Strategia ochrony zasobów IT

Michał Przygoda

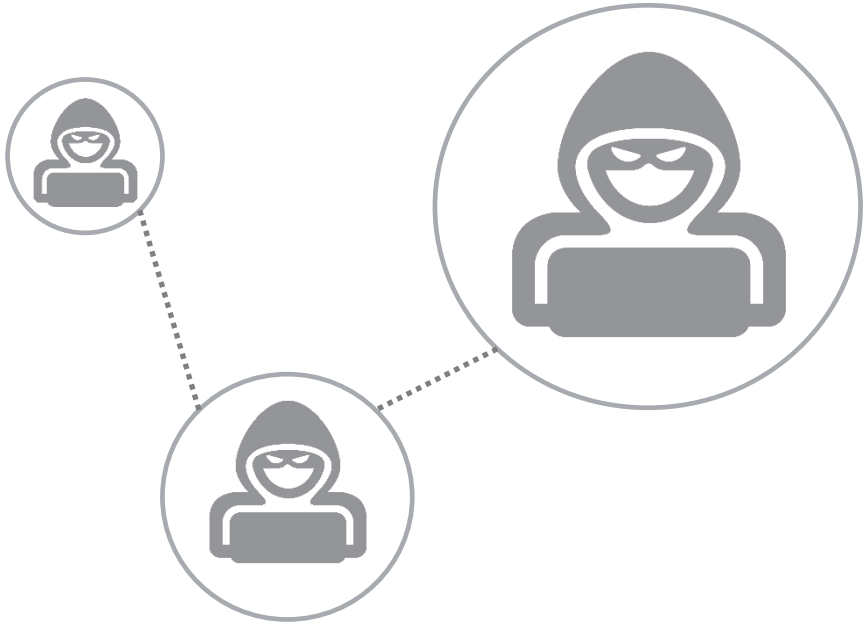
Cyberprzestępczość

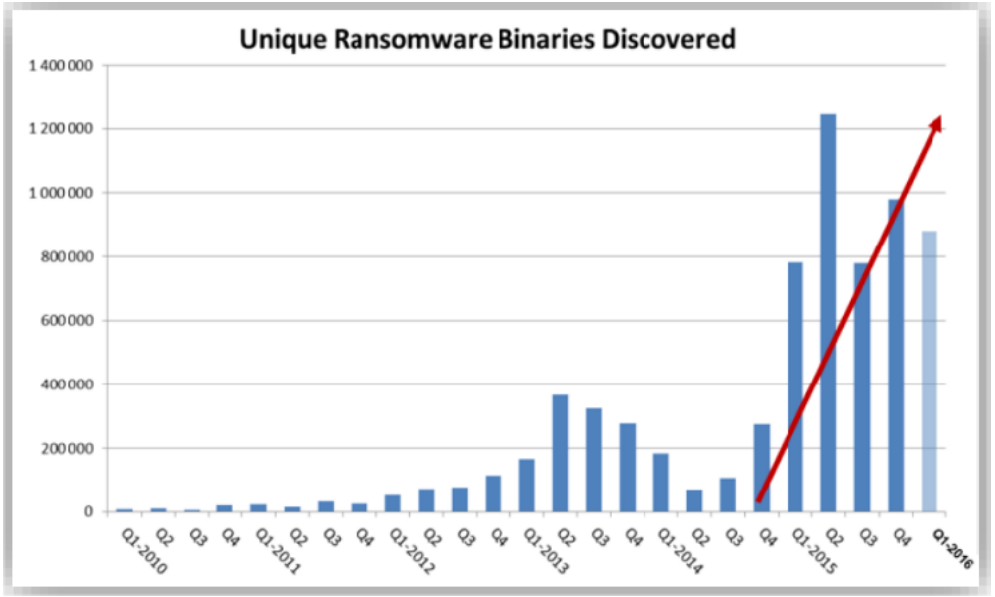
Liczba wykrytych **naruszeń bezpieczeństwa IT** w Polsce wzrosła o **46%** w porównaniu do zeszłego roku.

Ponad połowa firm i organizacji w Polsce odnotowała nie mniej niż 6 cyberataków w 2015r.

Ransomware - przychody z okupów w ramach jednej kampanii cyberprzestępców sięgnęły **325 mln USD**!

Cyberprzestępczość - ransomware





Internet – kto jest po drugiej stronie ?

Atak/niebezpieczny kod jako usługa

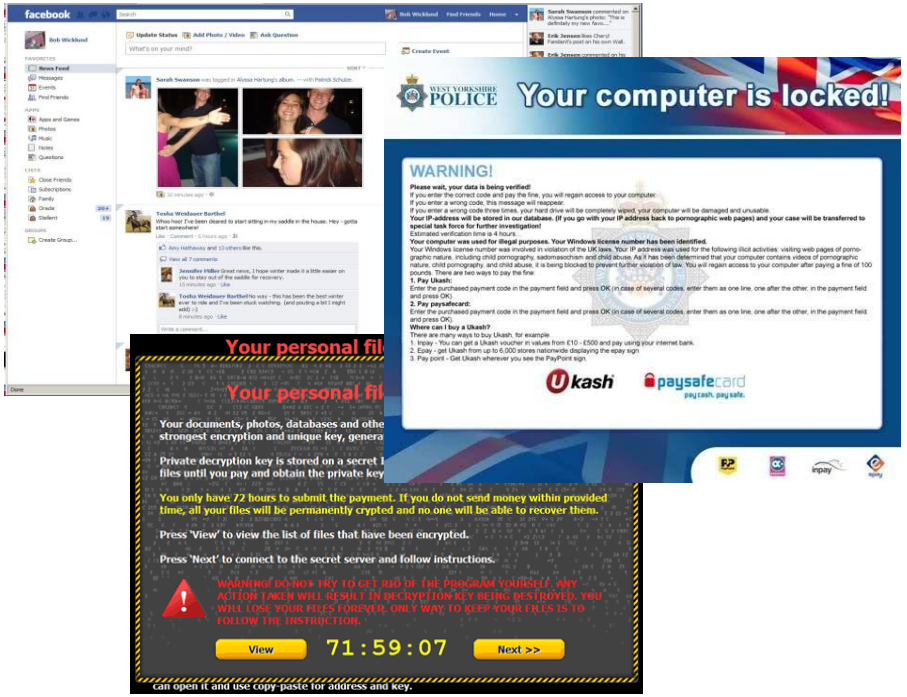
- **Inżynierowie**
  - Niebezpieczny kod rozpowszechniany jest za pomocą tzw. „dark web”.
  - Określ wymagania, zdefiniuj swój cel i odbierz przygotowany dla ciebie malware.
- **Marketing**
  - Zaprojektuj i przetłumacz treści wiadomości email.
  - Sieci BOT dostarczą twoją wiadomość do właściwych odbiorców.

  Za dodatkowa opłatą możesz również otrzymać: informacji o zabezpieczeniach organizacji, informacji dot. polityki bezpieczeństwa, a nawet diagramów sieci.
- **Handel**
  - Napisałeś malware? Chcesz zarobić? Za odpowiednią prowizję możesz dać reklamę która na pewno dotrze do zainteresowanych osób.
- **Wsparcie**
  - Potrzebujesz pomocy jak kupić malware?
  - Potrzebujesz się dokształcić – może specjalistyczne szkolenie jak przeprowadzić udany atak?
  - …A może jesteś ofiarą, która chce zapłacić okup w bitcoin’tach i nie masz bladego pojęcie jak to zrobić?

... „DZIĘKUJEMY … ZAPRASZAMY PONOWNIE”

Skutki

… niezabezpieczonego komputera oraz połączenia do sieci Internet



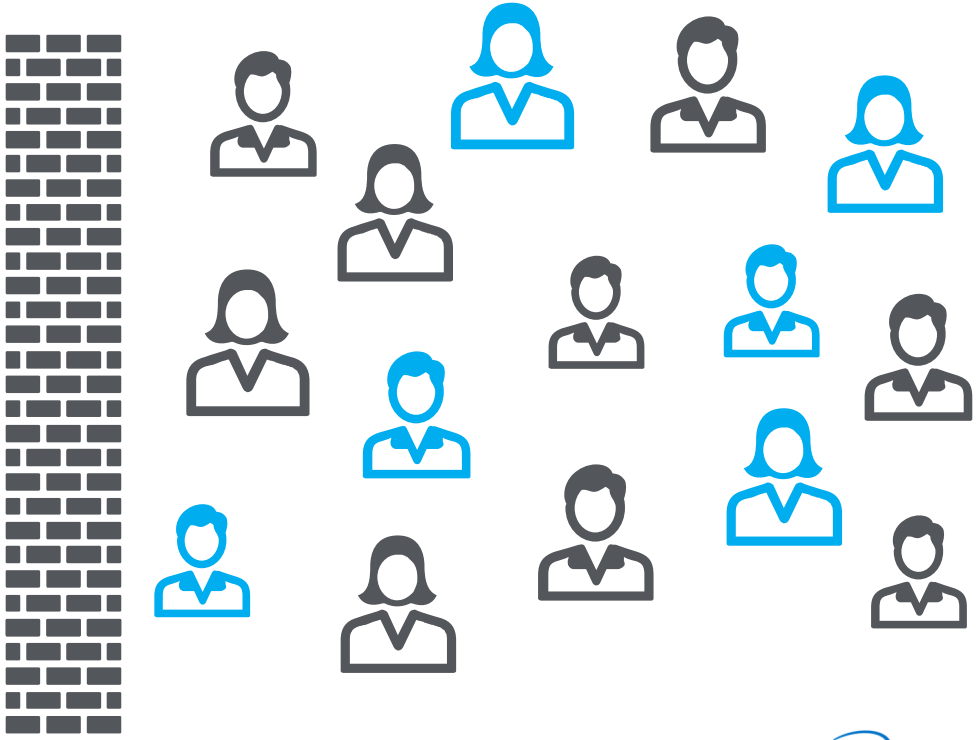
- **Ryzyko** utraty wartościowych, poufnych danych
- **Ryzyko** propagacji zagrożenia na inne zasoby
- **Wysokie koszty** związane z odzyskaniem danych oraz usunięciem zagrożenia
- **Negatywny** wpływ na użytkowników komputerów i sieci Internet
- **Utrata** reputacji

Sposoby ataków

Przed czym powinniśmy się chronić

Zagrożenia

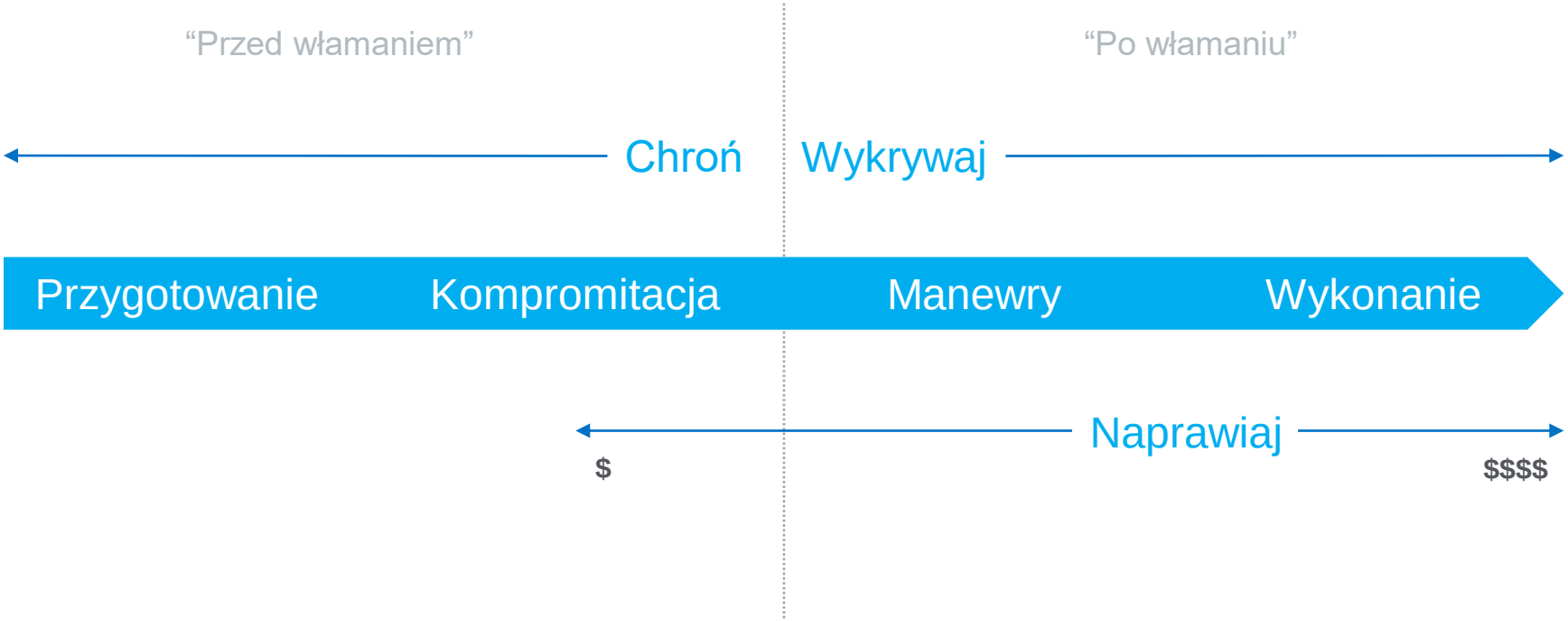
- Niebezpieczne strony Internetowe
- Niebezpieczne pliki pobierane z Internetu
- Niebezpieczne pliki przenoszone za pomocą pamięci przenośnych
- Niebezpieczne oprogramowanie
- Wiadomości email



Ciemne charaktery są już w Twojej sieci

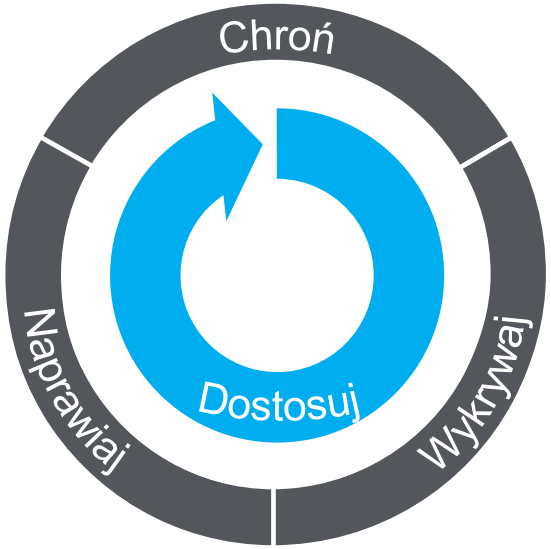
OCHRONA nie jest już wystarczająca. Należy skupić się również na **WYKRYWANIU** oraz **NAPRAWIANIU SZKÓD**

Cykl życia ataku – Strategia Ochrony



Chroń, Wykrywaj, Naprawiaj

Kompleksowe podejście do bezpieczeństwa



Chroń – Neutralizuj zagrożenia zanim pojawią się w lokalnej sieci i wyrządzą szkody. Skutecznie egzekwuj politykę korzystania z zasobów IT.

Wykrywaj – Wykrywaj anomalie, zagrożenia, zainfekowane zasoby, wykorzystanie zasobów IT niezgodne z przyjętą polityką/regulaminem.

Naprawiaj – Minimalizuj straty, usuwaj zagrożenia.

Dostosuj – Zastosuj wiedzę natychmiast dla całej organizacji w celu ochrony przed podobnymi zagrożeniami.

Chroń

Aktywna ochrona przed zagrożeniami

Wiedza: globalna, organizacji oraz firm trzecich.

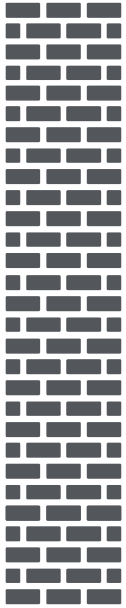
Współpracująca infrastruktura działa jako jeden adaptacyjny system.

Wszechstronna ochrona

Siła wiedzy

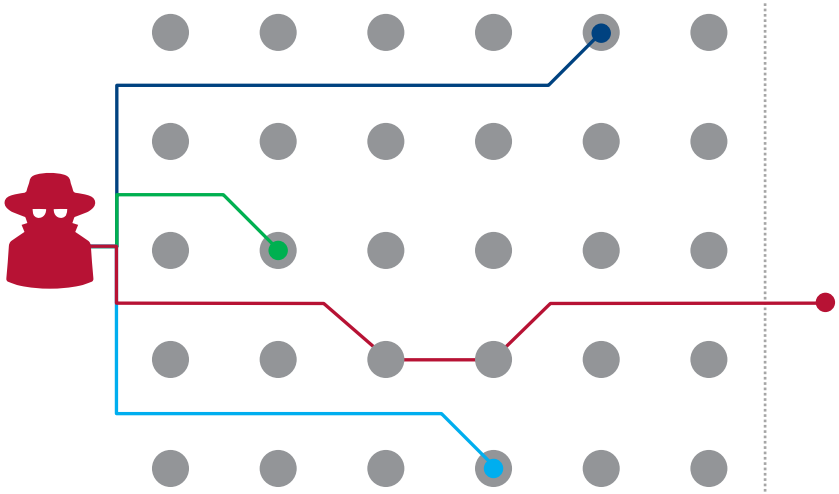
Zagrożenia

- Niebezpieczne strony Internetowe
- Niebezpieczne pliki pobierane z Internetu
- Niebezpieczne pliki przenoszone za pomocą pamięci przenośnych
- Niebezpieczne oprogramowanie
- Wiadomości email



Tradycyjna wyspowa struktura bezpieczeństwa

Gromada samodzielnych żołnierzy: adaptacja manualna lub brak



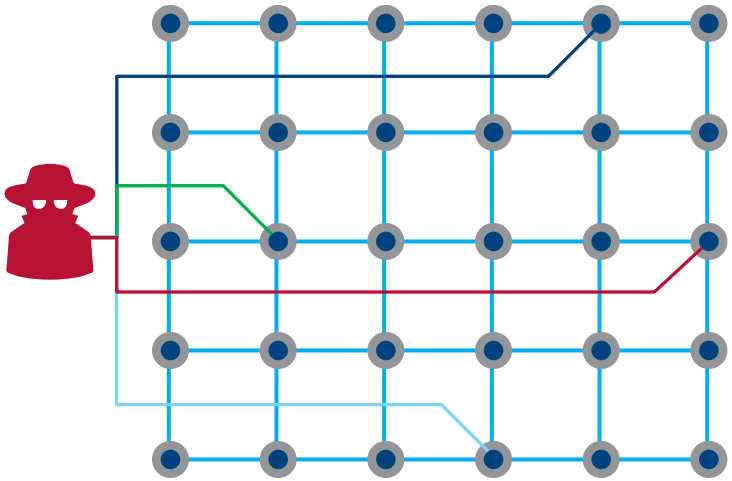
Przed włamaniem

Po włamaniu

Pojedyncze technologie mogą być bardzo efektywne, jednak poszczególne elementy nie uczą się od siebie.

Skuteczna ochrona dzięki wymianie informacji

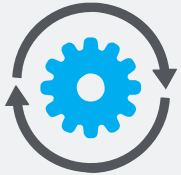
Deterministyczne i automatyczne reakcje: dostosuj ochronę w czasie rzeczywistym



Przed włamaniem | Po włamaniu

Dostarcza wglądu w sytuację poprzez współpracującą infrastrukturę.

Wykrywaj



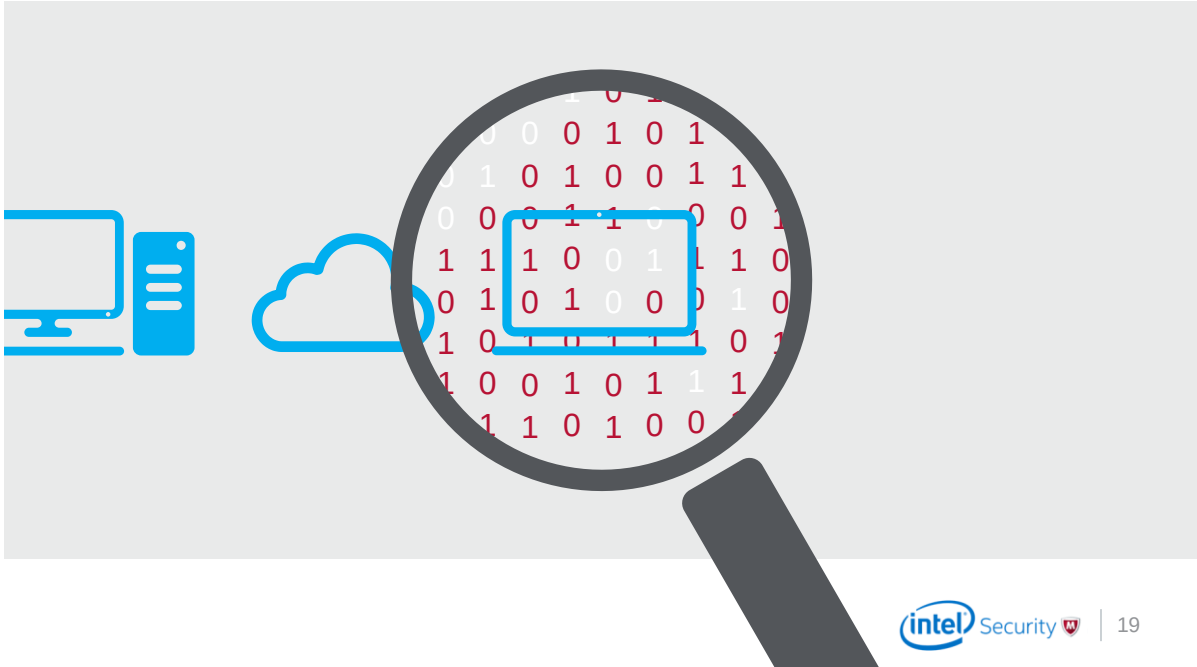
Głębokie, ciągłe i automatyczne monitorowanie.

Odchylenia i korelacja oparta o reguły by wychwycić nawet pozornie mało istotne sygnały.

Automatyzacja bazy informacji o zagrożeniach by aktywnie „łowić” ślady ataków.

Głębokie, ciągłe i automatyczne monitorowanie

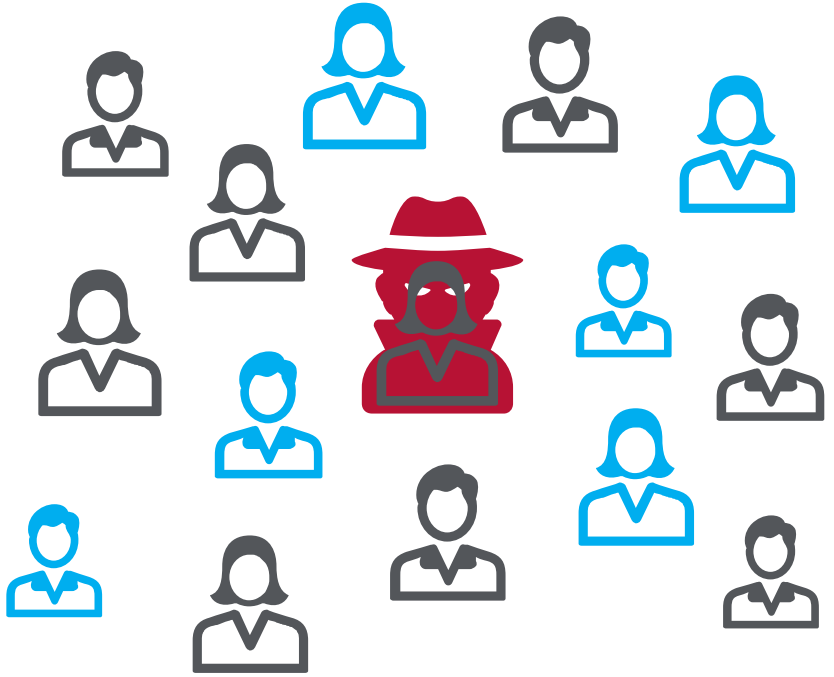
Automatyczne zbieranie, normalizacja i korelacja danych z cennych, „gadatliwych” źródeł danych dają bardzo dużo informacji kontekstowej, która jest niezbędna przy wykrywaniu zaawansowanych ataków.



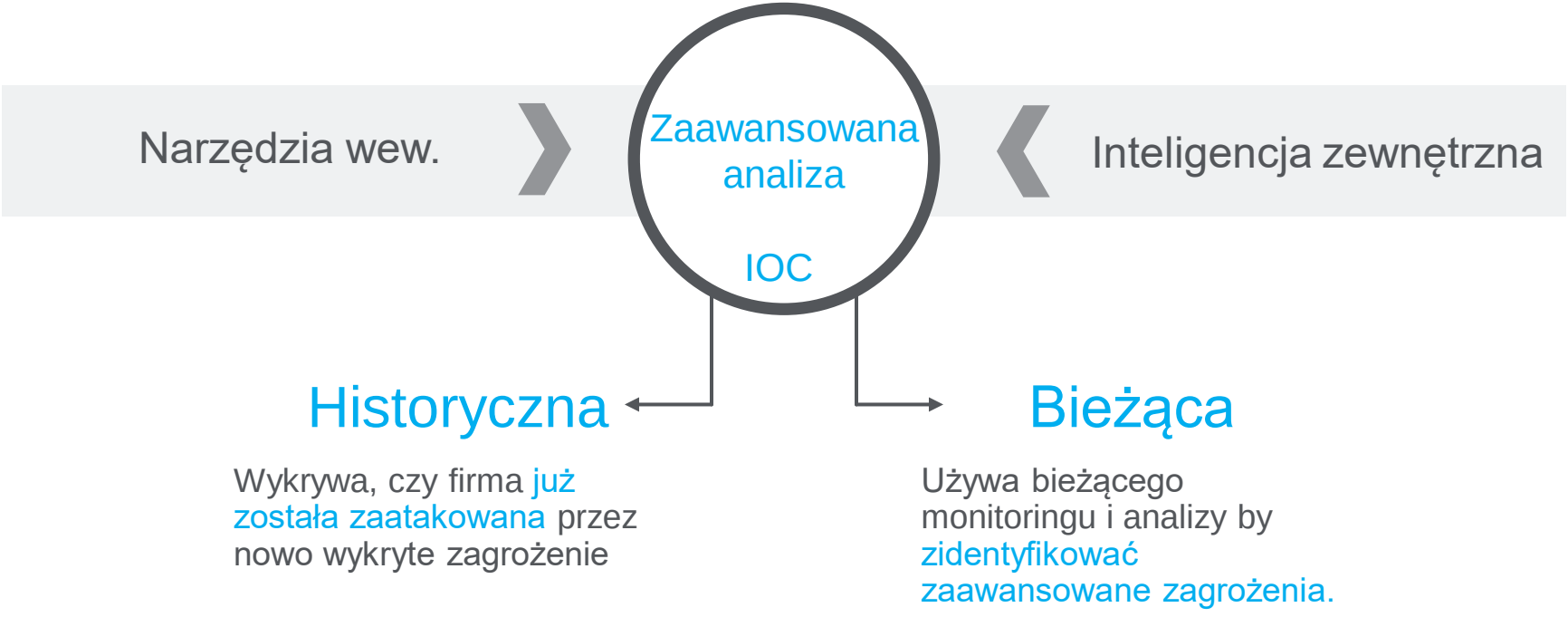
Analityka odchyleń i korelacji.

Identyfikacja nisko-progowych aktywności poprzez zaawansowaną analizę wzorców i ryzyka.

Redukcja czasu analizy incydentów poprzez zwieszenie widoczności najbardziej znaczących i istotnych zdarzeń.

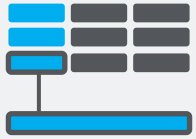


Zautomatyzowane, proaktywne „łowienie”

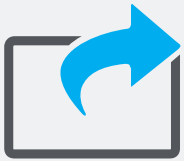


Naprawiaj

Priorytetyzacja by zająć się najbardziej krytycznymi incydentami posiadając ograniczone zasoby.



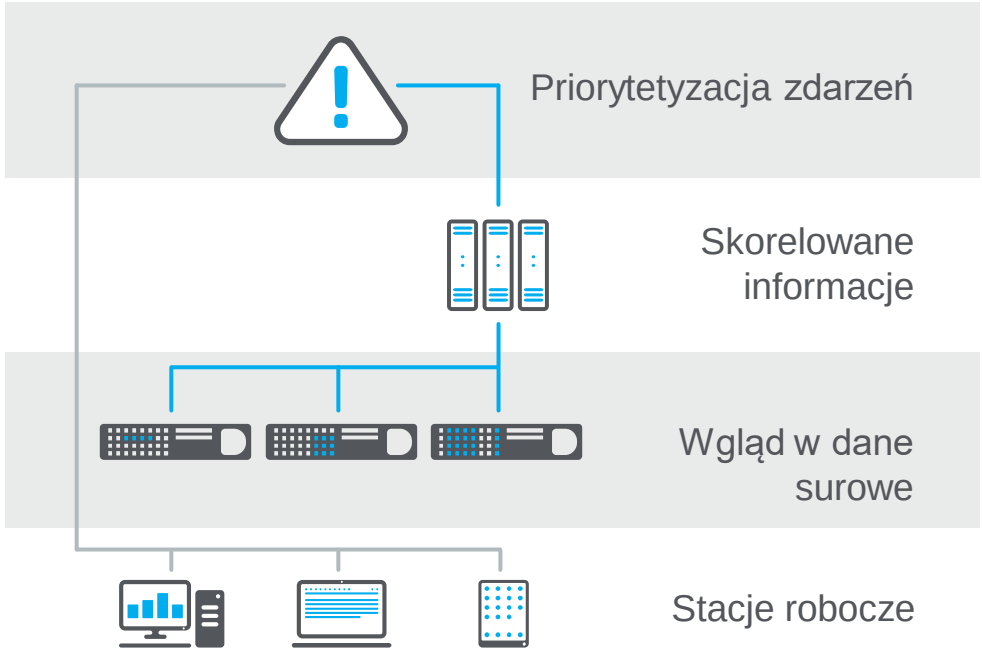
Płynne śledztwo z zaawansowanymi widokami, drążeniem danych oraz rzeczywistym wykrywaniem i odpowiedzią.



Automatyczna i rzeczywista odpowiedź w reakcji na incydenty bez przestojów operacyjnych.

Płynne postępowanie

- Zoptymalizowane procesów i przypadków użycia w samym narzędziu analitycznym.
- Ocena sytuacji w czasie rzeczywistym wraz z wglądem w warstwę plików, sieci i użytkowników.



Automatyczna, rzeczywista, interaktywna odpowiedź

Zautomatyzowana

Oparta o decyzję człowieka

Isolate	Contain	Convict	Remediate
Notify	Alert	Report	Deploy

Chroń, Wykrywaj, Naprawiaj, Dostosuj

Chroń

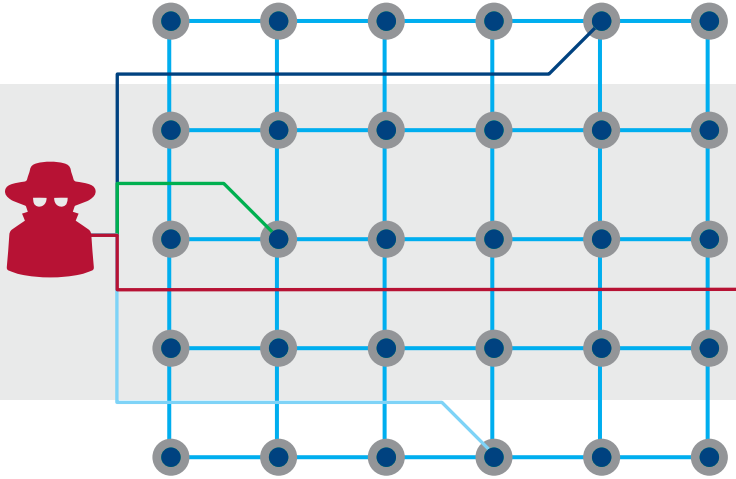
Współpracująca architektura wykrywa bieżące zagrożenia.

Wykrywaj

Stały wgląd w sytuacje wykrywa historyczne i bieżące zagrożenia.

Naprawiaj

Ocenia i pomaga przeprowadzić reakację na incydenty z użyciem ograniczonych zasobów.

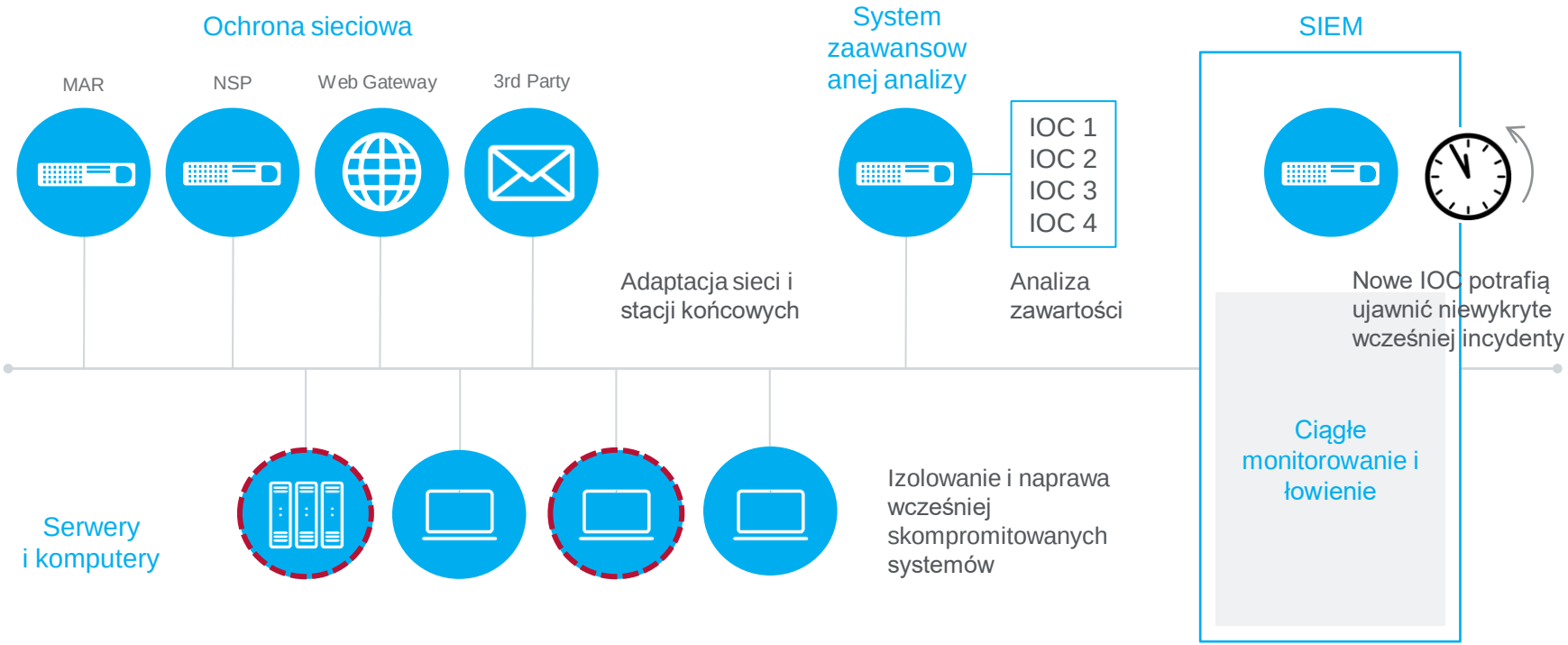


Adapt

Przed włamaniem

Po włamaniu

Security Connected – Kompresja czasu odpowiedzi




intel
Security