SOAR – co zarząd firmy wiedzieć powinien

Gartner pisząc w roku 2017 o SOAR (Security Orchestration, Automation and Response) podkreślił, iż platforma taka musi łączyć trzy technologie: orkiestrację i automatyzację bezpieczeństwa (Security Orchestration and Automation – SOA), platformę reagowania na incydenty bezpieczeństwa (Security Incident Response Platform – SIRP) oraz platformę analizy zagrożeń (Threat Intelligence Platform – TIP).

Gartner zdefiniował SOAR jako:

„Zespół technologii, które umożliwiają organizacjom zbieranie danych bezpieczeństwa i alertów z różnych źródeł. SOAR umożliwia analizę i segregację incydentów przy wykorzystaniu kombinacji zasobów ludzkich i maszynowych. Pomaga to definiować, ustalać priorytety i zarządzać działaniami reagowania na incydenty zgodnie ze standardowym obiegiem pracy ”.

Poniżej zaprezentowane zostały wybrane, kluczowe dla kadry zarządzającej zagadnienia dotyczące rozwiązania SOAR:

- **Jakie problemy może rozwiązać wdrożenie SOAR?**
- **Czy SOAR może zmniejszyć zatrudnienie w SOC i / lub być źródłem oszczędności w firmie?**
- **Co jest wyróżnikiem SOAR i dlaczego platforma ta nie zastępuje działających w organizacji narzędzi bezpieczeństwa?**
- **Co w zespołach operacji bezpieczeństwa można faktycznie zautomatyzować dzięki wdrożeniu SOAR?**
- **Czy można wdrożyć automatyzację przed zdefiniowaniem schematu przepływu pracy lub procesu?**
- **Jaką trwałą wartość daje skutecznie wdrożony system SOAR?**
- **Które z nie realizowanych obecnie operacji i procesów staną się możliwe po wdrożeniu SOAR?**
- **Jakie wnioski można wyciągnąć z wdrożenia SOAR i jakie wyzwania stają przed dostawcami takiego rozwiązania?**

Jakie problemy może rozwiązać wdrożenie SOAR?

SOAR jest zcentralizowaną platformą zarządzania operacjami bezpieczeństwa obejmującą zespoły, procesy i technologie. Dzięki SOAR zespoły SOC otrzymują możliwość normalizacji przepływów pracy – zarówno przebiegających automatycznie, jak i sterowanych decyzjami ludzkimi. Analitycy mogą konsekwentnie i metodycznie wykonywać te same zadania w sposób mierzalny, zgodnie z ustandaryzowanymi procesami. SOAR umożliwia skalowanie różnych przepływów pracy (manualnych i zautomatyzowanych), a także zapewnia ich śledzenie i rozliczalność, co bez wdrożenia systemu tej klasy mogło być trudne lub wręcz niemożliwe.

Jednym z obszarów, w których rozwiązanie SOAR może być szczególnie pomocne, jest zarządzanie przypadkami. Zazwyczaj zespoły operacji bezpieczeństwa wykorzystują systemy biletowe, które już wcześniej były używane w organizacji, ale za rozwiązania te odpowiadają zazwyczaj inne działy np. IT.

Dlatego też zespoły SOC postrzegają SOAR jako źródło danych związanych z obsługą incydentu, które umożliwi im śledzenie przypadków w sposób bardziej dostosowany do ich potrzeb i zdefiniowany zgodnie z ich wymaganiami. Zapewnia to nie tylko specjalizację i skupienie się na incydentach, ale umożliwia też zespołowi bezpieczeństwa korzystanie z własnej specjalistycznej platformy, która może być odseparowana od reszty organizacji, co jest istotne z punktu widzenia zgodności.

Typowy przypadek użycia to powiązanie SOAR z systemem SIEM; inne przypadki są często bagatelizowane. Natomiast funkcjonalność platformy SOAR można łatwo rozszerzyć poza integrację z SIEM i nie ograniczać jej możliwości tylko do współpracy z rozwiązaniem tej klasy. Jednym z przykładów jest ochrona fizyczna, dla której można opracować schematy postępowania związane z monitorowaniem dostępu personelu do szczególnie chronionych stref w organizacji. Jeśli wykryta zostanie nietypowa aktywność, zostanie ona natychmiast oznaczona do celów dalszej analizy. Elastyczność w zastosowaniu SOAR w różnych obszarach organizacji może być jednak znacznie szersza. Dziś rozwiązanie to przynosi korzyści nie tylko centrum operacji bezpieczeństwa, ale całej organizacji i jest to jeden z unikalnych aspektów SOAR, oprócz automatyzacji i orkiestracji.

Czy SOAR może zmniejszyć zatrudnienie w SOC i / lub być źródłem oszczędności w firmie?

Bardzo rzadko zdarza się słyszeć, że w zespole operacji bezpieczeństwa (SOC) pracuje zbyt wiele osób. Większość organizacji, które planują lub już wdrożyły SOAR, robi to ponieważ musi zwiększyć wydajność zespołu SOC. SOAR powinien być w tym kontekście postrzegany jako multiplikator zasobów umożliwiający obecnemu zespołowi realizację większej ilości zadań bez zwiększania nakładów, a zatem pozwalający na zwiększenie efektywności i wydajności całego programu bezpieczeństwa firmy.

SOAR stanowi istotną wartość dla wszystkich przedsiębiorstw, które trapi problem niedoboru wysokokwalifikowanych specjalistów z dziedziny cyberbezpieczeństwa. Jest to dotkliwie odczuwalne zwłaszcza w firmach typu MSSP (Managed Security Service Provider) ze względu na ilość wspieranych przez nie klientów. SOAR może tu znacząco zaoszczędzić czas i pieniądze, zwiększając wydajność zespołu bezpieczeństwa poprzez automatyzację żmudnych i powtarzalnych zadań oraz orkiestrację narzędzi i procesów. Jednak nawet wykorzystanie w SOAR uczenia maszynowego i sztucznej inteligencji nie zastąpi w procesie obsługi incydentów pracy analityków.

Co jest wyróżnikiem SOAR i dlaczego platforma ta nie zastępuje działających w organizacji narzędzi bezpieczeństwa?

Organizacja musi być świadoma problemów, które próbuje rozwiązać. Musi też zdawać sobie sprawę z jakich technologii i narzędzi obecnie korzysta i ocenić jakie nowe rozwiązania są jej potencjalnie potrzebne. A zatem zespoły bezpieczeństwa powinny dochować należytej staranności przed zakupem i poddać ocenie wiele platform i wielu dostawców, tak aby spełnić indywidualne wymagania organizacji i uwzględnić występujące w niej przypadki użycia.

SOAR nie jest zamiennikiem systemu SIEM, choć może wykonywać niektóre z jego zadań. Istotne jest by pamiętać, iż SOAR został zaprojektowany w celu rozszerzenia możliwości SIEM. Niezależnie od SIEM i innych narzędzi, SOAR pełni w SOC rolę platformy nakładkowej, płynnie orkiestrując wszystkie narzędzia i technologie bezpieczeństwa oraz wspierając podejmowanie kluczowych decyzji.

Co w zespołach operacji bezpieczeństwa można faktycznie zautomatyzować dzięki wdrożeniu SOAR?

SOAR ma szeroki zakres zastosowań, zarówno w operacjach bezpieczeństwa jak i w dziedzinie bezpieczeństwa fizycznego, zarządzaniu podatnościami, czy internetu rzeczy (IoT). Od strony technicznej SOAR ma możliwość automatyzacji wszystkich etapów cyklu życia incydentu, od momentu jego wykrycia aż do fazy remediacji. Organizacje najczęściej automatyzują zbieranie i zestawianie informacji w fazie segregacji incydentów. Typowe przypadki użycia SOAR obejmują analizę phishingu i złośliwego oprogramowania, ale występują też sytuacje, gdy systemy zapobiegające wyłudzeniom (antyfraud) nie są w stanie zautomatyzować ostatniej fazy procesu badania danego przypadku. W tym momencie do akcji wkracza SOAR i w sposób zautomatyzowany kontynuuje działania śledcze.

SOAR staje się coraz powszechniej stosowanym rozwiązaniem, co raz to powstają kolejne, specyficzne przypadki użycia i można go wykorzystać w każdej sytuacji, kiedy wymagana będzie określona reakcja na zagrożenie, w formie decyzji ludzkiej lub realizacji działań zapobiegawczych.

Czy można wdrożyć automatyzację przed zdefiniowaniem schematu przepływu pracy lub procesu?

W większości przypadków właściwe planowanie i przygotowanie jest kluczem do sukcesu i wdrożenie SOAR nie jest tu wyjątkiem. SOAR umożliwia wykorzystanie technologii na bazie już wcześniej istniejących lub precyzyjnie opisanych procesów, dlatego ważne jest, aby organizacja właściwie zdefiniowała te procesy jeszcze przed wdrożeniem platformy SOAR.

SOAR może pomóc w usprawnieniu istniejących procesów i operacji oraz pozwoli na wdrożenie przepływów prac, które byłyby niemożliwe do wykorzystania bez pomocy tej platformy.

Jaką trwałą wartość daje skutecznie wdrożony system SOAR?

Sukces może być mierzony na wiele sposobów i zależy od wielu czynników, w tym między innymi od wielkości i dojrzałości organizacji, a także od przedziału czasu, dla którego dokonywany jest pomiar. Zautomatyzowanie w wyniku wdrożenia SOAR żmudnych i powtarzalnych zadań pozwala analitykom lepiej wykorzystać ich czas pracy na ustalanie priorytetów i skupienie się na zadaniach proaktywnych, takich jak wychwytywanie nowych zagrożeń i prowadzenie analiz oraz rozwiązywanie złożonych problemów. Automatyzacja pozwala również na szybszą segregację i remediację, co podnosi skuteczność zespołu i pozwala na lepsze wykorzystanie talentów jego członków.

Które z nie realizowanych obecnie operacji i procesów staną się możliwe po wdrożeniu SOAR?

Firmom typu MSSP trudno jest efektywnie realizować umowy SLA jeśli wykonują swoje procesy manualnie. SOAR wywarł ogromny wpływ na ten sektor umożliwiając automatyzację, dzięki zastosowaniu playbooków i runbooków. Automatyzacja jest tu o wiele bardziej skuteczna niż procesy manualne w osiąganiu ustalonych kryteriów SLA, zapewnia większą wartość dla klientów i stanowi istotną przewagę konkurencyjną MSSP.

SOAR nie zastępuje istniejących procesów, poprawia jednak ich wydajność i umożliwia szybszą reakcję dzięki automatyzacji, redukując w wielu przypadkach czas realizacji niektórych zadań z godzin do zaledwie kilku minut.

SOAR zapewnia szybkość i skalowalność, a trzeba pamiętać, że niektóre procesy nie dają się skalować ręcznie. Jest to kolejna unikalna funkcja tego rozwiązania.

Jakie wnioski można wyciągnąć z wdrożenia SOAR i jakie wyzwania stają przed dostawcami takiego rozwiązania?

Przy wdrażaniu nowego rozwiązania technologicznego kluczowe jest wykazanie uzyskania wartości dodanej w konkretnym czasie. Dobrą praktyką jest rozpoczęcie implementacji SOAR od wdrożenia już istniejących w organizacji przypadków użycia oraz wprowadzenia automatyzacji do rozwiązywania problemów, takich jak usuwanie konfliktów kompetencyjnych między różnymi zespołami (np. SOC i NOC), wspólne korzystanie z tych samych narzędzi bezpieczeństwa lub dzielenie się wiedzą o zagrożeniach w obrębie całej organizacji. Nowe rozwiązanie może szybciej wykazać swoją wartość, jeśli rezultaty jego działania będą widoczne również dla innych departamentów.

Ważne jest, aby przed rozpoczęciem wdrożenia SOAR zespół SOC zdefiniował procesy, schematy przepływów pracy i scenariusze. Nie mając solidnie opracowanych procesów i procedur, na których można oprzeć projekt organizacje ryzykują, że automatyzacja obejmie niewłaściwe elementy.
Integracja z innymi narzędziami operacyjnymi i departamentowymi jest ważnym czynnikiem pełnego wykorzystania możliwości operacyjnych SOAR. Organizacje coraz częściej stawiają na jakość, a nie tylko na ilość integracji. Rozwiązanie o otwartej architekturze zapewnia możliwość szybkiego wdrożenia nowych integracji, elastyczność w dokonywaniu zmian i kompletność w spełnieniu potrzeb organizacji.

Wdrożenie każdego nowego rozwiązania może być dodatkowym obciążeniem i ważne jest, aby organizacja miała ujednoliconą i nakreśloną od samego początku strategię. Kluczem do sukcesu jest posiadanie szerszej wizji, szerszej strategii i zapewnienie spójności SOAR z ogólną wizją programu bezpieczeństwa całej organizacji.

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