Orion
Instruments Polska

WSKAŹNIKI KPI W OPERACJACH BEZPIECZEŃSTWA I ZARZĄDZANIU INCYDENTAMI cz. 1

Kluczowe wskaźniki efektywności (KPI – Key Performance Indicators) wykorzystywane są przede wszystkim do pomiaru stopnia realizacji operacyjnych i strategicznych celów organizacji. Każda organizacja definiuje swój własny zestaw KPI i dotyczy to także operacji cyberbezpieczeństwa, ponieważ ustanowienie właściwych wskaźników daje zespołom SOC (Security Operations Center) możliwość oceny skuteczności wdrożonego programu bezpieczeństwa. Pierwszym krokiem do ustalenia kluczowych wskaźników efektywności powinna być identyfikacja najważniejszych celów programu operacji bezpieczeństwa. Kolejnym – wybór wskaźników KPI. Istotne jest przy tym, aby zdefiniować optymalne wskaźniki i wybrać odpowiednią ich liczbę.

W niniejszym artykule przedstawiamy próbę odpowiedzi na pytania nurtujące kadrę zarządzającą operacjami bezpieczeństwa:

- **Jakie znaczenie dla operacji bezpieczeństwa mają KPI?**
- **Jak zdefiniować swoje własne KPI?**
- **Na jakich wskaźnikach koncentrują się analitycy operacji bezpieczeństwa?**
- **Jakie KPI należy ustanowić?**
- **Ile mierników KPI ustanowić?**
- **Co sprawia, że dany KPI może być uznany za skuteczny?**
- **Jak we właściwy sposób mierzyć KPI?**
- **Jak upewnić się, że wybrano odpowiednie i optymalne KPI?**
- **Jak wykorzystać platformę SOAR do pomiaru KPI?**
- **Dla których elementów programu bezpieczeństwa warto wyznaczyć KPI?**
- **Jakie są kluczowe ryzyka?**
- **Jak skuteczny jest proces wykrywania zagrożeń?**
- **Jak skuteczny jest proces mitygacji incydentów?**
- **Jak wykorzystać KPI do optymalizacji procesów?**
- **Jak wykorzystać KPI do optymalizacji prac analitycznych?**
- **Jak wykorzystać KPI do optymalizacji obciążenia pracą?**
- **Czy program bezpieczeństwa organizacji będzie działać poprawnie bez ustanowionych kluczowych wskaźników wydajności?**

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

JAKIE ZNACZENIE DLA OPERACJI BEZPIECZEŃSTWA MAJĄ KPI?

Większość zespołów operacji bezpieczeństwa nie stosuje tradycyjnego podejścia do KPI, które polega na sprawdzaniu czy osiągnięto zamierzony cel. Skupiają się raczej na nieustannej obserwacji wskaźników wydajności w czasie i tym samym obserwują pozytywne i negatywne trendy w operacjach bezpieczeństwa oraz rozpoznają niepożądane wzorce.

Przykładami wykorzystania KPI w SOC może być:

- **wyszukiwanie powtarzających się wzorców w celu rozpoznania potencjalnych ataków i złośliwych działań;**
- **ocena obciążenia pracą członków zespołu i ogólna analiza jego wydajności;**
- **analiza czasu potrzebnego do wykrycia i obsługi cyberataków;**
- **analiza trafności alertów fałszywie dodatnich i fałszywie ujemnych.**

Wybór kluczowych wskaźników efektywności operacji bezpieczeństwa zależy przede wszystkim od tego co dany SOC chce osiągnąć. Każda organizacja może mieć inny sposób mierzenia swojego sukcesu w zależności od przyjętych priorytetów, co oznacza indywidualny zestaw kluczowych wskaźników wydajności. Istotne jest jednak to, że tylko optymalnie dobrane KPI mogą przyczyniać się do nieustannego wspierania i wzmacniania operacyjnych programów bezpieczeństwa.

JAK ZDEFINIOWAĆ SWOJE WŁASNE KPI?

Jeśli organizacja wie, co chce osiągnąć poprzez wdrożenie programu operacji bezpieczeństwa, to można stosunkowo szybko określić bazowe KPI.

Jeśli organizacji zależy na:

- **ochronie wrażliwych danych,**
- **zmniejszeniu ilości fałszywych alarmów zakłócających wydajność zespołu SecOps,**
- **zwiększeniu wydajności procesu przepływu prac,**
- **zoptymalizowaniu średniego czasu potrzebnego na wykrycie i usunięcie rzeczywistych zagrożeń,**

to warto ustalić dla każdego aspektu poziomy odniesienia i badać w jakim stopniu osiąga się założone cele. Ważne jest, aby wszystkie wybrane KPI były odpowiednie dla danej organizacji, co należy potwierdzić w trakcie szczegółowej oceny programu operacji bezpieczeństwa. Istotne jest też, aby po dokonaniu wyboru wskaźników, ponownie przejrzeć program bezpieczeństwa pod kątem tego, czy dany miernik pozwoli nam uzyskać informację, której oczekujemy.

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

PRZYKŁADOWE KLUCZOWE WSKAŹNIKI WYDAJNOŚCI, NA KTÓRYCH KONCENTRUJĄ SIĘ ANALITYCY OPERACJI BEZPIECZEŃSTWA

Mimo, że każda organizacja inaczej definiuje swój sukces to większość zespołów SOC i analityków bezpieczeństwa śledzi następujące kluczowe wskaźniki efektywności:

- **ilość błędów uwierzytelnienia**
- **ilość naruszeń polityk**
- **czas potrzebny na rozwiązanie błędów określonej klasy**
- **średni koszt jednego incydentu**
- **ilość zdarzeń złośliwego oprogramowania w jednostce czasu**
- **ilość zdarzeń phishingowych w zadanym okresie czasu**
- **ilość wykorzystanych podatności**
- **średni czas poświęcany przez analityka na zbadanie incydentu**
- **procent niepowodzenia phishingu**
- **liczba wykrytych fałszywych alarmów**
- **liczba monitorowanych urządzeń**
- **całkowita ilość zdarzeń**

Kolejność powyższych wskaźników jest przypadkowa i nie oznacza, że organizacja powinna się skoncentrować tylko na nich i w takim właśnie porządku. W świecie bezpieczeństwa cybernetycznego dostępnych jest bardzo wiele kluczowych wskaźników efektywności, a co tydzień powstają nowe.

Rosnąca ilość dostępnych KPI w zakresie bezpieczeństwa cybernetycznego nie powinna jednak odrywać organizacji od pierwotnego celu ustanowienia tych mierników, czyli przede wszystkim od monitorowania, pomiaru i poprawy wydajności cyberbezpieczeństwa.

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