KOMPAS IT

DELL Technologies

Dell MDR (Managed Detection and Response) – efektywne monitorowanie środowiska IT

W ubiegłym roku ponad połowa firm (54%) padła ofiarą cyberataku lub incydentu, który uniemożliwił dostęp do danych, wynika z badania Dell Technologies Global Data Protection Index 2023, przeprowadzonego wśród 1 000 decydentów IT (ITDM) i 500 decydentów w obszarze bezpieczeństwa IT.

Jak wynika z badania, aż 67 proc. liderów IT obawia się, że środki ochrony danych, z których korzystają, mogą być niewystarczające w obliczu zagrożeń takich jak złośliwe oprogramowanie oraz ransomware. Innym wyzwaniem, z którym mierzą się organizacje, jest rosnąca luka kompetencyjna w obszarze cyberbezpieczeństwa. Aby chronić się przed współczesnymi zagrożeniami, instytucje potrzebują spójnej strategii bezpieczeństwa oraz kompleksowych, intuicyjnych rozwiązań, które będą realnym wsparciem dla zespołów zajmujących się cyberbezpieczeństwem oraz IT.

Model klasycznej platformy bezpieczeństwa opierał się na podziale sieci na „strefy" – tzw. Zony - Trusted/Untrusted/DMZ. Model ten możemy porównać do budowy muru. Jednak, jak każda twierdza, istnieje ryzyko, że znajdzie się sposób by ją zdobyć. Współczesne platformy bezpieczeństwa IT projektowane są w modelu Zero Trust Security, zgodnie z którym każdy użytkownik, każde urządzenie, sieć, adres IP, traktowane są jako niezaufane i potencjalne zagrożenie, dopóki nie udowodni, że jest inaczej.

Wiele dużych firm decyduje się na utworzenie wewnętrznego centrum operacji bezpieczeństwa (SOC – Security Operations Center), które zajmuje się obsługą wszystkich zadań związanych z cyberbezpieczeństwem. Zadaniem pracowników SOC jest monitorowanie, wykrywanie i reagowanie na wszelkie alerty i incydenty jak najszybciej, będąc na posterunku 24/7. Własny zespół specjalistów do spraw cyberbezpieczeństwa dostępnych przez całą dobę, jest niewątpliwie skutecznym rozwiązaniem, jednak niezwykle kosztownym.

Alternatywą dla wewnętrznego SOC-u jest rekomendowana usługa Dell MDR (Managed Detection and Response), czyli platforma funkcjonująca w ramach tzw. SOC as a Service łącząca monitorowanie zagrożeń w czasie rzeczywistym, narzędzia analizy danych oraz doświadczenie profesjonalistów zajmujących się cyberbezpieczeństwem.

ROLA I ZNACZENIE

Wzrost cyberprzestępczości oraz kosztów ataków na infrastrukturę IT wymaga od organizacji podjęcia rzetelnych kroków zapobiegawczych w celu ochrony środowiska IT. Pełna ochrona infrastruktury wymaga szybkiego wykrywania i skutecznej reakcji na nowe zagrożenia w całym środowisku. Jest to trudne ze względu na punktowe produkty i narzędzia, które to umożliwiają widoczność tylko fragmentów infrastruktury IT, również wyzwania związane ze znalezieniem i utrzymaniem wykwalifikowanych specjalistów ds. bezpieczeństwa i zespołów IT, które są już w pełni zajęte krytycznymi wymaganiami oraz codziennymi operacjami.

Dell MDR odpowiada na kilka kluczowych wyzwań, z którymi mierzą się współczesne organizacje w obszarze cyberbezpieczeństwa:
- **Rosnąca złożoność zagrożeń**
- **Niedobór wykwalifikowanych specjalistów**
- **Fragmentacja narzędzi bezpieczeństwa**
- **Szybkość reakcji na incydenty**
- **Złożoność zarządzania zgodnością z regulacjami**
- **Obciążenie zespołów IT**
- **Proaktywne podejście do bezpieczeństwa**
- **Koszty i przewidywalność budżetu.**

MOŻLIWOŚCI I ZASTOSOWANIE

Usługa Dell MDR skierowana jest do organizacji, które zdają sobie sprawę z potrzeby zwiększenia bezpieczeństwa informatycznego poprzez stworzenie dedykowanej komórki SOC zarówno dla klientów nie posiadających własnego SOC-a, jak i dla organizacji dojrzałych, posiadających już narzędzia i personel SOC, świadomych jednak swoich braków lub po prostu organizacji którym zależy na skuteczniejszej detekcji incydentów i skróceniu czasu reakcji na powstałe zagrożenia.

Usługa Dell MDR jest aktywna całą dobę, przez 365 dni w roku pomagając organizacjom, które:
- mają trudności ze znalezieniem i utrzymaniem wykwalifikowanych specjalistów ds. bezpieczeństwa;
- nie chcą dokonywać dużych inwestycji w operacje zapewniające pełne bezpieczeństwo;
- chcą zoptymalizować i odciążyć część swoich operacji związanych z bezpieczeństwem, aby umożliwić swoim zespołom ds. bezpieczeństwa wewnętrznego skupienie się na bardziej strategicznych inicjatywach w zakresie bezpieczeństwa;
- posiadają (lub zamierzają posiadać) 50–10 000 punktów końcowych.

ARCHITEKTURA – STRUKTURA I DZIAŁANIE

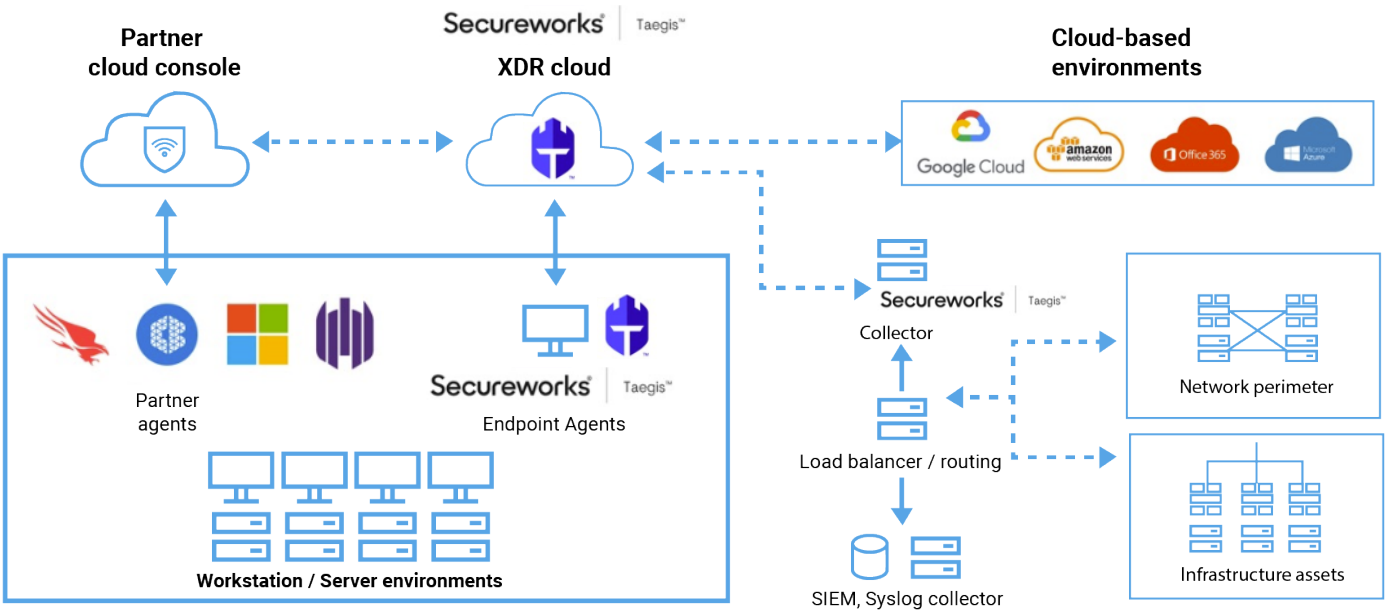
Usługa Dell MDR działa w oparciu o narzędzie Secureworks Taegis XDR. Jak sama nazwa wskazuje jest to narzędzie klasy XDR (Extended Detection and Response), czyli narzędzie będące rozwinięciem systemu EDR (Endpoint Detection and Response). Systemy XDR (w tym zakresie również EDR) monitorują i analizują działania na punktach końcowych pod kątem podejrzanego zachowania, rejestrując każdą podejrzaną aktywność np. uruchomienie procesu, czy użycie biblioteki. Często są nazywane antywirusami nowej generacji, ponieważ idą o krok dalej względem tradycyjnych systemów antywirusowych - nie skupiają się na identyfikacji złośliwego oprogramowania, lecz na detekcji nieprawidłowych działań.

Podczas gdy EDR zbierał i korelował dane wyłącznie z punktów końcowych, XDR rozszerza ten zakres poza punkty końcowe, zapewniając wykrywanie i analizę informacji także w sieciach, serwerach, chmurze, SIEM i wielu innych.

XDR przeprowadza w czasie rzeczywistym analizę zdarzeń, wykrywa zagrożenia i incydenty bezpieczeństwa, koreluje zdarzenia z różnych systemów z incydentami, a także posiada możliwości automatyzacji reakcji na incydenty (tzw. playbook).

Secureworks Taegis XDR to narzędzie chmurowe (działa w modelu SaaS). W głównej mierze działa w oparciu o agenta zainstalowanego na stacjach końcowych i serwerach, które w czasie rzeczywistym monitorują hosty i wysyłają telemetrię wprost do chmury Taegis (dla klientów z UE, chmura XDR ulokowana jest na terenie Europejskiego Obszaru Gospodarczego – EOG).

Dell MDR (Managed Detection and Response) – efektywne monitorowanie środowiska IT



W celu integracji z lokalnymi (on-premise) systemami, np. UTM, routery, przełączniki, w lokalnym środowisku klienta należy zainstalować kolektor logów, a następnie podłączyć do niego integrowane rozwiązania. Kolektor zbiera zdarzenia z lokalnego środowiska i przesyła je do chmury Taegis, gdzie poddawane są analizie bezpieczeństwa.

Integracja z rozwiązaniami chmurowymi (m.in.: Google Cloud, Azure, AWS, Office 365) odbywa się za pośrednictwem API, wprost z konsoli Taegis XDR.

Warto podkreślić, że w ramach usługi Dell MDR, klient otrzymuje administracyjny dostęp do swojej instancji Secureworks Taegis XDR, tożsamy z dostępem analityków cyberbezpieczeństwa firmy Dell.

KLUCZOWE FUNKCJE I KORZYŚCI

Dell MDR (Managed Detection and Response) z technologią Secureworks Taegis XDR to w pełni zarządzana, kompleksowa usługa działająca 24 godziny na dobę, 7 dni w tygodniu, która monitoruje, wykrywa, bada i reaguje na zagrożenia w całym środowisku IT, pomagając organizacjom z 50 lub więcej punktami końcowymi, aby szybko i znacząco poprawić ich bezpieczeństwo przy jednoczesnym zmniejszeniu obciążenia działu IT.

Usługa wykorzystuje dwie kluczowe możliwości:

1. doświadczenie analityków bezpieczeństwa firmy Dell Technologies zdobyte przez lata poprzez pomaganiu organizacjom na całym świecie w lepszej ochronie ich działalności;
2. moc narzędzia do analizy bezpieczeństwa Secureworks Taegis XDR z ponad 20-letnim doświadczeniu w wykrywaniu i reagowania na zagrożenia w świecie rzeczywistym.

Usługa Dell Managed Detection and Response z wykorzystaniem technologii Secureworks Taegis XDR zapewnia następujące elementy:

1. **Wdrażanie:**
   - spotkanie w sprawie inicjacji usługi
   - przygotowanie wstępnej listy kontrolnej
   - przegląd środowiska IT Klienta
   - włączenie aplikacji Secureworks XDR
   - pomoc we wdrożeniu agenta

2. **Wykrywanie:**
   - dostęp do analityków zabezpieczeń
   - wykrywanie zagrożeń i prowadzenie dochodzeń
   - wyszukiwanie zagrożeń

3. **Reagowanie i usuwanie skutków:**
   - działania w odpowiedzi na zagrożenie
   - zdalne rozwiązywanie problemów

4. **Przegląd kwartalny:**
   - 40 godzin (kwartalnie)
   - przegląd dochodzeń i trendów alarmowych
   - omówienie analiz
   - wytyczne dotyczące zabezpieczeń

5 **Reagowanie na incydenty:**
- 40 godzin (rocznie)
- inicjowanie zdalnej reakcji na incydenty

6 **Rozliczenie w formie subskrypcji:**
- elastyczne rozliczenie miesięczne
usługa jest dostępna już od 50 stacji roboczych

Dell MDR pozwala eliminować określone we wstępie wyzwania cyberbezpieczeństwa:

Rosnąca złożoność zagrożeń
Dell MDR wykorzystuje zaawansowane narzędzia, takie jak platformy XDR (Extended Detection and Response) i sztuczną inteligencję, aby skutecznie wykrywać i reagować na te zagrożenia.

Niedobór wykwalifikowanych specjalistów
Dell MDR dostarcza ekspertów, którzy monitorują, analizują i reagują na zagrożenia 24/7, co pozwala firmom skorzystać z zaawansowanej wiedzy bez konieczności zatrudniania dodatkowych pracowników.

Fragmentacja narzędzi bezpieczeństwa
Dell MDR integruje różne źródła danych i platformy XDR, zapewniając jednolitą i spójną ochronę całego środowiska IT.

Szybkość reakcji na incydenty
Czas reakcji na incydent cybernetyczny jest kluczowy, a tradycyjne podejścia mogą być zbyt wolne. Dell MDR oferuje natychmiastowe wsparcie i zautomatyzowane narzędzia, które pozwalają na szybkie podjęcie działań i minimalizację skutków ataku.

Złożoność zarządzania zgodnością z regulacjami
Utrzymanie zgodności z regulacjami i standardami bezpieczeństwa staje się coraz bardziej skomplikowane. Dell MDR pomaga organizacjom nie tylko chronić dane, ale także spełniać wymogi regulacyjne, dostosowując swoje rozwiązania do obowiązujących norm i przepisów.

Obciążenie zespołów IT
Zespoły IT są często przeciążone codziennymi operacjami i nie mają czasu na skuteczne zarządzanie zagrożeniami. Dell MDR przejmuje znaczną część odpowiedzialności za monitorowanie i reagowanie na zagrożenia, co pozwala zespołom IT skoncentrować się na innych, strategicznych zadaniach.

Proaktywne podejście do bezpieczeństwa
W tradycyjnych modelach bezpieczeństwa firmy często reagują dopiero po wystąpieniu incydentu. Dell MDR zmienia to podejście, oferując proaktywne polowanie na zagrożenia, co pozwala wykrywać i neutralizować zagrożenia, zanim spowodują one szkody.

Predykcja zagrożeń – testy penetracyjne (znane również jako pentesty)
to symulowane ataki hakerskie na systemy informatyczne.
Mają one na celu rzeczywistą ocenę stanu bezpieczeństwa danych zasobów informatycznych. W przypadku Dell Managed Detection and Response (MDR) testy penetracyjne są istotnym elementem w procesie zabezpieczania infrastruktury IT.

Koszty i przewidywalność budżetu
Zarządzanie kosztami bezpieczeństwa IT może być trudne, zwłaszcza w obliczu nieprzewidywalnych zagrożeń. Dell MDR jest oferowany za stałą, przewidywalną cenę, co upraszcza planowanie budżetu i zarządzanie kosztami ochrony.

CERTYFIKACJE

Rozwiązanie Dell MDR jest zgodne z normą SOC 2 typu 2.

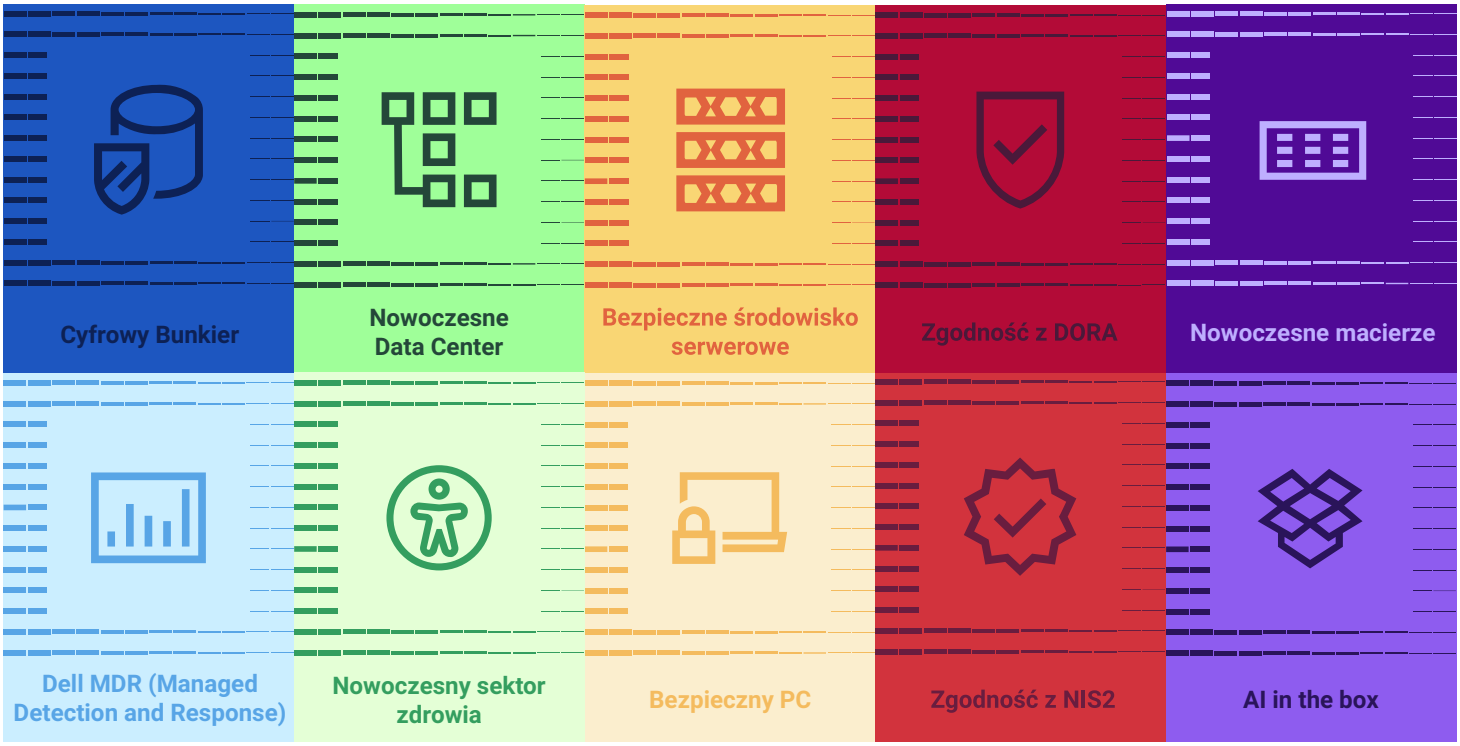
ZOBACZ TAKŻE

> Zgodność z NIS2 – cyberbezpieczeństwo w zgodzie z dyrektywą europejską

> Zgodność z DORA – efektywne strategie bezpieczeństwa cyfrowego

> Cyfrowy Bunkier – nowy standard cyfrowej odporności organizacji

Kompas IT – innowacyjne rozwiązania dla efektywności i cyfrowej odporności IT



Poznaj rozwiązania Dell Technologies

Porozmawiajmy o efektywnym monitorowaniu środowiska IT i Dell MDR

Przemysław Wachowicz
Senior Systems Engineer,
ISG Technology Consulting
Przemyslaw.Wachowicz@dell.com

Radosław Piedziuk
Storage Platforms & Solutions,
Sales Leader
Radoslaw.Piedziuk@dell.com

DELL Technologies