Orion
Instruments Polska

WSKAŹNIKI KPI W OPERACJACH BEZPIECZEŃSTWA I ZARZĄDZANIU INCYDENTAMI cz. 2

JAKIE KPI NALEŻY USTANOWIĆ?

Ilość kluczowych wskaźników wydajności, które należy zdefiniować dla operacji bezpieczeństwa i reakcji na incydent jest w każdej organizacji ściśle powiązana z jej celami w zakresie cyberbezpieczeństwa. Po prostu definiując własne cele automatycznie definiuje się odpowiadające im KPI. Warto określić zarówno priorytetowe jak i pomocnicze KPI, po to aby na ich podstawie przeprowadzić właściwą analizę i ocenić postęp na drodze do osiągania zamierzonych celów.

- **Priorytetowe wskaźniki KPI – kluczowe wskaźniki efektywności, które są podstawą do oceny skuteczności realizacji programu bezpieczeństwa;**
- **Pomocnicze KPI – kluczowe wskaźniki efektywności, które są istotne, ale nie odgrywają decydującej roli w programie bezpieczeństwa.**

ILE MIERNIKÓW KPI NALEŻY USTANOWIĆ?

Określenie liczby kluczowych wskaźników efektywności jest zadaniem do wykonania wewnątrz każdej organizacji. Nie należy zlecać tej operacji na zewnątrz, ponieważ firma sama powinna określić ile krytycznych operacji lub celów musi monitorować, aby zapewnić optymalny poziom swojego programu bezpieczeństwa.

Mierniki mają dostarczać danych, które będą stanowiły podstawę podejmowanych decyzji dotyczących programu bezpieczeństwa. Ustanowienie zbyt wielu wskaźników będzie niepotrzebnie rozpraszać uwagę decydentów, a ponadto stanowić będzie zbędne obciążenie dla wyznaczających KPI analityków.

Jaką więc ilość wskaźników należy uznać za wystarczającą? Niektórzy specjaliści sugerują od 1 do 3 na każdy wybrany cel programu, inni uważają, że łączna ich ilość powinna wynosić od 5 do 9. W praktyce powyższe liczby wydają się rozsądne dla standardowego programu bezpieczeństwa. Ważniejsze jednak niż konkretna liczba KPI jest to, czy są one dopasowane do potrzeb organizacji. Przy ustanawianiu wskaźników dobrze jest uwzględnić odpowiedzi na następujące pytania:

- **czy dany wskaźnik będzie wykorzystywany przez wąską czy szerszą grupę odbiorców?**
- **czy wskaźnik ma szansę być inspiracją do wprowadzenia istotnych zmian w organizacji?**
- **czy dany wskaźnik można śledzić w czasie i ile wysiłku to wymaga?**
- **czy wskaźnik można dobrać tak, aby ukazywał istniejące niedociągnięcia?**
- **czy wskaźnik można dostosować tak, aby rozszerzyć jego wykorzystanie?**

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

Pierwsza burza mózgów owocuje zazwyczaj bardzo długą listą KPI. Jeśli tak się nie dzieje, to najprawdopodobniej w dyskusji nie wzięto pod uwagę wszystkich aspektów programu bezpieczeństwa. Kolejne iteracje, zgodnie z powyższymi wytycznymi, mają jednak znacząco skrócić tę listę. Te wskaźniki, które zostaną zachowane powinny być skutecznym i wydajnym sposobem na badanie sukcesu programu bezpieczeństwa.

Nie ma uniwersalnego zestawu mierników KPI, bo każda organizacja jest inna i różne mogą być cele programów bezpieczeństwa. Ustanowione wskaźniki powinny odzwierciedlać nasze priorytety, obejmować pełny zakres SecOps i mieć realny wpływ na program bezpieczeństwa naszej organizacji.

CO SPRAWIA, ŻE DANY KPI MOŻE BYĆ UZNANY ZA SKUTECZNY? JAK WE WŁAŚCIWY SPOSÓB MIERZYĆ KPI?

Kluczowe wskaźniki wydajności powinny być mierzalne, czyli przedstawiać konkretne wartości oraz porównywalne, co oznacza, że wyniki kolejnych pomiarów będą różnić się między sobą w zauważalnym stopniu. Optymalnie dobrane KPI powinny zachowywać zgodność z kryteriami „SMART" (Simple, Measurable, Actionable, Relevant, Time Based), czyli być:

- **Proste: łatwe do zmierzenia i równocześnie mające bezpośrednie przełożenie na program bezpieczeństwa.**
- **Mierzalne: ilościowo lub jakościowo. Wszystkie KPI powinny być mierzalne w konkretny i konsekwentny sposób.**
- **Przydatne dla decydentów: celem KPI powinno być dostarczanie wyników służących do podejmowania decyzji w oparciu o realne dane.**
- **Istotne: o dużym znaczeniu dla funkcjonowania programu bezpieczeństwa. Kluczowe wskaźniki wydajności muszą mieć bezpośrednie powiązanie z funkcjonowaniem SOC.**
- **Osadzone w czasie: mają służyć do pokazania, jak efektywność zespołu lub operacji zmienia się w czasie.**

KPI powinny obejmować serce i duszę programu operacji bezpieczeństwa i oddawać precyzyjnie jego charakter. Dlatego właśnie w procesie wyboru KPI warto stosować kryteria SMART.

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

JAK UPEWNIĆ SIĘ, ŻE WYBRANO ODPOWIEDNIE KLUCZOWE WSKAŹNIKI WYDAJNOŚCI?

W zasadzie jedynym aspektem oceny danego KPI jest odpowiedź na pytanie czy umożliwia on śledzenie ważnych elementów sukcesu programu bezpieczeństwa. Aby upewnić się czy kluczowe wskaźniki efektywności są odpowiednie dla naszej organizacji warto rozważyć następujące kwestie:

- **Czy wybrane KPI śledzą istotne informacje dotykające istoty operacji bezpieczeństwa w organizacji?**
- **Czy KPI dostarczają informacje nieodgrywające istotnej roli w operacjach bezpieczeństwa organizacji?**
- **Czy KPI są stosunkowo łatwe do obliczenia, zrozumienia i zaraportowania?**
- **Ile dodatkowej pracy trzeba włożyć w wyznaczenie i obserwowanie KPI?**

Takie podejście jest najlepszym sposobem określenia jakości wybranych kluczowych wskaźników efektywności. KPI mają na bieżąco ilustrować stan najważniejszych operacji i nie powinny kierować uwagi na aspekty poboczne. Jeśli ustawione wskaźniki nie dostarczają istotnych informacji o poziomie bezpieczeństwa w organizacji i kierunkach zmian w tym zakresie, to trzeba uznać, że nie są one właściwe i należy je zmienić.

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

JAK WYKORZYSTAĆ SOAR DO POMIARU KPI?

Z założenia system SOAR (Security Orchestration, Automation and Response) służy do radykalnego ulepszania operacji bezpieczeństwa poprzez automatyzację i organizację dużej części codziennych procedur operacji bezpieczeństwa. Dodatkowo jednak SOAR daje możliwość mierzenia informacji istotnych przy podejmowaniu taktycznych i strategicznych decyzji dotyczących bezpieczeństwa. Dlatego tak kluczowe jest wykorzystanie SOAR do pomiaru KPI.

Przykładowo rozwiązanie DFLabs IncMan SOAR zapewnia:

- **świadomość sytuacyjną aktualnego stanu operacji bezpieczeństwa;**
- **optymalizację operacji bezpieczeństwa i działań responsywnych oraz analizę porównawczą;**
- **analizę ponad 140 prekonfigurowanych wskaźników KPI dostępnych z poziomu pulpitu nawigacyjnego;**
- **mierzenie wszystkich faz przepływu pracy w procesie odpowiedzi na incydent w celu umożliwienia analitykom optymalizacji wydajności.**

SOAR dostarcza w czasie rzeczywistym dane, które mogą pomóc w ocenie i optymalizacji operacji bezpieczeństwa, dlatego warto go wykorzystać do śledzenia najważniejszych wskaźników KPI.

Orion Instruments Polska jest doświadczonym dostawcą systemów oraz usług z zakresu SIEM i SOAR.

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar