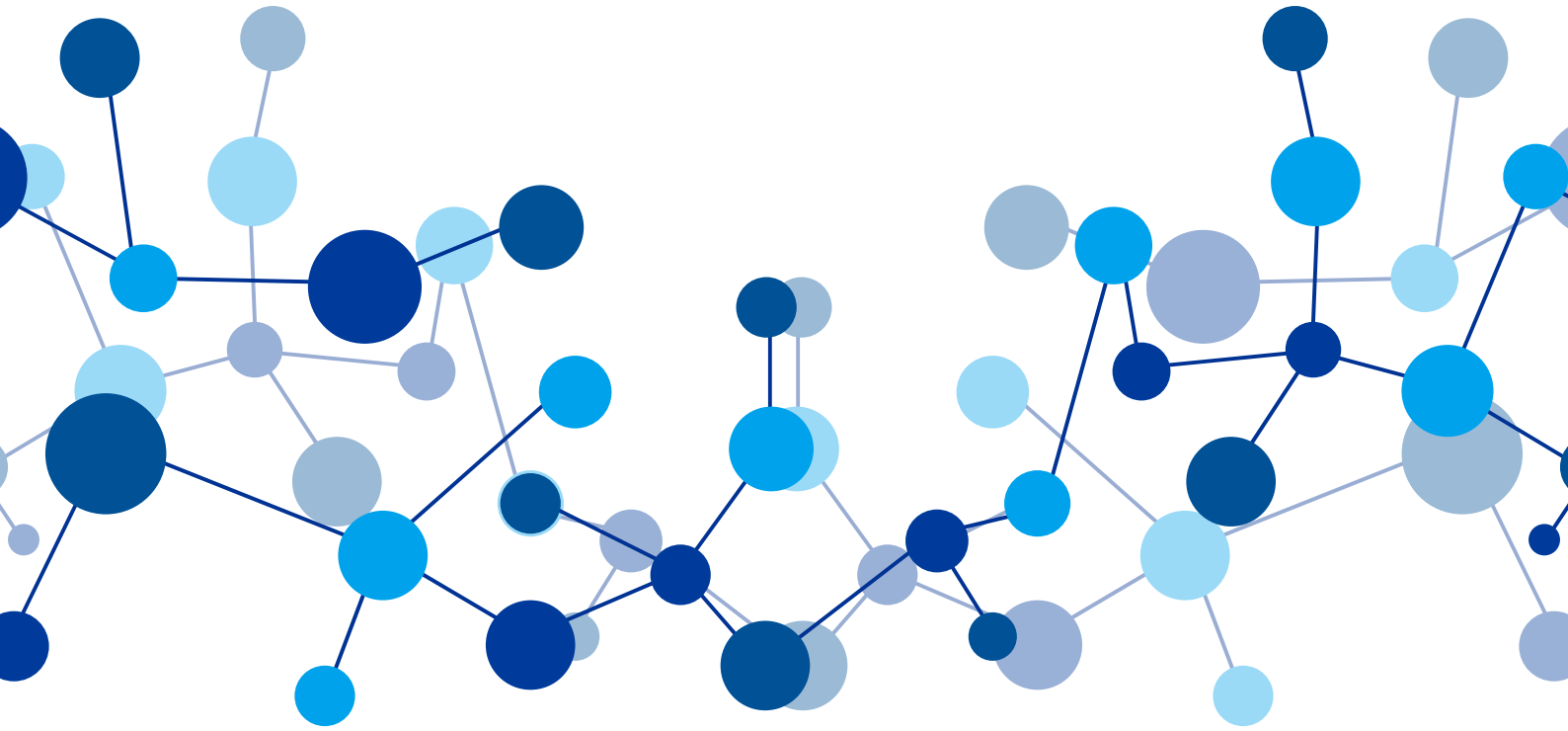
DFLABS
CYBER INCIDENTS UNDER CONTROL

Orion
Instruments Polska

Jakie korzyści wynikają z powiązania systemu SIEM z technologią SOAR?

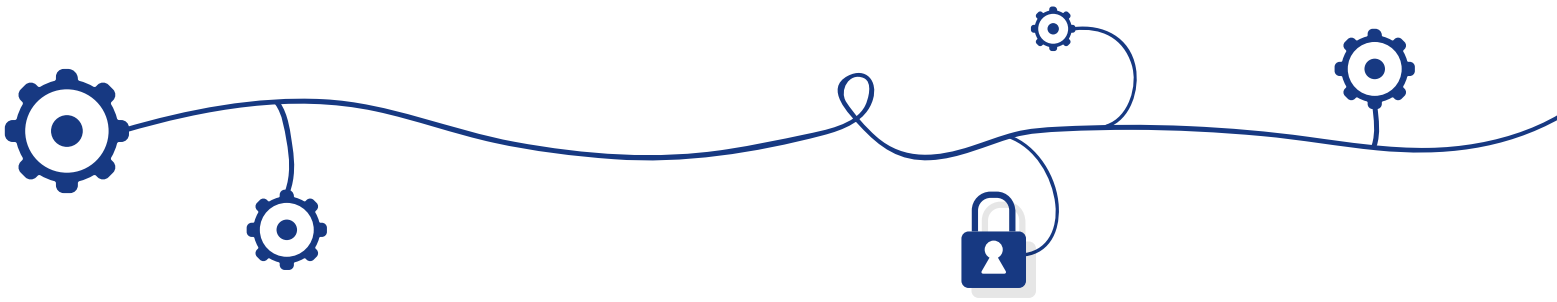
Fuzja inteligencji, skrócenie czasu odpowiedzi na incydent, wzrost wskaźnika rentowności dla wykorzystywanych narzędzi bezpieczeństwa.

John Moran, Senior Product Manager



www.dflabs.com

www.orion.pl



Spis treści

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, poziomem komplikacji i stopniem wyrafinowania zagrożeń cybernetycznych. Konieczność wzięcia pod uwagę takich czynników jak ograniczony budżet, brak zasobów ludzkich oraz wymogi zgodności z przepisami prawnymi 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. Powszechnie przyjętą praktyką jest wykorzystywanie systemu SIEM, obok lub powyżej pozostałych rozwiązań bezpieczeństwa takich jak: system zapobiegania włamaniom (IPS), system monitorowania aktywności baz danych (DAM), zapora aplikacyjna (WAF), system zapobiegania wyciekowi danych (DLP), system oceny podatności na zagrożenia (VAS). Pojawia się pytane: 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?

Celem niniejszego dokumentu jest udzielenie odpowiedzi na te pytania. Najpierw określimy czym są rozwiązania SIEM i SOAR, a następnie omówimy różnice między nimi. Przedstawimy dlaczego zespoły bezpieczeństwa powinny rozważyć wdrożenie rozwiązania SOAR na bazie SIEM, jakie korzyści pozwala to osiągnąć, kiedy należy taki model wykorzystywać i, co najważniejsze, jak przeprowadzić skuteczne wdrożenie.

Czym jest SIEM?

SIEM jest rozwiązaniem łączącym funkcje zarządzania informacjami i zdarzeniami w jeden system, dający wgląd w obraz bezpieczeństwa IT całej organizacji. Podstawową funkcją SIEM jako systemu monitorowania bezpieczeństwa jest zestawianie odpowiednich danych z wielu źródeł, takich jak aplikacje i sprzęt sieciowy, co umożliwia przeprowadzenie analizy w czasie rzeczywistym i identyfikację odchyleń od normy. W przypadku wykrycia anomalii SIEM generuje odpowiednie alerty, które powinny być na bieżąco analizowane przez zespół bezpieczeństwa. Typową jednak cechą działania systemów SIEM jest generowanie dużej liczby alertów, w tym wielu, które po dodatkowym śledztwie okazują się być fałszywymi trafieniami. Na podstawowym poziomie działanie SIEM'a może być oparte na regułach lub zastosowaniu statystycznego mechanizmu korelacji do określania współzależności pomiędzy poszczególnymi wpisami dziennika zdarzeń (event log). Zaawansowane systemy SIEM ewoluują w kierunku uwzględnienia analityki zachowania użytkowników i jednostek (UEBA – User and Entity Behavior Analytics) oraz niektórych możliwości orkiestracji i automatyzacji.

Czym jest SOAR?

Platforma orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydent (SOAR – Security Orchestration, Automation and Response) to podejście do operacji bezpieczeństwa i reagowania na incydenty mające na celu poprawę skuteczności, wydajności i spójności działań w zakresie bezpieczeństwa. Gartner definiuje SOAR jako technologię umożliwiającą organizacjom zbieranie danych i alertów bezpieczeństwa z różnych źródeł. SOAR zapewnia przeprowadzanie analizy incydentów oraz ich sortowanie i kategoryzację, łączy wykorzystanie możliwości czynnika ludzkiego z maszynowym, a zatem pozwala wspólnie definiować, priorytetyzować i sterować ustandaryzowanymi procesami reagowania na incydenty w przepływie pracy[1].

Rosnąca złożoność IT, ewoluujące zagrożenia i konieczność koordynacji wielu rozwiązań z zakresu bezpieczeństwa dały początek technologii SOAR, która jest często wdrażana przez centra bezpieczeństwa (SOC – Security Operations Center), zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT – Computer Security Incident Response Team) i dostawców zarządzalnych usług z dziedziny bezpieczeństwa (MSSP – Managed Security Service Provider).

Działając jako multiplikator zasobów SOAR pozwala zespołom bezpieczeństwa realizować więcej zadań, zapewniając jednocześnie funkcje automatyzacji, orkiestracji i pomiaru w całym cyklu życia reakcji na incydent, w tym wykrywanie i kwalifikowanie incydentów bezpieczeństwa, ich segregację, eskalację, wzbogacanie, ograniczanie i usuwanie skutków. Celem wdrożenia technologii SOAR jest skrócenie czasu od wykrycia naruszenia do rozwiązania problemu oraz zminimalizowanie ryzyka związanego z incydentami bezpieczeństwa, przy jednoczesnym zwiększeniu zwrotu z inwestycji w istniejące technologie.

Czym SOAR różni się od SIEM'a?

SIEM zestawia i analizuje informacje przesyłane z różnych źródeł, identyfikując problemy i generując wstępne alerty bezpieczeństwa. Selekcja takich alertów jest często przeprowadzana przez analityków bezpieczeństwa w sposób ręczny i podlega licznym błędom wynikającym z samego wolumenu danych oraz liczby powtarzalnych i rutynowych czynności. W rezultacie przebieg całego procesu nie jest satysfakcjonujący. Historycznie jedną z podstawowych funkcjonalności technologii SIEM jest przetwarzanie dużych ilości zdarzeń związanych z bezpieczeństwem – tę funkcję SIEM doskonali do dnia dzisiejszego. Pomimo, że niektóre zaawansowane rozwiązania SIEM zawierają dodatkowe funkcjonalności, takie jak integracja z analizą zagrożeń i innymi rozwiązaniami stron trzecich, wiele SIEM'ów nadal koncentruje się głównie na przetwarzaniu i prezentacji danych.

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

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

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

Po wygenerowaniu alertu przez SIEM incydent zostanie automatycznie utworzony na platformie SOAR. Dalej następuje interakcja procesów automatycznych i reakcji ludzkich w celu przeprowadzenia szeregu działań wzbogacających i odpowiadających na zagrożenie. Zestaw działań oparty na uprzednio zdefiniowanych (w oparciu o wcześniej rozwiązywane incydenty) procedurach postępowania może być, w połączeniu z uczeniem maszynowym, wykorzystany do zautomatyzowania i kierowania całym procesem reagowania. Przykładem będą tu zestawy schematów postępowania typu playbook i runbook używane do wzbogacania danych, ograniczenia zagrożenia i remediacji w przypadku zdarzeń takich jak phishing lub ransomware.

[1]Gartner Technical Paper, Preparing Your Security Operations for Orchestration and Automation Tools, February 2018.

Kiedy należy rozważyć wdrożenie systemu SOAR?

Liczba zdarzeń, z którymi analitycy bezpieczeństwa mają do czynienia każdego dnia, jest przytłaczająca, co oznacza, że muszą się oni przekopywać przez istny zalew danych. 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 niewystarczająca jej ilość.

SIEM pomaga scentralizować dane pozyskiwane z różnych narzędzi bezpieczeństwa. Często oznacza to konieczność przetwarzania przytłaczających 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 ogromnej liczby alertów może prowadzić do zalania informacją analityków bezpieczeństwa, nie będących w stanie określić, które alerty powinny mieć pierwszeństwo. Taki stan rzeczy ma wpływ na krytyczny zasób organizacji jakim jest zespół bezpieczeństwa.

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

Rozważając potrzebę wdrożenia rozwiązania klasy SOAR, kluczową kwestią dla kierownika zespołu bezpieczeństwa i / lub dyrektora ds. bezpieczeństwa informatycznego (CISO – Chief Information Security Officer) 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 to fałszywe alarmy, ile czasu zajmuje wykrycie alertu, a ile reakcja nań, ile jest stosowanych narzędzi bezpieczeństwa i które z nich muszą być używane podczas sprawdzania alarmów, ile alertów pozostaje na uboczu i 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 danych liczbowych, ich analizie oraz porównaniu ze zdefiniowanymi wcześniej zestawami operacji bezpieczeństwa, celami reagowania na incydenty oraz najlepszymi praktykami, stanie się oczywiste, czy istnieje potrzeba biznesowa wdrożenia rozwiązania SOAR, które ograniczy zalew zgłoszeń, zapewni orkiestrację różnych narzędzi bezpieczeństwa i zautomatyzuje żmudne zadania.

W większości przypadków zespół bezpieczeństwa nie działa z maksymalną wydajnością, a istniejące zasoby nie są wykorzystywane w optymalny sposób. Rosnąca liczba cyberzagrożeń powoduje, że zespoły bezpieczeństwa są przeciążone alertami i rutynowymi zadaniami, co obniża ich skuteczność. Może to również powodować, że zespoły takie, starając się uporać z napływającymi zdarzeniami tak szybko, jak to tylko możliwe, nie będą postępować zgodnie z obowiązującymi procedurami. Skutkować to będzie brakiem transferu wiedzy, co jest niezbędne do obsługi przyszłych alertów. W takim przypadku jedynym rozwiązaniem dla organizacji jest wdrożenie platformy SOAR.

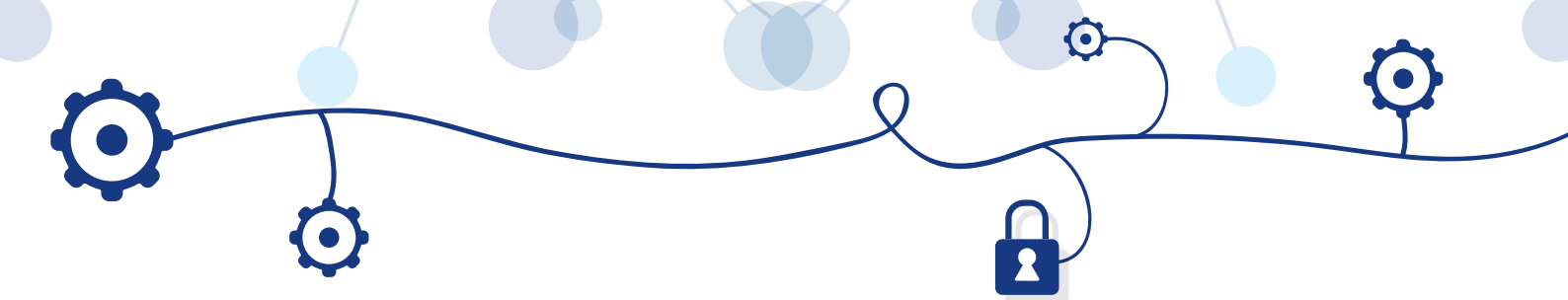
Zalety wdrożenia platformy SOAR wraz z SIEM

Integracja SIEM z rozwiązaniem SOAR łączy w sobie moc obu tych narzędzi, 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 „nałożona" na system SIEM w celu zarządzania procesem reagowania na incydenty dla każdego alarmu, 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 wiarygodne 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, po usunięciu niektórych niepotrzebnych obciążeń, stają się zdecydowanie bardziej proaktywni. Mogą oni także zrestrukturyzować swoje obciążenia, aby lepiej wykorzystać czas na podejmowanie działań, takich jak wychwytywanie zagrożeń, tak by być o krok przed potencjalnym alertem, zanim jeszcze zostanie on wygenerowany.

Połączenie mocy rozwiązania SOAR z SIEM'em ma kluczowe znaczenie dla zagwarantowania, że alerty nie pozostaną niezauważone lub zignorowane. Co ważniejsze, taka struktura zapewnia, że wszystkie powiadomienia będą rozpatrywane w odpowiednim czasie i obsługiwane zgodnie ze standardowym zestawem spójnych i powtarzalnych praktyk i procedur. Czynnik ten jest tym bardziej istotny w związku regulacjami, takimi jak RODO, w odniesieniu do którego wdrożenie SOAR zapewnia spełnienie wymogów zgłaszania w określonym czasie incydentów i naruszeń.

Rozwiązanie SOAR automatyzuje otwieranie związanych z incydentami bezpieczeństwa biletów, a przy pomocy zdefiniowanych schematów działania takich jak playbooki i runbooki podejmuje odpowiednie kroki, aby przeprowadzić niektóre rutynowe walidacje. Zapewnia to automatyczne i właściwe wzbogacenie informacji o incydencie zwiększając czas potrzebny na remediację. Za pośrednictwem rozwiązania SOAR dostępne są również opcje ograniczające lub naprawcze, które mogą być w razie potrzeby automatycznie uruchamiane i aranżowane. W zależności od konkretnych wymagań organizacyjnych i bezpieczeństwa, platforma SOAR pozwala decydentom wstępnie 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 dostroić 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 platformy SOAR oraz, że wysyłana jest ograniczona liczba zdarzeń niepożądanych.

Przekazywanie zdarzeń z platformy SIEM do SOAR można zrealizować na kilka różnych sposobów. Najczęściej stosowanym i najprostszym rozwiązaniem jest wykorzystanie programu syslog, ponieważ zarówno SIEM, jak i SOAR powinny z łatwością go obsługiwać. Wykorzystanie syslog będzie wymagało odpowiedniego skonfigurowania reguł w systemie SIEM, tak aby przekazywane były tylko niezbędne zdarzenia. Będzie to również wymagać skonfigurowania reguł analizy składniowej w ramach rozwiązania SOAR, tak by informacje z komunikatów syslog były poprawnie parsowane w użytecznym formacie.

Większość rozwiązań SOAR, w tym DFLabs IncMan, oferuje także specjalnie zaprojektowane integracje z najpopularniejszymi produktami SIEM. Zastosowanie tego typu wbudowanej integracji za pośrednictwem syslog'a daje szereg korzyści. Pobieranie danych z SIEM'a w oparciu o dostosowywane zapytania zapewnia 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 rozwiązania SOAR. Integracje między SOAR a SIEM umożliwiają uzyskiwanie dodatkowych danych od SIEM'a, a także od wszelkich innych produktów 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 w prosty sposób wprowadzić te procesy do rozwiązania SOAR. Jeśli takie szczegółowe przepływy nie istnieją, pierwszym krokiem będzie ustalenie, jakie powinny być właściwe przepływy. Będzie to wymagało określenia, jakie są obecne nieudokumentowane procesy dla każdego typu zdarzenia. Procesy te powinny najpierw zostać sformalizowane i dopracowane w wersji papierowej, a następnie wprowadzone do SOAR.

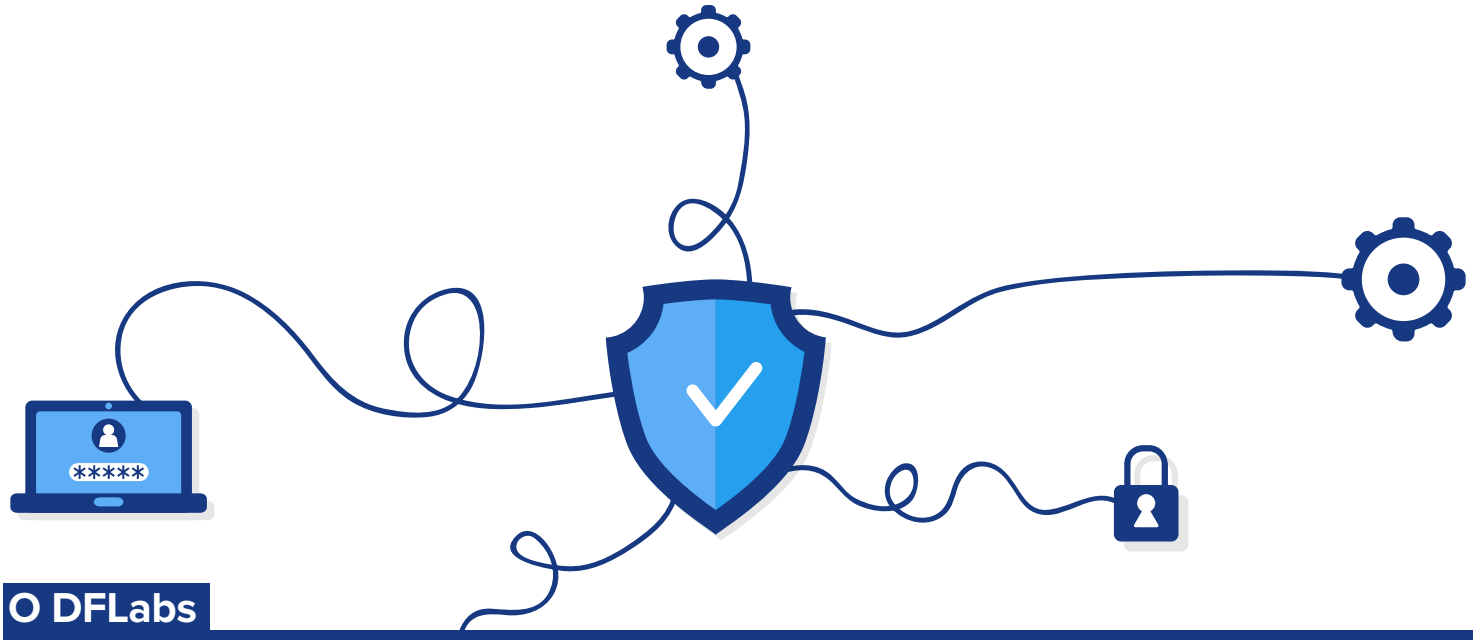
Podsumowanie

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 przenieść je w inteligentny i z góry określony sposób na 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 jak multiplikator dla zespołu bezpieczeństwa, umożliwiając mu 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.

DFLABS
CYBER INCIDENTS UNDER CONTROL



O DFLabs

DFLabs IncMan jest pionierską platformą technologiczną do zarządzania, pomiaru i orkiestracji zadań z dziedziny bezpieczeństwa w tym kwalifikacji incydentów bezpieczeństwa, ich segregacji i eskalacji, wychwytywania i badania zagrożeń oraz podejmowania działań naprawczych. IncMan wykorzystuje uczenie maszynowe i automatyzację do zwiększenia ludzkich możliwości w celu maksymalizacji efektywności i skuteczności zespołów operacji bezpieczeństwa. Redukuje również czas od momentu odkrycia włamania do rozwiązania problemu, co skutkuje zwiększeniem zwrotu z inwestycji wykorzystywanych technologii bezpieczeństwa. Osoby tworzące zespół zarządzający firmy DFLabs cieszą się bardzo wysokim uznaniem w branży ze względu na za wkład w powstanie i rozwój standardów takich jak ISO 27043 i ISO 30121.

www.dflabs.com

O Orion Instruments Polska

Orion Instruments Polska działa od roku 1990 i koncentruje się na rozwiązaniach klasy SIEM, monitoringu baz danych i aplikacji oraz wdrażaniu systemów zarządzania, pomiaru i orkiestracji zadań z dziedziny bezpieczeństwa (SOA) w tym kwalifikacji incydentów bezpieczeństwa, ich segregacji i eskalacji, wychwytywania i badania zagrożeń oraz podejmowania działań naprawczych. Firma zapewnia ekspercką ofertę o wysokiej wartości dodanej, a oferowane rozwiązania są implementowane przez doświadczonych i certyfikowanych architektów systemowych z dopuszczeniem do informacji niejawnej. Od roku 2005 Orion Instruments posiada certyfikat ISO 9001 w zakresie dos-tawy sprzętu, oprogramowania i usług serwisowych w zakresie infrastruktury informatycznej, usług i doradztwa związanego z prawidłowym funkcjonowaniem systemów informatycznych.

www.orion.pl

Partner DFLabs w Polsce:

Orion
Instruments Polska

Orion Instruments Polska Sp. z o. o.
05-082 Latchorzew, ul. Warszawska 164
tel. 22 638 31 45, e-mail orion@orion.pl
więcej informacji: www.orion.pl/incident-response