Orion
Instruments Polska

WSKAŹNIKI KPI W OPERACJACH BEZPIECZEŃSTWA I ZARZĄDZANIU INCYDENTAMI cz. 3

DLA KTÓRYCH ELEMENTÓW PROGRAMU BEZPIECZEŃSTWA WARTO WYZNACZYĆ KPI?

Warto skupić się na sześciu kluczowych obszarach programu bezpieczeństwa. Należy uwzględnić podstawowe ryzyka (1), bo to one wyznaczają zakresy operacji bezpieczeństwa. Nie mniej istotna jest ocena wykorzystywanej technologii wykrywania (2) i mitygacji (3) – bowiem technologie te są głównym źródłem informacji o wykrytych zdarzeniach i pierwszym etapem postępowania z incydentami. Równie ważne jest obserwowanie obciążenia/zaangażowania analityków (4) i ich umiejętności (5), tak aby maksymalnie wykorzystać potencjał zespołu. Z kolei ocena procedur i procesów (6) daje szanse na ich ulepszanie. W ten sposób obejmujemy istotne aspekty technologii, ludzi i procesów z uwzględnieniem perspektywy ryzyk.

KLUCZOWE RYZYKA

Jakie są kluczowe ryzyka dla organizacji? Jest ich wiele, a budżet zawsze jest ograniczony. Podejmowanie decyzji, które z ryzyk zostaną zaadresowane, a które zaakceptowane jest żmudnym procesem. Należy zatem wybrać KPI dla kluczowych ryzyk. Warto również rozważyć te, które mają szanse dostarczyć danych przydatnych w ogólnym szacowaniu ryzyka. Przykładowe mierniki w tym zakresie to:

- **całkowita ilość zdarzeń bezpieczeństwa**
- **liczba zdarzeń przypadająca na urządzenie**
- **liczba zdarzeń na usługę lub aplikację**
- **liczba zdarzeń na konto/użytkownika**
- **liczba zdarzeń w danej lokalizacji**
- **liczba zdarzeń przypadająca na źródło zdarzeń/technologię wykrywania**
- **ilość fałszywych trafień z podziałem na technologie.**

SKUTECZNOŚĆ WYKRYWANIA

Jak skuteczne są wykorzystywane technologie ochrony i wykrywania? Jak dużo jest sytuacji generujących fałszywe alerty lub zdarzeń, które nie wygenerowały alarmu mimo, że wystąpiło zagrożenie? Nieskuteczne technologie ochrony i wykrywania zwiększają prawdopodobieństwo pominięcia incydentu bezpieczeństwa i równocześnie zmuszają analityków do wykonywania dodatkowych manualnych analiz. Wyznaczenie mierników KPI w tym obszarze daje szanse na identyfikację odstępstw, strojenie aktualnych lub dołożenie dodatkowych technologii ochrony i wykrywania. Możemy tu wykorzystać mierniki takie jak:

- **Ilość zdarzeń na urządzenie. Ile zdarzeń generuje każde urządzenie? Czy pewne urządzenia mają skłonność do przysparzania problemów zwiększając tym samym ryzyko? Które urządzenia mają tendencję do generowania alertów fałszywie dodatnich? Warto wykorzystać pomiar ilości zdarzeń na urządzenie w skali dnia/miesiąca/roku, jak również z podziałem na systemy operacyjne czy typy urządzeń.**

- **Ilość zdarzeń przypadających na usługę lub aplikację. Ile zdarzeń generuje każda usługa/aplikacja? Które usługi/aplikacje mają tendencję do sprawiania kłopotów? Które dają najwięcej fałszywych alarmów? Przydatne są tu mierniki liczby zdarzeń dla kluczowej usługi/aplikacji.**

- **Ilość zdarzeń przypadających na konto lub użytkownika odpowie na pytanie ile zdarzeń jest związanych z danym kontem, a także czy pewni użytkownicy są skłonni do ryzykownych zachowań, które przyczyniają się do wzrostu ryzyka.**

- **Ilość fałszywych alarmów – czy jest akceptowalna? Czy można ją zredukować? Warto sprawdzić ilość fałszywych trafień w perspektywie godziny/dnia/miesiąca/roku. Jaka jest procentowa wartość fałszywych alarmów w stosunku do wszystkich zdarzeń?**

- **Czas wykrycia zdarzenia bezpieczeństwa – ile wynosi i czy można go skrócić? Pomiar każdego zdarzenia, jak również średni czas przypadający na technologię lub typ zdarzenia.**

- **Źródło zdarzenia – które technologie wykrywania są mniej, a które bardziej skuteczne, które z nich generują więcej fałszywych alarmów, jak często zdarza się, że użytkownik lub analityk wykrywa zdarzenie przed pojawieniem się alarmu?**

EFEKTYWNOŚĆ MITYGACJI

Jak skuteczne ograniczać skutki incydentów? Każdy incydent wymaga powstrzymywania, dlatego należy ustanawiać mierniki KPI również do oceny tego procesu. Podobnie jak w odniesieniu do technologii ochrony i wykrywania, KPI mogą być wykorzystywane do poprawy efektywności procesu mitygacji, tym bardziej, że mało skuteczne technologie powstrzymywania mogą dawać gorsze rezultaty niż mitygacja manualna. Wykorzystanie KPI do pomiaru wydajności powstrzymywania daje szanse na znalezienie luk, które mogą zostać usunięte poprzez wprowadzenie dodatkowych lub modyfikację aktualnie wykorzystywanych technologii mitygacji.

- **Czas rozwiązania – ile czasu zajmuje rozwiązanie faktycznego zdarzenia bezpieczeństwa, czy można skrócić ten czas poprzez modyfikację procesów i procedur, czy mogą pomóc dodatkowe szkolenia lub dodatkowy personel? Można również mierzyć średni czas rozwiązania w podziale na typ zdarzenia czy strategię rozwiązania.**

Orion
Instruments Polska

SKUTECZNOŚĆ PROCESÓW

Procesy i procedury są podstawą działania zespołów bezpieczeństwa, ale nie da się ich ustanowić raz a dobrze i raz na zawsze. Skuteczne i wydajne zarządzanie incydentami wymusza nieustanne doskonalenie programu bezpieczeństwa poprzez ocenę stanu i wprowadzanie korekt. Nieoptymalne procesy i procedury frustrują analityków działających według kiepskich scenariuszy, co negatywnie przekłada się na proces obsługi incydentów. Rozsądnym wydaje się więc wykorzystanie KPI do mierzenia na bieżąco wydajności procesów i procedur, tak by mieć pewność, że są one optymalne i skuteczne w odniesieniu do szerokiego spektrum incydentów.

- **Czas do wykrycia/rozwiązania – ile czasu potrzeba na wykrycie/rozwiązanie zdarzenia bezpieczeństwa; warto mierzyć również średni czas dla danej technologii i typu zdarzenia.**

- **Czas identyfikacji fałszywych trafień, czyli ile czasu zajmuje określenie, że zdarzenie jest fałszywym alarmem; czy analitycy nie spędzają zbyt wiele czasu na badaniu fałszywych trafień? Można mierzyć średni czas identyfikacji dla każdej technologii lub typu zdarzenia.**

- **Poziom eskalacji czyli np. ile zdarzeń jest eskalowanych i do którego poziomu, czy zdarzenia nie są eskalowane zbyt szybko/późno, czy można poprawić proces eskalacji. Można mierzyć średnią ilość zdarzeń na poziom, poziom eskalacji dla danego typu zdarzenia/technologii, średni czas eskalacji.**

UMIEJĘTNOŚCI ANALITYCZNE

Czy posiadany zestaw umiejętności analityków odpowiada aktualnym potrzebom organizacji? Brak umiejętności może prowadzić do zmniejszenia efektywności procesu zarządzania incydentami i tym samym do zwiększenia ryzyka dla organizacji. Warto wykorzystać KPI do pomiaru faktycznych umiejętności analityków w celu identyfikacji potrzeby zatrudnienia dodatkowych osób lub przeszkolenia personelu, co zaowocuje wyższą gotowością organizacji do zarządzania incydentami.

- **Czas identyfikacji fałszywego trafienia, ile czasu trwa określenie że alarm jest nietrafiony? Czy analitycy nie spędzają zbyt dużo czasu na badaniu fałszywych alarmów? Czy dodatkowe szkolenie może pomóc? Mierzenie czasu/średniego czasu identyfikacji przypadającego na technologię czy typ zdarzenia.**

- **Ilość przypisanych analityków – ilu analityków przypisuje się do zdarzenia, czy jest to właściwa liczba? Czy przypisanie do jednego zdarzenia zbyt wielu analityków nie oznacza, że pozostałe zdarzenia nie mają zapewnionej właściwej obsługi? Czy zbyt mała ilość dedykowanych analityków nie wynika z braków kadrowych?**

- **Poziom eskalacji – ile zdarzeń jest eskalowanych, czy eskalacja odbywa się za szybko czy za późno, czy można ulepszyć proces eskalacji tak, aby obsługa incydentów była lepsza? Czy dla każdego poziomu organizacja ma wystarczający poziom umiejętności? Można mierzyć średnią ilość zdarzeń dla każdego poziomu, obserwować zmiany w czasie, badać średni czas do eskalacji i poziom eskalacji z uwzględnieniem typu zdarzenia i technologii.**

Orion
Instruments Polska

OBCIĄŻENIE PRACĄ

Czy analitycy są odpowiednio dociążeni? Przeciążeni chadzają na skróty lub umykają im istotne wskaźniki incydentów. Mogą też rozważać wykorzystanie swojej wiedzy, umiejętności i doświadczenia gdzie indziej. Warto zatem wykorzystać wskaźniki KPI do równoważenia obciążenia personelu.

- **Ilość monitorowanych urządzeń, w tym również ilość urządzeń przypadających na analityka oraz obserwowanie zmiany tego wskaźnika w czasie.**
- **Ilość przypisanych analityków, czyli średnia liczba zaangażowanych analityków dla każdego zdarzenia/typu zdarzenia. Czy to jest właściwa ilość? Zbyt mała może wynikać z braków kadrowych, a zbyt duża może oznaczać, że nie ma kto zająć się zdarzeniami czekającymi w kolejce.**

CZY PROGRAM BEZPIECZEŃSTWA ORGANIZACJI BĘDZIE DZIAŁAĆ POPRAWNIE BEZ USTANOWIONYCH KLUCZOWYCH WSKAŹNIKÓW WYDAJNOŚCI?

Teoretycznie program bezpieczeństwa organizacji może działać bez wskaźników, ale w praktyce będzie to jak żeglowanie bez steru po wzburzonym morzu. KPI wskazują kluczowe kierunki działania dla operacji bezpieczeństwa. Wyznaczone KPI dotyczą komponentów, które mają największe znaczenie dla programu bezpieczeństwa organizacji. Takie podejście pozwala wszystkim pracownikom zrozumieć jak definiuje się sukces programu bezpieczeństwa.

Próby realizacji programu bezpieczeństwa bez ustawienia KPI zazwyczaj przynoszą efekt przeciwny do zamierzonego. Bez wiedzy jak mierzyć sukces i przy braku zrozumienia, którą ścieżką powinna podążać organizacja, nie będziemy wiedzieli, które obszary należy poprawić. I jest to najgorsza możliwa droga dla organizacji, która powinna być nastawiona na stałe podnoszenie poziomu swojego bezpieczeństwa.

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