Malwarebytes

OPIS ROZWIĄZANIA

Malwarebytes Incident Response

Najbardziej kompleksowe i niezawodne usuwanie skutków ataku

NAJWAŻNIEJSZE ZALETY

- Zautomatyzowane, dokładne i skuteczne usuwanie skutków ataków
- Łączenie odseparowanych silosów operacyjnych
- Redukcja czasu obecności złośliwego oprogramowania
- Wypełnianie luk w umiejętnościach i dostępnych zasobach ludzkich
- Redukcja kosztów i złożoności procesu reagowania na zdarzenia

NAGRODY

Forbes — Najbardziej obiecująca firma w Stanach Zjednoczonych

CRN — Produkt roku

V3 — Innowacja roku w dziedzinie zabezpieczeń

Liczba i różnorodność zdarzeń, jakim muszą stawiać czoła zespoły ds. reagowania na incydenty cybernetyczne (CIRT), nieustannie rośnie — podobnie jak koszt i złożoność procesu usuwania ich skutków.

Jak wynika z badań, usunięcie skutków ponad 60% ataków wymaga więcej niż 9 godzin[1]. Przechodzenie z mechanizmów reaktywnych na automatyczne reagowanie na zdarzenia jest dziś ważniejsze niż kiedykolwiek — zwłaszcza w obliczu ograniczonych zasobów i ogromnej skali zaawansowanych zagrożeń.

Malwarebytes Incident Response to niezawodne rozwiązanie do dokładnego i kompleksowego usuwania skutków ataków, zapewniające optymalną wydajność i skuteczność technik reagowania na zdarzenia. Nasze zautomatyzowane podejście wzmacnia stosowany model zabezpieczeń i łączy ze sobą odseparowane silosy operacyjne.

Najważniejsze funkcje i cechy

Automatyczne usuwanie skutków ataków

Funkcje automatycznego usuwania skutków ataków pozwalają zespołowi CIRT wyeliminować ręczne, doraźne czynności, podejmowane dotychczas w celu czyszczenia i przywracania urządzeń po infekcji złośliwego oprogramowania. Dzięki temu cenny czas i zasoby można przeznaczyć na inne działania. Wykonywanie zautomatyzowanych zadań jest przy tym szybsze i dokładniejsze oraz skraca czas obecności złośliwego oprogramowania w systemach.

Dokładne usuwanie skutków ataków

Większość rozwiązań jest w stanie usuwać wyłącznie aktywne komponenty złośliwego oprogramowania, co nie wystarcza do jego całkowitej eliminacji. Mechanizm Malwarebytes Linking Engine wykorzystuje zastrzeżone podejście, pozwalające jednocześnie wykrywać i usuwać powiązane i dynamiczne pozostałości zagrożeń. Nasz mechanizm wykorzystuje metodę sekwencjonowania powiązanych elementów, aby trwale usuwać mechanizmy utrzymywania złośliwych programów. Dzięki naszej zaawansowanej metodologii organizacje otrzymują możliwość łatwego i dokładnego usuwania złośliwych programów.

Najlepsza w branży telemetria

Dzięki rozległej specjalistycznej wiedzy jesteśmy w stanie zrozumieć metody działania ataków, które z powodzeniem infekują firmowe urządzenia. Dysponujemy systemami analizy big data oraz analizy badań eksperckich, dzięki którym każdego dnia przetwarzamy dane ponad 3 milionów usuniętych ataków. W ten sposób uzyskujemy cenną wiedzę na temat złośliwego oprogramowania typu zero-day, co pozwala nam lepiej reagować na powstające zagrożenia i przewidywać ich dalszy rozwój.

Aktywne wyszukiwanie

Zagrożenia są aktualnie obecne w wielu środowiskach. Po pomyślnym zainfekowaniu punktu końcowego atakujący często wykonują dodatkowe kroki, aby zainfekować inne punkty końcowe. Dzięki Malwarebytes firmy mogą uruchamiać zaplanowane zadania skanowania, które w proaktywny sposób wyszukują niedawno zidentyfikowane wskaźniki naruszeń (IOC). Nasze rozwiązanie pozwala na łatwe stosowanie procesu zakładającego wystąpienie naruszenia, co w znacznym stopniu poprawia jakość ochrony.

Elastyczne wdrażanie i gotowość do integracji

Malwarebytes udostępnia elastyczne opcje wdrażania, dostosowane do potrzeb użytkowników: przy użyciu trwałego agenta punktu końcowego zarządzanego z poziomu chmury lub agenta nietrwałego (Breach Remediation). Zastosowanie agenta nietrwałego ułatwia przy tym jego integrację z istniejącym systemem SIEM oraz systemem zarządzania punktami końcowymi. Nasze rozwiązanie pozwala ponadto podejmować działania w czasie rzeczywistym, w oparciu o wskaźniki naruszeń (IOC) identyfikowane w sieci przez system SIEM. Oprogramowanie Malwarebytes może na przykład zareagować na zdarzenie w oparciu o alert z rozwiązania Splunk lub ForeScout.

Zasoby internetowe

Więcej informacji na temat Malwarebytes Incident Response można znaleźć na stronie: malwarebytes.com/business/incidentresponse/

Najnowsze wiadomości: blog.malwarebytes.com/

Uzyskaj wersję próbną: malwarebytes.com/business/licensing

Odniesienia

[1] *Understanding the Depth of the Global Ransomware Problem*, Osterman Research

Santa Clara, CA | malwarebytes.com | corporate-sales@malwarebytes.com | 1.800.520.2796

Malwarebytes jest nowoczesną firmą zajmującą się cyberbezpieczeństwem, której zaufały miliony użytkowników na całym świecie. Malwarebytes aktywnie chroni firmy i użytkowników indywidualnych przed zagrożeniami takimi jak złośliwe oprogramowanie, programy ransomware i programy wykorzystujące luki w zabezpieczeniach, których nie są w stanie wykryć tradycyjne rozwiązania antywirusowe. Flagowy produkt firmy łączy zaawansowane heurystyczne wykrywanie zagrożeń z bezsygnaturowymi technologiami wykrywania cyberataków i przeciwdziałania im jeszcze przed wystąpieniem strat. Ponad 10 000 firm na całym świecie korzysta, ufa i poleca Malwarebytes. Firma została założona w 2008 roku. Jej siedziba główna znajduje się w Kalifornii, a jej filie znajdują się w Europie i Azji. Firma dysponuje także globalnym zespołem badaczy i ekspertów w dziedzinie zabezpieczeń.