



Wykrywanie i reagowanie na zagrożenia w cyberprzestrzeni

Spis treści

Znaczenie skutecznego wykrywania i reagowania na incydenty	3
Czym jest SIEM?	3
Kluczowe funkcje nowoczesnego systemu SIEM	4
KPI w systemach SIEM – jak mierzyć skuteczność SOC	4
Czym jest SOAR?	6
Analiza przypadku: atak typu brute force – od detekcji w SIEM do zamknięcia incydentu przez SOAR.....	9

Znaczenie skutecznego wykrywania i reagowania na incydenty

Każda nowoczesna organizacja przetwarza ogromne ilości danych generowanych przez sieci, systemy, aplikacje oraz urządzenia użytkowników. Każdego dnia infrastruktura IT/OT generuje miliony zdarzeń, spośród których tylko niewielki odsetek stanowi realne zagrożenie. Jednocześnie cyberprzestępcy stosują coraz bardziej wyrafinowane techniki – od ataków wykorzystujących sztuczną inteligencję, przez ransomware, po długotrwałe kampanie APT (*ang. Advanced Persistent Threat - APT*), które potrafią pozostawać niewykryte przez wiele miesięcy.

W takich warunkach kluczowe staje się posiadanie mechanizmów, które w czasie rzeczywistym zbierają, korelują i analizują dane pochodzące z całego środowiska IT/OT, a następnie automatyzują proces reagowania na wykryte incydenty. Odpowiedzią na te potrzeby są dwie uzupełniające się klasy rozwiązań: systemy klasy SIEM (*ang. Security Information and Event Management - SIEM*) oraz platformy SOAR (*ang. Security Orchestration, Automation and Response - SOAR*).

Czym jest SIEM?

Proces działania SIEM można podzielić na kilka etapów:

- **Zbieranie danych** – system pobiera logi i zdarzenia z setek różnych źródeł, wykorzystując zarówno metody bez agentowe (SNMP (*ang. Simple Network Management Protocol*), WMI (*ang. Windows Management Instrumentation*), syslog, API (*ang. Application Programming Interface*)), jak i dedykowane agenty instalowane na końcówkach, umożliwiające między innymi monitorowanie integralności plików (*ang. File Integrity Monitoring - FIM*) czy analizę zachowań użytkowników (*ang. User and Entity Behavior Analytics - UEBA*).
- **Normalizacja i parsowanie** – surowe dane są ujednolicane do wspólnego formatu, co pozwala na ich porównywanie i korelację niezależnie od producenta źródłowego systemu.
- **Korelacja i analiza** – silnik reguł korelacyjnych, wspierany coraz częściej przez modele uczenia maszynowego (UEBA), analizuje wzorce zachowań i wykrywa odstępstwa od normy.
- **Ocena ryzyka i priorytetyzacja** – wykryte incydenty są automatycznie oceniane pod kątem krytyczności aktywów, typu zagrożenia oraz liczby powiązanych zdarzeń, co pozwala analitykom skupić się w pierwszej kolejności na najważniejszych alarmach.

- **Dochodzenie i raportowanie** – system dostarcza narzędzi do wizualizacji powiązań między zdarzeniami, hostami, adresami IP i użytkownikami, ułatwiając analitykom pełne zrozumienie kontekstu incydentu.

Kluczowe funkcje nowoczesnego systemu SIEM

Obecnie platformy SIEM oferują znacznie więcej niż tylko podstawowe zbieranie logów:

- **Uniwersalne zbieranie zdarzeń** – integracja z setkami źródeł IT/OT, w tym platformami chmurowymi oraz urządzeniami lokalnymi.
- **Wbudowana baza CMDB** (*ang. Configuration Management Database*) – automatyczna identyfikacja i kategoryzacja aktywów, monitorowanie ich stanu oraz zmian konfiguracji.
- **Zaawansowane wykrywanie behawioralne z użyciem AI** – tysiące reguł korelacyjnych aktualizowanych na podstawie najnowszych informacji o zagrożeniach, wsparte modelami ML możliwymi do trenowania przez samych użytkowników.
- **Ocena ryzyka w czasie rzeczywistym** – dynamiczne przypisywanie poziomu ryzyka użytkownikom i hostom na podstawie krytyczności zasobów oraz liczby powiązanych incydentów.
- **Wbudowana automatyzacja (SOAR)** – możliwość uruchamiania gotowych playbooków bezpośrednio z poziomu incydentu.
- **Architektura rozproszona i skalowalność** – możliwość rozbudowy systemu poprzez dodawanie kolejnych węzłów przetwarzających bez przestojów.
- **Raportowanie zgodności** – gotowe raporty wspierające spełnienie wymagań regulacyjnych (RODO/GDPR, ISO 27001, PCI DSS, NIS2 i inne).
- **Elastyczne modele wdrożenia** – on-premise, w chmurze prywatnej lub jako usługa SaaS.

KPI w systemach SIEM – jak mierzyć skuteczność SOC

Wdrożenie systemu SIEM to dopiero pierwszy krok – kluczowe jest, aby organizacja potrafiła mierzyć, czy inwestycja przekłada się na realną poprawę bezpieczeństwa. Do najważniejszych wskaźników efektywności (*ang. Key Performance Indicators - KPI*), które warto monitorować w kontekście działania SOC (*ang. Security Operations Center*), należą:

Wskaźnik	Opis	Znaczenie
MTTD (Mean Time to Detect)	Średni czas od wystąpienia zdarzenia do jego wykrycia	Im krótszy, tym mniejsze okno czasowe dla atakującego
MTTR (Mean Time to Respond/Resolve)	Średni czas od wykrycia incydentu do jego pełnego zamknięcia	Bezpośrednio wpływa na skalę potencjalnych strat
MTTC (Mean Time to Contain)	Średni czas do ograniczenia (powstrzymania) zagrożenia	Kluczowy przy ograniczaniu rozprzestrzeniania się ataku
Liczba fałszywych alarmów (False Positive Rate)	Odsetek alertów niebędących realnym zagrożeniem	Wysoki wskaźnik prowadzi do zmęczenia analityków (alert fatigue)
Wskaźnik automatyzacji (Automation Rate)	Procent incydentów obsługiwanych automatycznie przez playbooki	Pokazuje dojrzałość procesów SOAR i obciążenie analityków
Liczba obsługiwanych incydentów wg priorytetu	Rozkład incydentów według krytyczności	Pomaga w planowaniu zasobów zespołu
Koszt na incydent / ROI (ang. Return on Investment) automatyzacji	Szacowane oszczędności wynikające z automatyzacji zadań	Argument biznesowy dla dalszych inwestycji w SOC
SLA (ang. Service Level Agreement) compliance	Odsetek incydentów obsługiwanych w ramach ustalonych okien czasowych	Miernik jakości usług, szczególnie istotny dla MSSP (ang. Managed Security Service Provider)

Nowoczesne platformy SIEM oferują dedykowane dashboardy operacyjne SOC prezentujące te wskaźniki w czasie rzeczywistym – liczbę aktywnych alertów, wskaźnik konwersji zdarzeń na incydenty, średni czas triage'u, czy wartość ROI wygenerowaną przez automatyzację. Regularna analiza tych danych pozwala nie tylko oceniać efektywność zespołu, ale również identyfikować obszary wymagające dostrojenia reguł korelacyjnych czy dodatkowego szkolenia analityków.

Czym jest SOAR?

Platforma SIEM odpowiada za wykrywanie zdarzeń, natomiast platforma SOAR odpowiada za reagowanie. Systemy SOAR pozwalają zespołom bezpieczeństwa zautomatyzować powtarzalne czynności związane z obsługą incydentów, zredukować czas reakcji oraz skoordynować działania pomiędzy różnymi narzędziami i zespołami – nie tylko w obszarze SecOps, ale również NetOps, ITOps, CloudOps czy OTOps.

Główne obszary funkcjonalne SOAR

Automatyzacja i orkiestracja działań

Platforma SOAR integruje się z setkami rozwiązań bezpieczeństwa (firewalle, systemy EDR – *(ang. Endpoint Detection and Response)*, narzędzia do zarządzania podatnościami, systemy ticketowe, poczta, komunikatory) poprzez gotowe konektory, umożliwiając wykonywanie akcji – takich jak blokowanie adresu IP, izolacja hosta czy wzbogacanie danych o wskaźnikach kompromitacji (*ang. Indicators of Compromise - IOC*) – bez ręcznej interwencji analityka.

Playbooki i kreator o niskim progu wejścia (low-code)

Wizualny kreator playbooków pozwala budować scenariusze reagowania bez konieczności zaawansowanego programowania. Coraz częściej wsparcie w tym procesie zapewnia generatywna sztuczna inteligencja, która na podstawie opisu w języku naturalnym potrafi wygenerować strukturę playbooka lub konektora.

Zarządzanie incydentami i przypadkami (case management)

SOAR wykonuje automatycznie tzw. triaż i wzbogaca zdarzenia napływające z systemów SIEM oraz innych źródeł. Rutynowe alerty mogą być zamykane automatycznie, natomiast zdarzenia o wysokim priorytecie są mapowane do frameworku MITRE ATT&CK i grupowane w przypadki (case) wymagające przeprowadzenia dalszej analizy zdarzenia.

Zarządzanie Threat Intelligence

Automatyczne pobieranie, normalizacja i wzbogacanie danych o zagrożeniach z zewnętrznych źródeł (feedy STIX/TAXII (*ang. Structured Threat Information Expression/Trusted Automation Exchange of Intelligence Information*), bazy reputacji, informacje o zagrożeniach) pozwala analitykom podejmować szybsze i lepiej uzasadnione decyzje.

Zarządzanie zasobami i podatnościami

Integracja z systemami skanowania podatności oraz bazami aktywów pozwala uzyskać pełny, oparty na ryzyku obraz infrastruktury IT/OT, co ułatwia priorytetyzację działań naprawczych w przypadku wystąpienia incydentu.

War Room – centrum dowodzenia w sytuacji kryzysowej

Jednym z kluczowych, choć często niedocenianych elementów nowoczesnych platform SOAR jest funkcja **war room** (pokoju kryzysowego). W przypadku poważnych incydentów – takich jak atak ransomware, wyciek danych czy naruszenie zasad/polityk bezpieczeństwa o dużej skali – szybka i skoordynowana reakcja wielu zespołów jest krytyczna w celu ograniczenia strat.

War room to dedykowana, bezpieczna przestrzeń do współpracy, uruchamiana bezpośrednio z poziomu incydentu. Do jej najważniejszych cech należą:

- **Dostęp wyłącznie na zaproszenie** – ograniczenie kręgu osób zaangażowanych w obsługę incydentu do niezbędnego minimum, co ma istotne znaczenie zarówno organizacyjne, jak i prawne (np. przy obsłudze incydentów podlegających obowiązkowi zgłoszenia do CSIRT (*ang. Computer Security Incident Response Team*)).
- **Integracja z narzędziami komunikacyjnymi** – połączenie z pocztą, Slackiem, Teams i innymi platformami, tak aby zespoły mogły pracować w znanym sobie środowisku, zachowując jednocześnie centralny nadzór nad przebiegiem incydentu.
- **Zarządzanie zadaniami** – przypisywanie i śledzenie zadań poszczególnym członkom zespołu w czasie rzeczywistym.
- **Rejestrowanie działań na poziomie śledczym (forensic-grade logging)** – każda czynność, decyzja i komunikat są dokumentowane, co jest niezbędne przy późniejszej analizie post-incydentalnej oraz w kontekście wymogów regulacyjnych (np. *ang. Network and Information Security Directive 2 – NIS2*, RODO).
- **Prywatna komunikacja i raportowanie** – możliwość generowania raportów podsumowujących przebieg reakcji na incydent na potrzeby zarządu, audytu czy organów nadzorczych.

Funkcja war room realnie skraca czas potrzebny na zebranie odpowiednich osób i uruchomienie procedury reagowania, a także zapewnia rozliczalność działań – co w erze rosnących wymogów regulacyjnych (dyrektywa NIS2, *ang. Digital Operational Resilience Act – DORA*) staje się nie tyle udogodnieniem, co koniecznością.

Rekomendacje dotyczące wdrażania systemów SIEM/SOAR

1. **Zacznij od inwentaryzacji źródeł danych** – zidentyfikuj wszystkie systemy, które powinny przesyłać logi do SIEM, uwzględniając środowiska IT oraz OT.
2. **Wdrażaj automatyzację stopniowo** – zacznij od prostych, powtarzalnych scenariuszy (np. wzbogacanie danych, blokowanie znanych IOC), a dopiero potem przechodź do bardziej złożonych playbooków.
3. **Regularnie dostrajaj reguły korelacyjne** – statyczny zestaw reguł szybko traci skuteczność wobec ewoluujących technik ataku; korzystaj z aktualizowanych źródeł threat intelligence.
4. **Monitoruj KPI i raportuj je do zarządu** – przełożenie działań SOC na język biznesowy (koszty, ryzyko, zgodność regulacyjna) ułatwia uzasadnienie dalszych inwestycji.
5. **Przygotuj procedury war room jeszcze przed incydem** – zdefiniuj role, kanały komunikacji i kryteria eskalacji, zanim będą one potrzebne w realnej sytuacji kryzysowej.
6. **Zadbaj o zgodność z wymogami regulacyjnymi** – szczególnie w kontekście dyrektywy NIS2, obowiązku zgłaszania incydentów do właściwego CSIRT oraz wymogów dotyczących retencji i integralności logów.
7. **Inwestuj w rozwój kompetencji zespołu** – nawet najlepsza automatyzacja nie zastąpi doświadczonych analityków zdolnych do interpretacji złożonych, nietypowych incydentów.

Skuteczna ochrona przed współczesnymi cyberzagrożeniami wymaga połączenia dwóch komplementarnych zdolności: szerokiej widoczności i analizy danych (SIEM) oraz szybkiej, skoordynowanej reakcji (SOAR). Systemy te, wspierane coraz częściej przez mechanizmy sztucznej inteligencji i automatyzacji, pozwalają organizacjom nie tylko skrócić czas wykrycia i reakcji na incydent, ale również usystematyzować procesy bezpieczeństwa, poprawić zgodność regulacyjną i realnie ograniczyć skutki finansowe i wizerunkowe cyberataków. Kluczowym elementem dojrzałej organizacji jest przy tym nie tylko posiadanie odpowiednich narzędzi, lecz również wypracowanych procedur – takich jak war room – oraz systematyczne mierzenie efektywności działania SOC za pomocą jasno zdefiniowanych wskaźników KPI.

Analiza przypadku: atak typu brute force – od detekcji w SIEM do zamknięcia incydentu przez SOAR

Scenariusz:

System SIEM monitoruje w czasie rzeczywistym logowania do domeny Active Directory oraz do systemu pocztowego dostępnego z internetu i systemu VPN (*ang. Virtual Private Network*). W nocy, w krótkim odstępie czasu, z jednego zewnętrznego adresu IP rejestrowane są wielokrotne nieudane próby logowania na różne konta użytkowników, w tym – w pewnym momencie – na konto należące do CEO (*ang. Chief Executive Officer*) organizacji.

Poniżej przedstawiono pełny przebieg obsługi takiego zdarzenia, od momentu detekcji aż po zamknięcie incydentu.

Etap 1: Detekcja w SIEM

Zbieranie zdarzeń

SIEM zbiera logi uwierzytelniania z kontrolerów domeny, serwera VPN oraz bramy pocztowej. Każda próba logowania (udana i nieudana) jest normalizowana do wspólnego formatu, zawierającego m.in.: znacznik czasu, adres IP źródłowy, nazwę konta, wynik logowania oraz system docelowy.

Korelacja

Reguła korelacyjna odpowiedzialna za wykrywanie brute force analizuje częstotliwość nieudanych logowań w krótkim oknie czasowym. Typowy wzorzec wyzwalający alert to np. **więcej niż 10 nieudanych logowań w ciągu 5 minut z jednego adresu IP**, niezależnie od tego, czy dotyczą one jednego, czy wielu kont (co odróżnia klasyczny brute force od ataku typu password spraying, gdzie próbuje się jednego hasła na wielu kontach).

W analizowanym przypadku silnik korelacyjny wykrywa:

- 47 nieudanych prób logowania w ciągu 8 minut,
- z jednego adresu IP (spoza znanej puli adresów firmowych),
- dotyczących 12 różnych kont, w tym konta CEO,
- zakończonych jedną udaną autoryzacją na koncie CEO.

Wzbogacenie i ocena ryzyka

System automatycznie sprawdza reputację adresu IP w zewnętrznych bazach threat intelligence (adres figuruje jako powiązany z wcześniejszą infrastrukturą botnetową) oraz konfrontuje docelowe konto z bazą CMDB, gdzie konto CEO jest oznaczone jako zasób o **najwyższej krytyczności** (VIP/high-value target). Te dwa czynniki – zła reputacja źródła oraz krytyczność konta – silnik ryzyka przekłada na najwyższy możliwy priorytet incydentu (Critical).

Wygenerowanie incydentu

SIEM grupuje wszystkie powiązane zdarzenia w jeden incydent, wizualizując graf powiązań: adres IP → 12 kont docelowych → jedno konto z udaną autoryzacją. Incydent jest automatycznie przekazywany do platformy SOAR w celu podjęcia działań.

Etap 2: Automatyczna reakcja w SOAR

Po otrzymaniu incydentu z SIEM, SOAR uruchamia dedykowany playbook „Brute Force Response”, którego przebieg wygląda następująco:

Krok 1 – Wzbogacenie kontekstu

Playbook automatycznie odpytuje dodatkowe źródła: system EDR (czy na stacji CEO występują podejrzane procesy), system pocztowy (czy po udanym logowaniu wysłano jakieś wiadomości lub utworzono reguły przekierowania poczty) oraz bazę zasobów (jakie uprawnienia i dostęp do systemów posiada konto CEO).

Krok 2 – Automatyczna blokada adresu IP

Bez oczekiwania na decyzję analityka, playbook wykonuje akcję niskiego ryzyka biznesowego, ale wysokiej skuteczności: blokuje adres IP źródłowy na urządzeniu brzegowym (firewall/VPN gateway). Jest to działanie odwracalne i nieinwazyjne dla użytkowników, dlatego może być realizowane w pełni automatycznie.

Krok 3 – Warunkowa blokada konta

Ponieważ zaistniała **udana** autoryzacja na koncie CEO po serii nieudanych prób (silny wskaźnik kompromitacji), playbook wykonuje kolejne, bardziej inwazyjne działanie: **wymusza natychmiastowe wygaśnięcie aktywnej sesji oraz tymczasową blokadę konta** w Active Directory / systemie IAM (ang. *Identity and Access Management*). Dla kont oznaczonych jako VIP (ang. *Very Important Person*) część organizacji definiuje tę akcję jako w pełni automatyczną (priorytet bezpieczeństwa nad dostępnością), inne – jako wymagającą jednego kliknięcia i zatwierdzenia przez analityka drugiej linii (L2), aby

uniknąć zakłócenia pracy kluczowej osoby bez potwierdzenia zagrożenia. Wybór modelu zależy od polityki organizacji i powinien być ustalony z wyprzedzeniem, a nie w trakcie incydentu.

Krok 4 – Eskalacja

Ze względu na krytyczność konta i potwierdzoną kompromitację, playbook automatycznie podnosi priorytet incydentu do najwyższego poziomu i uruchamia procedurę eskalacyjną, obejmującą powiadomienie kierownika SOC, CISO (*ang. Chief Information Security Officer*) oraz – w zależności od polityki organizacji – asystenta lub biuro CEO poprzez ustalony, zaufany kanał komunikacji (nigdy przez potencjalnie skompromitowane konto pocztowe ofiary).

Etap 3: Uruchomienie war room

Z uwagi na wagę incydentu (skompromitowane konto najwyższego kierownictwa) analityk L2 lub kierownik zmiany podejmuje decyzję o uruchomieniu **war room** – dedykowanej, dostępnej wyłącznie na zaproszenie przestrzeni koordynacji kryzysowej.

Skład zespołu war room w tym scenariuszu zwykle obejmuje:

- analityka SOC prowadzącego incydent,
- kierownika SOC / CISO,
- przedstawiciela zespołu IT odpowiedzialnego za tożsamość i dostęp (IAM),
- w razie potrzeby – przedstawiciela działu prawnego lub compliance (ze względu na potencjalny obowiązek zgłoszenia incydentu do CSIRT w ramach NIS2, jeśli dojdzie do potwierdzonego naruszenia danych),
- osobę kontaktową po stronie biura zarządu, bez ujawniania szczegółów technicznych szerszemu gronu.

Działania podejmowane w war room:

1. **Weryfikacja skali kompromitacji** – zespół sprawdza, czy z konta CEO w okresie między udanym logowaniem a blokadą doszło do dodatkowych działań: dostępu do wrażliwych dokumentów, prób transferu danych, zmian uprawnień innych kont, wysyłki wiadomości (możliwy wektor do dalszego ataku typu BEC – Business Email Compromise).

2. **Przydział zadań** – każdemu członkowi zespołu przypisywane są konkretne działania (np. „IAM – reset hasła i wymuszenie ponownej rejestracji MFA”, „SOC – pełna analiza logów z 72h wstecz”), z jasno określonym czasem realizacji.
3. **Komunikacja z użytkownikiem** – bezpośredni, zweryfikowany kontakt z CEO (telefonicznie lub osobiście, nie mailowo) w celu potwierdzenia, czy logowanie było świadome, oraz przekazanie instrukcji dotyczących bezpiecznego odzyskania dostępu.
4. **Rejestrowanie działań** – wszystkie decyzje, godziny i osoby odpowiedzialne są automatycznie logowane w sposób odporny na manipulację (forensic-grade logging), co jest kluczowe zarówno dla późniejszej analizy powłamaniowej, jak i ewentualnego postępowania regulacyjnego czy ubezpieczeniowego.
5. **Decyzja o zakresie komunikacji wewnętrznej** – ze względu na wrażliwość sytuacji (konto najwyższego kierownictwa), krąg osób poinformowanych o szczegółach jest celowo ograniczany do niezbędnego minimum, przy jednoczesnym zachowaniu pełnej przejrzystości działań w ramach samego zespołu reagowania.

Etap 4: Odzyskanie dostępu i działania naprawcze

Po potwierdzeniu, że zagrożenie zostało opanowane, zespół podejmuje działania przywracające normalne funkcjonowanie, przy zachowaniu podwyższonego nadzoru:

- wymuszenie zmiany hasła oraz ponownej rejestracji uwierzytelniania wieloskładnikowego na koncie CEO,
- przegląd i ewentualne cofnięcie zmian dokonanych w trakcie okna kompromitacji (np. reguł przekierowania poczty, jeśli takie znaleziono),
- utrzymanie wzmocnionego monitoringu (dodatkowe reguły korelacyjne, niższy próg alertowania) na koncie CEO przez określony czas po incydencie,
- aktualizacja list blokad (blacklist) o wykryty adres IP oraz powiązane z nim wskaźniki kompromitacji w module threat intelligence, aby przyspieszyć wykrycie ewentualnego powrotu tej samej grupy przestępczej lub atakującego.

Etap 5: Zamknięcie incydentu i wnioski

Na zakończenie SOAR automatycznie generuje raport podsumowujący pełny przebieg incydentu – czas wykrycia (MTTD), czas do pierwszej automatycznej reakcji, czas do pełnego opanowania zagrożenia (MTTC) oraz czas całkowitego zamknięcia (MTTR). Dane

te trafiają do dashboardu operacyjnego SOC, gdzie wpływają na ogólne wskaźniki efektywności zespołu.

Z incydentu wyciągane są również wnioski proceduralne, np.:

- czy próg reguły korelacyjnej dla kont VIP powinien być jeszcze bardziej restrykcyjny (niższa liczba prób wyzwalająca alert),
- czy konto CEO i innych kluczowych osób powinno mieć wymuszone dodatkowe zabezpieczenia (np. uwierzytelnianie adaptacyjne uwzględniające lokalizację i urządzenie),
- czy procedura war room zadziałała zgodnie z założeniami czasowymi, czy wymaga aktualizacji.

Podsumowanie

Przedstawiony scenariusz pokazuje, jak SIEM i SOAR współpracują na każdym etapie obsługi incydentu: od automatycznej detekcji wzorca ataku brute force, przez natychmiastową, częściowo automatyczną reakcję (blokada IP, blokada konta), aż po skoordynowaną pracę zespołu w war room w sytuacji, gdy zagrożone jest konto o szczególnym znaczeniu biznesowym. Kluczowym elementem skuteczności całego procesu jest wcześniejsze zdefiniowanie polityk dla kont VIP – w tym granicy między działaniami w pełni automatycznymi a tymi wymagającymi potwierdzenia człowieka – ponieważ to właśnie te decyzje, podjęte z wyprzedzeniem, decydują o szybkości i skuteczności reakcji w realnej sytuacji kryzysowej.