ITCSECadmin

Platforma Bezpieczeństwa Sieciowego

Detekcja DDoS · Mitygacja BGP · 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, dywersję ruchu BGP, SIEM, monitoring sieci, zarządzanie BGP z **integracją multi-vendor**, 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 Traffic Diversion, SIEM, monitoring sieci, 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 z automatyczną mitygacją poprzez BGP blackholing lub dywersję ruchu do ścieżki scrubbingowej.

BGP Traffic Diversion bez blackholingu

Przekierowanie atakowanego ruchu na ścieżkę scrubbingową bez konieczności całkowitego czarnego dziurowania. Natywna integracja z urządzeniami wielu producentów. Auto-trigger i auto-revert na podstawie wykrytego ataku rozproszonego.

Zgodność z NIS2
Wbudowany moduł compliance: raportowanie incydentów (Art. 23), zarządzanie ryzykiem, polityki bezpieczeństwa, rejestry szkoleń i tamper-evident 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.

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 i integracją FlowSpec — obsługiwane platformy: FRR, Huawei NE8000 (VRP), Cisco ASR (IOS-XE)
- **Zarządzanie białą/czarną listą** — whitelisting i blacklisting adresów IP
- **Obsługa różnych typów ataków** — volumetryczne, protokołowe i warstwy aplikacji

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)
- **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 konfigurowalny próg Mbps
- **Auto-Revert** — automatyczne cofnięcie polityki po konfigurowalnym oknie czasowym
- **Potwierdzenie CIDR** — obowiązkowa brama potwierdzenia zakresu CIDR przed każdym wykonaniem SSH — zapobiega przypadkowej aktywacji
- **Per-peer selection** — wybór, z których peerów eBGP wycofać prefiks, a na których utrzymać ogłoszenie; automatyczne wzajemne wykluczanie opcji
- **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** — zgodne z Art. 23 NIS2, śledzenie terminów 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** — śledzenie szkoleń z zakresu bezpieczeństwa i dat ich wygaśnięcia
- **Logi audytowe** — tamper-evident logowanie wszystkich działań bezpieczeństwa
- **Zbieranie logów** — kolektor Syslog RFC 3164 dla urządzeń wielu producentów
- **Silnik reguł** — dopasowywanie wzorców PCRE z poziomami ważności
- **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 — nie jest wymagany żaden agent Python ani dodatkowe oprogramowanie 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 obecności 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** — wizualizacja klauzul match/set, local-pref i prependów bezpośrednio w UI
- **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 dla zerowego przestoju

Obsługiwane platformy — BGP Manager:

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

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** — reverse-lookup translacji NAT do identyfikacji wewnętrznych IP (LER)
- **Eksport danych** — CSV, JSON, PDF

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
- Integracja routingu BGP: FRR (vtysh), Huawei NE8000 (SSH/VRP), Cisco ASR (SSH/IOS-XE)

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 LTS, Debian 12/13	Ubuntu 22.04 LTS
Interfejs sieciowy	1 Gbps	10 Gbps

Bezpieczeństwo i zgodność regulacyjna

- **Uwierzytelnianie** — sesje z przesuwnym czasem wygaśnięcia
- **Autoryzacja** — RBAC: Admin, User, Viewer
- **Szyfrowanie** — HTTPS/TLS
- **Audit log** — logowanie wszystkich działań administracyjnych
- **Air-gap** — zero zewnętrznych wywołań w trybie operacyjnym
- **NIS2** — framework zarządzania ryzykiem
- **RODO/GDPR** — kontrola retencji danych
- **ISO 27001** — dopasowanie kontroli bezpieczeństwa
- **PCI DSS** — wsparcie segmentacji sieciowej
- **HIPAA** — możliwości compliance

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 — bez konieczności utrzymywania własnego zespołu operacyjnego.

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	FRR, BIRD	Email (SMTP)	PeeringDB
sFlow, PCAP	Cisco IOS / IOS-XE	Webhooks (HTTP/S)	MaxMind GeoIP
Syslog (UDP/TCP/TLS)	Juniper Junos	Slack	RIPE NCC
SNMP	Arista EOS	Microsoft Teams	Własne REST API
Dane routingu BGP	MikroTik RouterOS	Własne API	
	Huawei NE8000 (VRP)		

Przewagi konkurencyjne

vs. komercyjne DDoS (Arbor, Cloudflare)

- ✓ Brak opłat per Gbps — nieograniczona analiza ruchu
- ✓ Self-hosted — pełna suwerenność danych
- ✓ Zintegrowany SIEM i skaner — brak potrzeby osobnych narzędzi
- ✓ BGP Traffic Diversion wbudowany — przekierowanie bez blackholingu, bez kosztów scrubbing center
- ✓ Jednorazowy koszt — brak subskrypcji cyklicznych

vs. open source (ELK, Prometheus)

- ✓ 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

vs. tradycyjne SIEM (Splunk, QRadar)

- ✓ 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%

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

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 (24h), poprawki, kwartalne aktualizacje
- **Premium** (dodatkowo płatne) — Wsparcie 24/7, SLA 8h, dedykowany inżynier, miesięczne przeglądy
- **Enterprise** (indywidualnie) — Nazwany zespół, SLA 1h, priorytet rozwoju

Zapytania ogólne
Email: info@ispadmin.pl
Tel: +48 (32) 720 36 81
Fax: +48 (32) 720 36 82

Dział techniczny / NOC
Email: noc@ispadmin.pl
Tel: +48 (32) 720 36 84
Fax: +48 (32) 720 36 82

Dokument:
Opis Produktu ITCSECadmin
Wersja: 2.9.4+
Data: Luty 2026