] Iqbal	● Medium (57%)	4	N/A
☐	NN [redacted] Nicol	● Medium (57%)	5	N/A

9 Items
FIRST PAGE < | 1 of 1 > LAST PAGE
Show 20 ▾

Severity: ● Medium (54%)

User Name: [redacted]

Device Name: TEST-LARI

Status: Active

[Ignore User](#)

MITIGATIONS/USER ACTIONS

RISKS (4):

- Low password complexity policy

DETAILS

Verifies if there is any password complexity policy in-place on the endpoint.

Severity: ● Medium (50%)

Status: Active

● Idle User
+

● Low password complexity policy
+

● Idle User
+

Rys. 4.1: Dzięki pulpitowi Risk Management zespoły zajmujące się cyberbezpieczeństwem mogą szybko namierzyć użytkowników, których zachowania stanowią potencjalne zagrożenie dla bezpieczeństwa systemów.

GravityZone Risk Management daje zespołom zajmującym się bezpieczeństwem efektywne, wszechstronne narzędzie do identyfikacji słabych punktów w zakresie bezpieczeństwa firmy i podejmowania odpowiednich działań zaradczych. Narzędzie to pozwala na szybkie rozpoznanie zagrożeń o wysokim priorytecie, które muszą zostać zneutralizowane w pierwszej kolejności. Taka zapobiegawcza aktywność oznacza oszczędność czasu, zasobów i zwiększa prawdopodobieństwo zapobieżenia potencjalnie zgubnemu w skutkach atakowi.

Centrala

Siedziba przedsiębiorstwa – Santa Clara, California, 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.pl>.

Wszelkie prawa zastrzeżone. © 2022 Bitdefender.

Wszystkie znaki handlowe, nazwy handlowe i produkty wymienione w niniejszym dokumencie są własnością ich właścicieli.