

Stały monitoring cyberbezpieczeństwa

Firma Bitdefender przedstawia Executive Summary, funkcję zaprojektowaną specjalnie w celu identyfikacji problemów związanych z bezpieczeństwem sieci. Jako część pulpitu nawigacyjnego Control Center, Executive Summary prezentuje zwięzły przegląd bezpieczeństwa wszystkich chronionych punktów końcowych w Twojej sieci.

Walka o bezpieczeństwo sieci w organizacji polega na ciągłym wyścigu między hakerami a ludźmi stojącymi po dobrej stronie mocy. Chodzi o to, by stale monitorować sieć i jak najszybciej przeciwdziałać zagrożeniom. Pomagają w tym wyspecjalizowane firmy.

Właściwa analiza bezpieczeństwa sieci wymaga dostępności i korelacji danych. Posiadanie scentralizowanych informacji o bezpieczeństwie pozwala monitorować cały system i zapewniać zgodność z politykami bezpieczeństwa organizacji, szybko identyfikować problemy, zagrożenia i luki. Dzięki temu kierownictwo otrzymuje dane łatwe do interpretacji.

Firma Bitdefender przedstawia Executive Summary, funkcję zaprojektowaną specjalnie w tym celu. Jako część pulpitu nawigacyjnego Control Center, Executive Summary prezentuje zwięzły przegląd bezpieczeństwa wszystkich chronionych punktów końcowych w Twojej sieci. Złożony głównie z widżetów, zawiera szczegółowe informacje na temat punktów końcowych, typów i technik zagrożeń, wykryć i podjętych działań, oceny ryzyka w firmie i wielu innych.

Ograniczanie szkodliwego oprogramowania

Jak wiadomo, szczepionki zapewniają odporność. Ale co się dzieje, gdy są aplikowane za późno? Oparty na proaktywnych i wielokrotnie nagradzanych technologiach wykrywania Ransomware Mitigation pozwala na wczesną odpowiedź na ataki ransomware. Wykrywa je na bieżąco, blokuje niezależnie od tego, czy zostały uruchomione lokalnie, czy ze zdalnego punktu końcowego, a następnie odzyskuje zaszyfrowane pliki.

Po zastosowaniu ochrony na punktach końcowych, będziesz otrzymywać powiadomienia o każdym ataku. Możesz wyświetlać szczegółowe informacje o atakach ransomware i odzyskiwać zaszyfrowane pliki na stronie Aktywność ransomware. Takie zdarzenia zobaczysz w raporcie Audytu bezpieczeństwa.

Uwaga: Executive Summary jest dostępne z modułami GravityZone Business Security, GravityZone Advanced Business Security, GravityZone Elite, GravityZone Ultra, Cloud Security for MSP.

EDR dla każdego

Rozwiązanie Endpoint Detection and Response (EDR) dla systemów opartych na Windows, zasilane przez najwyższej klasy technologie uczenia maszynowego i skanowania w chmurze, charakteryzuje się niskim zużyciem zasobów, łatwym wdrażaniem oraz konserwacją i może działać wraz z dowolną platformą ochrony punktów końcowych innych firm.

To rozwiązanie obejmuje technologie zawarte w najnowocześniejszych funkcjach GravityZone, takich jak:

- Wykrywanie punktów końcowych i reagowanie na nie (EDR),
- Bezplikowa ochrona przed atakami,
- Ochrona przed atakami sieciowymi,
- Zaawansowana kontrola zagrożeń (ATC),
- Analizator piaskownicy,
- Analiza ryzyka punktów końcowych (ERA).

Uwaga: dostępne jako samodzielne rozwiązanie Bitdefender EDR.