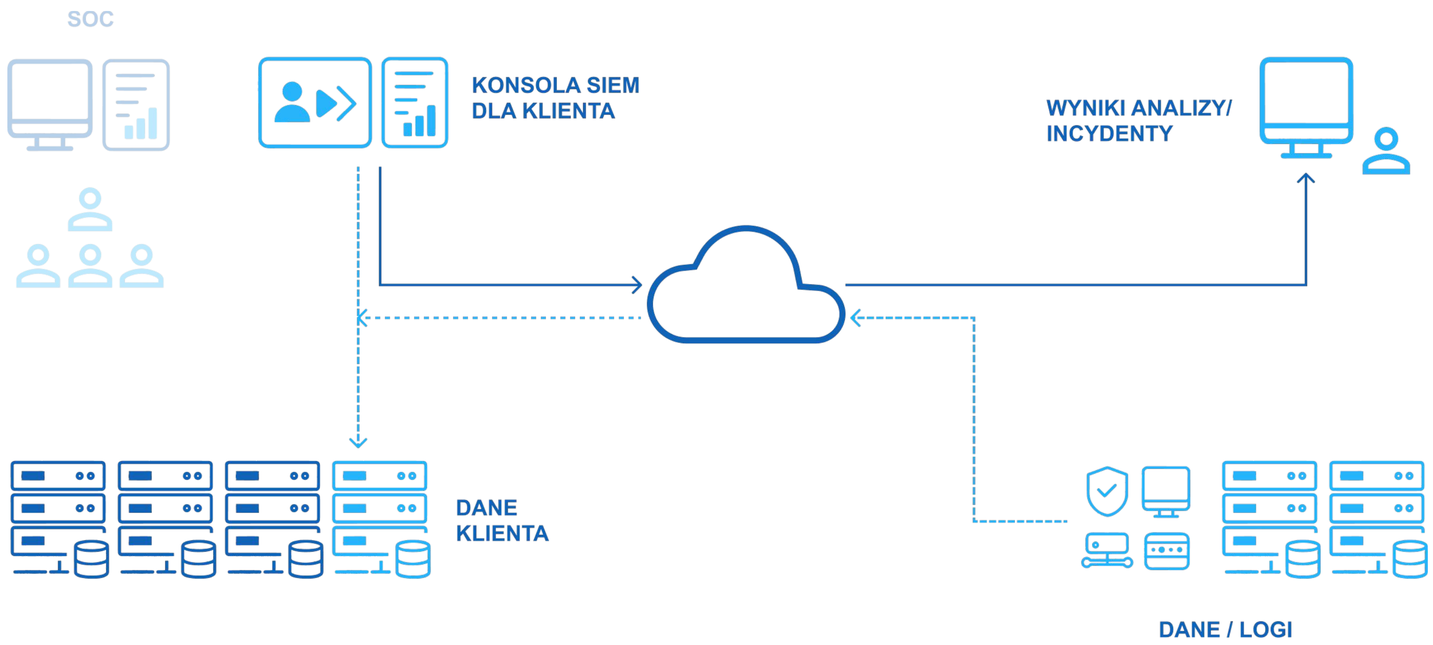
NASZE USŁUGI
MODELE GROMADZENIA I PRZETWARZANIA DANYCH

WARIANT MINIMALNY - MANAGED SIEM

Wariant minimalny - Managed SIEM umożliwia pełne korzystanie z technologii SIEM/SOAR/XDR bez konieczności instalowania, konfigurowania i utrzymywania jej we własnej infrastrukturze. Wszystkie niezbędne konfiguracje oraz integracje są wykonywane przez inżynierów NonStop SOC zgodnie z wymaganiami Klienta, podobnie jak wszelkie obowiązki związane z utrzymaniem systemu. Klient może korzystać ze wszystkich funkcjonalności systemu tak, jakby posiadał go w swojej infrastrukturaze. W tym modelu gromadzone dane i logi są przetwarzane oraz przechowywane w centrum danych NonStop SOC.



Infrastruktura NonStop SOC (SIEM, SOAR, XDR, TI)

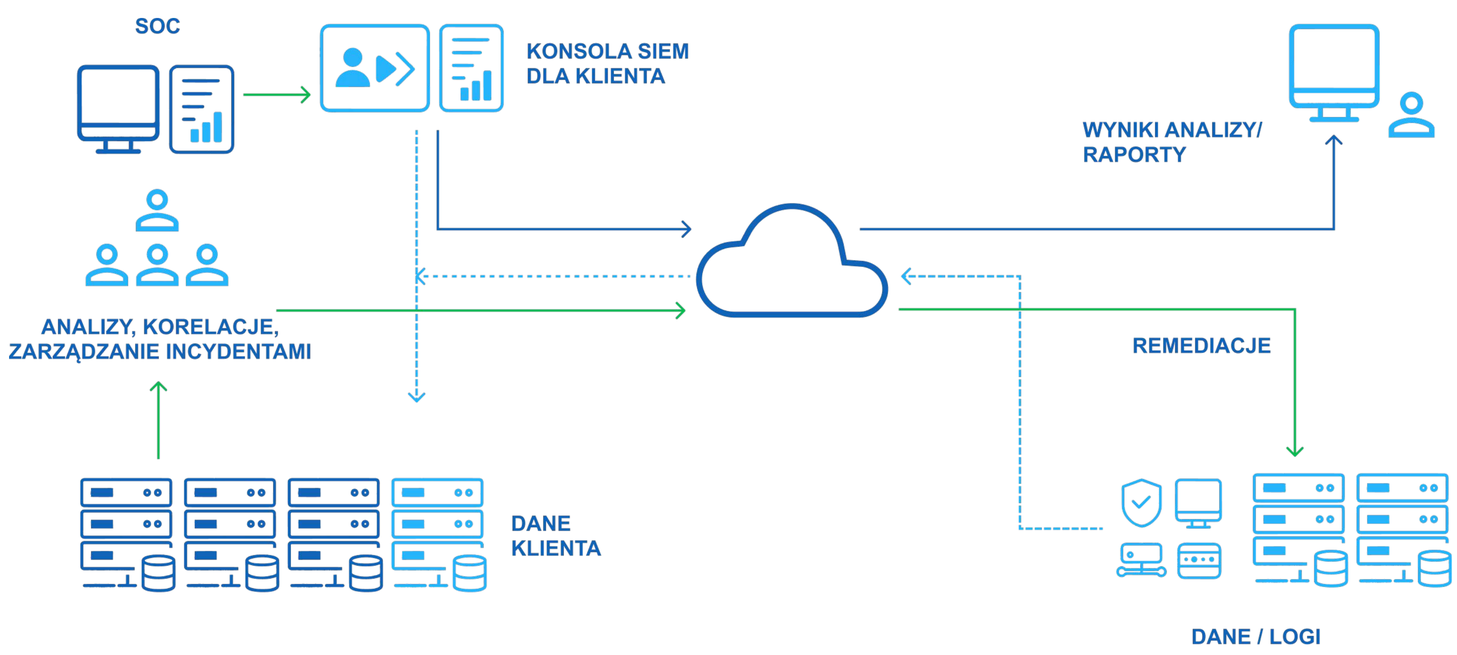
- Przetwarzanie danych w DC NonStop SOC
- Konsola informacyjna i operacyjna dla Klienta w infrastrukturze NonStop SOC

Infrastruktura Klienta

- Przesyłanie danych w całości do NonStop SOC
- Dostęp do pełnej konsoli informacyjnej i operacyjnej dla Klienta w infrastrukturze NonStop SOC

WARIANT MINIMALNY - MANAGED SOC I SIEM

Wariant minimalny - Managed SOC i SIEM zapewnia wykorzystanie technologii SIEM/SOAR/XDR do monitorowania systemów informacyjnych oraz zarządzania incydentami bezpieczeństwa w imieniu Klienta przez zespół NonStop. Podobnie jak w wariancie Managed SIEM, Klient może korzystać ze wszystkich funkcjonalności systemu, a dodatkowo otrzymuje pełen zakres usług Managed SOC. Wszystkie niezbędne konfiguracje i integracje SIEM/SOAR/XDR są realizowane przez inżynierów NonStop SOC zgodnie z wymaganiami Klienta, a całość obowiązków związanych z utrzymaniem systemu pozostaje po stronie dostawcy usług. W tym modelu - podobnie jak w poprzednim - gromadzone dane i logi są przetwarzane oraz przechowywane w centrum danych NonStop SOC.



Infrastruktura NonStop SOC (SIEM, SOAR, XDR, TI)

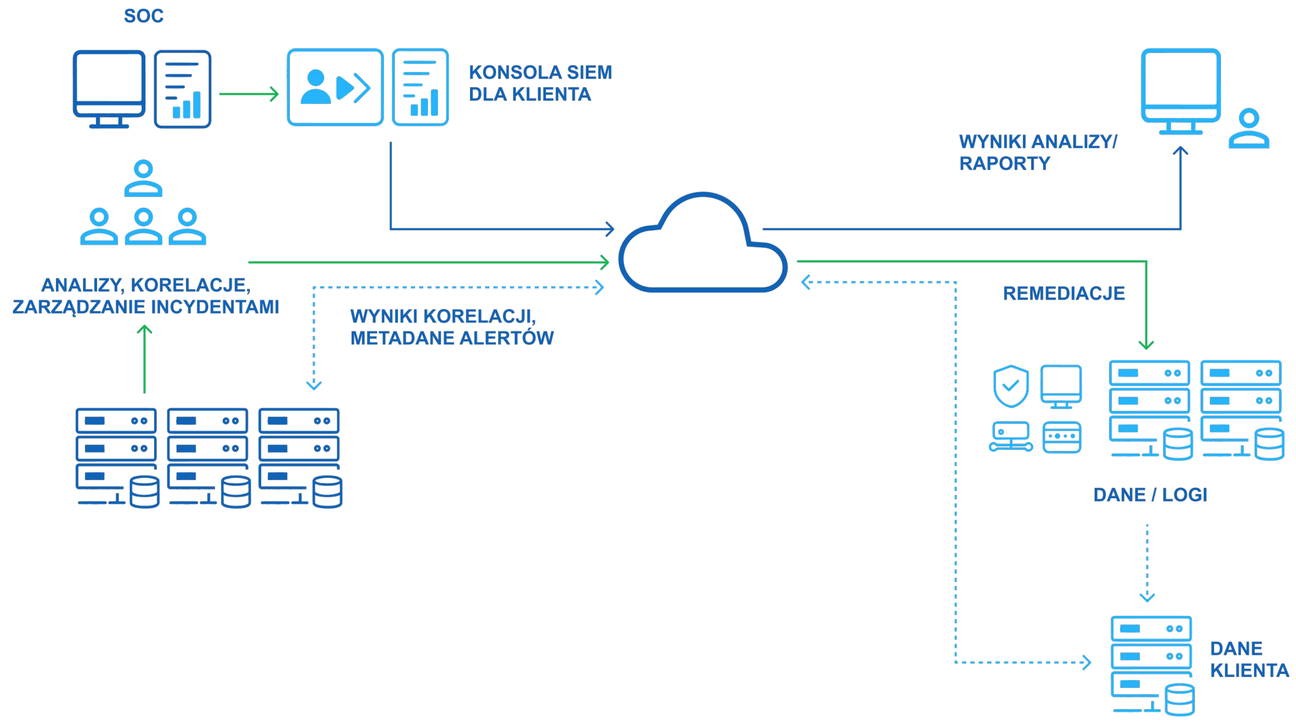
- Bieżące monitorowanie i zarządzanie incydentami (usługi managed SOC)
- Przetwarzanie danych w DC NonStop SOC
- Konsola informacyjna i operacyjna dla Klienta w infrastrukturze NonStop SOC

Infrastruktura Klienta

- Przesyłanie danych/logów w całości do NonStop SOC
- Dostęp do konsoli informacyjnej dla Klienta w infrastrukturze NonStop SOC
- Remediacje, informacje i analizy (wynikające z usług managed SOC)

WARIANT OPTYMALNY - MANAGED SOC, MIXED SIEM

Wariant optymalny - Managed SOC, Mixed SIEM umożliwia wykorzystanie technologii SIEM/SOAR/XDR do monitorowania systemów informacyjnych oraz zarządzania incydentami bezpieczeństwa w imieniu Klienta przez zespół NonStop SOC. Podobnie jak w wariancie Managed SIEM, Klient może korzystać ze wszystkich funkcjonalności systemu, a dodatkowo otrzymuje pełen zakres usług Managed SOC. Wszystkie niezbędne konfiguracje i integracje SIEM/SOAR/XDR są realizowane przez inżynierów NonStop SOC zgodnie z wymaganiami Klienta. W tym modelu - w odróżnieniu od poprzednich - gromadzone dane i logi są przetwarzane oraz przechowywane w infrastrukturze Klienta, bez konieczności ich transferu do centrum danych NonStop SOC. Takie rozwiązanie jest szczególnie korzystne dla Klientów, którzy chcą utrzymać dane i logi we własnym środowisku, a jednocześnie zapewnić zgodność z przyjętymi zasadami compliance.



Infrastruktura NonStop SOC (SIEM, SOAR, XDR, TI)

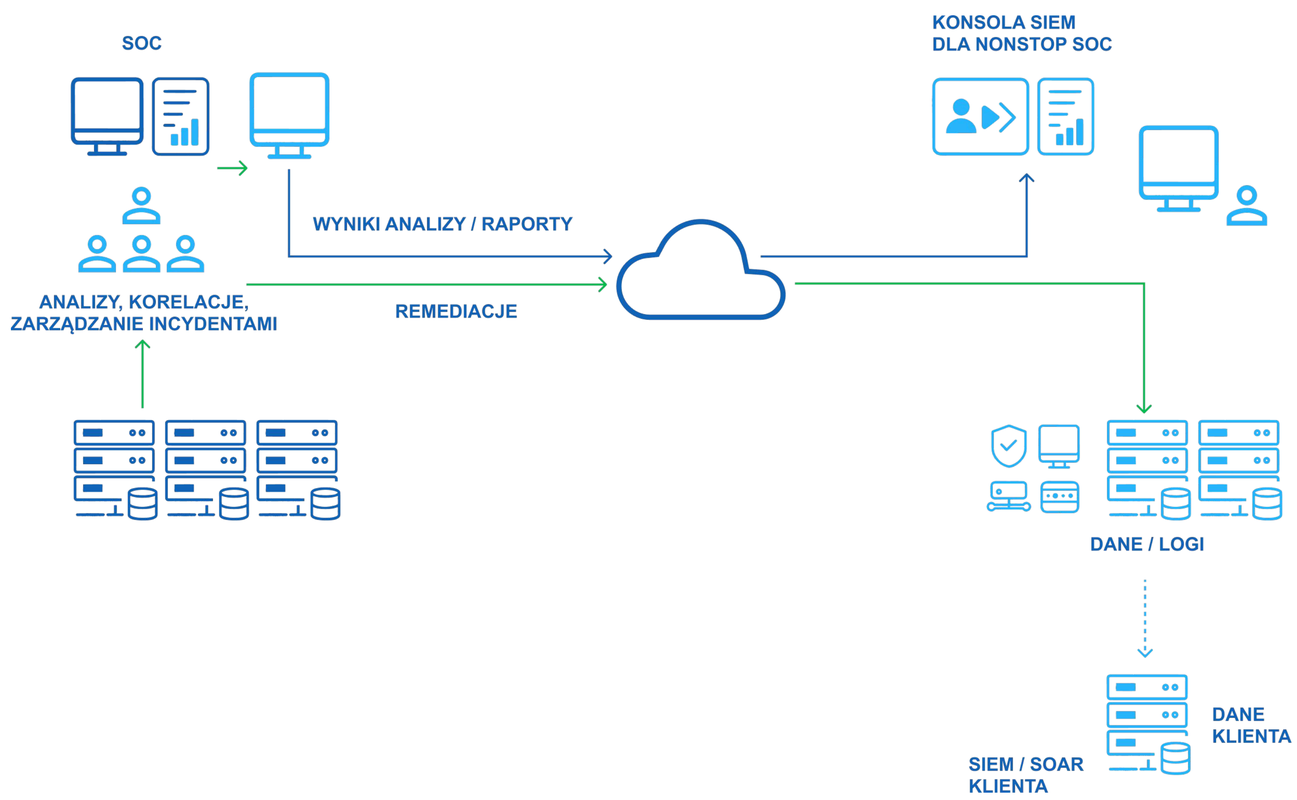
- Bieżące monitorowanie i zarządzanie incydentami (usługi managed SOC)
- W DC NonStop SOC przetwarzane są jedynie wyniki korelacji i metadane alertów
- Konsola dla Klienta w infrastrukturze NonStop SOC

Infrastruktura Klienta

- Dane i logi w całości pozostają w DC Klienta
- Dostęp do konsoli informacyjnej i operacyjnej dla Klienta w infrastrukturze NonStop SOC.

WARIANT EXTERNAL - MANAGED SOC, SIEM KLIENTA

Wariant external - Managed SOC, SIEM Klienta zapewnia monitorowanie systemów informacyjnych oraz zarządzanie incydentami bezpieczeństwa (usługi Managed SOC) w imieniu Klienta przez zespół NonStop SOC, z wykorzystaniem technologii SIEM/SOAR/XDR należącej do Klienta. Niezbędne konfiguracje i integracje SIEM/SOAR/XDR mogą być wykonywane przez inżynierów NonStop SOC zgodnie z wymaganiami Klienta oraz potrzebami procesów zaprojektowanych dla SOC. W tym modelu gromadzone dane i logi są przetwarzane oraz przechowywane w centrum danych Klienta, bez konieczności ich transferu do centrum danych NonStop SOC. Takie rozwiązanie jest szczególnie korzystne dla Klientów, którzy posiadają już technologię SIEM/SOAR/XDR, a chcieliby wzmocnić swoje zabezpieczenia cybernetyczne poprzez skorzystanie z usług SOC.



Infrastruktura NonStop SOC (SIEM, SOAR, XDR, TI)

- Bieżące monitorowanie i zarządzanie incydentami (usługi managed SOC)

Infrastruktura Klienta

- Dane i logi w całości pozostają w SIEM/SOAR Klienta.
- Dostęp do konsoli informacyjnej i operacyjnej dla NonStop SOC w infrastrukturze Klienta.

nonstop soc

KATALOG USŁUG

Katalog usług został skonstruowany w oparciu o uznany standard branżowy FIRST w zakresie operacji SOC/CSIRT, co umożliwia wymianę informacji pomiędzy różnymi uczestnikami procesu zarządzania cyberbezpieczeństwem na różnych poziomach - klientem, SOC i CSIRT - oraz dokonanie wyboru usług SOC w zależności od potrzeb i dojrzałości organizacyjnej. Minimalny pakiet usług NonStop SOC obejmuje usługi podstawowe z zakresu zarządzania zdarzeniami bezpieczeństwa oraz zarządzania incydentami bezpieczeństwa. Pozostałe usługi, należące do innych obszarów, mogą być świadczone w zależności od wyboru oraz potrzeb Klienta.

ZARZĄDZANIE ZDARZENIAMI BEZPIECZEŃSTWA

Usługi podstawowe

1. Monitorowanie i wykrywanie

- Zarządzanie logami i sensorami
- Zarządzanie use cases
- Zarządzanie danymi kontekstowymi

2. Analiza zdarzeń

- Korelacja
- Kwalifikacja

ZARZĄDZANIE INDYCENTAMI BEZPIECZEŃSTWA

Usługi podstawowe

1. Akceptacja zgłoszeń incydentów

- Odbiór zgłoszeń o incydencie
- Ocena i przetwarzanie incydentów

2. Analiza incydentów i reakcja

- Triage incydentów (priorytetyzacja i kategoryzacja)
- Gromadzenie informacji
- Koordynacja szczegółowej analizy
- Analiza przyczyn źródłowych
- Korelacja między incydentami
- Reakcja na incydent

Usługi dodatkowe

3. Analiza artefaktów i dowodów kryminalistycznych

- Analiza nosników lub innego medium
- Inżynieria odwrotna
- Analiza uruchomieniowa lub dynamiczna
- Analiza porównawcza

4. Łagodzenie skutków i odzyskiwanie danych

- Ustanowienie planu reagowania
- Środki ad hoc i powstrzymywanie wpływu incydentu
- Przywracanie systemu
- Wsparcie podmiotów odpowiedzialnych za bezpieczeństwo informacji

5. Koordynacja incydentów

- Komunikacja
- Dystrybucja powiadomień
- Koordynacja działań
- Raportowanie
- Komunikacja z mediami

6. Wsparcie zarządzania kryzysowego

- Dystrybucja informacji do odbiorców
- Raportowanie stanu bezpieczeństwa informacji
- Komunikacja w zakresie decyzji strategicznych

ZARZĄDZANIE PODATNOŚCIAMI

Usługi podstawowe

1. Wykrywanie i badanie luk w zabezpieczeniach

- Wykrywanie podatności na incydenty
- Wykrywanie podatności ze źródeł publicznych
- Badanie podatności na zagrożenia

2. Przyjmowanie raportów o podatnościach

- Odbiór raportu o podatnościach
- Triage i przetwarzanie raportów o podatnościach

3. Analizy podatności

- Selekcja podatności (walidacja i kategoryzacja)
- Analiza przyczyn źródłowych podatności
- Opracowywanie środków zaradczych

Usługi dodatkowe

4. Koordynacja podatności

- Powiadamianie / raportowanie o podatnościach
- Koordynacja interesariuszy podatności

5. Ujawnianie podatności

- Polityka ujawniania podatności
- Utrzymanie infrastruktury
- Ogłoszenie o podatności / Komunikacja / Rozpowszechnianie
- Informacje zwrotne po ujawnieniu podatności

6. Reakcja na podatność

- Wykrywanie / skanowanie podatności
- Usuwanie podatności

ŚWIADOMOŚĆ SYTUACYJNA

Usługi dodatkowe

1. Pozyskiwanie danych

- Agregacja i filtrowanie polityk, rozumienie wytycznych
- Mapowanie zasobów do funkcji, ról, działań i kluczowych zagrożeń
- Gromadzenie danych
- Przetwarzanie i przygotowywanie danych

2. Analityka i synteza

- Prognozowanie i wnioskowanie
- Wykrywanie zdarzeń (poprzez alarmowanie i/lub hunting)
- Wsparcie decyzyjne związane z zarządzaniem incydentami
- Szacowanie wpływu na stan bezpieczeństwa

3. Komunikacja

- Komunikacja wewnętrzna i zewnętrzna
- Raportowanie i wdrażanie zaleceń
- Rozpowszechnianie / integracja / współdzielenie informacji
- Zarządzanie wymianą informacji
- Informacje zwrotne

WIEDZA I JEJ TRANSFER

Usługi dodatkowe

1. Budowanie świadomości

- Badania i gromadzenie informacji
- Opracowywanie raportów i materiałów informacyjnych
- Rozpowszechnianie informacji
- Dotarcie do odbiorców

2. Szkolenia i edukacja

- Zbieranie wymagań dotyczących wiedzy, umiejętności i zdolności
- Opracowywanie materiałów edukacyjnych i szkoleniowych
- Dostarczanie treści
- Mentoring
- Rozwój zawodowy presonelu SOC

3. Ćwiczenia

- Analiza wymagań
- Rozwój formatów i środowiska ćwiczeń
- Opracowanie scenariuszy
- Wykonanie ćwiczenia
- Przegląd wyników ćwiczeń

4. Doradztwo techniczne

- Wsparcie w zarządzaniu ryzykiem
- Wsparcie w zakresie planowania ciągłości działania i odzyskiwania danych po awarii
- Wsparcie w zakresie tworzenia polityk, procesów i procedur
- Doradztwo techniczne

ZAPRASZAMY DO KONTAKTU

Telefon: +48 22 570 13 60

E-mail: kontakt@nonstopsoc.com.pl