PLATFORMY THREAT INTELLIGENCE JAKO WSPARCIE DLA ZESPOŁÓW REAGOWANIA NA INCYDENTY KOMPUTEROWE

21.06.2018

Pod pojęciem cyber threat intelligence (CTI) należy rozumieć gromadzenie, przetwarzanie i analizę danych o zagrożeniach bezpieczeństwa teleinformatycznego. Prawidłowe zaimplementowanie usług CTI pozwala na efektywniejsze zarządzanie incydentami komputerowymi w całym cyklu ich życia. Tego typu implementacja powinna zakładać przede wszystkim zdolność przekształcania surowych danych z konkretnego źródła w wartościową informację, która, przy odpowiednim wykorzystaniu, przyczyni się do zwiększenia bezpieczeństwa naszego constituency (obszaru świadczenia usług bezpieczeństwa teleinformatycznego). Na CTI składają się zarówno pojedyncze dane (hashe plików, adresy IP, domeny powiązane ze złośliwą aktywnością), jak i gotowe informacje, np. te o podatnościach, nowych kampaniach phishingowych czy wyciekach danych.

Pełny krajobraz o zagrożeniach teleinformatycznych wymaga gromadzenia danych z wielu źródeł. Dane te różnią się od siebie pod względem jakości i struktury, dlatego muszą być dodatkowo przeprocesowane, posortowane i na końcu zinterpretowane. Cały proces weryfikacji wymaga pracy ludzkiej połączonej z analizą maszynową, a do tego musi zostać zrealizowany możliwie szybko by móc zadziałać w porę. Negatywną konsekwencją takiego rozwiązania często bywa przeciążenie danymi, które, z uwagi na ograniczoną możliwość obsługi, nie stanowią wartości dodanej. W praktyce zatem, proces, który miał ułatwiać pracę analityka bezpieczeństwa bywa przeciw skuteczny. Przykładowo, ograniczona możliwość obsługi, a także brak okresowej weryfikacji danego źródła CTI może prowadzić do generowania nadmiarowych zdarzeń typu false positive (FP). W zależności od przyjętych procedur

i stosowanych technologii w danej organizacji, taka sytuacja wymusza dodatkowe czynności, np. zamknięcia długiej kolejki ticketów FP. Ryzyko takiego scenariusza dotyczy w szczególności mniejszych zespołów bezpieczeństwa czy niewielkich CERT-ów.

Jednym z dostępnych rozwiązań tego problemu na rynku produktów i usług cyberbezpieczeństwa są tzw. platformy CTI – dalej, zgodnie z przyjętą przez ENISA definicję, nazywane TIP (Threat Intelligence Platform). Eksperci ENISA określają TIP-y jako usługi wspierające dla już realizowanych czynności CTI, w szczególności na poziomie zarządzania całym procesem. Są to najczęściej aplikacje webowe, dostępne w modelu SaaS (Software as a Service). TIP skupia w jednym miejscu wszystkie czynności przypisane do obsługi źródeł. ENISA definiuje tego typu platformy poprzez 6 głównych funkcjonalności: analitykę danych, wizualizację, informatykę śledczą, przetwarzanie danych, raportowanie wyników i udostępnianie innym użytkownikom. Na rynku wyróżnia się 3 typy TIP-ów: komercyjne, open-source'owe i te opracowane przez społeczność. Nie będzie zatem przesadą nazwanie TIP-u kolektorem wiedzy o zagrożeniach bezpieczeństwa teleinformatycznego. Bez wątpienia najmocniejszą stroną, a zarazem fundamentem funkcjonowania tych platform jest aktywnie zaangażowana społeczność analityków, dzięki której platformy TIP są na bieżąco aktualizowane i same w sobie stanowią cenne źródło aktualności o zagrożeniach. Możliwość uzupełnienia informacji o danym zagrożeniu na podstawie własnych obserwacji, wiedzy i danych to tylko kolejny mechanizm, który oprócz tego, że zwiększa kompletność informacji, jest wymiernym przykładem współpracy społeczności cyberbezpieczeństwa.

> JEDNĄ Z NAJWAŻNIEJSZYCH GRUP WNOSZĄCYCH WKŁAD W ROZWÓJ TIP-ÓW, SZCZEGÓLNIE TYCH OPEN-SOURCE'OWYCH ORAZ SPOŁECZNOŚCIOWYCH, SĄ CSIRT-Y (ZESPOŁY REAGOWANIA NA INCYDENTY KOMPUTEROWE). ZESPOŁY TE MOŻNA NAZWAĆ TAKŻE GŁÓWNYMI BENEFICJENTAMI TIP-ÓW.

Jedną z najważniejszych grup wnoszących wkład w rozwój TIP-ów, szczególnie tych open-source'owych oraz społecznościowych, są CSIRT-y (zespoły reagowania na incydenty komputerowe). Zespoły te można nazwać także głównymi beneficjentami TIP-ów. Dzięki wykorzystaniu tych narzędzi, specjaliści CSIRT mogą w efektywniejszy sposób realizować szereg usług dla swojego constituency.

Mowa tu przede wszystkim o uświadamianiu użytkowników, alarmowaniu o bieżących zagrożeniach, rozpowszechnianiu informacji czy też opracowywaniu dedykowanych raportów czy analiz.
Z operacyjnego punktu widzenia korzystanie z TIP-ów pomaga np. w priorytetyzacji incydentów (proces triage), gdyż może dostarczyć szerszego kontekstu dla konkretnego alarmu czy zgłoszenia.

Ponieważ rynek TIP jest wciąż stosunkowo nowy, usługi przez niego dostarczane przyjmują różne formy. Mogą to być dane surowe, ale przefiltrowane pod kątem FP; zagregowane i skorelowane dane pochodzące z różnych źródeł czy też wyprofilowane alerty przesyłane organizacjom z konkretnego sektora, narażonym na pewne specyficzne typy zagrożeń. Niewątpliwą zaletą większości rozwiązań klasy TIP jest to, że umożliwiają dostarczanie danych w formacie rozpoznawalnym i obsługiwanym przez zautomatyzowane systemy bezpieczeństwa (jak firewalle czy systemy IPS), co pozwala odciążyć personel działu bezpieczeństwa IT.

Praktyczne korzyści z implementacji TIP-ów czerpią więc nie tylko dyżurni obsługujący incydenty, ale również firmy i organizacje, które zwiększając bezpieczeństwo swojej infrastruktury mogą jednocześnie oddelegować odciążonych analityków do innych zadań.

Autorzy:

Kamil Gapiński
Fundacja Bezpieczna Cyberprzestrzeń

Paweł Stępniak
ComCERT.pl

Śledź na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**