

Ataki DDoS

– dlaczego to dziś realny problem?

Skala ataków DDoS rośnie z roku na rok. Dostęp do botnetów i urządzeń IoT sprawia, że przeprowadzenie ataku jest łatwiejsze niż kiedykolwiek. Coraz częściej firmy nie wiedzą nawet, że zostały zaatakowane — bo wygląda to jak zwykła awaria.

Rosnąca skala

Rekordy wolumenu ataków bite co kwartał

Łatwiejszy dostęp

Botnety i IoT obniżają próg wejścia dla atakujących

Fałszywe awarie

Ataki maskowane jako zwykłe przestoje infrastruktury

Czym jest atak DDoS?



DDoS (**Distributed Denial of Service**) to nie włamanie. To zalanie systemu ogromną liczbą zapytań wysyłanych jednocześnie z tysięcy źródeł.



Ruch wygląda normalnie — ale w takiej skali całkowicie blokuje dostęp do usług.

- Ogromna liczba zapytań w krótkim czasie
- Ataki z wielu rozproszonych źródeł
- Cel: przeciążenie i niedostępność infrastruktury

Dlaczego standardowe zabezpieczenia nie wystarczają?

Większość firm chroni systemy *od środka* — ale nie kontroluje tego, co do nich trafia.
Gdy atak już dotrze do infrastruktury, reakcja często przychodzi za późno.

Ochrona „w środku”

Firewalle i IDS działają dopiero po wpuszczeniu ruchu do sieci

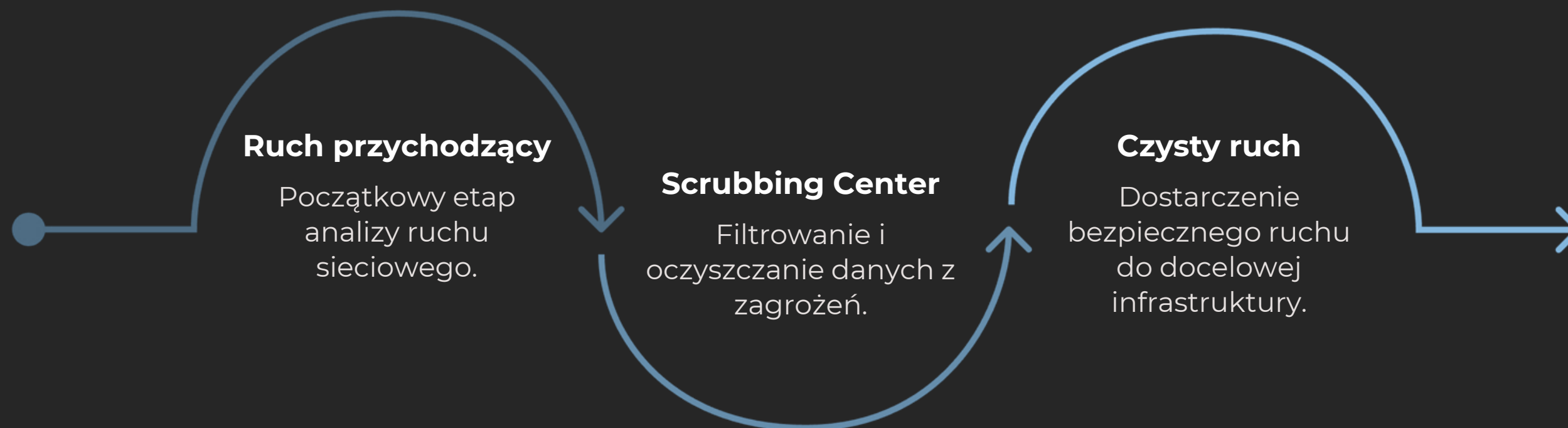
Reakcja zamiast zapobiegania

Tradycyjne narzędzia reagują na incydent, nie blokują go z wyprzedzeniem

Brak kontekstu ruchu

Bez analizy behawioralnej złośliwy ruch jest nieodróżnialny od legalnego

Jak działa Scrubbing Center?



Scrubbing Center działa jak zaawansowany filtr **przed** Twoją infrastrukturą. Cały ruch przychodzący jest analizowany w czasie rzeczywistym — do sieci klienta trafia wyłącznie ruch zweryfikowany jako bezpieczny.

Co nas wyróżnia?



Uczenie się profilu ruchu

System analizuje i zapamiętuje wzorce normalnego ruchu każdego klienta indywidualnie



Wykrywanie anomalii

Reagujemy tylko na odchylenia od normy — nie blokujemy całego ruchu pochopnie



Dopasowanie do środowiska

Ochrona skrojona na miarę konkretnej infrastruktury — nie rozwiązanie generyczne



Większość standardowych rozwiązań blokuje wszystko lub nic. My rozumiemy Twój ruch.

Poziomy ochrony

STEEL SHIELD

Ochrona podstawowa

- Stały monitoring i analiza ruchu
- Wykrywanie anomalii i alertowanie
- Podstawowa mitygacja ataków

Idealny punkt startowy dla organizacji budujących świadomość zagrożeń sieciowych.

TITANIUM SHIELD

Pełna ochrona aktywna

- Pełne filtrowanie ruchu w trybie online
- Reakcja i mitygacja w czasie rzeczywistym
- Inteligentna priorytetyzacja ruchu

Dla środowisk krytycznych wymagających zerowej tolerancji na przestoje.

Bezpieczeństwo zaczyna się wcześniej

„Jeśli atak dociera do Twojej infrastruktury — to znaczy, że jest już za późno.”

1. Nie w systemie
Zabezpieczenia aplikacyjne to za mało
2. Nie w aplikacji
Warstwa aplikacji jest już za blisko celu
3. W sieci
Filtrowanie ruchu zanim dotrze do infrastruktury





Dziękujemy za uwagę!

Masz więcej pytań? Skontaktuj się z nami:



www.omega-es.pl



19 007



kontakt@omega-es.pl

