OMÓWIENIE ROZWIĄZANIA

Zabezpieczanie systemów cyberfizycznych za pomocą platformy Fortinet OT Security Platform

Streszczenie

Cyberprzestępcy coraz częściej atakują systemy cyberfizyczne w branżach produkcji i użyteczności publicznej, co jest przyczyną strat w produkcji i przerw w działalności. Ze względu na zwiększone ryzyko bezpieczeństwo technologii operacyjnych (operational technology, OT) stało się kluczowym elementem strategii korporacyjnej. Coraz większym zmartwieniem dyrektorów ds. bezpieczeństwa systemów informatycznych jest rozbudowa i aktualizacja zabezpieczeń środowisk OT w przypadku obiektów, które wcześniej były fizycznie odizolowane od innych systemów[1].

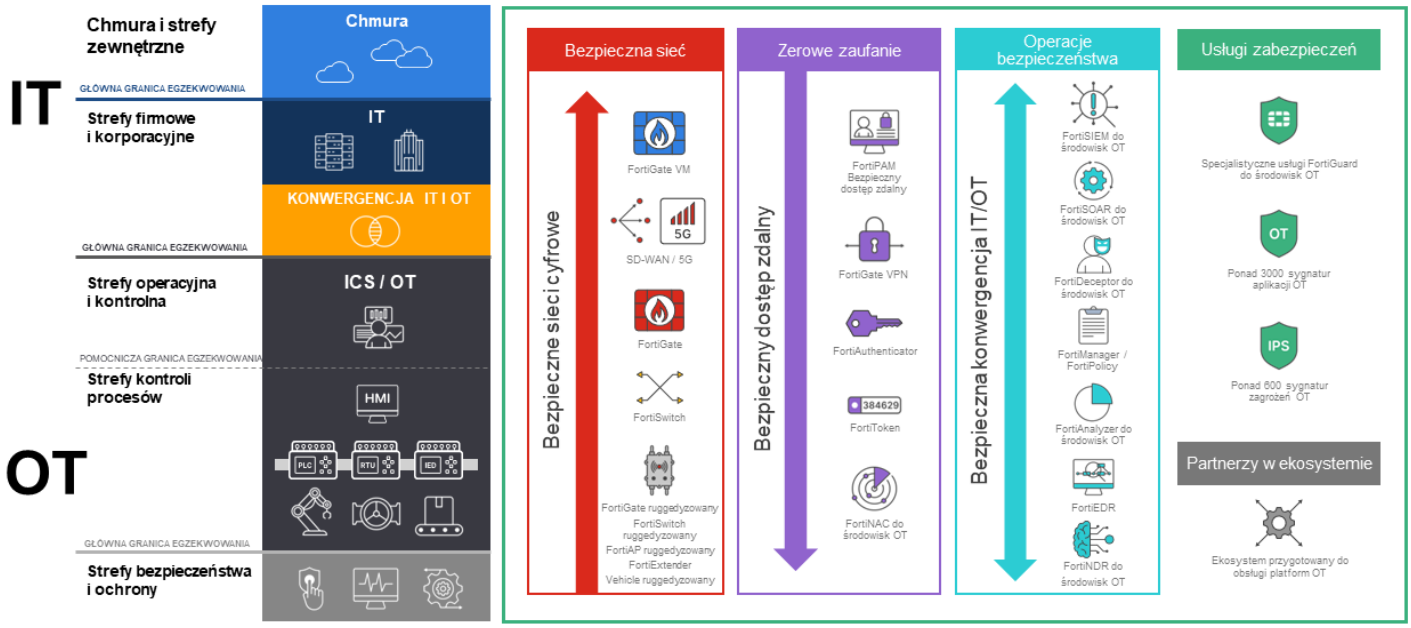
Fortinet OT Security Platform to kompleksowy system, którego zadaniem jest ochrona środowisk OT. W skład tej platformy wchodzi bezpieczna sieć, obsługa modelu zerowego zaufania, rozwiązania w zakresie operacji bezpieczeństwa, dedykowana analiza zagrożeń oraz rozbudowany i otwarty ekosystem partnerstw technologicznych. Wszystkie te rozwiązania są w pełni zintegrowane, aby umożliwić konsolidację dostawców i scentralizowane zarządzanie, upraszczając operacje i zwiększając bezpieczeństwo sieci przy jednoczesnym obniżeniu kosztów eksploatacji.

Platforma Fortinet OT Security Platform została uznana za absolutnego lidera w rankingu Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator[2].

Zapotrzebowanie na rozwiązania dla środowisk OT

Dyrektorzy ds. bezpieczeństwa systemów informatycznych oraz zespoły odpowiedzialne za ochronę środowisk OT i zarządzanie nimi stoją przed kilkoma niecodziennymi wyzwaniami, do których należy wybór dostawców i zarządzanie oferowanymi przez nich rozwiązaniami. Konfiguracja zabezpieczeń w tak złożonym środowisku OT przy jednoczesnym uwzględnieniu priorytetów operacyjnych, takich jak bezpieczeństwo personelu i ciągłość produkcji, nie jest łatwym zadaniem. Trzeba również pamiętać, że wiele firm musi sobie dziś radzić z konsolidacją dostawców, konwergencją rozwiązań IT i OT oraz optymalizacją obciążeń personelu zajmującego się cyberbezpieczeństwem, którego liczebność jest ograniczona. Aby sprostać tym wyzwaniom, dyrektorzy ds. bezpieczeństwa systemów informatycznych potrzebują platformy bezpieczeństwa dla środowisk OT, która zapewni ujednoliconą łączność, segmentację, obsługę modelu zerowego zaufania i rozwiązania w zakresie operacji bezpieczeństwa, które można płynnie zintegrować z już wdrożonymi rozwiązaniami.

Fortinet OT Security Platform to pełny pakiet rozwiązań w zakresie sieci przemysłowych i zabezpieczeń — oferujący zarówno niezbędne funkcje komunikacyjne, jak i zaawansowane rozwiązania dotyczące modelu zerowego zaufania i rozwiązania operacyjne w zakresie bezpieczeństwa OT.



Rysunek 1: Platforma Fortinet OT Security Platform

Łączenie i ochrona środowisk OT w ramach bezpiecznej sieci

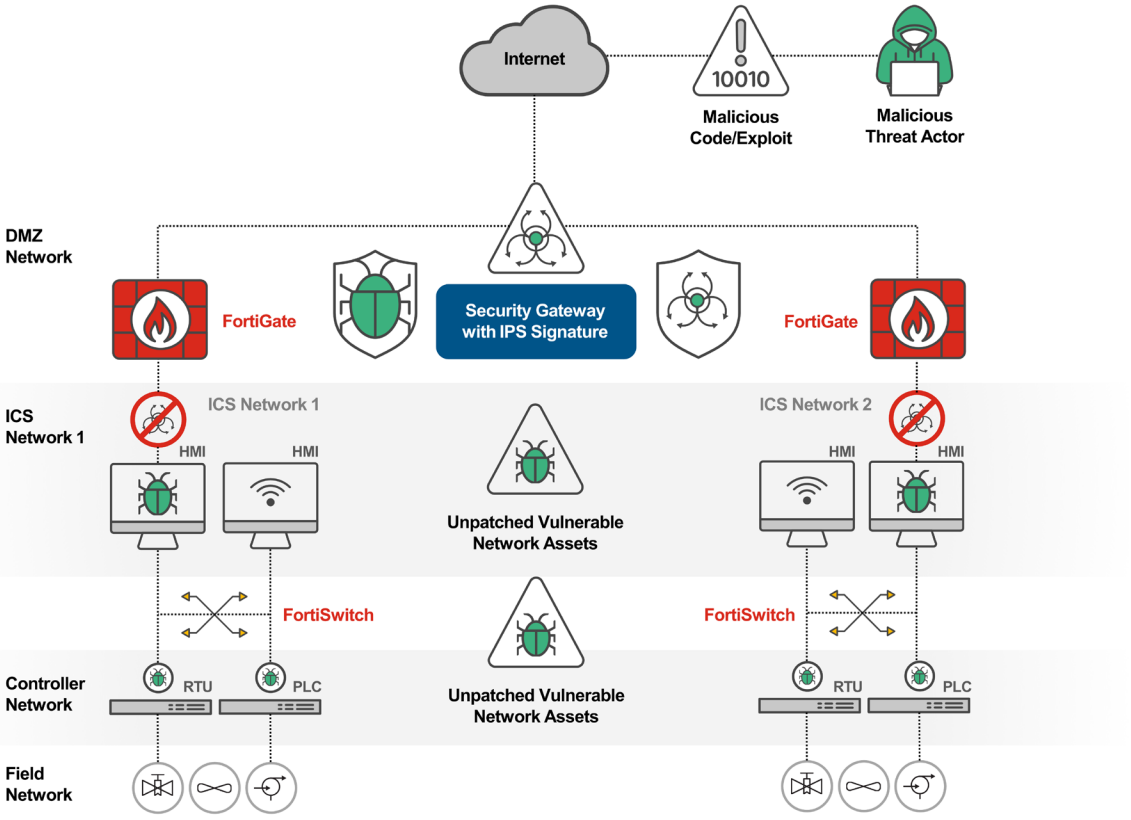
Platforma Fortinet OT Security Platform zapewnia niezbędną komunikację z systemami cyberfizycznymi za pomocą zapory nowej generacji FortiGate (FortiGate Next-Generation Firewall, NGFW) z dalszą segmentacją obsługiwaną przez rozwiązanie Fortinet FortiSwitch. Te kluczowe rozwiązania z zakresu komunikacji zostały zaprojektowane z myślą o środowiskach OT, dlatego wykorzystują komponenty sprzętowe o podwyższonej odporności i zaawansowane usługi bezpieczeństwa technologii operacyjnych.

Platforma OT Security Platform oferuje również rozwiązania innych typowych problemów, z którymi borykają się zespoły ds. bezpieczeństwa. Systemy i urządzenia OT często działają bez aktualnych poprawek z powodu niedostarczenia odpowiednich aktualizacji przez dostawców lub w związku z różnicami w priorytetach produkcyjnych — dlatego konieczne jest wdrożenie proaktywnych środków bezpieczeństwa. Platforma OT Security Platform obsługuje funkcje kontroli bezpieczeństwa aplikacji i protokołów OT, segmentację i mikrosegmentację sieci OT oraz mechanizmy kontroli zarządzania lukami w zabezpieczeniach, takie jak wirtualne wprowadzanie poprawek.

Oprócz widoczności zasobów i sieci platforma OT Security Platform oferuje usługę Fortinet OT Security Service, która zapewnia ochronę przed lukami w zabezpieczeniach aplikacji i protokołów OT największych producentów przemysłowych systemów sterowania (Industrial Control System, ICS). Dzięki zaktualizowanym sygnaturom i danym funkcji ochrony zapora NGFW FortiGate może wykrywać próby wykorzystania znanych luk w zabezpieczeniach systemów OT. Usługa OT Security Service uwzględnia ponad 70 protokołów automatyki przemysłowej i systemów sterowania oraz wykorzystuje ponad 19 000 sygnatur chroniących przed podatnościami, z których ponad 600 ma bezpośredni związek z bezpieczeństwem środowisk OT i jest wspomaganych przez mechanizm systemu wykrywania włamań FortiGate.

Jak już wspomniano, wiele urządzeń i systemów OT działa bez aktualnych poprawek i dlatego tak ważna jest możliwość wykrywania prób wykorzystania luk oraz zapobiegania atakom przez wirtualne wprowadzanie poprawek (czyli „osłanianie" luk w zabezpieczeniach). Platforma Fortinet OT Security Platform zapewnia następujące możliwości:

- Kontrola zabezpieczeń i egzekwowanie zasad przy użyciu zapory NGFW FortiGate
- Pełna widoczność i kontrola użytkowników oraz urządzeń w sieci, a także obsługa mikrosegmentacji sieci przy użyciu rozwiązania FortiSwitch
- Scentralizowane monitorowanie, rejestrowanie i raportowanie na potrzeby urządzeń FortiGate wdrożonych w środowiskach IT i OT przy użyciu rozwiązania FortiAnalyzer
- Scentralizowane zarządzanie urządzeniami i wdrażanie zasad zabezpieczeń na potrzeby urządzeń FortiGate w środowiskach IT i OT przy użyciu rozwiązania FortiManager
- Aktualizowane w czasie rzeczywistym, przydatne informacje i środki neutralizujące dotyczące zagrożeń, luk w zabezpieczeniach i luk typu zero-day od zespołu FortiGuard Labs



Rysunek 2: Wirtualne wprowadzanie poprawek w sieciach ICS/OT

Rozwiązania zgodne z modelem zerowego zaufania dla środowisk OT

Rozszerzenie strategii zerowego zaufania na sieci OT może sprawiać trudności ze względu na inne priorytety operacyjne, wrażliwość krytycznych sieci i urządzeń ICS oraz brak rozwiązań zgodnych z modelem zerowego zaufania opracowanych z myślą o środowiskach OT. Aby pomóc firmom przezwyciężyć te trudności, platforma OT Security Platform zapewnia funkcje bezpiecznego dostępu zdalnego (secure remote access, SRA), zarządzania dostępem uprzywilejowanym (privileged access management, PAM) i kontroli dostępu do sieci (network access control, NAC).

Każde z tych rozwiązań z osobna jest bardzo zaawansowane, a wszystkie razem tworzą platformę umożliwiającą sprawdzanie, jakie osoby i urządzenia łączą się z siecią OT. Pozwala to udzielać dostępu do właściwych zasobów na podstawie roli danego urządzenia lub użytkownika. Rozwiązania Fortinet zgodne z modelem zerowego zaufania umożliwiają bezpieczną łączność użytkowników z aplikacjami bez względu na lokalizację użytkownika i serwer, na którym działa aplikacja.

Funkcja NAC selektywnie przyznaje użytkownikom dostęp do aplikacji oraz identyfikuje i zabezpiecza środowiska IT, OT i przemysłowego Internetu rzeczy (Industrial Internet of Things, IIoT). Właściciele i operatorzy zasobów zyskują również pełną widoczność i kontrolę nad wszystkimi użytkownikami i urządzeniami łączącymi się z siecią. Dzięki współpracy rozwiązań do zarządzania tożsamościami i dostępem FortiPAM, FortiAuthenticator i FortiToken dostęp do zasobów mają tylko autoryzowani użytkownicy. Jednocześnie segmentacja zapewniana przez urządzenia FortiGate dodatkowo zwiększa skuteczność modelu zerowego zaufania, dzieląc sieci IT/OT zgodnie z potrzebami biznesowymi. Poniżej przedstawiamy listę rozwiązań Fortinet zgodnych z modelem zerowego zaufania:

- Zapora NGFW FortiGate — zapewnia kontrolę zabezpieczeń i egzekwowanie zasad.
- FortiNAC — zapewnia widoczność, kontrolę oraz zautomatyzowane reagowanie na działania użytkowników i urządzeń łączących się z siecią.
- FortiToken — zapewnia uwierzytelnianie dwuskładnikowe za pomocą aplikacji generującej hasła jednorazowe (one-time password, OTP), powiadomień push lub sprzętowego tokenu OTP z ograniczonym czasem ważności.
- FortiAuthenticator — zapewnia obsługę funkcji logowania jednokrotnego i autoryzacji użytkowników, która umożliwia identyfikację użytkowników, wysyłanie zapytań o uprawnienia dostępu z systemów zewnętrznych i przekazywanie żądań dostępu do zapory NGFW FortiGate w celu wdrożenia zasad zabezpieczeń opartych na tożsamości.
- FortiPAM — zapewnia obsługę funkcji zarządzania tożsamościami i dostępem uprzywilejowanym, umożliwiając wdrażanie zabezpieczeń zgodnych z modelem zerowego zaufania w przypadku krytycznych zasobów. Rozwiązanie to kontroluje dostęp użytkowników do krytycznych aplikacji i systemów, monitoruje i śledzi aktywność użytkowników oraz umożliwia bezpieczny dostęp zdalny do krytycznych zasobów.

Fragment raportu Gartner: „Współczesne firmy dążą do uproszczenia operacji, dlatego dostawcy konsolidują platformy wokół głównych dziedzin cyberbezpieczeństwa. Na przykład usługi zabezpieczania tożsamości są często oferowane za pośrednictwem wspólnej platformy łączącej funkcje zarządzania, dostępu uprzywilejowanego i zarządzania dostępem. Dyrektorzy ds. bezpieczeństwa i zarządzania ryzykiem muszą stale inwentaryzować mechanizmy kontroli bezpieczeństwa, aby wiedzieć, które rozwiązania się dublują, i zmniejszać nadmiarowość przy użyciu platformom skonsolidowanych[3]".

Poprawa bezpieczeństwa środowisk OT dzięki operacjom bezpieczeństwa zoptymalizowanym pod kątem tych środowisk

Korzystanie z platformy przeznaczonej do środowisk OT umożliwia integrację wielu źródeł danych, przyspieszając wykrywanie i umożliwiając automatyzację reakcji systemu zabezpieczeń. Rozwiązania Fortinet z zakresu operacji bezpieczeństwa zostały dostosowane do wymagań zabezpieczeń środowisk OT. Obejmują one identyfikację zasobów i komunikację sieciową z mapą topologii wykorzystującą model Purdue, a także macierz MITRE ATT&CK do systemów ICS oraz raporty dotyczące ryzyka i przestrzegania zasad.

Zespoły IT i OT muszą również znaleźć kompromis między potrzebami w zakresie bezpieczeństwa a priorytetami operacyjnymi. W przypadku ograniczania ryzyka może być konieczne wstrzymanie działań naprawczych przez zespoły ds. bezpieczeństwa lub operacji OT, aby nie doszło do zakłóceń produkcji i ciągłości usług. Ostatecznym celem jest optymalizacja zintegrowanego centrum operacji bezpieczeństwa IT/OT, w którego skład wchodzą analiza zagrożeń, analityka, wykrywanie zagrożeń, decepcja (pułapki typu honeypot), reagowanie na incydenty, wyszukiwanie i wykrywanie zagrożeń oraz funkcje zarządzania i egzekwowania zasad, które nie zakłócają pracy środowiska OT. Aby osiągnąć ten cel, stosowane są następujące rozwiązania Fortinet z zakresu operacji bezpieczeństwa:

- Zapora NGFW FortiGate — zapewnia kontrolę zabezpieczeń i egzekwowanie zasad.
- FortiEDR — umożliwia zautomatyzowane wykrywanie zagrożeń i ochronę punktów końcowych w czasie rzeczywistym. Obsługuje również skoordynowane reagowanie na incydenty i analizę śledczą.

- FortiSIEM — umożliwia pozyskiwanie i analizowanie danych dzienników z systemów IT i OT oraz zapewnia skorelowaną analizę działań hakerskich w obu środowiskach. Rozwiązanie FortiSIEM może również udostępniać informacje o aktywnych zagrożeniach w ramach macierzy MITRE ATT&CK na potrzeby korporacyjnych środowisk IT i ICS.
- FortiSOAR — konfigurowalna platforma operacji bezpieczeństwa zapewniająca zautomatyzowane skrypty postępowania, klasyfikację incydentów i działania naprawcze w czasie rzeczywistym, które ułatwiają przedsiębiorstwom wykorzystującym środowiska OT identyfikowanie i odpieranie ataków oraz obronę przed nimi.
- FortiDeceptor — umożliwia wprowadzanie hakerów w błąd, a także ujawnianie i eliminowanie zagrożeń zewnętrznych i wewnętrznych, zanim spowodują one znaczące szkody, przy użyciu pułapek typu honeypot.
- FortiNDR — oferuje funkcje wykrywania i reagowania w sieci (network detection and response, NDR) wykorzystujące sztuczną inteligencję i sztuczne sieci neuronowe, umożliwiając analizę zagrożeń w czasie poniżej jednej sekundy. Rozwiązanie to korzysta z technologii uczenia głębokiego, która pomaga analitykom w centrach operacji bezpieczeństwa (security operations center, SOC) poprzez zautomatyzowane odpieranie różnych rodzajów ataków. Aby skutecznie realizować to zadanie, rozwiązanie FortiNDR zawiera funkcję wirtualnego analityka zabezpieczeń, który szybko identyfikuje, klasyfikuje i reaguje na zagrożenia.
- Security Operations Center-as-a-Service (SOCaaS) — chmurowa, zarządzana zewnętrznie usługa monitorowania zabezpieczeń, która analizuje zdarzenia bezpieczeństwa generowane przez zapory NGFW FortiGate i inne produkty w systemie zabezpieczeń. Przeprowadza ona klasyfikację alertów i eskaluje powiadomienia o potwierdzonych zagrożeniach.
- FortiRecon — działająca w modelu SaaS usługa ochrony przed ryzykiem cyfrowym (digital risk protection, DRP), w której skład wchodzą trzy zaawansowane moduły: zarządzanie podatnością na ataki z zewnątrz, ochrona marki i analiza ukierunkowana na atakujących. Usługa FortiRecon pozwala sprawdzić, co widzą, robią i planują atakujący, co pomaga w przeciwdziałaniu atakom na etapie rozpoznania i znacznie zmniejsza ryzyko, skracając czas oraz obniżając koszty późniejszej neutralizacji zagrożeń.

Łatwiejsza konsolidacja i konwergencja zabezpieczeń dzięki platformie Fortinet OT Security Platform

Zabezpieczanie systemów cyberfizycznych jest złożonym zadaniem technicznym, które często jest utrudnione ze względu na różnice w priorytetach operacyjnych. Pierwszym krokiem w zabezpieczaniu środowisk OT jest zapewnienie bezpiecznej łączności sieci OT z resztą przedsiębiorstwa (często po raz pierwszy), a ostatnim — wdrożenie w pełni funkcjonalnego centrum operacji bezpieczeństwa OT. Należy też pamiętać, że wiele firm wykorzystujących środowiska OT dąży do optymalizacji operacji przez konsolidację dostawców oraz konwergencję zasobów IT i OT. Platforma Fortinet OT Security Platform ułatwia realizację tych zadań dzięki łączności sieciowej zoptymalizowanej pod kątem środowisk OT, obsłudze modelu zerowego zaufania i rozwiązaniom SecOps. Dyrektorzy ds. bezpieczeństwa systemów informatycznych odpowiedzialni za zabezpieczenia środowisk OT z pewnością docenią elastyczność platformy Fortinet OT Security Platform i wchodzące w jej skład rozwiązania przeznaczone do zastosowań przemysłowych.

[1] Raport Fortinet o stanie OT i cyberbezpieczeństwa w 2023 r..

[2] Firma Fortinet uznana za absolutnego lidera w raporcie IT/OT Network Protection Platforms Navigator™ 2023, 27 lipca 2023 r.

[3] Gartner: Gartner wskazuje najważniejsze trendy w cyberbezpieczeństwie na rok 2023, 12 kwietnia 2023 r.

29 lutego 2024 11:45
2436831-0-0-PL