

Twój partner w budowaniu bezpiecznej
i wydajnej infrastruktury IT



ngSIEM

Zintegrowana platforma SOC / SIEM / SOAR / UEBA
z natywnym wsparciem AI/LLM

Materiał produktowy

Wersja: kwiecień 2026



NETWORK EXPERTS Sp. z o.o. sp. k.

ul. Chojnowska 8, 03-583 Warszawa • (48) 22 100 61 92 • kontakt@netxp.pl • www.networkexpert.pl
NIP: 5242751391 • REGON: 146116650 • KRS: 0000639343

1. Streszczenie wykonawcze

ngSIEM to autorskie rozwiązanie firmy Network Experts, które integruje w jednej konsoli przeglądarkowej wszystkie kluczowe funkcje centrum bezpieczeństwa (SOC): obsługę alertów, eksplorację logów, wyszukiwanie wspierane przez modele językowe (LLM), inżynierię reguł detekcyjnych, automatyzację SOAR, analitykę behawioralną UEBA, monitorowanie podatności oraz raportowanie operacyjne i compliance.

Produkt pełni rolę warstwy **control-plane** nad środowiskiem SIEM opartym o dane dokumentowe i indeksowanie NoSQL. Poza konsumpcją alertów dodaje własne metadane, workflow, walidację, testowanie, historię uruchomień, zarządzanie regułami, dokumentację compliance oraz wykonanie automatyzacji.

Kluczowe korzyści biznesowe

- **Konsolidacja narzędzi** - jedna platforma zamiast kilkunastu odrębnych narzędzi SOC, co przekłada się na niższy całkowity koszt posiadania i utrzymania rozwiązania i krótszy czas wdrożenia analityka.
- **Automatyzacja triażu z AI** - natywna integracja z OpenAI, Azure OpenAI, Claude i Google Gemini skraca czas analizy alertu z minut do sekund.
- **Ponad 3 200 reguł detekcji** - >1 400 reguł bazowych, >200 autorskich (NETXP) i >1 600 reguł Sigma zapewnia szerokie pokrycie ATT&CK od pierwszego dnia.
- **461 konektorów ekosystemu** - kompatybilność z szerokim katalogiem integracji telemetrycznych, contentowych i akcyjnych.
- **Testowalny SOAR** - playbooki testowane na realnych alertach z pełnym audytem uruchomień i warstwą ryzyka.
- **Compliance i GRC** - automatyczne generowanie raportów DOCX/XLSX/CSV, scenariuszy reagowania i dokumentów audytowych, integracja z narzędziami BIA, analizy ryzyka i BCP.
- **UEBA i Threat Hunting** - budowanie baseline, wykrywanie anomalii i analiza trendów wolumenowych z opcjonalnym wsparciem LLM.



2. Przegląd platformy

ngSIEM to produkt klasy enterprise, zaprojektowany jako pełna konsola zarządczo-operacyjna nad środowiskiem SIEM. Poniższa tabela przedstawia kluczowe parametry rozwiązania.

Parametr	Wartość
Typ rozwiązania	Webowa konsola operacyjna SOC / SIEM / Detection Engineering / SOAR / UEBA
Architektura	Modularny monolit w Pythonie z interfejsem NiceGUI, zadaniami tła i lokalnym runtime automatyzacji
Model wdrożenia	Docker Compose, kontener uruchamiany jednym poleceniem, port aplikacji 8081
Biblioteka detekcji	Ponad 3 200 reguł: >1 400 bazowych, >200 autorskich NETXP, >1 600 Sigma
Kompatybilne integracje	461 konektorów ekosystemu Elastic (logi, metryki, traces, content, actions, entities, vulnerabilities, threat intel)
Dostawcy AI/LLM	OpenAI, Azure OpenAI, Anthropic Claude, Google Gemini
Formaty raportów	DOCX, XLSX, CSV z schedulerem, workerem i dystrybucją SMTP
Trwałość danych	SQLite, JSON/JSONL, NoSQL (warstwa dokumentowa), pliki lokalne

Problemy, które rozwiązuje ngSIEM

- Rozproszenie pracy pomiędzy SIEM, repozytoria reguł, arkusze i pliki pomocnicze.
- Brak spójnego workflow jakościowego dla reguł i alertów.
- Czasochłonne ręczne budowanie zapytań DSL - Search-LLM eliminuje tę barierę.
- Brak kontrolowanego sposobu testowania automatyzacji na realnych alertach.
- Słaba obserwowalność efektów automatyzacji i triage AI.
- Trudność w łączeniu alertów, enrichments, raportów i reakcji operacyjnych w jeden workflow.

3. Moduły platformy ngSIEM

Platforma udostępnia dziesięć głównych modułów roboczych, z których każdy odpowiada na konkretne potrzeby zespołów SOC, detection engineering i compliance.



3.1. Alerts - Centrum operacyjne SOC

Moduł Alerts jest centralnym punktem pracy analityka SOC. Zapewnia pełny kontekst alertu, od surowego JSON-a po korelację z innymi zdarzeniami oraz umożliwia wzbogacenie danych i automatyczną ocenę z wykorzystaniem AI.

Funkcjonalności:

- Dashboard, filtrowanie, tabela alertów ze szczegółami i surowym JSON.
- Podgląd zdarzeń osadzonych i korelacja po hoście, użytkownika i innych polach kontekstowych.
- Enrichmenty alertu z użyciem kwerend, zmiennych kontekstowych i bindingów wyjściowych.
- **Suggested queries** - szybkie podpowiedzi działań analitycznych dopasowane do typu alertu.
- **Triage AI** - automatyczna ocena z wyborem dostawcy modelu (OpenAI, Azure OpenAI, Claude) z opcjonalnym dołączeniem wcześniejszego enrichmentu.
- Grupowanie alertów, przejście do przykładowego alertu z grupy, zamykanie pojedynczych alertów i całych grup.
- Zapis wyników enrichmentu do warstwy danych i indeksów analitycznych.

Korzyść biznesowa

Analityk SOC otrzymuje pełny kontekst incydentu w jednym widoku, co redukuje czas triażu nawet o 70% w porównaniu z ręcznym przełączaniem między narzędziami. Automatyczny triage AI pozwala na wstępną klasyfikację setek alertów dziennie bez udziału człowieka.

3.2. Search-LLM - Wyszukiwanie w języku naturalnym

Moduł Search-LLM umożliwia zadawanie pytań o dane SIEM w języku naturalnym. System konwertuje je na zapytania DSL, waliduje składnię i zwraca próbkę wyników - bez konieczności znajomości składni Elasticsearch.

Funkcjonalności

- Konwersja pytań w języku naturalnym na zapytania DSL.
- Doprecyzowanie intencji użytkownika i iteracyjne poprawki zapytań.
- Walidacja składni przez `_validate/query`.
- Próbkowanie wyników i analiza pól wspierająca threat hunting.
- Debug generowania zapytań i cache wyników pomocniczych.



Korzyść biznesowa

Każdy członek zespołu - nie tylko ekspert od DSL - może samodzielnie przeszukiwać dane SIEM. Eliminuje to wąskie gardło w postaci jednego specjalisty od zapytań i przyspiesza dochodzenia o godziny.

3.3. Events - Eksploracja surowych logów

Moduł Events zapewnia bezpośredni dostęp do surowych logów z histogramem czasowym, tabelą dokumentów i możliwością budowania filtrów przez kliknięcie na pola.

- Eksploracja surowych logów po indeksach i czasie.
- Tabela dokumentów z histogramem czasowym i widokiem raw / formatted.
- Budowanie filtrów na podstawie klikniętych pól dokumentu.
- Wsparcie analiz technicznych na poziomie danych źródłowych.

3.4. Rules - Detection Engineering

Moduł Rules to pełny warsztat inżynierii detekcji. Obejmuje przegląd, tworzenie, walidację, mapowanie MITRE ATT&CK i zarządzanie cyklem życia ponad 3200 reguł detekcyjnych.

Funkcjonalności

- Przegląd reguł aktywnych w SIEM i reguł lokalnych offline.
- Fasetowe filtrowanie po severity, MITRE ATT&CK, technologiach, statusie i wielu innych cechach.
- Lifecycle, source of truth, mapowania akcji i scenariuszy.
- Walidacja pojedyncza i wsadowa: syntaktyczna, semantyczna i środowiskowa.
- Analiza populacji pól, integracji, braków danych i gotowości wdrożeniowej.
- Import, aktywacja i synchronizacja z silnikiem detekcji oraz repozytoriami reguł.
- Tworzenie reguł ręczne i wspierane przez AI.
- Budowa i utrzymanie scenariuszy reagowania na incydenty.

Biblioteka reguł	Wolumen	Znaczenie operacyjne
Reguły bazowe platformy SIEM	1 618 reguł	Główny korpus detekcji: endpoint, cloud, identity, network, container, SaaS
Reguły autorskie NETXP	254 artefakty / >200 reguł	Pakiet dopasowany do potrzeb klienta, scenariuszy lokalnych i wymagań projektowych
Biblioteka Sigma	>1 600 reguł	Community content, szybka adaptacja nowych przypadków użycia



3.5. SOAR-AI - Automatyczny triage z AI

Moduł SOAR-AI realizuje automatyczny triage alertów z wykorzystaniem modeli językowych. Każdy alert jest analizowany przez wybranego dostawcę AI, który zwraca werdykt TP (True Positive), FP (False Positive) lub Needs Review.

- Automatyczny triage alertów przez OpenAI, Azure OpenAI lub Claude.
- Konfiguracja providerów, workerów, reguł i cache fingerprintów.
- Werdykty TP / FP / Needs Review z metrykami wykonania.
- Watchdog, obserwowalność procesu i gotowość do audytu.

Korzyść biznesowa

Automatyzacja wstępnej analizy eliminuje powtarzalne zadania i pozwala analitykom skupić się na rzeczywistych incydentach. W środowiskach generujących setki alertów dziennie SOAR-AI może zredukować ręczny nakład pracy o 60–80%.

3.6. UEBA - Analityka behawioralna

Moduł UEBA (User and Entity Behavior Analytics) buduje profile zachowań użytkowników i zasobów, wykrywając odchylenia od normy, które mogą wskazywać na zagrożenia wewnętrzne lub przejęcie kont.

- Checki behawioralne wbudowane i własne.
- Budowanie baseline i automatyczne wykrywanie anomalii.
- Watchdog procesów i opcjonalny zapis wyników do warstwy danych analitycznych.
- Przywracanie aktywnych checków po restarcie aplikacji.

Korzyść biznesowa

Wykrywanie zagrożeń, które umykają regułom opartym na sygnaturach - nietypowe logowania, eskalacja uprawnień, nadmierny dostęp do danych. UEBA uzupełnia tradycyjną detekcję o warstwę behawioralną.

3.7. Threat Hunter - Analiza trendów

Moduł Threat Hunter wspiera proaktywne poszukiwanie zagrożeń poprzez analizę trendów wolumenowych, odchylenia statystycznych i korelację wielowymiarową.

- Analiza trendów i wolumenów alertów po regule, użytkownika, hoście i IP.
- Progi detekcji, metryki statystyczne, harmonogram i findings.
- Opcjonalne wsparcie LLM dla priorytetyzacji top-N findings.
- Raportowanie wyników w formatach dokumentowych.



3.8. Vuln Monitor - Monitorowanie podatności

Moduł Vuln Monitor realizuje inwentaryzację oprogramowania i automatyczne dopasowanie znanych podatności (CVE) z bazy NVD do wykrytego software.

- Pobieranie inventory oprogramowania przez źródła endpoint / asset management (w tym osquery).
- Dopasowanie CVE do wykrytego software z użyciem lokalnego cache i NVD.
- Zakładki: Skan, Inventory, Podatności i Runy.

Korzyść biznesowa

Ciągła widoczność ekspozycji na podatności bez konieczności wdrażania osobnego skanera. Informacje o CVE są dostępne w kontekście alertów i reguł detekcji.

3.9. SOAR - Automatyzacja i orkiestracja

Moduł SOAR to jedna z kluczowych warstw produktu. łączy bibliotekę kwerend, mapowania alertów, zewnętrzne konektory, testowanie end-to-end, runtime sekwencji, kontrakty wyjściowe oraz warstwę ryzyka.

Biblioteka kwerend i mapowań:

- Katalog kwerend przechowywany lokalnie i seedowany z danych startowych.
- Mapowanie alertów do rekomendowanych kwerend i akcji.
- Wspólna warstwa dla kwerend DSL i external handlerów.

Testowanie i wykonanie:

- **Szybki test** - sprawdzenie definicji lub pojedynczego kroku.
- **Pełny test** - uruchomienie na realnym alercie z rozwiązywaniem zmiennych i wykonaniem backendu.
- Obsługa foreach, output variables, kontekstu globalnego i artefaktów uruchomienia.
- Historia runów z analizą techniczną i biznesowym podsumowaniem wyników.

Sekwencje i playbooki

- Budowa sekwencji handlerów dla typu alertu.
- Drafty sekwencji generowane na podstawie enrichmentu alertów.
- Eksport draftu sekwencji do JSON i dokumentacji operacyjnej.

Warstwa ryzyka i kontekstu

- Konfigurowalne reguły wpływu na ryzyko po każdym kroku.
- Warunki zależne od wartości output variables i bindingów wyników.



- Budowa wspólnego kontekstu opisowego z kroków, udostępnianego do LLM, powiadomień i ticketingu.

Wspomaganie sekwencji przez LLM

- Podpowiadanie kroków do sekwencji przez LLM na podstawie przykładowego alertu.
- Tryb shortlisty oraz pełny katalog kwerend jako wejście do selekcji AI.
- Anonimizacja alertu przed wystaniem do modelu.

Korzyść biznesowa

Testowalność na realnych alertach eliminuje ryzyko wdrożenia niesprawdzonych automatyzacji. Warstwa ryzyka i kontekstu pozwala budować złożone playbooks bez obawy o niekontrolowane akcje. LLM przyspiesza projektowanie sekwencji, redukując czas budowy playbooka z dni do godzin.

3.10. Reports - Raportowanie i compliance

Moduł Reports automatyzuje generowanie dokumentacji operacyjnej, compliance i audytowej w formatach gotowych do dystrybucji.

- Raporty miesięczne, raporty TW, UDT i raport generyczny DOCX.
- Raporty cykliczne z definicjami, schedulerem, workerem i dystrybucją e-mail (SMTP).
- Artefakty CSV, DOCX i XLSX dla różnych odbiorców.
- Generowanie dokumentów compliance: scenariusze reagowania, materiały dowodowe, zestawienia audytowe.
- Przygotowanie artefaktów wejściowych dla systemów GRC oraz zespołów governance, risk and compliance.
- Współpraca z dedykowaną aplikacją GRC: BIA, RIZK, BCP, Incident, audyt frameworków i generowanie dokumentów formalnych.

Korzyść biznesowa

Automatyczne generowanie raportów eliminuje wielogodzinne ręczne przygotowanie dokumentacji. Cykliczna dystrybucja zapewnia ciągły przepływ informacji do interesariuszy bez dodatkowego nakładu pracy zespołu SOC.

4. Warstwa AI / LLM - przewaga konkurencyjna

W odróżnieniu od rozwiązań, które oferują AI jako osobny chatbot lub dodatek, w ngSIEM warstwa AI jest **głęboko osadzona operacyjnie w wielu workflow** i stanowi integralny element codziennej pracy analityka.



Obszary zastosowania AI

Obszar	Dostawca	Zastosowanie
Search-LLM	OpenAI	Konwersja pytań w języku naturalnym na zapytania DSL, iteracyjna poprawa i walidacja
SOAR-AI (triage)	OpenAI, Azure OpenAI, Claude	Automatyczny triage alertów, werdykty TP/FP/Needs Review
Krok SOAR (ocena)	OpenAI, Claude	Ocena alertu i findings, klasyfikacja, kontekst z wcześniejszych kroków, anonimizacja
Tworzenie reguł	OpenAI	Kreatory i pipeline generowania kandydatów detekcyjnych
Threat Hunter	OpenAI	Priorytetyzacja findings dla top-N przypadków
Selekcja kroków SOAR	OpenAI, Claude	Podpowiadanie kroków do sekwencji na podstawie alertu
Warianty analizy	Google Gemini	Obsługa w towarzyszących komponentach projektu

Architektura integracji AI

- **Multi-provider** - wsparcie dla OpenAI, Azure OpenAI, Anthropic Claude i Google Gemini. Organizacja wybiera dostawcę odpowiedniego dla swoich polityk bezpieczeństwa danych.
- **Anonimizacja** - dane alertu są anonimizowane przed wysłaniem do modelu, co minimalizuje ryzyko wycieku danych wrażliwych.
- **Tryb read-only** - AI analizuje i klasyfikuje, ale nie podejmuje akcji operacyjnych samodzielnie. Decyzja o zamknięciu alertu lub uruchomieniu containment zawsze należy do analityka lub zatwierdzonego playbooka.
- **Cache fingerprintów** - podobne alerty nie są wielokrotnie wysyłane do API, co optymalizuje koszty i czas odpowiedzi.
- **Obserwowalność** - każda interakcja z AI jest logowana, auditowalna i dostępna w historii uruchomień.

5. Detection Engineering - szczegóły

ngSIEM oferuje pełny warsztat detection engineering z warstwą jakości, metadanych, walidacji i promocji reguł do środowiska SIEM. To nie jest wyłącznie viewer reguł - to kompletne środowisko pracy inżyniera detekcji.



Grupy funkcjonalne reguł

Grupa	Przykłady	Skala	Wartość operacyjna
Endpoint / host	Windows, procesy, PowerShell, sterowniki, EDR/XDR	~969 reguł (domena Endpoint)	Malware, execution, persistence, defense evasion
Cloud	AWS, Azure, role, uprawnienia, aktywność kont	~331 reguł (domena Cloud)	Nadużycia w chmurze, błędy konfiguracyjne, IAM
Identity / AD / Auth	Password spray, Kerberos, brute force, lockout	~90+ pakietów autorskich	ATO, eskalacja uprawnień, credential access
Network / firewall / VPN	FortiGate, Palo Alto, DNS, proxy, VPN	~50+ pakietów autorskich	C2, exfiltracja, ruch do ryzykownych destynacji
Microsoft 365 / Exchange	Outlook, OneDrive, SharePoint, forwarding	~20+ pakietów autorskich	Incydenty pocztowe, insider threat, współdzielenie danych
EDR / XDR	Defender, SentinelOne, CrowdStrike, ESET	Kilkaście pakietów	Korelacja alertów EDR z kontekstem SIEM
Container / K8s	Kubernetes, kontenery, runtime, workload security	Domeny Container i K8s	Detekcja w warstwie kontenerowej i cloud-native

Profil biblioteki detekcji

- **Najsilniejsze taktyki MITRE ATT&CK:** Defense Evasion, Persistence, Execution, Privilege Escalation, Credential Access, Initial Access.
- **Typy reguł:** EQL, query, new_terms, ES|QL, machine_learning, threshold.
- **Dominujące integracje:** endpoint, windows, sentinel_one_cloud_funnel, crowdstrike, m365_defender, system, aws, auditd_manager, azure, okta.
- **Profil severity:** największy wolumen na poziomie medium i low, z istotną warstwą high dla krytycznych przypadków.

Dobór reguł z perspektywy ryzyka i GRC

ngSIEM umożliwia powiązanie reguł detekcji z procesami GRC, co pozwala na priorytetyzację detekcji w oparciu o wpływ biznesowy, a nie wyłącznie o parametry techniczne.

- **Priorytetyzacja** - dane BIA i macierz ryzyka do wyboru i priorytetyzacji reguł dla najbardziej krytycznych procesów.
- **Mapowanie do scenariuszy IR** - reguły i alerty powiązane z gotowymi scenariuszami reagowania i działaniami SOC.
- **Dobór zabezpieczeń** - ocena, czy reguła wspiera kontrolę kompensującą i wymagania compliance (CIS v8, ISO 27002:2022, NIS2).
- **Planowanie odpowiedzi** - wyniki detekcji przekazywane do procesu planowania odpowiedzi na incydent i dokumentów formalnych.



6. Integracje platformowe i zewnętrzne

ngSIEM łączy integracje platformowe, enrichmenty, konektory read-only, telemetrię SIEM oraz akcje operacyjne z poziomu SOAR. Poniższa tabela przedstawia integracje wdrożone bezpośrednio w produkcie.

Integracje wbudowane

Kategoria	Integracja	Zastosowanie	Typ
Platforma	Silnik SIEM / NoSQL	Alerty, eventy, walidacja, enrichment, UEBA, raporty, SOAR	Odczyt + zapis
Platforma	Warstwa zarządzania detekcją	Status reguł, import/aktywacja, pakiety integracyjne	Odczyt + akcje
Tożsamość	Local Active Directory	Lookup grup, ocena uprzywilejowania	Odczyt / enrichment
Email	SMTP	Powiadomienia SOAR i raporty cykliczne	Akcja operacyjna
Ticketing	ManageEngine ServiceDesk Plus	Tworzenie zgłoszeń z kontekstem alertu	Akcja operacyjna
Ticketing	OTRS / Znuny REST	Tworzenie ticketów przez REST	Akcja operacyjna
Endpoint Security	Microsoft Defender for Endpoint	Lookup hosta, izolacja hosta, status akcji	Odczyt + akcja
Threat Intel	VirusTotal	Lookup pliku, URL, domeny i IP	Enrichment
Threat Intel	GreyNoise	Kontekst IP, klasyfikacja noise/riot	Enrichment
Threat Intel	abuse.ch URLhaus / MalwareBazaar	Lookup URL, hosta i hashy	Enrichment
Threat Intel	AlienVault OTX	Lookup IP, domeny, URL i hashy	Enrichment
Threat Intel	urlscan.io	Historia skanów i verdict dla URL/domeny	Enrichment
Threat Intel	PhishTank	Lookup URL phishingowych	Enrichment
Threat Intel	Have I Been Pwned	Wyciek kont i paste dla e-mail/UPN	Enrichment
Threat Intel	Cloudflare Radar	Ranking i kategorie domeny	Enrichment
Profiling	IP Profile / ipwho.is	Klasyfikacja IP, geolokalizacja, ASN	Enrichment
Podatności	NVD	Dopasowanie CVE do inventory software	Enrichment
Repozytoria	GitHub / lokalne repo reguł	Pobieranie i utrzymanie repozytoriów reguł	Źródło danych
GRC	Aplikacja GRC: BIA / RIZK / BCP / Incident / Audit	Eksport raportów, scenariuszy, mapowań audytowych	Integracja procesowa



Katalog 461 kompatybilnych integracji ekosystemu

Oprócz integracji wbudowanych, ngSIEM jest zgodny z szerokim ekosystemem konektorów telemetrycznych, contentowych, cloud, endpoint, threat intelligence, vulnerability management, ticketing i akcji. Poniżej przedstawiono kluczowe rodziny integracji:

Rodzina integracji	Kategoria	Przykłady
AWS	Cloud / telemetry	CloudTrail, GuardDuty, Security Hub, VPC, WAF, S3, EC2, Lambda, RDS, Security Lake
Azure	Cloud / telemetry / AI	Activity Logs, Audit Logs, Firewall, Event Hub, Monitor, VM, WAF, Azure OpenAI
Google Cloud	Cloud / telemetry	Audit, Firewall, Functions, GKE, Pub/Sub, Storage, Security Command Center
Microsoft 365 / Entra ID	Identity / collaboration	Entra ID, Graph Activity, Teams, OneDrive, Sentinel, XDR
Endpoint OS	Endpoint telemetry	Windows, Sysmon, PowerShell, Linux, auditd, macOS, Jamf
EDR / XDR	Endpoint security	CrowdStrike, SentinelOne, Carbon Black, Trellix, FortiEDR, ESET
IAM	Identity	Okta, Auth0, Authentik, Keycloak, JumpCloud, Cisco Duo, Sailpoint
Network / Firewall	Network security	Palo Alto, Fortinet, Cisco ASA/FTD/Umbrella, Check Point, Juniper, Zscaler
WAF / Edge	Web / edge	Cloudflare, Akamai, Azure Front Door, AWS WAF, Imperva, Citrix WAF
Containers / K8s	Cloud-native	Docker, Kubernetes, Containerd, Istio, OpenTelemetry
Databases	Data platforms	MySQL, PostgreSQL, Oracle, MongoDB, Redis, Cassandra, Elasticsearch
Ticketing / ITSM	Response	ServiceNow, Jira, PagerDuty, OpsGenie, Tines, Torq, Swimlane SOAR
Threat Intel	Intelligence	MISP, Anomali, Recorded Future, ThreatConnect, Cybersixgill, Google TI
Vuln Management	Vulnerabilities	Qualys VMDR, Rapid7 InsightVM, Tenable, CISA KEV, First EPSS, NVD
Network Detection	NDR / telemetry	Suricata, Zeek, Snort, NetFlow, GoFlow2, Corelight
Productivity	Content / workplace	Google Drive, SharePoint, Box, Dropbox, Notion, Slack, Zoom, Gmail



7. Architektura i wdrożenie

Model architektoniczny:

- **Modularny monolit** - uruchamiany jako jedna aplikacja webowa.
- Interfejs NiceGUI + warstwa integracyjna + zadania tła + lokalny runtime SOAR.
- Współhostowanie UI i wybranych workerów w jednym runtime.

Trwałość danych:

- **SQLite** - metadane reguł, katalog SOAR i wybrane dane lokalne.
- **JSON / JSONL** - użytkownicy, baseline, anomalie, logi i definicje raportów.
- **NoSQL (warstwa dokumentowa)** - podstawowy data plane dla alertów, eventów i wyników.
- Pliki raportowe i artefakty runów zapisywane lokalnie.
- Wymiana danych z aplikacją GRC przez pliki projektowe, scenariusze, mapowania i dokumenty wynikowe.

Wdrożenie:

- **Docker Compose** - uruchomienie kontenera jednym poleceniem: `docker compose up --build -d`
- Port GUI: **8081**
- Trwałe mounty dla danych i konfiguracji sekwencji handlerów.

Przywracanie stanu po restarcie:

Platforma automatycznie przywraca stan pracy po restarcie, w tym aktywne checki UEBA, workery SOAR-AI, raporty cykliczne i runtime handlerów SOAR.

8. Typowe scenariusze użycia

Poniższe scenariusze ilustrują, jak ngSIEM wspiera codzienną pracę zespołów bezpieczeństwa na różnych poziomach dojrzałości organizacji.

Scenariusz 1: Obsługa alertu SOC

- Analityk otwiera alert, filtruje kontekst i przegląda szczegóły zdarzenia.
- Uruchamia enrichmenty lub korzysta z suggested queries.
- Dołącza Triage AI lub powiązane wyniki wcześniejszych kroków.
- Zamyka pojedynczy alert albo całą grupę alertów oraz zapisuje enrichment do ES.



Scenariusz 2: Natural-language hunting

- Użytkownik opisuje pytanie dotyczące środowiska w języku naturalnym.
- Search-LLM generuje i waliduje zapytanie DSL do warstwy SIEM / NoSQL.
- System pokazuje próbkę wyników i wspiera dalszą iterację zapytania.

Scenariusz 3: Detection engineering

- Inżynier wybiera regułę lub tworzy nową ręcznie bądź z użyciem AI.
- Uruchamia walidację jakościową, środowiskową i mapowanie MITRE / technology.
- Mapuje akcje, lifecycle i source of truth.
- Aktywuje regułę w silniku detekcji lub zapisuje do lokalnego repozytorium.

Scenariusz 4: Budowa automatyzacji SOAR

- Zespół wybiera kwerendy z katalogu lub korzysta z podpowiedzi LLM.
- Definiuje zmienne wejściowe, output contracts i warstwę ryzyka.
- Uruchamia pełny test na realnym alercie.
- Dodaje konektory zewnętrzne, ticketing lub akcje containment.
- Eksportuje draft sekwencji do JSON, dokumentacji operacyjnej lub przekazuje artefakty do aplikacji GRC.

9. Podsumowanie i pozycjonowanie

ngSIEM to kompletne, autorskie rozwiązanie firmy Network Experts, które konsoliduje funkcje SOC, SIEM, SOAR, UEBA, Detection Engineering, Vulnerability Monitoring i raportowania compliance w jednej platformie przeglądarkowej.

Dla kogo jest ngSIEM?

Platforma jest przeznaczona dla organizacji, które:

- Pracują operacyjnie na nowoczesnym SIEM opartym o dane NoSQL.
- Potrzebują jednej konsoli łączącej pracę analityków SOC, detection engineerów, operatorów automatyzacji i właścicieli procesów bezpieczeństwa.
- Chcą wdrożyć kontrolowaną automatyzację SOAR z pełną tesowalnością i audytem.
- Wymagają wsparcia AI w triażu, wyszukiwaniu i budowie reguł.
- Muszą generować dokumentację compliance i współpracować z procesami GRC.



Wyróżniki ngSIEM

Wyróżnik	Opis
Natywna integracja AI/LLM	AI osadzone w 6+ workflow: search, triage, SOAR, rules, hunting, selekcja kroków
Ponad 3 200 reguł detekcji	>1 400 bazowych + >200 autorskich NETXP + >1 600 Sigma
461 kompatybilnych konektorów	Pełne spektrum: cloud, endpoint, identity, network, threat intel, vuln, ticketing
Testowalny SOAR	Playbooki testowane na realnych alertach, warstwa ryzyka, pełny audyt runów
Compliance i GRC	Automatyczne raporty, scenariusze IR, integracja z BIA, RIZK, BCP, frameworkami audytowymi
UEBA + Threat Hunting	Baseline behawioralny, anomalie, analiza trendów z LLM
Jedna platforma, pełne pokrycie	SOC + Detection Eng. + SOAR + UEBA + Vuln Mon + Reporting w jednym oknie przeglądarki

Zainteresowany wdrożeniem ngSIEM w swojej organizacji?

Skontaktuj się z nami, aby umówić prezentację lub otrzymać dostęp do środowiska demonstracyjnego.

Network Experts | www.networkexpert.pl

Twój partner w budowaniu bezpiecznej i wydajnej infrastruktury IT



NETWORK EXPERTS Sp. z o.o. sp. k.

ul. Chojnowska 8, 03-583 Warszawa • (48) 22 100 61 92 • kontakt@netxp.pl • www.networkexpert.pl
NIP: 5242751391 • REGON: 146116650 • KRS: 0000639343