Orion
Instruments Polska

NAJLEPSZE PRAKTYKI W OCENIE ROZWIĄZAŃ SOAR I DOSTAWCÓW SOAR

Zdefiniowanie podstawowego zestawu pytań, które należy zadać każdemu dostawcy systemu SOAR (Security Orchestration, Automation and Response) ma kluczowe znaczenie dla dokładnego i obiektywnego porównania różnych rozwiązań tej klasy. Pytania takie powinny umożliwić określenie, w jakim stopniu określony produkt spełnia zdefiniowane cele projektu. Pełny zestaw pytań powinien powstać przed oceną pierwszego rozwiązania.

Oto kilka pytań, które mogą pomóc w ocenie różnych rozwiązań SOAR:

OGÓLNE

- Jakie problemy rozwiązuje oceniane rozwiązanie?
- W jaki sposób to robi?
- Co stanowi wyróżnik danego rozwiązania?
- Jakie są typowe, a jakie specyficzne przypadki użycia systemu podawane przez klientów?

AUTOMATYZACJA I ORKIESTRACJA

- Czy rozwiązanie daje operatorowi możliwość podjęcia decyzji w krytycznych punktach procesu obsługi incydentu? Jak się to odbywa?
- W jaki sposób w ramach obsługi danego incydentu realizowana jest orkiestracja działań wykorzystujących różne integracje?

REALIZACJA

- Jak wdrażane jest rozwiązanie?
- Ile czasu potrzeba na dostosowanie rozwiązania do stanu pełnej funkcjonalności?

Orion
Instruments Polska

tel. 22 638 31 45
orion@orion.pl

www.orion.pl/soar

Orion
Instruments Polska

ZARZĄDZANIE INCYDENTAMI

- Jakie możliwości w zakresie zarządzania incydentami zapewnia dane rozwiązanie?
- W jaki sposób rozwiązanie wspiera pracę zespołową i dzielenie się informacjami?
- Czy rozwiązanie obsługuje zarządzanie materiałem dowodowym?

INTEGRACJE

- Jakie integracje dostępne są w rozwiązaniu?
- Ile integracji niezbędnych dla organizacji jest dostarczanych wraz z systemem?
- Czy w ramach dostarczanych integracji rozwiązanie umożliwia wykonanie niezbędnych dla nas akcji?
- Jak wygląda proces tworzenia nowych integracji; czy użytkownik może to zrobić samodzielnie?

CENY

- Jakie są dostępne modele licencjonowania?
- Co obejmuje cena bazowa, a za co trzeba będzie dodatkowo zapłacić?
- Czy do uruchomienia rozwiązania wymagane są dodatkowe konsultacje lub usługi profesjonalne; kto je świadczy?

RAPORTOWANIE I WIZUALIZACJA

- Czy rozwiązanie zapewnia możliwość generowania niestandardowych raportów i metryk?
- Czy rozwiązanie obsługuje konfigurowalne pulpity nawigacyjne lub inne wizualizacje?
- Czy rozwiązanie umożliwia rejestrowanie i raportowanie niestandardowych atrybutów incydentu?

OCENA DOSTAWCY

Rozwiązanie SOAR jest inwestycją długoterminową. Po wdrożeniu i zintegrowaniu określonej platformy SOAR z procesami bezpieczeństwa występującymi w danej organizacji koszt ewentualnej wymiany takiego systemu będzie bardzo wysoki.
Dlatego też istotne jest dokonywanie oceny zarówno dostawcy SOAR jak i samego systemu. Dobrą praktyką jest wybór takiego dostawcy, który będzie w stanie zapewnić zarówno wdrożenie rozwiązania SOAR, jak i efektywną obsługę klienta w przyszłości.

Obiektywna ocena dostawcy rozwiązania to proces, który powinien być dostosowany do indywidualnych wymagań każdej organizacji. Choć przedstawiamy pewne sugestie dotyczące typowych pytań, które mogą zostać wykorzystane przy ocenie rozwiązań SOAR, ważne jest, aby każda firma rozważyła, jakie pytania będą najlepiej odzwierciedlać jej konkretne potrzeby.

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