4 kluczowe funkcje rozwiązania SOAR

Chociaż poszczególne cechy i możliwości dostępnych na rynku platform klasy SOAR (Security Orchestration Automation and Response) będą się różnić w zależności od producenta, istnieją pewne kluczowe funkcjonalności, które każdy taki system powinien posiadać. W zależności od unikalnego zestawu potrzeb i wyzwań, przed którymi stoi organizacja, niektóre parametry mogą okazać się ważniejsze niż inne. Poniższy tekst prezentuje cztery zasadnicze funkcje, niezbędne do maksymalnego wykorzystania technologii SOAR.

1. **Elastyczne integracje**

Wraz z rosnącą liczbą dostępnych rozwiązań bezpieczeństwa IT, niezależnie od tego, czy są one tworzone wewnątrz organizacji, nabywane od dostawców zewnętrznych, czy też przybierają formę usług (Security as a Service), każde rozwiązanie SOAR powinno być na tyle elastyczne, aby obsługiwać wiele różnych narzędzi bezpieczeństwa oraz umożliwiać łatwą dwukierunkową integrację z produktami firm trzecich. Metody używane do obsługi takich integracji mogą się różnić, ale powinny one obejmować popularne języki skryptowe, takie jak Perl lub Python, przy wykorzystaniu interfejsów API. Niezależnie jednak od wybranego sposobu tworzenia integracji, powinien on być łatwy w implementacji i prosty w obsłudze.

Dwukierunkowa integracja jest niezwykle istotna dla zapewnienia pełnej automatyzacji i orkiestracji, ale nie jest ona niezbędna dla każdej organizacji. W przypadku niektórych technologii zabezpieczających istotne może być tylko pozyskiwanie danych w celu dalszego ich przetwarzania przez SOAR. Takie jednokierunkowe integracje są zazwyczaj znacznie łatwiejsze do utworzenia niż pełna dwukierunkowa integracja. Platforma SOAR powinna zatem obsługiwać popularne metody pobierania danych, takie jak syslog, połączenia z bazami danych, interfejsy API, wiadomości e-mail i formularze online, a także wspólne standardy danych, takie jak CEF, OpenIOC i STIX / TAXII.

2. **Przetwarzanie przepływów pracy (workflow)**

Jedną z najważniejszych funkcji rozwiązania SOAR jest możliwość automatyzacji i orkiestracji przepływów pracy w celu zmniejszenia obciążeń analityków bezpieczeństwa, zwłaszcza w zakresie powtarzalnych zadań. W związku z tym platforma SOAR musi być w stanie obsługiwać elastyczne metody implementacji przepływów pracy. Istnieją dwa podstawowe sposoby tworzenia takich przepływów w ramach SOAR:

- schematy działania przetwarzane liniowo – **playbooki**
- warunkowe schematy działania – **runbooki**

Ponieważ obie metody mają swoje wady i zalety, a każda z nich może lepiej nadawać się do określonych przypadków użycia, rozwiązanie SOAR powinno zapewniać obsługę tak jednego, jak i drugiego schematu. W obydwu przypadkach implementacja przepływów pracy musi być jednak na tyle elastyczna, aby wspierać niemal każdy proces, który może wymagać skodyfikowania reakcji na zagrożenie. Schematy przepływu pracy powinny przy tym obsługiwać zarówno integracje wbudowane, jak i niestandardowe.

Automatyczne przepływy pracy muszą też umożliwiać analitykom manualne podejmowanie decyzji przed dalszym kontynuowaniem schematu. Zapewnienie opcji przejmowania kontroli nad procesem przez człowieka pozwala na znacznie większą elastyczność i umożliwia kontynuację procesu po podjęciu w danym punkcie decyzji przez analityka.

Budowanie schematu przepływu pracy nie powinno wymagać wysokiego poziomu znajomości języków skryptowych lub programowania. Ponieważ przepływy pracy są rdzeniem procesów automatyzacji i orkiestracji w ramach SOAR, należy zwrócić szczególną uwagę na elastyczność i łatwość ich użycia. Trzeba pamiętać, że przepływy pracy trudne do zbudowania i obsługi znacząco zmniejszą wydajność obsługi incydentów i utrudnią lub opóźnią ich wykrycie.

3. Zarządzanie incydentami

Reakcja na incydent jest wielowarstwowym, złożonym procesem. W tym kontekście orkiestracja i automatyzacja zapewnia wartość dodaną każdemu programowi bezpieczeństwa. Nie jest to jednak wartość jedyna. SOAR jest znaczącą inwestycją i dlatego warto wykorzystać ją szerzej, czyniąc użytek z szeregu funkcji wykraczających poza powyższy obszar takich jak np. śledzenie spraw, rejestrowanie działań podjętych podczas incydentu, czy wyznaczanie i raportowanie krytycznych wskaźników oraz współczynników KPI.

Możliwości zarządzania incydentami w SOAR nie powinny obejmować wyłącznie zarządzania sprawami. Aby zapewnić prawidłowe zarządzanie całym cyklem życia incydentu, SOAR powinien również zapewniać następujące funkcjonalności:

- szczegółowe śledzenie zadań, w tym ich przypisania, poświęconego czasu i bieżącego statusu;
- śledzenie wszystkich zasobów fizycznych i wirtualnych związanych z incydentem, zarządzanie aktywami;
- gromadzenie materiału dowodowego i zarządzanie łańcuchem dowodowym;
- śledzenie wskaźników i próbek, korelacja i dzielenie się wiedzą o zagrożeniach;
- zarządzanie dokumentami i raportami;
- śledzenie czasu obsługi i nakładów finansowych.

4. Analiza zagrożeń

Wiedza stanowi kluczowy element skutecznej reakcji na incydenty. Proste źródła informacji o zagrożeniach nadal zachowują pewną wartość i powinny być wykorzystywane przez SOAR, ale przy dzisiejszym krajobrazie cyberbezpieczeństwa, wiedza o zagrożeniach musi wykraczać poza proste kanały informacyjne. Kluczowym elementem zarządzania incydentami pozostaje śledzenie wskaźników takich jak adresy IP, adresy URL oraz próbek takich jak przykłady złośliwego oprogramowania i TTP.

SOAR zajmuje wyjątkową pozycję w gromadzeniu informacji tego typu ponieważ ma dostęp nie tylko do samych wskaźników, ale także do pozostałych informacji o incydencie, które mogą zapewnić szerszy kontekst, co tworzy realnie użyteczną wiedzę o zagrożeniach. Proaktywny program bezpieczeństwa wymaga, by wiedza taka była odpowiednio skorelowana z informacją dotyczącą wykrywania wzorców ataku, potencjalnych podatności i innych bieżących zagrożeń. Taka korelacja powinna być przeprowadzana automatycznie i natychmiast ujawniać, czy trwające zdarzenie może mieć elementy wspólne z jakimikolwiek wcześniejszymi incydentami.

Automatyczna korelacja ma krytyczne znaczenie dla analityków przy podejmowaniu przez nich decyzji w trakcie całego cyklu życia incydentu. Równie ważną funkcjonalnością SOAR jest możliwość analizy

zagrożeń w postaci korelacji wizualnej. Wiele proaktywnych programów bezpieczeństwa obejmuje dziś różne formy identyfikowania zagrożeń, aktywnie wyszukując ataki i wzorce, które mogły nie zostać wykryte za pomocą metod automatycznych. Aby ten proces ułatwić, informacje o zagrożeniach i skorelowane zdarzenia powinny być wizualizowane w taki sposób by umożliwić pracownikom SOC szybką i skuteczną analizę informacji.

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