# Kompletny **SOAR** interpretuje rzeczywisty kontekst

Przykładem kompletnego rozwiązania **SOAR** jest SECUREVISIO polskiej firmy esecure
To rozwiązanie na tyle udane i skuteczne, że może stanowić standard dla rozwiązań **SOAR**, który powinien zawierać:

**MAPOWANIE:**
tworzenie rzeczywistej mapy logicznej powiązań procesów i systemów.

**KOMUNIKACJĘ:**
klarowna komunikacja kwestii bezpieczeństwa, także z właścicielem procesu.

**PRIORYTETYZACJĘ:**
opis mapy przez pryzmat charakteru danych, procesów biznesowych i szacunku ryzyka.

**ZINTEGROWANE ZARZĄDZANIE:**
incydentami i podatnościami w skali całej organizacji z poziomu jednego panelu sterowania gromadzącego niezbędne źródła informacji.


## REJESTRACJA I KLASYFIKACJA ZDARZENIA W 15 SEKUND

Nowe zdarzenie zostaje zarejestrowane z nadanym priorytetem i podlega triażowi: w oparciu o analizę szerszego kontekstu i dodatkowych informacji może być uznane za incydent. Taki proces zajmuje **SecureVisio** 10-15 sekund, podczas gdy ręczne zebranie przez dział bezpieczeństwa informacji z różnych źródeł i wykrycie powiązań, o ile by się powiodło, musiałoby zająć w dużej organizacji około tygodnia.

## KLASYFIKACJA INCYDENTU

Incydent jest następnie analizowany pod kątem możliwości naruszenia bezpieczeństwa, zakresu skutków incydentu i jego klasyfikacji.

## KOMUNIKACJA BEZPIECZEŃSTWA

W tym czasie prowadzona jest już komunikacja z właścicielem procesu biznesowego, którego dotykają skutki incydentu.

## RZECZYWISTA ANALIZA RYZYKA

Wyróżnikiem **SecurVisio** jest obiektywna priorytetyzacja biznesowa incydentów i szacowanie ryzyka. W odróżnieniu od np. „klasycznych" rozwiązań SIEM, priorytet nie jest arbitralnym wskazaniem, tylko wynika z podejścia typu Business Impact Analysis – dokonanej automatycznie, w oparciu o działające rozwiązanie. Zarządzanie incydentami musi określić, jakiego systemu dotyczy incydent, jakich procesów biznesowych, czy zawierają one dane wrażliwe, czy (jakie) posiadają luki bezpieczeństwa, czy korespondują z tym jakieś inne incydenty bezpieczeństwa, mogące w sumie składać się w szerzej zakrojony atak albo dawać przesłanki prawdziwych intencji atakujących. Szacujemy wówczas rzeczywiste ryzyko i odgadujemy rzeczywiste intencje cyberprzestępców.

## REAKCJA NA INCYDENT

Reakcja następuje w oparciu o zebraną wiedzą, w tym na temat skutków naruszenia bezpieczeństwa. **SecureVisio** udostępnia scenariusz działań, stosownie do klasyfikacji incydentu i naruszenia, np. „złośliwy kod", „fraud" czy „zbieranie informacji". Wybrany scenariusz uruchamia odpowiednie, gotowe narzędzia.

## WYKRYWANIE ZACHOWAŃ ATYPOWYCH

**SecureVisio** korzystając np. z technologii UEBA identyfikuje nietypowe zachowania procesów, aplikacji, urządzeń. Wcześniejsza klasyfikacja i mapowanie pozwolą operatorom zorientować się, co jest właściwym celem zidentyfikowanego ataku i szybko zareagować.

## MAPOWANIE RZECZYWISTEGO KONTEKSTU BIZNESOWEGO

**SOAR SecureVisio** buduje logiczną architekturę bezpieczeństwa, strefy i obszary na podstawie logów firewalli. Obiektywnie odtworzona logiczna architektura jest następnie definiowana i opisywana pod kątem rozmieszczenia danych osobowych, finansowych, itd. Celem takiego podejścia jest oczywiście zarządzanie bezpieczeństwem w kontekście biznesowym. To wymóg i założenie nowoczesnego cyberbezpieczeństwa zawarty w regulacjach i standardach. Zarządzanie incydentami i podatnościami nie może się dokonywać w oderwaniu od procesów biznesowych, których dotyczą, w oderwaniu od oceny wpływu na biznes. Ta cecha SecureVisio pozwala w pełni zrozumieć zdarzenia bezpieczeństwa, interpretować, co się naprawdę dzieje, kiedy pojawiają się incydenty i nietypowe zachowanie.

## DOKUMENTACJA BEZPIECZEŃSTWA SOAR

**SecureVisio** automatycznie dostarcza dokumentację niezbędną w dopełnieniu reguł i regulacji nowoczesnego cyberbezpieczeństwa. Pozwala spełnić wymogi RODO w zakresie metodyki i dokumentacji szacowania ryzyka zgodnie z ISO 27005, które rekomenduje ENISA, oraz zdolności szybkiego przekazywania informacji o incydentach w myśl ustawy o Krajowym Systemie Cyberbezpieczeństwa.