Trzy czynniki istotne przy wyborze SOAR

Głównym celem implementacji rozwiązania SOAR jest zwiększenie skuteczności i wydajności programu bezpieczeństwa w organizacji. Będzie to możliwe, jeśli uda się w pełni wykorzystać potencjał wdrażanego systemu.

Nie ma dwóch identycznych platform SOAR. Niektóre cechy SOAR mogą się nam wydawać ważniejsze niż inne, ale zawsze można wyróżnić trzy funkcjonalności istotne dla każdej organizacji:

- konfigurowalność,
- zdolność do współpracy i wymiany informacji,
- wieloinstancyjność.

Konfigurowalność

SOAR musi zapewniać elastyczność w zakresie:

- implementacji,
- sposobu gromadzenia danych,
- metod integracji z innymi narzędziami bezpieczeństwa.

Platforma SOAR powinna umożliwiać wdrożenie w sposób optymalnie dostosowany do potrzeb całej organizacji, w tym:

- zespołów reagowania na incydenty komputerowe (CSIRT),
- centrów operacyjnych ds. bezpieczeństwa (SOC),
- dostawców usług zarządzania bezpieczeństwem (MSSP).

Rozwiązanie klasy SOAR powinno wspierać wprowadzanie danych z wielu źródeł takich jak np.:

- dwukierunkowe integracje,
- wiadomości e-mail,
- zgłoszenia operatorów systemu SOAR,
- zgłoszenia pracowników organizacji.

Istotne jest też, aby system umożliwiał definiowanie komu udostępniane są określone informacje oraz decydowanie o tym, które atrybuty danego incydentu mają być śledzone.

Wysoka konfigurowalność SOAR oznacza łatwość użytkowania systemu oraz lepsze jego dopasowanie do potrzeb organizacji, a w rezultacie znacznie wyższy zwrot z inwestycji (ROI).

Współpraca i wymiana informacji

Dla zapewnienia efektywności w środowisku pracy zespołowej rozwiązanie SOAR musi wspierać współpracę i wymianę (w kontrolowany sposób) informacji pomiędzy członkami zespołów bezpieczeństwa.

Osoby posiadające odpowiednie uprawnienia powinny mieć natychmiastowy dostęp do:

- statusu incydentu, w którego obsługę są zaangażowane,
- wszelkich zebranych o tym incydencie informacji,

- działań wykonywanych przez pozostałych członków zespołu.

Osoby takie powinny również mieć możliwość bezpiecznej komunikacji w ramach platformy SOAR, co jest niezwykle istotne w sytuacji, gdy standardowo używane kanały komunikacji zostały skompromitowane.

Konieczność współpracy i wymiany informacji, która jest kluczowym czynnikiem w zwalczaniu cyberprzestępczości dotyczy nie tylko samej organizacji, ale również podmiotów zewnętrznych. Udostępnianie wiedzy o wykrytych zagrożeniach może odbywać się w oparciu o różne bazy wiedzy: otwarte, zamknięte czy branżowe. Większość platform wykorzystuje do wymiany informacji jeden z otwartych standardów takich jak STIX / TAXII, OpenIOC lub MISP. Platforma SOAR powinna wspierać kontrolowanie i bezpieczne przekazywanie oraz udostępnianie informacji o zagrożeniach za pośrednictwem powyższych standardów.

Wieloinstancyjność

W dużych przedsiębiorstwach często działa wiele wewnętrznych zespołów bezpieczeństwa. Każdy z nich może wykonywać unikalny zestaw zadań. Zdarza się, że niektóre wewnętrzne jednostki nie powinny mieć dostępu do danych zebranych przez inne zespoły. Również dostawcy usług z zakresu bezpieczeństwa (MSSP) coraz częściej wykorzystują rozwiązania SOAR, co wymaga ścisłej separacji danych poszczególnych klientów.

W obu powyższych przypadkach wdrożenie odrębnej platformy SOAR dla każdego pojedynczego zespołu lub klienta nie będzie opłacalne. Rozwiązanie SOAR powinno więc być w stanie obsługiwać jednocześnie wiele instancji, zapewniając przy tym dokładną separację danych i kontrolę dostępu do informacji każdej z nich.

Przed przystąpieniem do oceny systemu SOAR i jego dostawcy bardzo ważne jest odniesienie się do powyższych funkcjonalności w kontekście potrzeb własnej organizacji. Jeśli tego nie zrobimy, to ryzykujemy inwestycję czasu i pieniędzy w rozwiązanie, które może nie dostarczyć pożądanego rezultatu.

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