Poprawa wydajności zabezpieczeń w architekturze Security Fabric za pomocą funkcji szybkiego reagowania

Spis treści

Streszczenie

W samym tylko roku 2019 na cyberbezpieczeństwo wydano ponad 124 mld USD[1], a jednak wiele przedsiębiorstw ma nadal problemy w tym obszarze. Problemy te obejmują zbyt dużą liczbę pulpitów, przeciążenie liczbą alertów, uzależnienie się od procesów ręcznych oraz niedobór specjalistów ds. cyberbezpieczeństwa.

Model dojrzałości centrum zarządzania bezpieczeństwem (SOC) ma pomóc działom IT w określeniu możliwości architektury Fortinet Security Fabric w oparciu o dotychczasowe inwestycje w pracowników i procesy obecne w centrum SOC, a tym samym zapewnić narzędzia niezbędne do rozwiązywania problemów, z którymi borykają się działy IT na każdym poziomie dojrzałości.

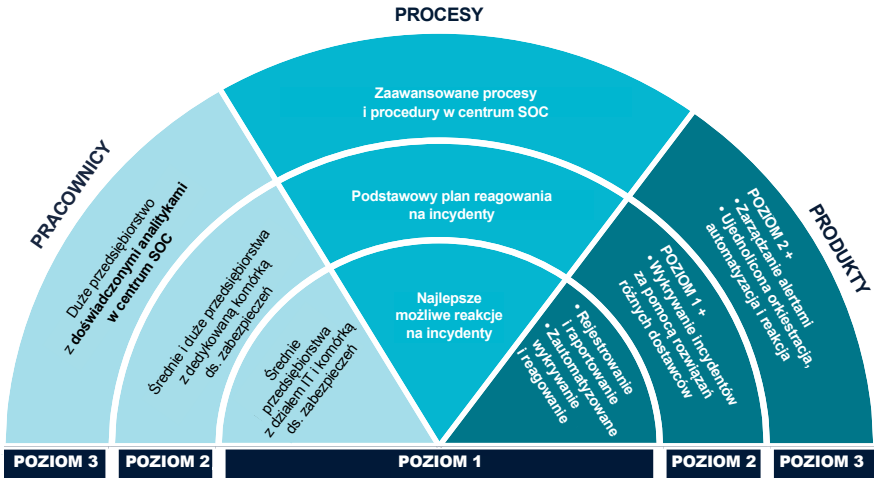
Rozwiązania Fortinet, takie jak FortiAnalyzer (analityka i automatyzacja w architekturze Security Fabric), FortiSIEM (zarządzanie informacjami i zdarzeniami dotyczącymi bezpieczeństwa) i FortiSOAR (orkiestracja i automatyzacja zabezpieczeń oraz reagowanie na incydenty), wykorzystują zautomatyzowane procesy bezpieczeństwa, aby rozwiązywać kluczowe problemy stojące przed architektami zabezpieczeń i rozwijać automatyzację centrum SOC. Architektura Security Fabric łączy w sobie wszystkie te rozwiązania i maksymalizuje zdolności nawet skromnie obsadzonych działów IT do ochrony przedsiębiorstwa.

Automatyzacja zabezpieczeń w architekturze Security Fabric

Wyzwaniem dla takich działów IT jest złożoność operacyjna. Model automatyzacji centrum „SOC Automation” pomaga działowi IT określić swój bieżący poziom dojrzałości i wybrać rozwiązania zabezpieczające Fortinet, które są najbardziej odpowiednie dla danego środowiska.

Model automatyzacji centrum SOC dzieli się na trzy kluczowe obszary: pracownicy, procesy i produkty. W ramach każdego obszaru przedsiębiorstwo może być sklasyfikowane na poziomie dojrzałości od 1 do 3 na podstawie stanu bezpieczeństwa w tym obszarze. Na przykład przedsiębiorstwo, które znajduje się na poziomie 1 we wszystkich obszarach, ma niewielki dział IT bez wydzielonej komórki ds. zabezpieczeń (pracownicy), ma nie najlepsze procedury reagowania na incydenty (procesy) oraz nie ma dedykowanych rozwiązań w zakresie bezpieczeństwa (produkty). Przedsiębiorstwo na poziomie 3 będzie natomiast mieć liczną komórkę ds. zabezpieczeń z doświadczonymi analitykami w centrum SOC, dysponować dobrze zdefiniowanymi procedurami reagowania na incydenty oraz nie tylko mieć wdrożone rozwiązania SIEM i SOAR, ale także móc mierzyć ich efektywność.

W kontekście niedoboru ponad 4 mln specjalistów ds. cyberbezpieczeństwa, który stale się zwiększa[2], działania naprawcze w obszarze pracowników mogą okazać się niewykonalne. Wdrożenie właściwych procesów i dobór odpowiednich produktów może jednak zrekompensować braki kadrowe w komórce ds. zabezpieczeń.



Rysunek 1. Model automatyzacji centrum SOC.

Poziom 1. Zapewnienie widoczności przy użyciu narzędzi analitycznych w architekturze Security Fabric

Na poziomie 1 modelu automatyzacji centrum SOC dział IT nie ma dedykowanej komórki ds. zabezpieczeń ani odpowiednich procedur postępowania w przypadku potencjalnych incydentów. Ponadto przeciętne przedsiębiorstwo na tym poziomie otrzymuje ponad 10 tys. alertów dziennie[3], co oznacza, że analitycy z centrum SOC są przytłoczeni pracą i mają mało czasu na zajmowanie się identyfikacją i neutralizacją prawdziwych cyberzagrożeń.

Bez dedykowanych rozwiązań dział IT nie ma widoczności potencjalnych zagrożeń dla sieci przedsiębiorstwa. Wszystkie dane z dzienników muszą być zbierane i korelowane ręcznie przed wykonaniem analizy. Wiele centrów SOC na poziomie 1 nie ma też specjalistów ani zasobów umożliwiających identyfikację prawdziwych zagrożeń, co naraża przedsiębiorstwo na udany atak.

FortiAnalyzer to łatwe do wdrożenia rozwiązanie zapewniające scentralizowaną widoczność i możliwość wykrywania zagrożeń w całej architekturze Fortinet Security Fabric, zarówno lokalnie, jak i w chmurze. FortiAnalyzer koreluje dane z dzienników wielu urządzeń Fortinet, zapewniając analitykom zabezpieczeń cenny kontekst. Poddając te dane analizie za pomocą mechanizmów uczenia maszynowego oraz przy użyciu danych o symptomach ataku uzyskiwanych z globalnego kanału informacji o zagrożeniach, FortiAnalyzer może pomóc nawet najmniej licznej komórce ds. zabezpieczeń w identyfikacji i szybkiej reakcji na cyberzagrożenia.

Poziom 2. Poprawa widoczności urządzeń różnych dostawców przy użyciu funkcji SIEM

Przeciętne przedsiębiorstwo korzysta w ramach swojej sieci z 75 różnych punktowych rozwiązań zabezpieczających[4]. Każde z tych rozwiązań dostarcza cennych informacji o potencjalnych zagrożeniach dla sieci przedsiębiorstwa, często brakuje jednak kontekstu wymaganego do odróżnienia prawdziwego zagrożenia od fałszywego alarmu. Ponadto stosowanie takich rozwiązań punktowych utrudnia przedsiębiorstwu prowadzenie spójnej polityki bezpieczeństwa i przestrzeganie restrykcyjnych przepisów prawa ochrony danych, takich jak unijne ogólne rozporządzenie o ochronie danych (RODO) lub ustawa o ochronie prywatności konsumentów w Kalifornii (CCPA).

Podejście SIEM to logiczne rozwiązanie problemu złożoności architektury zabezpieczeń obejmującej produkty różnych dostawców. Rozwiązanie SIEM analizuje dane pochodzące z takich produktów i przeprowadza automatyczne korelacje i analizy tych danych w celu uzyskania bardziej przejrzystego obrazu ogólnego stanu chronionego środowiska.

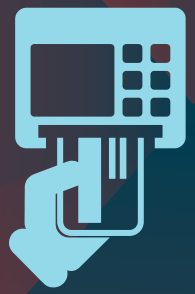
Rozwiązanie FortiSIEM umożliwia komórkom ds. zabezpieczeń podejmowanie działań jak najbardziej zgodnych z najlepszymi praktykami branżowymi i standardami bezpieczeństwa, takimi jak te standardy NIST (National Institute of Standards and Technology) i CIS (Center for Internet Security). W ten sposób FortiSIEM poprawia widoczność zapewnianą przez rozwiązanie FortiAnalyzer w kontekście architektury Fortinet Security Fabric.

Poziom 3. Wdrożenie zautomatyzowanych reakcji przy użyciu funkcji SOAR

Metody włamań dynamicznie się zmieniają, ponieważ cyberprzestępcy w coraz większym stopniu korzystają z mechanizmów automatyzacji. O ile widoczność z poziomu jednej konsoli pozwala na szybsze wykrycie potencjalnego zagrożenia, o tyle poleganie na procesach ręcznego reagowania na incydenty oznacza, że obrońcy zawsze będą o krok za atakującymi.

Rozwiązania SOAR pozwalają na zautomatyzowanie reakcji na incydenty. Dzięki utworzeniu zautomatyzowanej struktury spinającej całą architekturę zabezpieczeń w przedsiębiorstwie działania obronne mogą być podejmowane wspólnie przez wiele różnych systemów. Ogranicza to konieczność wymiany informacji o zagrożeniach między personelem działu IT, ogranicza zjawisko zmęczenia alertami oraz przyspiesza reakcje na incydenty.

Ponadto rozwiązanie FortiSOAR pozwala zoptymalizować procesy bezpieczeństwa w drodze wykorzystania dobrze zdefiniowanych procedur bezpieczeństwa. Dzięki zautomatyzowaniu powtarzalnych zadań i reakcji na typowe zagrożenia, FortiSOAR umożliwia skupienie wysiłków i ograniczonych zasobów na zadaniach o najwyższym priorytecie.



Automatyzacja procesów może skrócić czas reakcji z dni do minut.

Zastosowanie modelu automatyzacji centrum SOC w celu inteligentnego uproszczenia procesów SOC

Metody włamań dynamicznie się zmieniają, wiele przedsiębiorstw nadal nie ma jednak odpowiednich zasobów i wykwalifikowanego personelu, aby się przed nimi bronić. Obrona taka wymaga bowiem wdrożenia zabezpieczeń, które odciążą przeciążone i niedostatecznie obsadzone zespoły w centrum SOC.

Model automatyzacji centrum SOC pomaga architektom zabezpieczeń określić bieżący poziom dojrzałości centrum SOC oraz działania niezbędne do przejścia na wyższy poziom. Rozwiązania Fortinet, takie jak FortiAnalyzer, FortiSIEM i FortiSOAR, mają w tym przejściu pomóc.

Dzięki zastosowaniu funkcji inteligentnej automatyzacji procesów bezpieczeństwa rozwiązania te skracają średni czas wykrycia zagrożenia (MTTD) i średni czas reakcji na zagrożenie (MTTR), ograniczając podatność przedsiębiorstwa na działalność cyberprzestępców.

W ciągu jednego roku w 65 krajach zgłoszono[5]:

- **2216 przypadków naruszeń ochrony danych**
- **53 000 incydentów dotyczących cyberbezpieczeństwa**

[1] Lawrence Pingree, et al., „Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 3Q19 Update", Gartner, 3 października 2019 r.

[2] „(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide", (ISC)², 6 listopada 2019 r.

[3] „How Many Daily Cybersecurity Alerts does the SOC Really Receive?", Bricata, 2 października 2019 r.

[4] Kacy Zurkus, „Defense in depth: Stop spending, start consolidating", CSO, 14 marca 2016 r.

[5] Gil Press, „60 Cybersecurity Predictions For 2019", Forbes, 3 grudnia 2018 r.

www.fortinet.com

616492-0-0-PL

sierpnia 31, 2020 12:39 PM

ebook-FA-accelerate-efficiency-of-security-operations-across