ITCSECadmin

Platforma Bezpieczeństwa Sieciowego

Detekcja DDoS · BGP FlowSpec · Traffic Diversion · SIEM · NIS2 Compliance

Czym jest ITCSECadmin?

ITCSECadmin to modularna, samodzielnie hostowana platforma bezpieczeństwa sieciowego zaprojektowana dla dostawców usług internetowych (ISP), punktów wymiany ruchu internetowego (IXP) oraz sieci korporacyjnych. Platforma łączy ochronę DDoS, granularną mitygację **BGP FlowSpec**, dywersję ruchu BGP, SIEM z parsowaniem logów wielu producentów, monitoring sieci (SNMP/NMS), zarządzanie BGP z **integracją multi-vendor**, ochronę przed spoofingiem (BCP38), skanowanie podatności oraz analitykę AI w jednym, zunifikowanym interfejsie.

< 2 sek.	< 5 sek.	< 10 sek.	70–80%	< 0,1%	99,99%
czas detekcji ataku	aktywacja blackhole	dywersja ruchu BGP	redukcja TCO	false positives	dostępność

Kluczowe korzyści

Wszystko w jednym

Ochrona DDoS, BGP FlowSpec, BGP Traffic Diversion, SIEM, monitoring sieci (SNMP/NMS), zarządzanie BGP z integracją multi-vendor, skanowanie podatności i analityka AI w jednej platformie — koniec z płaceniem za wiele oddzielnych narzędzi.

Pełna kontrola nad danymi

Rozwiązanie self-hosted, bez zależności od zewnętrznej chmury. Idealne dla środowisk air-gap i sieci o podwyższonych wymaganiach bezpieczeństwa. Zero zewnętrznych wywołań w trybie operacyjnym.

Wykrywanie zagrożeń w czasie rzeczywistym

Detekcja ataków DDoS w mniej niż 2 sekundy. Automatyczna odpowiedź dopasowana do kształtu ataku: blackhole, FlowSpec lub dywersja ruchu — z symulatorem „what-if" przed każdą akcją.

BGP FlowSpec — chirurgiczna mitygacja

Gdy pełny blackhole to za dużo — reguły FlowSpec (RFC 5575) przez ExaBGP v5 wstrzykiwane bezpośrednio do peerów upstream. Drop lub rate-limit tylko ruchu ataku (per prefiks, protokół, port, flagi TCP, DSCP) — legalny ruch do tego samego IP działa bez zakłóceń.

BGP Traffic Diversion bez blackholingu

Przekierowanie atakowanego ruchu na ścieżkę scrubbingową bez konieczności całkowitego czarnego dziurowania. Inteligentne selektywne ogłaszanie: prefiks pozostaje osiągalny przez krytycznych peerów (Google, Meta, Akamai…). Auto-trigger i auto-revert.

Zgodność z NIS2

Wbudowany moduł compliance: raportowanie incydentów (Art. 23), zarządzanie ryzykiem, polityki

bezpieczeństwa, rejestr szkoleń z katalogiem szkoleń obowiązkowych i pełny audit log.

Sztuczna inteligencja
Zintegrowany asystent AI wspierający analizę sieci, troubleshooting i podejmowanie decyzji operacyjnych w języku naturalnym.

Niższy koszt posiadania
Redukcja TCO o 70–80% w porównaniu z komercyjnymi rozwiązaniami. Brak opłat per Gbps, brak subskrypcji za ingestion danych, FlowSpec bez dodatkowych licencji.

Moduły i funkcjonalności

Ochrona przed DDoS

- **Analiza ruchu w czasie rzeczywistym** — obsługa NetFlow v5/v9/IPFIX, sFlow oraz PCAP
- **Hierarchiczne progi detekcji** — na poziomie sieci, protokołu, portu i TOS
- **Country Risk Scoring** — ważenie ruchu na podstawie profilu ryzyka kraju źródłowego
- **Automatyczna mitygacja** — BGP blackholing z tagowaniem community — platformy multi-vendor
- **Tryb mitygacji per próg** — blackhole, flowspec, both lub none — dobierany indywidualnie dla każdego progu detekcji
- **Odpowiedź dopasowana do kształtu ataku** — pojedyncze IP → blackhole RTBH, rozproszony prefiks → dywersja BGP, rozproszony o niskim wolumenie → FlowSpec; cooldowny per reguła i pełny audit trail
- **Symulator What-If** — podgląd skutków blackhole i scoringu przed wykonaniem akcji; domyślnie tryb alert-only
- **Zarządzanie białą/czarną listą** — whitelisting i blacklisting adresów IP
- **Obsługa różnych typów ataków** — volumetryczne, protokołowe i warstwy aplikacji

Ochrona przed spoofingiem i odbiciami (BCP38)

- **Monitor egress spoofingu** — detekcja w czasie rzeczywistym fałszowanego ruchu źródłowego opuszczającego sieć, z przypisaniem do interfejsu ingress i eksportera
- **Atrybucja source-MAC** — wskazanie konkretnego portu, z którego pochodzi sfałszowany ruch — gotowe dane do wdrożenia BCP38/uRPF
- **Wykluczenia bez false-positives** — multicast wewnątrzsieciowy (IPTV) i prywatny ruch east-west nie generują fałszywych alarmów
- **Detekcja odbić SYN-ACK** — wykrywanie własnych hostów wykorzystywanych jako ofiary odbicia, z rekomendacją dywersji zamiast blackhole
- **Bezpieczne cele detekcji** — identyfikatory nie-IP (interfejs@eksporter) — automatyczna odpowiedź nigdy nie zablackholuje adresu routera lub eksportera

BGP FlowSpec — granularna mitygacja (ExaBGP v5)

Wstrzykiwanie reguł per-flow (RFC 5575) bezpośrednio do peerów BGP upstream — bez scrubbing center i bez dodatkowych licencji. Ruch ataku jest odrzucany lub limitowany, a legalny ruch do tego samego adresu działa dalej.

- **Kryteria dopasowania** — prefiks docelowy i źródłowy, protokół, port dst/src, flagi TCP, DSCP, fragmentacja
- **Akcje** — drop (null-route tylko pasujących flowów) lub rate-limit (konfigurowalne kbps per neighbor)
- **Nieblokująca kolejka** — pipeline detekcji nigdy nie czeka na ogłoszenie BGP; FlowSpec Worker przetwarza kolejkę inject/withdraw co ~10 sekund

- **Automatyczne wycofanie** — reguły wygasają po konfigurowalnym czasie życia po ustaniu zagrożenia
- **Śledzenie statusu** — per-neighbor per-rule: pending / active / withdrawn / failed
- **Kontrola manualna** — ręczny inject/withdraw z modułu FlowSpec oraz ze strony szczegółów zagrożenia
- **Zarządzanie peerami** — pełny CRUD neighborów FlowSpec — IP, ASN, akcja per neighbor, włącz/wyłącz
- **Generator konfiguracji** — jeden klik generuje exabgp.conf z podglądem i bezpiecznym zapisem; przycisk Test CLI weryfikuje łączność z ExaBGP na żywo

BGP Traffic Diversion

Przekierowanie atakowanych prefiksów do ścieżki scrubbingowej lub alternatywnej bez konieczności całkowitego blackholingu. Obsługa wielu platform routingowych.

- **Trzy mechanizmy dywersji** — Withdraw (usunięcie prefiksu), Prefix-List (permit-only na wybranych peerach), Route-Map (deny via route-map)
- **Inteligentne selektywne ogłaszanie** — prefiks pozostaje osiągalny przez krytycznych peerów (Google, Meta, Akamai, Amazon, Cloudflare…) dzięki liście ASN allowlist — wycofywany tylko od pozostałych
- **SSH z audytem** — wykonywanie poleceń SSH (RSA 4096 / Ed25519) z podglądem wyników na żywo i pełną historią sesji
- **Auto-Trigger** — automatyczna aktywacja polityki dywersji gdy daemon wykryje atak rozproszony (fan-out) przekraczający próg Mbps
- **Auto-Revert** — automatyczne cofnięcie polityki po konfigurowalnym oknie czasowym
- **Potwierdzenie CIDR** — obowiązkowa brama potwierdzenia zakresu CIDR przed każdym wykonaniem SSH
- **Per-peer selection** — wybór, z których peerów eBGP wycofać prefiks, a na których utrzymać ogłoszenie
- **One-click Divert** — przycisk bezpośrednio w dashboardzie Distributed Alerts
- **Duplikacja polityk** — skopiowanie polityki na wiele routerów jednym kliknięciem
- **Historia zdarzeń** — pełny audit trail z output SSH dla każdej operacji

Obsługiwane platformy — BGP Traffic Diversion:

Linux FRR	Huawei NE8000	Cisco ASR
Free Range Routing vtysh / BGP daemon	VRP (Versatile Routing Platform)	IOS-XE (ASR 1000 / 9000)
agentowa + SSH	*SSH — bez agenta*	*SSH — bez agenta*

SIEM i zgodność z NIS2

- **Raportowanie incydentów** — workflow zgodny z Art. 23 NIS2 wspierający przygotowanie i dokumentację zgłoszeń, z automatycznym śledzeniem terminów od momentu detekcji (24h / 72h / 1 miesiąc)
- **Zarządzanie politykami** — wersjonowane polityki bezpieczeństwa z potwierdzeniem zapoznania się przez pracowników
- **Zarządzanie ryzykiem** — framework oceny ryzyka z systemem scoring
- **Rejestr szkoleń** — rejestracja szkoleń z pełną listą uczestników — także pracowników bez konta w systemie; szkolenia wewnętrzne i zewnętrzne, instruktor, daty i wbudowany katalog szkoleń obowiązkowych (polityka haseł, phishing, incident response, RODO, NIS2/KSC, DDoS, BCP/DR)
- **Logi audytowe** — kompleksowe logowanie działań administracyjnych (kto, co, kiedy, adres IP)
- **Zbieranie logów** — kolektor Syslog RFC 3164/5424 dla urządzeń wielu producentów
- **Parsowanie multi-vendor** — dedykowane parsery dla Juniper JunOS (UI_COMMIT/UI_AUTH, stany BGP rpd, sshd, link up/down, LACP, LLDP), Cisco IOS/IOS-XE, Linux syslog oraz generyczny fallback RFC 3164

- **Konfigurowalne reguły detekcji** — logika detekcji sterowana SQL — progi i włączanie reguł z UI, bez zmian w kodzie; biblioteka: brute force, port scan, DDoS volumetryczny, SYN flood, DNS abuse, porty C2, odbicia SYN-ACK, egress spoofing
- **Reguły własne** — możliwość dodania własnych zapytań detekcyjnych; reguły domyślne chronione i resetowalne
- **Trwałe detekcje** — wykryte zagrożenia z dekodowanym materiałem dowodowym (source MAC, próbki flowów, właściciel IP/ASN) zasilają silnik odpowiedzi
- **Silnik reguł** — dopasowywanie wzorców PCRE z poziomami ważności
- **Korelacja** — łączenie zdarzeń syslog z danymi ruchu NetFlow/sFlow
- **Powiadomienia** — alerty w czasie rzeczywistym przez email i webhook

Zarządzanie BGP i peeringiem

- **Synchronizacja konfiguracji — bez agenta** — bezpośredni pull SSH konfiguracji z routerów wielu producentów po stronie aplikacji — bez agenta ani dodatkowego oprogramowania na routerze; dla FRR dostępna również synchronizacja agentowa
- **Dynamiczne mapowanie peerów** — automatyczne dopasowanie sąsiadów BGP do interfejsów fizycznych i prędkości pasma poprzez wieloliniową analizę tablic ARP
- **Diagnostyka** — automatyczne sprawdzanie ARP, łączności interfejsów, wykrywanie problemów z peerami i stan sesji BGP
- **Monitorowanie pasma** — wykresy pasma per-interfejs z obsługą VLAN-tagged flows (indirect monitoring)
- **Analiza route-map / policy** — wizualizacja klauzul match/set, local-pref i prependów w UI — dla FRR, NE8000, ASR i Juniper MX
- **Inteligencja polityk Juniper MX** — ekstrakcja local-preference z rozróżnieniem prependów domyślnych od wyzwalanych community; polityki warunkowe z tooltipem informacyjnym
- **Billing i pasmo** — śledzenie 95. percentyla, CIR i PIR per peer
- **Terminal SSH** — bezpieczny, audytowany dostęp webowy do routerów (RSA / Ed25519) z kontrolą whitelist
- **Backup konfiguracji** — wersjonowane kopie zapasowe z unified diff, wykrywaniem zmian (SHA256) i etykietowaniem
- **Tablica routingu** — wydajna obsługa pełnych tablic (1M+ tras) z wykorzystaniem atomic swap

Obsługiwane platformy — BGP Manager (synchronizacja konfiguracji):

Linux FRR	Huawei NE8000	Cisco ASR	Juniper MX
vtysh / BGP daemon	VRP	IOS-XE	JunOS
agentowa + SSH	*SSH — bez agenta*	*SSH — bez agenta*	*SSH — bez agenta*

Skaner podatności sieciowych

- **Detekcja CVE** — skanowanie oparte na Nmap z wykrywaniem podatności (vulners script)
- **Skanowanie portów** — monitorowanie 55+ portów wysokiego ryzyka (bazy danych, C2, zdalny dostęp)
- **Przetwarzanie równoległe** — silnik batch dla dużych zakresów sieciowych
- **Integracja z SIEM** — podatności automatycznie generują zdarzenia bezpieczeństwa
- **Raporty** — automatyczne raporty email z podziałem na kategorie ważności

Monitoring sieci (NMS)

- **Monitoring interfejsów SNMP** — zbieranie liczników per-interfejs (bity/pakiety, błędy, utylizacja) z historycznymi wykresami trendów
- **Dashboardy per urządzenie** — tabele interfejsów i status łączy w jednym widoku
- **Kontrole usług i uptime** — śledzenie dostępności monitorowanych usług z pełną historią wyników
- **Magazyn time-series** — liczniki i wyniki kontroli trwale zapisywane w TimescaleDB dla długoterminowych trendów

Portal klienta (edycja ISP/IXP)

- **Widoczność ruchu** — klienci widzą własne wykresy i statystyki ruchu sieciowego
- **Alerty DDoS** — historia ataków na prefiksy klienta
- **Raporty PDF** — raporty bezpieczeństwa do pobrania
- **Izolacja danych** — ścisła separacja danych na podstawie przypisanych CIDR

Analiza ruchu sieciowego

- **Wieloprotokołowa obsługa** — NetFlow v5/v9/IPFIX, sFlow, PCAP w zunifikowanym modelu danych
- **Zaawansowane wyszukiwanie** — filtrowanie po IP (CIDR), porcie, protokole, ASN, geolokalizacji i zakresie czasowym
- **Top talkers** — identyfikacja największych źródeł ruchu po IP, ASN, kraju, protokole
- **Interaktywna wizualizacja** — zoom w stylu Grafana z dynamicznym skalowaniem przedziałów czasowych
- **Diagramy Sankey** — wizualizacja dystrybucji ruchu sieciowego
- **Analiza forensic** — przeszukiwanie logów przepływowych na dysku (nfdump)
- **Wyszukiwanie CGNAT / NAT** — reverse-lookup translacji NAT (LER) — odczyt conntrack routera z automatycznym fallbackiem do pól translacji NetFlow XLT
- **Eksport danych** — CSV, JSON, PDF

Odkrywanie i konfiguracja kolektorów

- **Live Packet Capture** — skanowanie interfejsów sieciowych i automatyczne odkrywanie eksporterów NetFlow/sFlow
- **Głęboka analiza** — identyfikacja wersji flow, portu, ogłaszanej częstotliwości próbkowania oraz typu eksportu (ruch vs. rekordy zdarzeń/NAT)
- **Manualna mapa próbkowania** — ręczne wskazanie sampling rate per eksporter — poprawna renormalizacja liczników przy ingest
- **Konfiguracje single-writer** — configi pmacct generowane z bazy z walidacją, podglądem diff i zastosowaniem jednym kliknięciem

Asystent AI

- **Zapytania w języku naturalnym** — pytania o status sieci, analiza historyczna, identyfikacja trendów
- **Automatyczny troubleshooting** — wsparcie diagnostyczne i operacyjne
- **Integracja MCP** — rozszerzalny system narzędzi: Traffic Search, CGNAT Lookup, BGP Status, Vulnerability Analysis — z zatwierdzaniem wykonania
- **Obsługiwane backendy AI** — ITCare AI API oraz wewnętrzne serwery AI w bezpiecznej sieci (Ollama, vLLM, LM Studio, OpenAI-compatible)

Specyfikacja techniczna

Architektura

- Backend: PHP 8+ (Composer PSR-4)
- Bazy danych: MariaDB (konfiguracja), PostgreSQL + TimescaleDB (time-series i flow analytics)
- Frontend: Bootstrap 4 + jQuery + Chart.js — wszystkie zasoby lokalne, bez zewnętrznych CDN
- Serwer WWW: Apache2 (mod_php)
- Kolekcja danych: pmacct (nfacctd, sfacctd, nfpcapd) + nfdump
- Mitygacja FlowSpec: ExaBGP v5 (IPC przez named pipes, bez zależności od HTTP API)
- Integracja routingu BGP: multi-vendor — FRR (vtysh), Huawei NE8000 (SSH/VRP), Cisco ASR (SSH/IOS-XE), Juniper MX (SSH/JunOS), MikroTik RouterOS
- Licencjonowanie modułów premium: licencja związana ze sprzętem (Hardware ID + podpis Ed25519)

- Aktualne wydanie: v3.1.41 „Sentinel"

Wymagania sprzętowe

Parametr	Minimum (do 10 Gbit/s)	Produkcja (zalecane)
CPU	4 rdzenie / 8 wątków	16+ rdzeni
RAM	12 GB	64 GB
Dysk	256 GB SSD	2 TB NVMe SSD
System	Ubuntu 20.04/22.04, Debian 12/13	Ubuntu 22.04 LTS
Interfejs siec.	1 Gbps	10 Gbps

Opcje wdrożenia

- **On-Premises** — Pełna kontrola nad danymi i infrastrukturą na dedykowanych serwerach klienta. Idealne dla branż regulowanych i środowisk air-gap.
- **Usługa zarządzana** — Instalacja, utrzymanie, monitoring 24/7 i SLA po naszej stronie, na serwerach klienta.
- **Wdrożenie hybrydowe** — Kolektory na brzegu sieci, centralna konsola zarządzania. Widoczność wielu lokalizacji w jednym interfejsie.

Integracje

Źródła danych	Platformy routingu	Kanały powiadomień	Zewnętrzne API
• NetFlow v5/v9/IPFIX • sFlow, PCAP • Syslog (UDP/TCP/TLS) • SNMP • Dane routingu BGP	• FRR, BIRD • Cisco IOS / IOS-XE • Juniper JunOS / MX • Arista EOS • MikroTik RouterOS • Huawei NE8000 (VRP)	• Email (SMTP) • Webhooks (HTTP/S) • Slack • Microsoft Teams • Własne API	• PeeringDB • MaxMind GeoIP • RIPE NCC • Własne REST API

Przewagi konkurencyjne

vs. komercyjne DDoS (Arbor, Cloudflare)	vs. open source (ELK, Prometheus)	vs. tradycyjne SIEM (Splunk, QRadar)
• Brak opłat per Gbps — nieograniczona analiza ruchu • Self-hosted — pełna suwerenność danych • Zintegrowany SIEM i skaner — brak potrzeby osobnych narzędzi • BGP Traffic Diversion wbudowany — bez kosztów scrubbing center • BGP FlowSpec wbudowany — granularna mitygacja przez ExaBGP v5, bez	• Zaprojektowane specjalnie dla sieci ISP/IXP • Automatyczna mitygacja — nie tylko alerty • Zunifikowany interfejs — brak rozproszenia narzędzi • Gotowe do produkcji — enterprise od razu po instalacji • Zgodność NIS2 out-of-the-box	• Natywna obsługa sieci — rozumie flows, BGP, ASN • Mitygacja w czasie rzeczywistym — nie tylko detekcja • Brak opłat za ingestion danych • Szybsze wdrożenie — tygodnie zamiast miesięcy • Niższy TCO o 70–80%

dodatkowych licencji • Jednorazowy koszt — brak subskrypcji cyklicznych		

Modele licencjonowania

Licencja wieczysta	Licencja subskrypcyjna	Usługa zarządzana	Enterprise
• Jednorazowy zakup Core System • Bez limitu użytkowników i ruchu • 1 rok aktualizacji w cenie • Moduły dodatkowe: NIS2, AI Chat, Portal Klienta, Skaner	• Rozliczenie roczne lub miesięczne • Wszystkie moduły w cenie • Elastyczne skalowanie • Rezygnacja w dowolnym momencie	• Miesięczna opłata per lokalizacja • Sprzęt, oprogramowanie, wsparcie 24/7 • SLA gwarantowane po naszej stronie	• Indywidualna wycena • Rabaty wolumenowe • Dedykowany zespół wsparcia • Priorytet rozwoju funkcji

Moduły premium aktywowane licencją związaną ze sprzętem (Hardware ID + podpis Ed25519). Skontaktuj się z nami po szczegółową wycenę dopasowaną do Twoich potrzeb.

Wsparcie i usługi profesjonalne

Usługi profesjonalne

- Instalacja i konfiguracja: 1–5 dni
- Szkolenia zdalne i on-site
- Integracje niestandardowe: rozwój API, dedykowane kolektory
- Migracja z istniejących rozwiązań
- Kwartalne przeglądy kondycji systemu

Poziomy wsparcia

- **Standard (w ramach subskrypcji)** — Email (odpowiedź do 24h), poprawki, kwartalne aktualizacje
- **Premium (dodatkowo płatne)** — Wsparcie 24/7, SLA 8h, dedykowany inżynier, miesięczne przeglądy
- **Enterprise (indywidualnie)** — Nazwany zespół, SLA 1h, priorytet rozwoju funkcji

Zapytania ogólne: info@ispadmin.pl | +48 (32) 720 36 81 | Fax: +48 (32) 720 36 82
Dział techniczny / NOC: noc@ispadmin.pl | +48 (32) 720 36 84 | Fax: +48 (32) 720 36 82
Wersja dokumentu: v3.1.41 „Sentinel" — Lipiec 2026