FortiEDR to usługa zapewniająca zautomatyzowaną ochronę punktów końcowych w czasie rzeczywistym oraz zautomatyzowane reagowanie na incydenty na wszystkich urządzeniach komunikujących się w sieci. Chroni stacje robocze, serwery, komunikację z chmurą – zarówno z obecnymi jak i starszymi systemami operacyjnymi – a także systemy produkcyjne i OT. Jako pojedyncza zintegrowana platforma oferuje działanie w oparciu o natywną infrastrukturę chmury i zostanie wdrożona jako rozwiązanie hybrydowe.

FortiEDR to rozwiązanie zabezpieczające punkty końcowe zbudowane w celu wykrywania zaawansowanych zagrożeń i powstrzymywania naruszeń oraz szkód wyrządzanych przez oprogramowanie ransomware w czasie rzeczywistym, co pozwala na automatyczne reagowanie i usuwanie skutków incydentów w celu ochrony danych, zapewnienia działania systemu i zachowaniu ciągłości biznesowej. Pojedyncza, zintegrowana konsola zarządzania zapewnia funkcje zapobiegania, wykrywania i reagowania na incydenty w języku angielskim. Ochrona w trybie offline odbywa się na punkcie końcowym, chroniąc także odłączone punkty końcowe. Bezpieczna zdalna powłoka zapewnia administratorom możliwość zdalnego rozwiązywania problemów, dzięki czemu pracownicy mogą pracować z dowolnego miejsca, a pakiet narzędzi zabezpieczających, w tym certyfikaty czasowe, ogranicza ryzyko wykorzystania danych.

Wykonywane funkcjonalności usługi

Odkrywaj i przewiduj - Discover and Predict FortiEDR zapewnia najbardziej zaawansowaną i zautomatyzowaną kontrolę polityki miejsc ataku z oceną podatności i wykrywaniem, co pozwala zespołom ds. bezpieczeństwa na: odkrywanie i przewidywanie urządzeń nieuczciwych (np. niezabezpieczonych. niechronionych i niezarządzanych urządzeń) oraz urządzeń IoT; śledzenie aplikacji i ratingów; wykrywanie i usuwanie luk w systemie i aplikacjach za pomocą wirtualnego łatania; zmniejszenie możliwych miejsc ataku dzięki proaktywnym politykom opartym na analizie ryzyka.

Zapobieganie atakom - FortiEDR wykorzystuje mechanizm antywirusowy oparty na uczeniu maszynowym do zatrzymywania ataków jeszcze przed ich wykonaniem. Te możliwości NGAV dla różnych systemów operacyjnych są konfigurowalne i wbudowane w pojedynczego, lekkiego agenta, dzięki czemu użytkownicy mogą przypisać ochronę przed złośliwym oprogramowaniem do dowolnej grupy punktów końcowych bez konieczności dodatkowej instalacji. Zapobieganie atakom oparte jest na uczeniu maszynowym, NGAV oparte na jądrze, ochronie odłączonych punktów końcowych dzięki ochronie w trybie offline; wykorzystaniu kontroli aplikacji do łatwego dodawania dozwolonych lub zablokowanych aplikacji do wstępnie zdefiniowanych list; wykorzystaniu informacji o zagrożeniach w czasie rzeczywistym z ciągle aktualizowanej bazy danych w chmurze.

Wykrywanie i likwidowanie ataków - FortiEDR wykrywa i odpiera złośliwe oprogramowanie bez plików i inne zaawansowane ataki w czasie rzeczywistym, aby chronić dane i zapobiegać naruszeniom. Gdy FortiEDR wykryje podejrzane procesy i zachowania, natychmiast przeciwdziała potencjalnym zagrożeniom, blokując komunikację wychodzącą i dostęp do systemu plików z tych procesów kiedy tego zażądają. Kroki te zapobiegają eksfiltracji danych, komunikacji w trybie C2 (command and control), manipulowaniu plikami i szyfrowaniu oprogramowania ransomware. W tym samym czasie Fortinet Cloud Services (FCS), kontynuuje gromadzenie dodatkowych dowodów, uzupełniania dane o zdarzeniach i klasyfikowania incydentów w celu aktywowania potencjalnej polityki automatycznej reakcji na incydent. FortiEDR zatrzymuje naruszenia danych i szkody spowodowane przez oprogramowanie ransomware w czasie rzeczywistym, automatycznie zapewniając ciągłość działania nawet urządzeniu, które już zostało skompromitowane.

Funkcjonalności powiązane z wykrywaniem i likwidacją ataków:

- Detekcja ataków ukierunkowanych na system operacyjny, która pozwala bardzo dokładnie wykrywać ukryte ataki infiltracyjne, w tym bezplikowe ataki na pamięć operacyjną i ataki z wykorzystaniem natywnych komponentów systemu (LotL).
- Zatrzymywanie w czasie rzeczywistym prób naruszeń bezpieczeństwa i minimalizowanie czasu wykrycia zagrożeń
- Analiza pełnej historii dziennika zdarzeń
- Zapobieganie szyfrowaniu ransomware oraz modyfikacjom plików i wpisów w rejestrze
- Ciągłe sprawdzanie poprawności klasyfikacji zagrożeń
- Redukcja szumu informacyjnego i eliminacja zbędnych alertów

Reagowanie i usuwanie skutków incydentów - Organizacja operacji reagowania na incydenty za pomocą „playbooków" z wglądem w różne środowiska. Usprawnienie procesów reagowania na incydenty i naprawiania skutków. Ręczne lub automatyczne wycofywanie złośliwych zmian wprowadzonych przez już opanowane zagrożenia – na pojedynczym urządzeniu lub urządzeniach w całym środowisku.

Funkcjonalności powiązane z reagowaniem i usuwanie skutków incydentów:

- Automatyzacja klasyfikacji incydentów usprawnienia reagowania na incydenty i ułatwienia rozwiązywania problemów, rekomendowanie działań analitykom ds. bezpieczeństwa, standaryzacja procedur reagowania na incydenty dzięki automatyzacji „playbooków"
- Optymalizacja zasobów bezpieczeństwa poprzez automatyzację działania w odpowiedzi na incydenty, takie jak usuwanie plików, kończenie złośliwych procesów, odwracanie trwałych zmian, powiadamianie użytkowników, izolowanie aplikacji i urządzeń oraz otwieranie zgłoszeń (tickets)
- Umożliwienie kontekstowego reagowania na incydenty z wykorzystaniem klasyfikacji incydentów i przedmiotów ataków (np. grup punktów końcowych)
- Uzyskanie pełnej widoczności łańcucha ataku i złośliwych zmian dzięki opatentowanemu śledzeniu kodu
- Zautomatyzowane czyszczenie i wycofywanie złośliwych zmian z zachowaniem czasu działania systemu
- Dodatkowe wsparcie dzięki opcjonalnej usłudze zarządzania wykrywaniem i reagowaniem (MDR)
- FortiEDR automatycznie poszerza dane o szczegółowe informacje o złośliwym oprogramowaniu, zarówno przed, jak i po infekcji, w celu przeprowadzenia analizy śledczej na infiltrowanych punktach końcowych. Jego unikalny interfejs zapewnia pomocne wskazówki, najlepsze praktyki i sugeruje analitykom bezpieczeństwa kolejne logiczne kroki.

Czas realizacji usługi Forti Edr 36 miesięcy

Usługa serwisowa polegająca na aktualizacji oprogramowania usługi 36 miesięcy

Ilość obsługiwanych pkt końcowych (komputerów, serwerów) 500 szt.

Usługa wsparcia instalacji / uruchomienia hybrydowej usługi 12 miesięcy