ENERGY SOAR

bako tech®

SOAR dla początkujących

Wysoka częstotliwość ataków, złożoność sieci informatycznych i brak wykwalifikowanych specjalistów narażają wiele firm na utratę danych, straty finansowe i utratę reputacji. W odpowiedzi na te wyzwania wiele organizacji wykorzystuje rozwiązania SOAR (Security Orchestration, Automation and Response).

www.energysoar.com

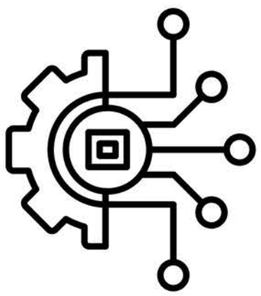
Co to jest SOAR?

SOAR to rozwiązanie umożliwiające automatyzację procesów reakcji na incydenty bezpieczeństwa. Energy SOAR to jedno z najnowszych i najbardziej innowacyjnych rozwiązań SOAR dostępnych na rynku. Jest to zintegrowana platforma z systemami informatycznymi firmy, której zadaniem jest zwiększenie szybkości i efektywności reakcji na incydenty bezpieczeństwa.

SOAR oznacza Security Orchestration, Automation and Response, a każdy komponent tej platformy odgrywa określoną rolę w procesie reagowania na incydenty bezpieczeństwa.

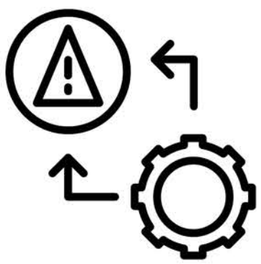
Orchestration

Orkiestracja w SOAR polega na koordynowaniu działań i integracji różnych narzędzi, systemów i procesów, aby skutecznie reagować na incydenty bezpieczeństwa. Orkiestracja umożliwia tworzenie zautomatyzowanych procesów reagowania na incydenty i usprawnia współpracę pomiędzy różnymi zespołami zaangażowanymi w reakcję na nie.



Automation

Automatyzacja jest kluczowym elementem SOAR, gdyż pozwala na szybszą i skuteczniejszą reakcję na ataki. Dzięki niej możliwe jest m.in. automatyczne uruchamianie odpowiednich procedur reagowania, wykrywanie i izolowanie zagrożeń oraz wysyłanie powiadomień o incydentach.



Response

Element reakcji w SOAR polega na szybkim i skutecznym podjęciu działań mających na celu minimalizację szkód powstałych w wyniku incydentu bezpieczeństwa. Obejmuje to identyfikację i klasyfikację incydentów, izolowanie i neutralizację zagrożeń, a także analizę i dokumentowanie incydentów.

Dlaczego warto wdrożyć SOAR?

Brak odpowiednich zasobów

Wiele organizacji zmaga się z niedoborem odpowiednio wykwalifikowanego personelu, zdolnego do skutecznego reagowania na incydenty bezpieczeństwa. SOAR umożliwia automatyzację procesów reagowania, oszczędzając czas i zasoby ludzkie, zapewniając jednocześnie skuteczną reakcję na incydenty.

Wymogi regulacyjne

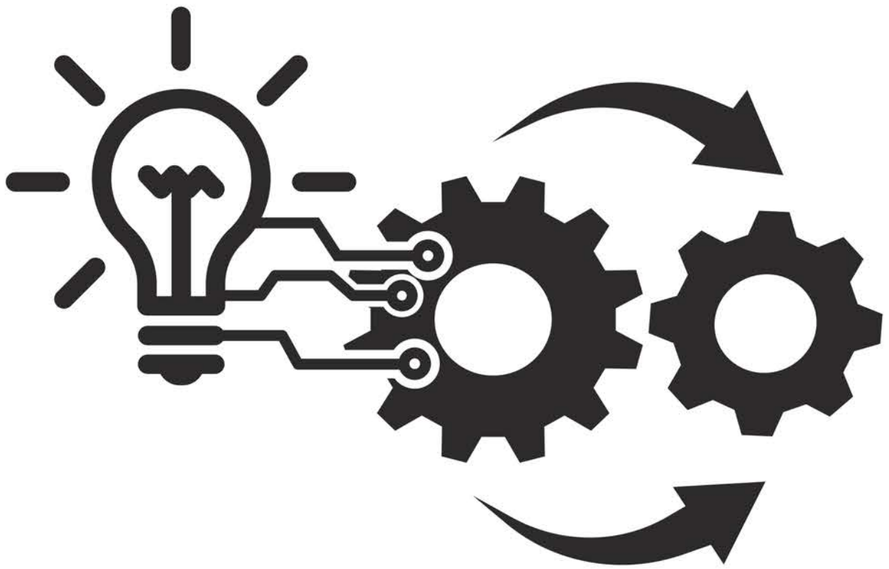
Wiele sektorów gospodarki podlega rygorystycznym wymogom regulacyjnym w zakresie cyberbezpieczeństwa. SOAR umożliwia organizacjom spełnienie tych wymagań poprzez automatyzację procesów reagowania na incydenty i raportowania wyników.

Potrzeba szybkiej reakcji

W dzisiejszym świecie reakcja na incydenty musi być szybka i skuteczna. SOAR pozwala na szybkie wykrywanie i reakcję na zagrożenia, minimalizując szkody powstałe w wyniku ataków.

Potrzeba ciągłego doskonalenia

Nowoczesne organizacje muszą stale udoskonalać swoje procedury i procesy w obszarze cyberbezpieczeństwa, aby stawić czoła rosnącym zagrożeniom. SOAR umożliwia ciągłe doskonalenie procesów reagowania na incydenty i usprawnia działanie zespołu ds. bezpieczeństwa IT.



Architektura

System Energy SOAR to kompleksowe rozwiązanie do obsługi incydentów bezpieczeństwa, konsolidujące informacje o zidentyfikowanych zagrożeniach. Bezproblemowo integruje się z różnorodnymi systemami IT i bezpieczeństwa organizacji, w tym SIEM, pocztą elektroniczną, środowiskami chmurowymi, systemami ticketowymi, zaporami sieciowymi i systemami bezpieczeństwa. Integracja ta umożliwia gromadzenie informacji z różnych źródeł w celu kompleksowego zarządzania incydentami.

Integracje

System Energy SOAR wykracza poza zbieranie danych z systemów źródłowych; może inicjować zautomatyzowane działania na zintegrowanych systemach informatycznych i bezpieczeństwa poprzez integrację API. Po wykryciu zagrożenia lub zdarzenia SOAR może wywołać określone reakcje, takie jak poddanie komputera kwarantannie lub zablokowanie adresu IP w zaporze. Dodatkowo może wysyłać powiadomienia do innych systemów lub zespołów, zachęcając je do podjęcia działań.

SOAR wykorzystuje różne mechanizmy, w tym skrypty PowerShell lub Python i integruje się z narzędziami do zarządzania siecią, narzędziami do analizy bezpieczeństwa i innymi funkcjonalnościami IT poprzez interfejsy API. Co ważne, administratorzy mogą skonfigurować SOAR tak, aby wybierał działania na podstawie określonych warunków, zgodnie z ustalonymi w organizacji regułami i zasadami bezpieczeństwa.

Integracja z CSIRT

Integracja systemu klasy SOAR z zewnętrznym zespołem CSIRT (Computer Security Incident Response Team) polega na ułatwieniu współpracy i wymiany informacji pomiędzy organizacją a zewnętrznym dostawcą usług CSIRT.

Cykl życia systemu SOAR w organizacji

Cykl życia Energy SOAR to cykliczny proces zaprojektowany z myślą o maksymalnej wydajności i zgodności z potrzebami bezpieczeństwa organizacji, wymagający metodycznego planowania i aktywnego udziału personelu na wszystkich etapach.

Kluczem do sukcesu wdrożenia systemu SOAR jest odpowiednie planowanie i dostosowanie się do potrzeb organizacji, a także ciągły rozwój i dostosowywanie się do zmieniających się wymagań.

1 PLANOWANIE

Ten podstawowy etap polega na ustaleniu jasnych celów zgodnych z celami organizacji w zakresie bezpieczeństwa. Obejmuje identyfikację typów incydentów i strategii zarządzania nimi oraz ocenę możliwości integracji z istniejącą infrastrukturą bezpieczeństwa.

2 REALIZACJA

Po zaplanowaniu w organizacji tworzony jest system SOAR. Wiąże się to z konfiguracją systemu zgodnie ze specyfikacjami organizacyjnymi, integracją z aktualnymi narzędziami bezpieczeństwa, zaprojektowaniem zautomatyzowanych przepływów pracy pod kątem wydajności oraz przeszkoleniem personelu odpowiedzialnego za jego obsługę.

3 EKSPLOATACJA I ROZWÓJ

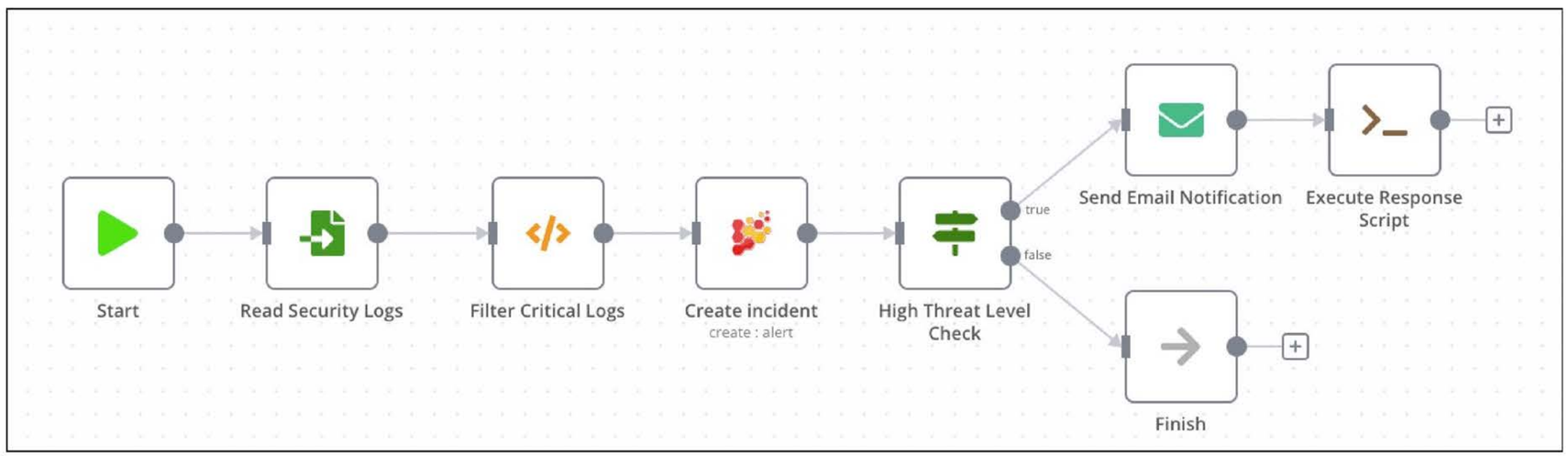
Po wdrożeniu system SOAR wymaga stałego monitorowania i iteracyjnego rozwoju, aby zachować aktualność i skuteczność. Jest to dynamiczny framework, wspierający rozwój organizacji poprzez ciągłą automatyzację nowych i bardziej złożonych procesów, zapewniający ewolucję środków bezpieczeństwa w odpowiedzi na zmieniające się zagrożenia i wymagania organizacyjne.

Tworzenie przepływów pracy

Proces przepływu pracy w systemie Energy SOAR został zaprojektowany przy użyciu takich elementów, jak reguły biznesowe, działania, warunki i integracje systemów. Użytkownicy konfigurują przepływy pracy w edytorze systemu, dodając etapy takie jak akcje, decyzje i warunki. Przepływy pracy mogą być uruchamiane ręcznie, automatycznie przez określone zdarzenia lub o określonych porach.

Każdy etap może wchodzić w interakcję z innymi systemami (np. informatycznymi, systemami bezpieczeństwa) w celu automatyzacji działań w odpowiedzi na zagrożenia. Na przykład wykrycie zagrożenia może aktywować przepływy pracy w systemach takich jak SIEM, IDS/IPS i programy antywirusowe, zwiększając automatyzację procesów i wydajność podczas incydentów bezpieczeństwa.

System obsługuje wiele gotowych integracji oraz pozwala na niestandardowe integracje z wykorzystaniem API.
Funkcje te usprawniają tworzenie przepływu pracy, automatyzują działania i skutecznie integrują systemy w celu reagowania na zdarzenia związane z bezpieczeństwem.



System SOAR w praktyce

Energy SOAR usprawnia i przyspiesza zarządzanie incydentami związanymi z bezpieczeństwem w całej organizacji.

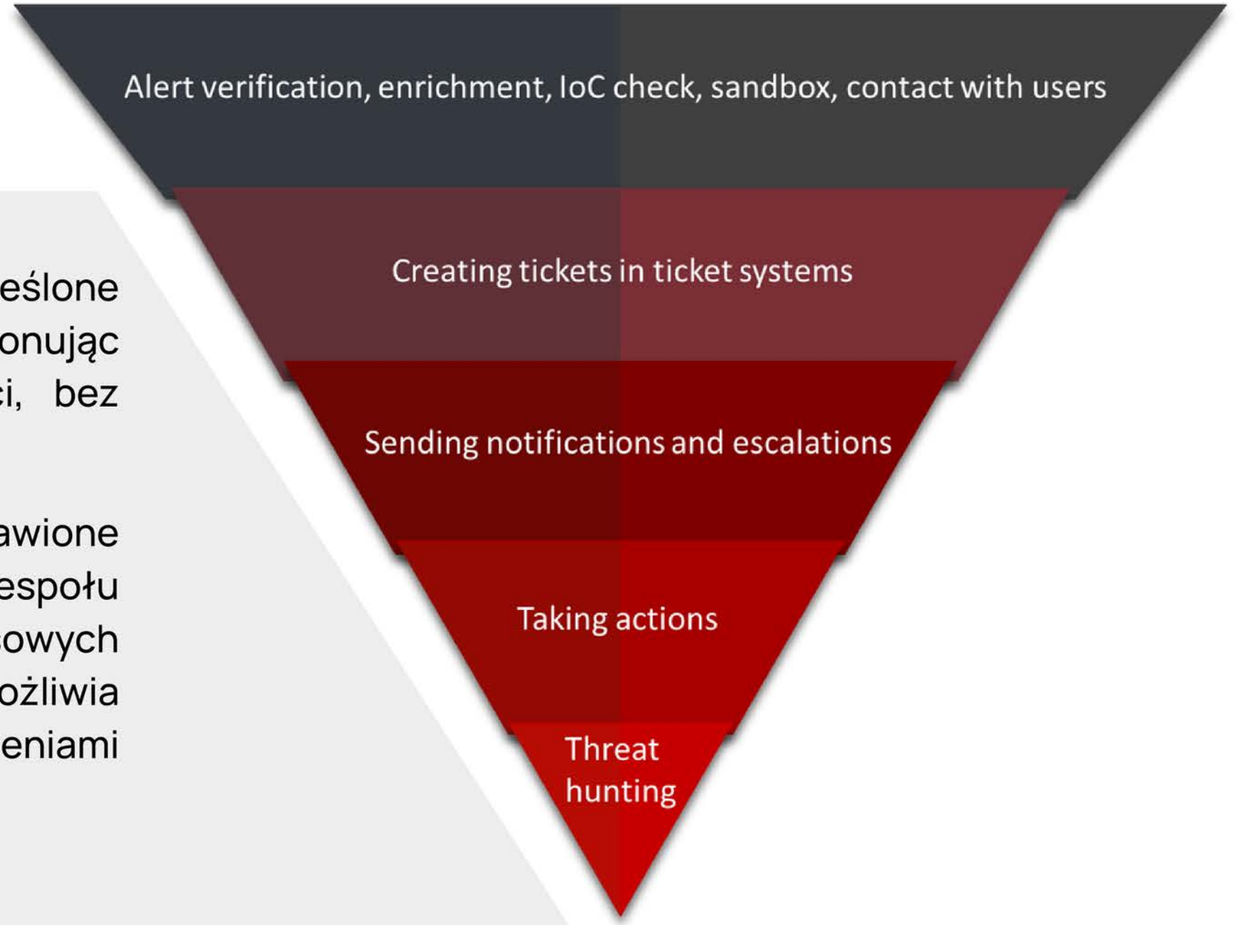
Przyjrzyjmy się szczegółowo procesowi od wykrycia do rozwiązania.

Początkowo SOAR integruje się z różnymi platformami bezpieczeństwa, takimi jak SIEM, IDS, IPS, EDR i systemami poczty elektronicznej, wydobywając dane o incydentach. Silnik przepływu pracy automatyzuje następnie sekwencję działań, zazwyczaj ręcznych, zwiększając wydajność.

System analizuje atrybuty zdarzeń (obserwowalne), takie jak adresy IP, nazwy hostów, nazwy użytkowników czy adresy URL. Rozszerza incydenty o dodatkowe dane, dodając je do listy spraw, gdzie każdy jest automatycznie oznaczany wagą i odpowiednimi etykietami. Operatorzy, przydzielani ręcznie lub automatycznie, otrzymują określone zadania. Użytkownicy mają przejrzystą listę zadań, a wszystkie czynności są rejestrowane w historii.

W niektórych przypadkach, gdy spełnione są warunki, takie jak określone reguły korelacji, SOAR autonomicznie zarządza odpowiedzią, wykonując takie działania, jak blokowanie adresów IP lub izolacja sieci, bez interwencji personelu IT.

Intuicyjny interfejs graficzny SOAR, wyposażony we wstępnie ustawione pulpity nawigacyjne, zapewnia wgląd w status zadań, obciążenie zespołu i przestrzeganie umów SLA. Ułatwia generowanie kompleksowych raportów prezentujących działania IT lub SOC. Narzędzie to umożliwia organizacjom szybkie i skuteczne radzenie sobie z zagrożeniami bezpieczeństwa, chroniąc integralność i prywatność danych.



Przykład użycia

Analiza poczty elektronicznej

W trakcie procesu bezpieczeństwa otrzymana podejrzana wiadomość e-mail jest kierowana do zintegrowanego systemu SOAR przez pracownika, który ją flaguje.

System SOAR przeprowadza dogłębną analizę treści i struktury wiadomości e-mail poprzez analizę syntaktyczną i semantyczną w celu wykrycia oznak phishingu, takich jak podejrzane linki lub załączniki. Odwołuje się do baz danych analizy zagrożeń w celu porównania wiadomości e-mail ze znanymi wzorcami zagrożeń.

Po wykryciu potencjalnego zagrożenia system SOAR klasyfikuje zdarzenie jako możliwą próbę phishingu. Następnie może automatycznie zainicjować środki ochronne, takie jak zablokowanie nadawcy lub jego adresu IP i przekazanie problemu wyspecjalizowanemu zespołowi ds. bezpieczeństwa w celu dalszej analizy.

Dodatkowo system SOAR jest przystosowany do szybkiego powiadamiania odpowiednich zespołów bezpieczeństwa wewnętrznego lub CSIRT, umożliwiając szybkie podjęcie działań przeciwko zagrożeniu. Zespoły te mogą przeprowadzić obszerną analizę zdarzenia w celu zidentyfikowania i zneutralizowania wszelkich dodatkowych zagrożeń.

Kluczową zaletą systemu SOAR jest jego zdolność do lokalizowania i neutralizowania równoległych zagrożeń phishingowych w organizacji. Wykorzystując dane z pierwszego zdarzenia, może wyszukiwać i ograniczać podobne zagrożenia w systemie poczty elektronicznej organizacji, automatycznie umieszczając je w spamie lub usuwając, wzmacniając w ten sposób zabezpieczenia organizacji.

Przykład użycia

Automatyczne blokowanie hosta lub adresu IP jest kluczowym przypadkiem użycia w systemie Energy SOAR, szczególnie w przypadku ochrony przed atakami złośliwego oprogramowania i naruszeniami sieci.
Oto uproszczony przegląd sposobu, w jaki system radzi sobie z tym scenariuszem:

Wykrywanie zagrożeń

System SOAR zintegrowany z narzędziami bezpieczeństwa, takimi jak IDS/IPS i ochrona przed złośliwym oprogramowaniem, identyfikuje podejrzane adresy IP lub nietypowy ruch sieciowy

Analiza i potwierdzenie

SOAR wykorzystuje analizę zachowań i trendów, a także analizę zagrożeń zewnętrznych, aby potwierdzić, czy wykryta aktywność jest prawdziwym zagrożeniem.

Klasyfikacja incydentów

Jeśli działanie zostanie uznane za złośliwe, incydent jest klasyfikowany jako zagrożenie, a odpowiednie informacje są przechowywane do dalszej analizy.

Automatyczne blokowanie

SOAR automatycznie podejmuje działania mające na celu zablokowanie złośliwego adresu IP lub hosta. Wiąże się to z konfiguracją zapór sieciowych lub wdrażaniem blokad na poziomie sieci.

Powiadomienie

Powiadomienia są automatycznie wysyłane do odpowiednich indywidualnych zespołów sortujących, dostarczając szczegółowych informacji o zdarzeniu i podjętych działaniach.

Analiza i reakcja

Zespół ds. bezpieczeństwa otrzymuje powiadomienie, przeprowadza dalszą analizę, podejmuje dodatkowe działania w celu zaradzenia incydentowi, takie jak śledzenie źródła ataku lub wzmocnienie środków bezpieczeństwa.

Rozdzielczość i raportowanie

Po rozwiązaniu incydentu informacje są przechowywane w SOAR w celu raportowania i ulepszania. Dane te wspierają analizę trendów i identyfikują luki w zabezpieczeniach

Przykład użycia

Wykorzystanie trendów analizy zagrożeń

System Energy SOAR nie tylko skutecznie zarządza incydentami związanymi z bezpieczeństwem, ale także bada wskaźniki zagrożenia (IoC) na podstawie list wywiadowczych dotyczących zagrożeń, wykorzystując aktualne trendy ataków w organizacji.

Przykład 1:

Po wykryciu kampanii złośliwego oprogramowania wykorzystującej określoną domenę do komunikacji HTTP użytkownicy SOAR mogą przeprowadzić analizę dzienników DNS w celu sprawdzenia komunikacji z tą domeną. Jeśli okaże się, że punkt końcowy nawiązał taką komunikację, działania w systemie SOAR, takie jak poddanie kwarantannie lub izolowanie hosta, mogą zminimalizować ryzyko dalszej rozprzestrzeniania się zagrożenia.

Przykład 2:

W kampaniach phishingowych wykorzystujących domeny przypominające popularne firmy (np. „mlcrosoft.com” zamiast „microsoft.com”) system SOAR analizuje logi pod kątem połączeń z podejrzanymi domenami. W przypadku znalezienia połączeń można zastosować szybkie środki, takie jak blokowanie dostępu lub ostrzeganie użytkowników, aby zabezpieczyć organizację przed zagrożeniami typu phishing.

Wykorzystując możliwości SOAR w zakresie integracji z listami zagrożeń i analizowania trendów ataków, system Energy SOAR umożliwia organizacjom szybką reakcję na potencjalne zagrożenia. Pełniąc funkcję scentralizowanego ośrodka zarządzania bezpieczeństwem, konsoliduje informacje o incydentach i zdarzeniach związanych z bezpieczeństwem, ułatwiając skuteczne monitorowanie i reagowanie na pojawiające się zagrożenia.

Przedstawiamy studium przypadku organizacji XYZ, która potrzebowała zabezpieczyć swój system przed nieautoryzowanym logowaniem administratorów poza godzinami pracy. Celem było wdrożenie mechanizmu weryfikacji logowania poprzez wykorzystanie wiadomości SMS z unikalnym linkiem, który administrator musiał potwierdzić w określonym terminie; w przeciwnym razie konto administratora zostanie automatycznie zablokowane.

Proces wdrażania:

1 Wykrywanie nieautoryzowanych prób logowania:

System Energy SOAR został skonfigurowany do monitorowania logów systemowych i zdarzeń związanych z czynnościami logowania. W przypadku wykrycia przez administratora próby nieautoryzowanego logowania poza godzinami pracy system inicjuje procedurę weryfikacji.

2 Generowanie wiadomości SMS:

System SOAR automatycznie generuje wiadomość SMS zawierającą unikalny link potwierdzający logowanie. Do każdej próby logowania przypisany jest konkretny link z określonym okresem ważności (np. 30 minut).

3 Wysyłanie wiadomości SMS:

System SOAR wysyła wygenerowaną wiadomość SMS zawierającą link potwierdzający logowanie na zarejestrowane urządzenie mobilne powiązane z kontem administratora.

4 Potwierdzenie logowania:

Administrator otrzymuje na swoje urządzenie mobilne wiadomość SMS z linkiem potwierdzającym logowanie. Aby potwierdzić logowanie, administrator musi kliknąć w podany link.

5 Blokada konta w przypadku braku potwierdzenia:

Jeżeli administrator nie potwierdzi logowania w określonym terminie, system SOAR automatycznie blokuje konto administratora, minimalizując ryzyko nieuprawnionego dostępu i działań w systemie.

6 Działania po potwierdzeniu logowania:

Po kliknięciu w link potwierdzający logowanie system SOAR otrzymuje potwierdzenie od strony administratora. Jeżeli potwierdzenie zostanie otrzymane w określonym terminie (np. 30 minut), logowanie uważa się za autoryzowane.

ENERGY SOAR

Energy SOAR to narzędzie, które nie zmusza do kompromisów i zmniejszania wymagań. Wręcz przeciwnie, rozszerza twoje możliwości i dodaje kontroli w najbardziej niewiarygodnych obszarach.

Aby uzyskać wersję demonstracyjną Energy SOAR, skontaktuj się z nami:

logserver@bakotech.pl
www.bakotech.pl/vendors/energy-logserver
www.energysoar.com

bakotech®