



JAKIE KORZYŚCI WYNIKAJĄ Z POWIĄZANIA SYSTEMÓW SIEM I SOAR

Fuzja
inteligencji

Skrócenie czasu
odpowiedzi
na incydent

Wzrost wskaźnika
rentowności dla
wykorzystywanych narzędzi
bezpieczeństwa

1

WPROWADZENIE

Z uwagi na powszechną dostępność szerokiej gamy technologii, narzędzi i platform dla zespołów bezpieczeństwa, coraz trudniej jest podjąć decyzję o wyborze właściwego rozwiązania do ochrony organizacji przed rosnącą z dnia na dzień liczbą, stopniem komplikacji i wyrafinowania zagrożeń cybernetycznych. Konieczność wzięcia pod uwagę takich czynników jak ograniczony budżet, brak zasobów ludzkich oraz wymogi zgodności z przepisami i regulacjami, jak również wydajność operacji bezpieczeństwa oraz zwrot z inwestycji w narzędzia i zasoby, wymaga dobrze zdefiniowanej strategii bezpieczeństwa.

Zakres i poziom dojrzałości programu bezpieczeństwa określa jego strukturę i stosowane technologie. Pojawia się jednak pytanie: kiedy i w jaki sposób należy wdrożyć platformę orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydent (SOAR – Security Orchestration, Automation and Response) na bazie istniejącej infrastruktury SIEM, aby lepiej zarządzać operacjami bezpieczeństwa i procesami reagowania na incydenty?

CZYM SOAR RÓŻNI SIĘ OD SIEM'A?

SIEM zestawia i analizuje informacje przesyłane z różnych źródeł, identyfikując problemy i generując alerty bezpieczeństwa. Selekcja takich alertów jest często przeprowadzana manualnie przez analityków bezpieczeństwa i wiąże się z licznymi błędami wynikającymi z samego wolumenu danych oraz liczby powtarzalnych, rutynowych i nużących czynności. W rezultacie przebieg całego procesu nie jest satysfakcjonujący.

Istotnym ograniczeniem technologii SIEM jest też jednokierunkowa komunikacja pomiędzy systemem tej klasy i innymi produktami. Rozwiązania SIEM zostały zaprojektowane do w miarę bezinwazyjnego zbierania i przetwarzania informacji, do czego nie jest niezbędne wsparcie dla dwukierunkowej komunikacji z narzędziami innych firm. W większości przypadków znacznie obniża to zdolność systemu SIEM do realizacji działań wykraczających poza wygenerowanie początkowego alarmu; w takich przypadkach SOAR może wnieść niezwykle istotną wartość dodaną.

Posiadanie systemu SIEM nie jest warunkiem koniecznym do wdrożenia i użytkowania SOAR. Platforma SOAR nie jest też zamiennikiem SIEM'a – systemy te są najczęściej użytkowane wspólnie. SOAR w połączeniu z SIEM'em powinien być wykorzystywany przez zespoły operacji bezpieczeństwa (SOC) do automatyzacji i orkiestracji działań oraz dwukierunkowej komunikacji ze wszystkimi narzędziami bezpieczeństwa, tak aby zmniejszyć ilość alertów angażujących analityków, skrócić czas odpowiedzi na incydent oraz obniżyć poziom ryzyka.

Rozwiązanie SOAR, umiejscowione w strukturze bezpieczeństwa organizacji powyżej systemu SIEM, zapewnia orkiestrację i automatyzację działań wielu narzędzi pochodzących od różnych dostawców, podczas gdy SIEM jest używany do zbierania, zestawiania i analizowania danych oraz generowania alertów, co jest pierwszym krokiem w wieloetapowym procesie obsługi incydentu. Technologia SOAR będzie w takim przypadku wykorzystywana po inicjalnym wykryciu zagrożenia bezpieczeństwa i utworzeniu związanego z tym alertu przez SIEM.

KIEDY NALEŻY ROZWAŻYĆ WDROŻENIE SYSTEMU SOAR?

Liczba zdarzeń, z którymi analitycy bezpieczeństwa mają do czynienia każdego dnia jest przytłaczająca. Sytuacja taka uniemożliwia skuteczne radzenie sobie z incydentami. Narzędzia klasy SIEM zbierają ogromne ilości danych z różnych obszarów IT, ale jak się okazuje nadmiar informacji jest czasami równie paraliżujący, jak jej brak.

SIEM pomaga scentralizować dane pozyskiwane z różnych narzędzi bezpieczeństwa. Często oznacza to konieczność przetwarzania ogromnych ilości informacji, które muszą następnie zostać przefiltrowane i skorelowane, aby wyeliminować fałszywe alarmy, pozostawiając tylko te zdarzenia, co do których należy podjąć działania naprawcze. Generowanie tysięcy alertów może prowadzić do zalania informacją analityków bezpieczeństwa, którzy nie będą mieli w takiej sytuacji szans trafego wytypowania alertów priorytetowych.



Ogromna liczba alertów oznacza również, że analitycy nie są w stanie skutecznie i wydajnie reagować na każde zdarzenie, co częstokroć powoduje, że większość alarmów nie jest właściwie sprawdzana i weryfikowana. A wystarczy jeden nieobsłużony alert, aby poważny incydent nabral rozmachu zagrażając bezpieczeństwu całej organizacji. Większość zespołów bezpieczeństwa nie zdaje sobie sprawy z tego, jak niewiarygodnie wielka jest liczba wpływających alertów, dopóki nie wdroży systemu SIEM i zaawansowanej architektury wykrywania zagrożeń. Nie zawsze zaś wprowadzenie do SIEM'a reguł korelacji w znaczący sposób zmniejsza liczbę generowanych alertów.

Rozważając potrzebę wdrożenia rozwiązania klasy SOAR, kluczową kwestią dla CISO jest przeprowadzenie dogłębnej analizy zarówno bieżących, codziennych, jak i ogólnych wyników wydajności zespołu bezpieczeństwa. Warto np. określić: ile jest generowanych alertów bezpieczeństwa, ile z nich jest uzasadnionych, a ile fałszywych, ile czasu zajmuje wykrycie alertu, a ile reakcja nań, ile mamy narzędzi bezpieczeństwa i które z nich muszą zostać użyte podczas sprawdzania alarmów, ile alertów nie wywołuje żadnych działań, jaki jest średni czas rozwiązania problemu, ilu jest dostępnych analityków bezpieczeństwa i czy aktualnie wykorzystywane zasoby zapewniają maksymalną wydajność i skuteczność działania zespołu? Po udzieleniu odpowiedzi na powyższe pytania i wyznaczeniu odpowiednich współczynników, ich analizie oraz porównaniu ze zdefiniowanymi wcześniej zestawami operacji bezpieczeństwa, celami reagowania na incydenty oraz najlepszymi praktykami, stanie się oczywiste, czy występuje potrzeba biznesowa wdrożenia platformy SOAR, która ograniczy ilość alertów, zapewni orkiestrację narzędzi, procedur i zespołów bezpieczeństwa oraz zautomatyzuje żmudne zadania.

ZALETY INTEGRACJI SIEM I SOAR

Integracja SIEM i SOAR łączy w sobie moc obu tych systemów, co pozwala stworzyć skuteczny, efektywny i odpowiadający potrzebom organizacji program bezpieczeństwa. Korzystając ze zdolności SIEM'a do przyswajania dużych ilości danych i generowania alertów, platforma SOAR może być niejako „nałożona” na system SIEM w celu zarządzania procesem reagowania na incydenty, a także automatyzacji i orkiestracji szeregu powtarzalnych zadań, które wymagałyby wielu godzin pracy operatora.



Platformy SOAR, takie jak IncMan firmy DFLabs, wspierają integrację z systemami SIEM i są kompleksowym rozwiązaniem dla wszystkich organizacji starających się stworzyć optymalny program bezpieczeństwa. SOAR skutecznie redukuje szum informacyjny generowany przez ogromną liczbę alertów, w tym również przez mało niekiedy przydatne informacje o zagrożeniach. W rezultacie umożliwia to zespołom bezpieczeństwa skrócenie czasu odpowiedzi, zwiększenie efektywności analityków i wzrost liczby obsługiwanych zgłoszeń. Analitycy bezpieczeństwa, korzystając z rozwiązania SOAR, stają się zdecydowanie bardziej proaktywni. Mogą oni także zrestrukturyzować swoje obciążenia, aby lepiej wykorzystać czas na podejmowanie działań takich jak wczesne wychwytywanie zagrożeń, by być o krok przed potencjalnym alertem, zanim jeszcze zostanie on wygenerowany.

Połączenie mocy SOAR i SIEM ma kluczowe znaczenie dla zagwarantowania, że alerty nie pozostaną niezauważone lub zignorowane. Co ważniejsze, taka struktura zapewnia, iż wszystkie powiadomienia będą rozpatrywane w odpowiednim czasie i obsługiwane zgodnie ze standardowym zestawem spójnych i powtarzalnych praktyk i procedur. Czynnikiem ten jest niezwykle istotny w związku regulacjami, takimi jak RODO, czy ustawa o krajowym systemie cyberbezpieczeństwa, w odniesieniu do których wdrożenie SOAR zapewnia spełnienie wymogów zgłaszania w określonym czasie incydentów i naruszeń.

Rozwiązanie SOAR automatyzuje otwieranie biletów związanych z incydentami bezpieczeństwa, a przy pomocy zdefiniowanych schematów działania takich jak playbooki i runbooki podejmuje odpowiednie kroki, aby przeprowadzić rutynowe walidacje. Zapewnia to automatyczne i właściwe wzbogacenie informacji o incydencie dając więcej czasu na remediację. Za pośrednictwem rozwiązania SOAR dostępne są również opcje ograniczające lub naprawcze, które mogą być w razie potrzeby uruchamiane automatycznie. W zależności od wymagań konkretnej organizacji platforma SOAR pozwala decydentom określić dla każdego incydentu właściwą równowagę działań automatycznych i podejmowanych przez operatorów.

JAK STWORZYĆ ZINTEGROWANY PRZEPŁYW PRAC ŁĄCZĄCY PLATFORMY SIEM I SOAR?

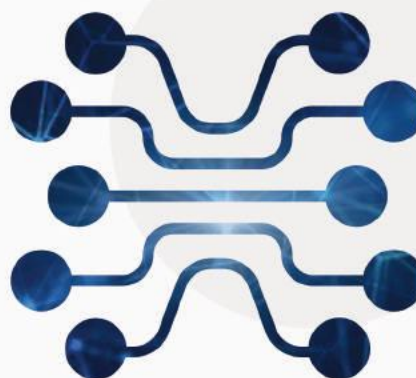
Aby w pełni wykorzystać funkcjonalność połączonych rozwiązań SIEM i SOAR, ważne jest zbudowanie zintegrowanych przepływów pracy, które pozwolą zespołom bezpieczeństwa na bardziej skuteczne i wydajne wykrywanie incydentów, reagowanie na nie i remediację. Przepływy te powinny koncentrować się na wykorzystaniu mocnych stron i pełnego potencjału każdego rozwiązania, maksymalizując efektywność ich współdziałania.

Ze względu na ilość danych, które SIEM przetwarza, a także możliwości korelacyjne tego typu rozwiązań, sensowne jest kontynuowanie zbierania przez SIEM surowych logów. SIEM będzie wówczas odpowiedzialny za agregowanie i przechowywanie nieprzetworzonych logów przez określony czas, jak również za korelację logów i zdarzeń. Jeśli aplikacje firm trzecich zostaną skonfigurowane tak, aby wysyłały swoje logi do SIEM'a, administratorzy tej platformy będą musieli odpowiednio dostosić system SIEM i określić, które zdarzenia powinny zostać przebadane, a zatem należy je przekazać do rozwiązania SOAR. Proces strojenia prawdopodobnie zajmie pewien czas, zanim uzyskamy pewność, że odpowiednie zdarzenia są eskalowane do SOAR oraz, że wysyłana jest ograniczona liczba zdarzeń niepożądanych.

Przekazywanie zdarzeń z SIEM do SOAR można zrealizować na kilka różnych sposobów. Najczęściej stosowanym i najprostszym rozwiązaniem jest wykorzystanie sysloga. Wymaga to wprowadzenia odpowiednich reguł w systemie SIEM, tak aby przekazywane były tylko niezbędne zdarzenia. Konieczne jest tu również skonfigurowanie reguł analizy składniowej w ramach SOAR, tak by informacje z komunikatów syslog były poprawnie parsowane.

Większość rozwiązań SOAR, w tym DFLabs IncMan, oferuje także specjalnie zaprojektowane integracje z najpopularniejszymi produktami SIEM. Zastosowanie tego typu wbudowanej integracji daje szereg korzyści. Pobieranie danych z SIEM'a w oparciu o dostosowywane zapytania gwarantuje wyższy poziom elastyczności decyzji, odnośnie tego, które zdarzenia są kierowane do SOAR. Ponieważ integracje te są specjalnie zaprojektowane dla określonych SIEM'ów, ich zastosowanie zmniejsza ilość reguł parsowania, które muszą zostać zdefiniowane w ramach SOAR, w porównaniu z sytuacją, gdy przekazywanie zdarzeń odbywa się wyłącznie poprzez syslog.

Po przekazaniu odpowiednich zdarzeń do platformy SOAR, ostatnim krokiem jest zdefiniowanie właściwych przepływów pracy do badania różnych typów zdarzeń w ramach SOAR. Od tego momentu zdarzenie będzie obsługiwane z poziomu SOAR. Dwukierunkowe integracje między SOAR a SIEM umożliwiają uzyskiwanie dodatkowych danych od SIEM'a, a także od wszelkich innych narzędzi bezpieczeństwa działających w danym środowisku.



Proces definiowania przepływów pracy w ramach SOAR będzie różny w zależności od dojrzałości występujących w organizacji przepływów prac związanych z bezpieczeństwem. Jeśli istnieją szczegółowe przepływy prac dla rozpowszechnionych typów zdarzeń, można je w prosty sposób zaimplementować do rozwiązania SOAR. Jeśli takie przepływy nie istnieją, pierwszym krokiem musi być ich zdefiniowanie. Będzie to wymagało określenia, jakie są obecnie nieudokumentowane procesy dla każdego typu zdarzeń. Procesy te powinny najpierw zostać sformalizowane i dopracowane, a dopiero następnie wprowadzone do SOAR.

PODSUMOWANIE

SIEM jest kluczowym narzędziem w każdej infrastrukturze bezpieczeństwa. Jednak ważne jest, abyśmy pamiętali do czego SIEM został zaprojektowany i co możemy przy jego pomocy osiągnąć, a także jakie luki, pomimo jego zastosowania, mogą nadal występować w systemie bezpieczeństwa. Połączenie rozwiązań SIEM i SOAR może przekształcić operacje bezpieczeństwa i zdolność reagowania na incydenty i podnieść je na zdecydowanie wyższy poziom.



Współdziałanie SIEM-SOAR pozwala na przekazanie wykrytego zagrożenia w postaci alertu bezpieczeństwa z SIEM'a i wygenerowanie incydentu w obrębie SOAR, co umożliwia modernizację i usprawnienie całego procesu odpowiedzi na incydent, ułatwia automatyzację i orkiestrację, przyspiesza zdolności reagowania.

Rozwiązanie SOAR działa dla zespołu bezpieczeństwa jak multiplikator, umożliwiając realizację większej liczby zadań bez konieczności powiększania zespołu, pozwala zaoszczędzić cenny czas analityków w obliczu przytłaczających ilości danych oraz żmudnych i wciąż powtarzających się zadań. Powoduje to, że zespół bezpieczeństwa staje się mniej przeciążony, bardziej wydajny i efektywny, a także – co niezwykle istotne – proaktywny.

Przyjęcie takiej struktury nieuchronnie skróci czas od wykrycia zagrożenia do rozwiązania problemu, zwiększy zwrot z inwestycji w istniejące technologie i rozwiązania bezpieczeństwa, zmniejszy ryzyko wynikające z incydentów bezpieczeństwa, a jednocześnie zapewni zgodność z wymogami prawnymi i regulacjami. A zatem struktura, w której rozwiązania SIEM i SOAR współpracują ze sobą, daje istniejącemu systemowi bezpieczeństwa ogromną wartość dodaną.



Orion Instruments Polska jest doświadczonym dostawcą systemów oraz usług z zakresu SIEM i SOAR.