Orion
Instruments Polska

JAK SKUTECZNIE WDROŻYĆ SOAR?

Każda organizacja przed rozpoczęciem oceny dowolnej platformy klasy SOAR powinna przeanalizować swój obecny program bezpieczeństwa oraz precyzyjnie zdefiniować problemy, które wymagają rozwiązania.

DEFINIOWANIE PROBLEMU PRZED WDROŻENIEM SOAR

Przed oceną potencjalnego rozwiązania SOAR i jego dostawcy, należy odpowiedzieć sobie na kilka zasadniczych pytań. Odpowiedzi te powinny stać się głównymi kryteriami procesu wdrożenia – od jego wstępnej oceny aż do zakończenia projektu.

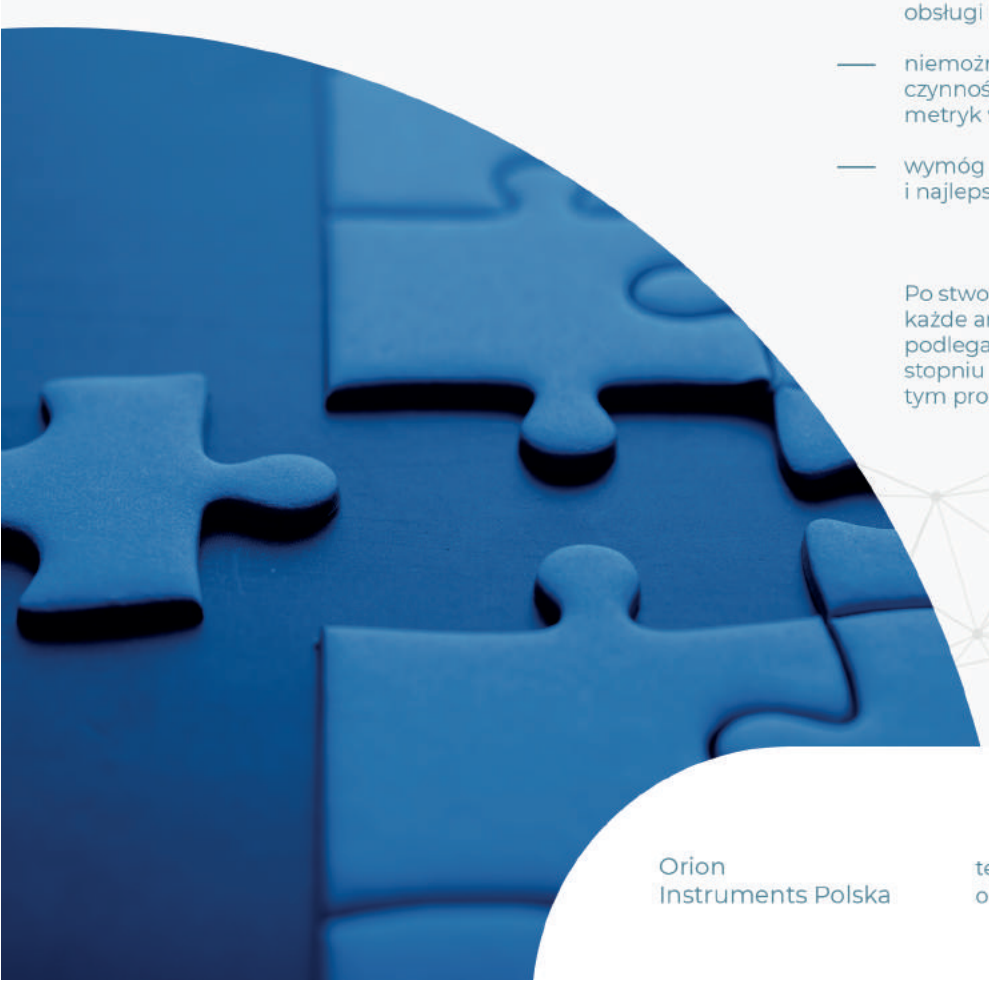
Jeśli pytania i odpowiedzi nie zostaną zdefiniowane na początku całego procesu to prawdopodobnie osiągnięte wyniki implementacji wybranego rozwiązania będą różne od oczekiwanych.

JAKI PROBLEM STARAMY SIĘ ROZWIĄZAĆ?

SOAR może rozwiązać różne problemy, ale ważne jest aby określić, które z nich są najważniejsze dla naszej organizacji. Firmy podają najczęściej następujące powody planowanego wdrożenia SOAR:

- zbyt wiele alarmów do obsłużenia przez zespół bezpieczeństwa
- brak wykwalifikowanych specjalistów,
- rutynowe, żmudne procesy absorbujące większość czasu operatorów SOC
- brak odpowiedniej funkcjonalności zarządzania incydentami
- nieudokumentowane lub niespójne procesy obsługi incydentów
- niemożność lub uciążliwość rejestrowania czynności i generowania związanych z nimi metryk w SOC
- wymóg przestrzegania przepisów, norm i najlepszych praktyk

Po stworzeniu indywidualnej listy problemów każde analizowane rozwiązanie powinno podlegać ocenie pod kątem tego, w jakim stopniu będzie ono w stanie zaradzić tym problemom.



Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

WYZNACZANIE CELÓW PRZED OCENĄ SOAR. JAK BĘDZIE MIERZONY SUKCES?

Odpowiedź na to pytanie jest ściśle związana z poprzednim zagadnieniem. Należy wprowadzić co najmniej jeden miernik sukcesu dla każdego zidentyfikowanego problemu. Wszystkie mierniki powinny być obiektywne i łatwe do wyznaczenia. Jeśli np. jednym z problemów jest nieakceptowalnie długi średni czas odpowiedzi na alert bezpieczeństwa, miernikiem sukcesu będzie skrócenie tej wartości.

Po określeniu tego co mierzymy, należy dla każdego współczynnika zdefiniować wartość, którą chcemy osiągnąć. Innymi słowy, jeśli wdrożymy dane rozwiązanie, to czego oczekujemy? Aby skutecznie zmierzyć sukces, cele powinny być jasno określone, mierzalne, osiągalne, istotne i osadzone w czasie czyli spełniać kryteria określane jako SMART (Specific, Measurable, Attainable, Relevant and Time Based). Jest bardzo prawdopodobne, że cele, które nie spełniają wszystkich powyższych kryteriów, nie zapewnią sukcesu wdrożenia. Przykładowo, celem może stać się skrócenie średniego czasu reakcji na alerty bezpieczeństwa o 50% w ciągu najbliższego roku.

Oto kilka ważnych pytań które należy postawić przed rozpoczęciem analizy i oceny rozwiązań SOAR:

- **Jakie są najważniejsze kamienie milowe tego projektu?**
- **Jaka wartość dodana dla organizacji ma wynikać z powiązania platformy SOAR z wykorzystywanymi już w organizacji rozwiązaniami bezpieczeństwa?**
- **Jakie funkcje są bezwzględnie wymagane, a jakie byłyby pożądane?**
- **Które integracje są niezbędne, a które będą stanowić istotne uzupełnienie?**
- **Jakie są wymagania techniczne, a jakie wdrożeniowe?**
- **Jaki jest budżet projektu?**

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

Gdy odpowiedzi na powyższe pytania zostaną dokładnie określone, udokumentowane i udostępnione całemu zespołowi oceniającemu, będzie on gotów do rozpoczęcia oceny różnych rozwiązań SOAR i wyboru tego, które zagwarantuje najlepsze rozwiązanie problemów i zaspokojenie potrzeb organizacji.

Mamy nadzieję, że powyższe informacje będą stanowiły istotne wskazówki przy podejmowaniu decyzji, którą platformę SOAR wybrać i jak dostosować ją do strategii danej organizacji. Mimo bowiem, że dostępne na rynku rozwiązania SOAR istotnie różnią się od siebie, to jednak istnieją funkcjonalności, wymienione powyżej, które powinny być uwzględniane jako standard przy ocenie narzędzi tej klasy.

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