Flowmon i Fortinet wspólnie dostarczają zautomatyzowane, wielowarstwowe cyberbezpieczeństwo

**Listopad 2020 - Flowmon Networks, wiodący dostawca rozwiązań do monitorowania i analizy ruchu sieciowego, połączył siły z firmą Fortinet, aby dostarczyć administratorom bezpieczeństwa zintegrowane rozwiązanie do automatycznego wykrywania i reagowania na nieznane i wewnętrzne zagrożenia.**



Wysiłki specjalistów ds. bezpieczeństwa, mające na celu skrócenie czasu odzyskiwania sprawności po ataku lub awarii są często hamowane przez reaktywną naturę tradycyjnych rozwiązań zabezpieczających. To powoduje dłuższe przestoje, mniej efektywne reakcje, a co za tym idzie dłuższe narażanie krytycznych zasobów na działanie masowych lub płynnych i trudnych do wykrycia zagrożeń. Wspólne rozwiązanie łączy doskonałą analizę ruchu Flowmon z nagradzanymi rozwiązaniami Next Generation Firewall Fortinet FortiGate. Zintegrowane podejście do bezpieczeństwa i sieci, tworzy wielowarstwową i wysoce zautomatyzowaną macierz bezpieczeństwa.

- *Przyspieszenie reagowania na zdarzenia dzięki automatyzacji to najlepszy sposób na ułatwienie pracy specjalistów ds. bezpieczeństwa. Cieszymy się mogąc to zrobić razem z Fortinetem, dzięki wysokowydajnemu, skalowalnego i łatwemu do wdrożenia rozwiązaniu* – mówi **Jiri Tobola, CEO Flowmon Networks**. – *Połączenie rozwiązania Flowmon z firewallami następnej generacji (NGFW) FortiGate eliminuje czasochłonne ręczne wyszukiwanie problemów, gwarantuje, że szkody są minimalizowane już na starcie i optymalizuje bezpieczeństwo przedsiębiorstwa.*

Sieć ukierunkowana na bezpieczeństwo (Security-driven Networking) według Fortinet, to niezbędna strategia bezpieczeństwa przy dzisiejszych dynamicznych i stale rozwijających się infrastrukturach sieciowych. FortiGate NGFW, kluczowy element sieci ukierunkowanej na bezpieczeństwo, zabezpiecza perymetr i chroni przed zewnętrznymi zagrożeniami, a Flowmon analizuje obustronny ruch sieciowy, aby wykryć niebezpieczeństwa, które mogą obejść systemy ochronne. Gdy Flowmon wykryje znacznik naruszenia bezpieczeństwa, np. próbę przeprowadzenia rozpoznania zabezpieczeń czy ruch poboczny, eksfiltrację danych czy komunikację CnC, wysyła wiadomość do FortiGate, aby zablokować niepożądaną komunikację. Zintegrowane rozwiązanie korzysta jednocześnie z wielu wdrożonych technik wykrywania, aby objąć szerszy zakres zagrożeń.

- *Dzisiejsi cyberprzestępcy korzystają z zaawansowanych technik, aby uniknąć wykrycia, ale i tak pozostawiają ślady rozrzucone po całej sieci. Cieszymy się z włączenia Flowmon do Fortinet Open Fabric Ecosystem, dzięki czemu możemy dostarczyć klientom zintegrowane rozwiązania zapewniające kompleksowe bezpieczeństwo. Wspomagany sztuczną inteligencją silnik Flowmon wykrywa znaczniki naruszenia bezpieczeństwa w ruchu sieciowym i integruje się z Fortinet Security Fabric, aby zapewnić klientom zaawansowaną, wielowarstwową ochronę* – powiedział **Neil Prasad, Kierownik Global Technology Alliances w Fortinet**.

Fortinet FortiGate NGFW wdrażają sieć ukierunkowaną na bezpieczeństwo i zbierają w jedno najlepsze rynkowe rozwiązania bezpieczeństwa, jak np. IPS (intrusion prevention system), web filtering, inspekcję SSL i zautomatyzowaną ochronę przed zagrożeniami.

Rozwiązania do analizy ruchu sieciowego Flowmon łączą operacje bezpieczeństwa i sieciowe w jedno elastyczne rozwiązanie. Dostarczają pozwalającego na działanie wglądu przez automatyczną analizę ruchu sieciowego i wykrywanie zaawansowanych zagrożeń, co eliminuje konieczność przedzierania się przez szum informacyjny. Pozwalają profesjonalistom IT reagować szybko na naruszenia bezpieczeństwa i spadki wydajności, zrozumieć ich kontekst, znaczenie, natężenie oraz przyczynę.

**Do pobrania:**

**Logo Flowmon Networks:** <https://bitubi.eu/flowmon/Flowmon_logo.zip>

**O Flowmon**

[Flowmon Networks](http://www.flowmon.com) oferuje firmom niezawodne narzędzia służące do monitorowania sieci komputerowych
i wykrywania zagrożeń. Nasze zaawansowane technologie monitorowania i analizowania zachowania sieci udostępniają specjalistom z działu IT szczegółowe informacje na temat ruchu sieciowego, dzięki czemu mogą oni zwiększać wydajność sieci i aplikacji oraz zapobiegać współczesnym zagrożeniom. Oferujemy innowacyjne, skuteczne, skalowalne i proste w użyciu rozwiązania do monitorowania sieci wykorzystujące protokoły NetFlow i IPFIX. Największe przedsiębiorstwa na świecie, dostawcy usług internetowych, organizacje rządowe, a nawet małe i średnie firmy polegają na naszych narzędziach, które zapewniają kontrolę nad środowiskiem sieciowym oraz umożliwiają ochronę sieci i eliminowanie potencjalnych zagrożeń.