HyperDetect
Dane Techniczne

Przegląd

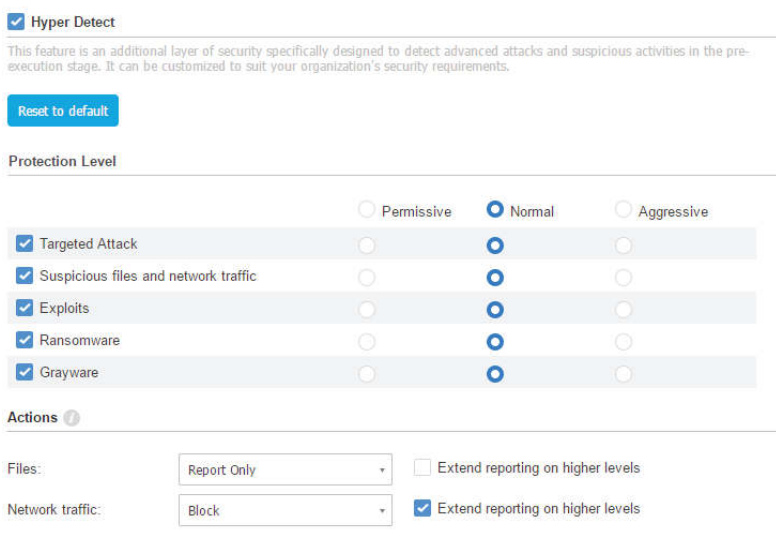
W obecnym krajobrazie cyberbezpieczeństwa, przedsiębiorstwa są stale narażone na działanie złośliwego oprogramowania, zakłócenia, naruszenia bezpieczeństwa danych oraz szereg innych incydentów wpływających na poprawne funkcjonowanie firmy. Platforma Bitdefender GravityZone Endpoint Security chroni punkty końcowe przed pełnym zakresem wyrafinowanych ataków cybernetycznych, zapewniając wysoką efektywność, niski wpływ na użytkowników końcowych i niskie koszty administracyjne. Składa się z wielowarstwowej ochrony, która stanowi dla hakerów nie lada wyzwanie. Każda z warstw ma na celu zablokowanie określonych typów zagrożeń, narzędzi lub technik ataków.

Bitdefender HyperDetect jest częścią platformy GravityZone Endpoint Security. Zawiera modele uczenia maszynowego i technologię wykrywania ataków stealth. Jest to dodatkowa warstwa zabezpieczeń zaprojektowana specjalnie w celu wykrywania zaawansowanych ataków i podejrzanych działań na etapie poprzedzającym wykonanie. Zagrożenia te mogą celować w branżę, organizację czy, w niektórych przypadkach, w jednostkę.

Etap Wykrywania	Typ Technologii	Zasięg Zagrożenia
Przed Wykonywanie	Uczenie maszynowe	Zero-day, Zawansowane złośliwe oprogramowanie, Zaciemnione złośliwe oprogramowanie, Ataki fileless (Niewłaściwe użycie programu PowerShell, WMI etc.), Kradzież danych uwierzytelniających, Ataki ukierunkowane, Niestandardowe złośliwe oprogramowanie, Ataki oparte na skryptach, Exploity, Narzędzia hakerskie, Podejrzany ruch w sieci, Potencjalnie niechciane aplikacje, Ransomware

Znaczenie HyperDetect

Cyberprzestępcy wykorzystują istniejące już zagrożenia i wprowadzają drobne modyfikacje kodu, próbując ominąć istniejące mechanizmy obronne oparte na sygnaturach. Wiele z dzisiejszych narzędzi bezpieczeństwa jest już w stanie wykryć niektóre z tych polimorficznych zagrożeń. Jednak napastnicy, którzy są bardziej zdeterminowani, cierpliwi i wykwalifikowani, inwestują swój czas i pieniądze, aby cały czas tworzyć zupełnie nowe, nieznane dotąd zagrożenia. Organizacje są nieustannie narażone na ryzyko spowodowane przez nieuchwytne zagrożenia, ponieważ mogą one ominąć sygnatury, heurystyki i podstawowe technologie uczenia maszynowego. HyperDetect został zaprojektowany do wczesnego wykrywania i zatrzymywania nieuchwytnych zagrożeń, zanim zaatakują one punkt końcowy (wykrywanie przed wykonaniem). Osiąga to poprzez kombinację przestrajalnych modeli uczenia maszynowego i technologii wykrywania ataków stealth. Można go dostosować do wymagań bezpieczeństwa organizacji.



Funkcje

- Zaawansowane technologie uczenia maszynowego (lokalne i w chmurze) oraz technologia wykrywania ataków typu stealth, która obejmuje:
- Wykrywanie potencjalnego niewłaściwego wykorzystania programu PowerShell, takiego jak: kod shell fileless /Pobieranie i Wykonywanie (pobieranie i uruchamianie pliku z lokalnej lub zdalnej lokalizacji), kradzież poświadczeń (invoke-mimikatz, out- Minidump), polecenia powersploit (wywołanie kodu shell, skanowanie portu, dll injection, get keystrokes, add-persistence), techniki stealth (zakodowana linia poleceń, np. Kodowana Base64, wykonanie obejścia polityk, tryb nieinteraktywny), uruchamianie przez przeglądarki/nietypowe pliki wykonywalne (np. IIS), próby unikania.
- Wykrywanie znanych Packerów
- Wykrywanie plików nie utworzonych przez znany kompilator (Visual Studio, Delphy itp.)
- Wykrywanie plików nie załadowanych znanym packerem
- Możliwość wyszukiwania kilku ciągów w pliku, które mogą wskazywać na oprogramowanie ransomware
- Wykrywanie niechcianych narzędzi, które mogą być użyte w atakach APT, takich jak schron, narzędzia do odrzucania haseł z narzędzi pamięciowych do mapowania sieci i narzędzi do ataków brute-force
- Wykrywanie adresów URL wygenerowanych dla konkretnych exploitów
- Wykrywanie podejrzanego drzewa wykonania, np. PowerShell, który wykonuje podejrzany plik
- Wykrywanie podejrzanych wierszy poleceń
- Wykrywanie potencjalnie niepożądanych aplikacji
- Dopasowana ochrona
- Możliwość konfiguracji klasyfikatorów wykrywania: ukierunkowane ataki, podejrzane pliki i ruch sieciowy, ransomware, exploity, grayware, konfiguracja czułości modeli uczenia maszynowego: "Tolerancyjny", "Normalny" i "Agresywny"
- Konfiguracja HyperDetect w trybie "Tylko raport" lub "Wdrażanie"
- Możliwość wykrycia i zgłoszenia na określonym poziomie i zablokowania (wdrożenia) na innym poziomie, np. Zablokuj na poziomie "Normalnym", ale kontynuuj raportowanie na poziomie "Agresywnym"
- Łatwe zarządzanie wyjątkami - Możliwość wykluczania procesów i aplikacji bezpośrednio ze zdarzeń

Korzyści

- Wykrywa zaawansowane ataki wcześniej i zapobiega naruszeniom, zmniejsza koszty i wysiłki związane z reagowaniem na incydenty.
- Chroni przed atakami fileless
- HyperDetect znacznie zwiększa wykrywalność nieuchwytnych zagrożeń na etapie przed-wykonaniem, w tym zagrożeń zero-day, zaawansowanych, trwałych zagrożeń, zaciemnionego złośliwego oprogramowania, ataków fileless (niewłaściwego użycia PowerShell, WMI itp.), kradzieży danych uwierzytelniających, ukierunkowanych ataków, niestandardowego złośliwego oprogramowania, ataków opartych na skryptach, exploitów, narzędzi hakerskich, podejrzanego ruchu w sieci, potencjalnie niechcianych aplikacji, oprogramowania ransomware
- Dzięki dostępności lokalnych modeli uczenia maszynowego, wykrywanie nie wymaga łączności z chmurą
- HyperDetect posiada unikalną zdolność do wykrywania i raportowania na określonym poziomie i blokowania (wymuszania) na innym poziomie, a także zdolność konfigurowania agresywności każdego klasyfikatora wykrywania, co pozwala administratorom dostosować ochronę w oparciu o profil zagrożeń organizacji, tolerancję ryzyka i potrzeby bezpieczeństwa
- Zapewnia wgląd w podejrzane aktywności już na wczesnym etapie
- Jest częścią jednego, zintegrowanego agenta bezpieczeństwa punktów końcowych i platformy centralnego zarządzania, co znacznie zmniejsza obciążenia administracyjne

Bitdefender

Bitdefender jest światowym dostawcą zabezpieczeń, który zapewnia najnowocześniejsze kompleksowe rozwiązania bezpieczeństwa ponad 500 milionom użytkowników w ponad 150 krajach. Bitdefender od 2001 roku tworzy nagradzane technologie zabezpieczeń dla firm i konsumentów oraz dostarcza rozwiązania z zakresu bezpieczeństwa infrastruktury hybrydowej i ochrony punktów końcowych. Dzięki R&D, współpracy i partnerstwu, Bitdefender ma wiodącą pozycję na rynku, zapewniając niezawodne zabezpieczenia, na których można polegać. Więcej informacji znajduje się na stronie: http://www.bitdefender.com.

Więcej informacji znajdziesz pod adresem: www.bitdefender.com/business