



Strategia ochrony zasobów IT

Michał Przygoda



TM

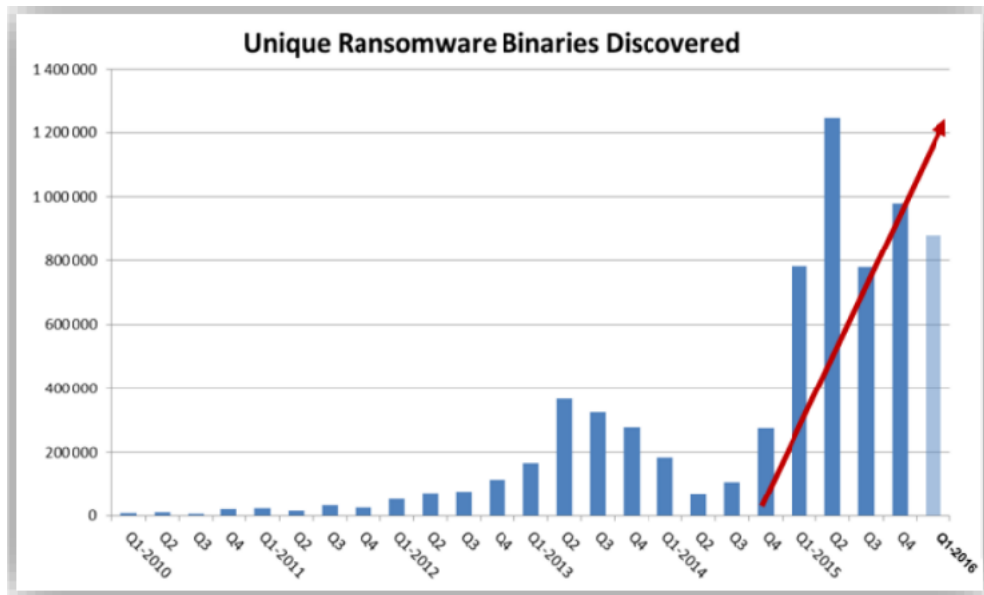
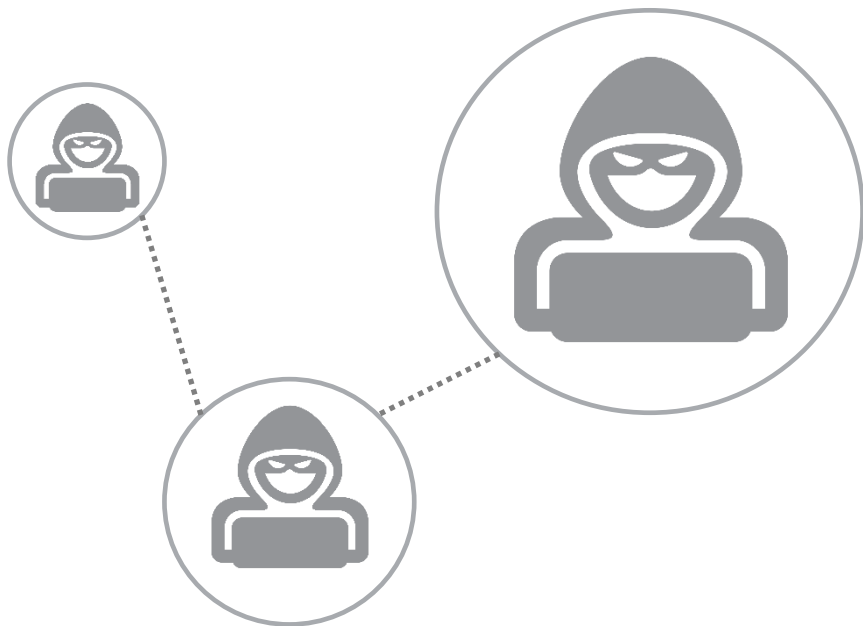
Cyberprzestępczość

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 doksztalić – 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

The image is a composite of three screenshots illustrating the consequences of an unsecured computer and internet connection. The top left shows a Facebook profile for 'Rob Wickhead' with a post from Sarah Swanson. The top right shows a blue warning box from 'WEST YORKSHIRE POLICE' titled 'Your computer is locked!'. The bottom part shows a ransomware payment screen with a black background and yellow text. The ransomware screen includes the following text: 'Your personal files are encrypted. Your documents, photos, databases and other strongest encryption and unique key, generated by our program. Private decryption key is stored on a secret server until you pay and obtain the private key. You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them. Press "View" to view the list of files that have been encrypted. Press "Next" to connect to the secret server and follow instructions. WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF, ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION. View 71:59:07 Next >>'. The ransomware screen also features logos for 'Ukash' and 'paysafecard'.

- ❑ **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

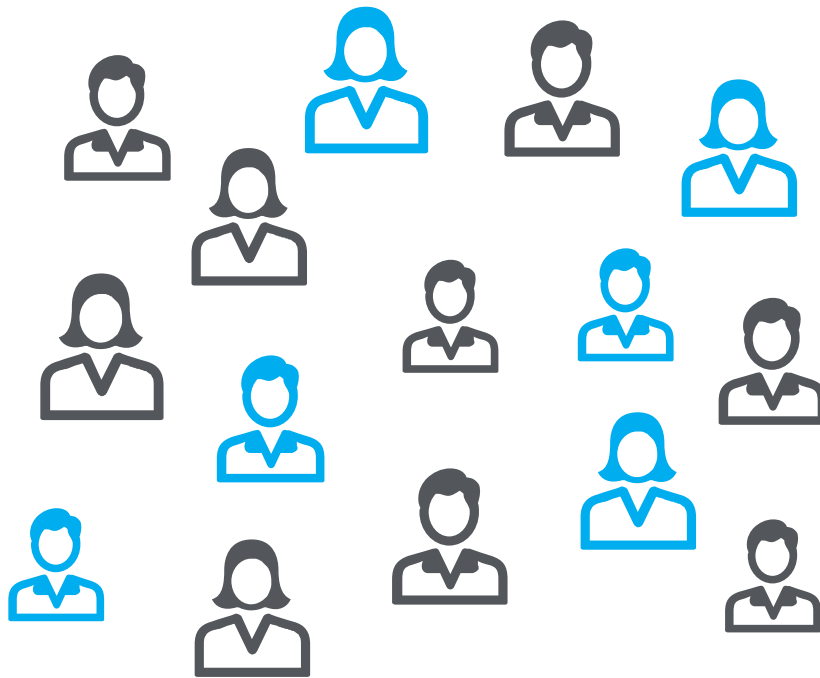
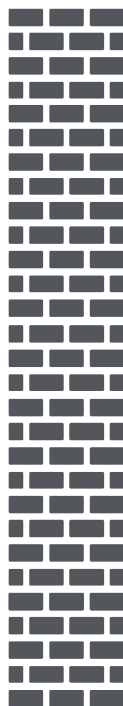
Niebezpieczne strony
Internetowe

Niebezpieczne pliki
pobierane z Internetu

Niebezpieczne pliki
przenoszone za pomocą
pamięci przenośnych

Niebezpieczne
oprogramowanie

Wiadomości email

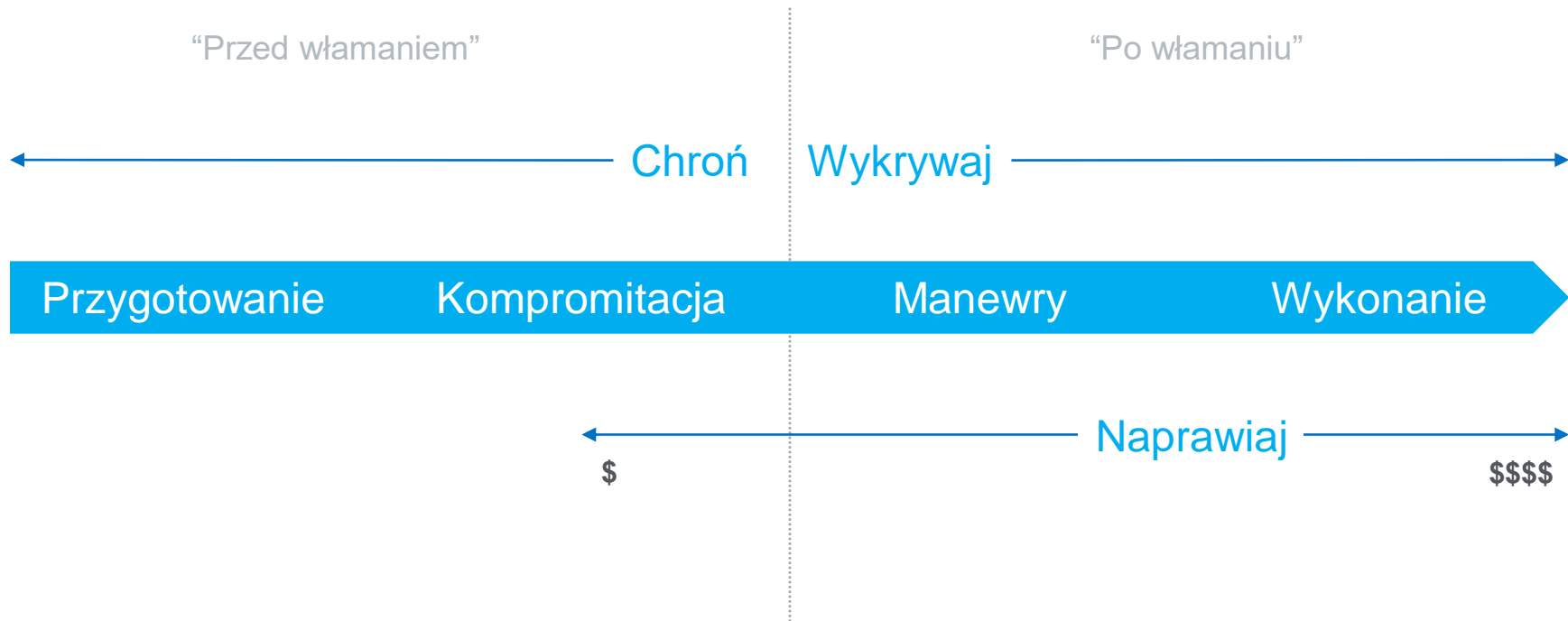


Ciemne charaktery są już w Twojej sieci



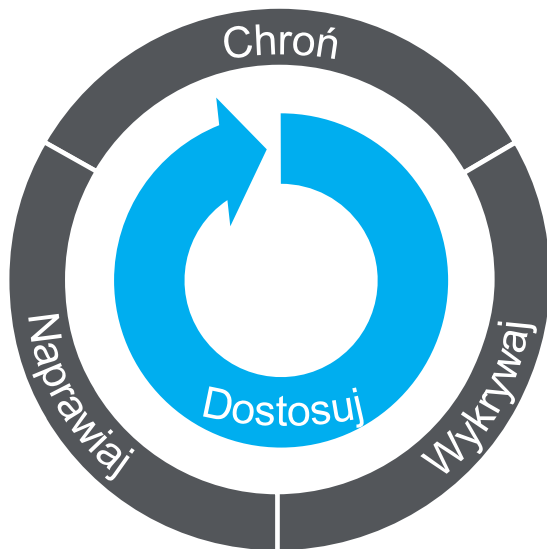
OCHRONA nie jest już wystarczająca. Należy skupić się również na **WYKRYWANIU** oraz **NAPRAWIANIU SZKÓD**

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.

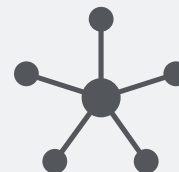
Chroń



Aktywna ochrona
przed zagrożeniami



Wiedza:
globalna, organizacji
oraz firm trzecich.



Współpracująca
infrastruktura działa
jako jeden
adaptacyjny system.

Wszechstronna ochrona

Siła wiedzy



Zagrożenia

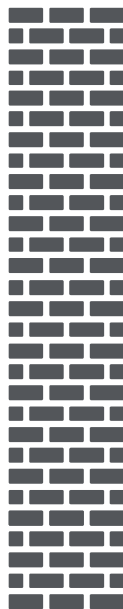
Niebezpieczne strony
Internetowe

Niebezpieczne pliki
pobierane z Internetu

Niebezpieczne pliki
przenoszone za pomocą
pamięci przenośnych

Niebezpieczne
oprogramowanie

Wiadomości email



Odpowiednie
technologie

Ochrona dostępu do Internetu
Ochrona sieci wewnętrznej
Ochrona komputerów
Ochrona informacji/danych

Wiedza o
zagrożeniach

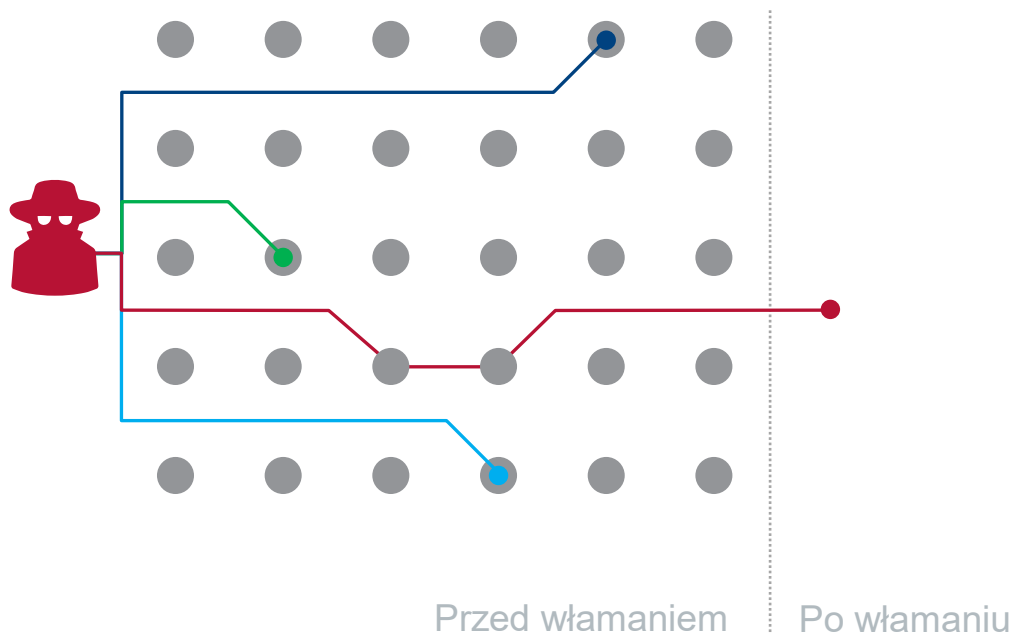
Globalne źródła reputacji
Wiedza administratorów

Otwarta na
firmy trzecie

Współpraca i
partnerstwa

Tradycyjna wyspowa struktura bezpieczeństwa

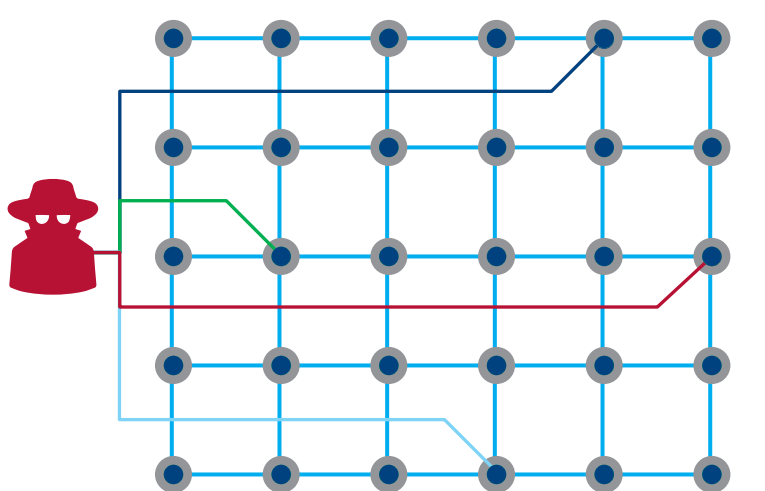
Gromada samodzielnych żołnierzy: adaptacja manualna lub brak



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

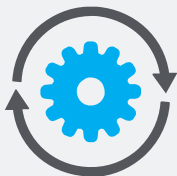


Przed włamaniem

Po włamaniu

Dostarcza wglądu w sytuację poprzez współpracującą infrastrukturę.

Wykrywaj



Głębokie, ciągłe i automatyczne monitorowanie.



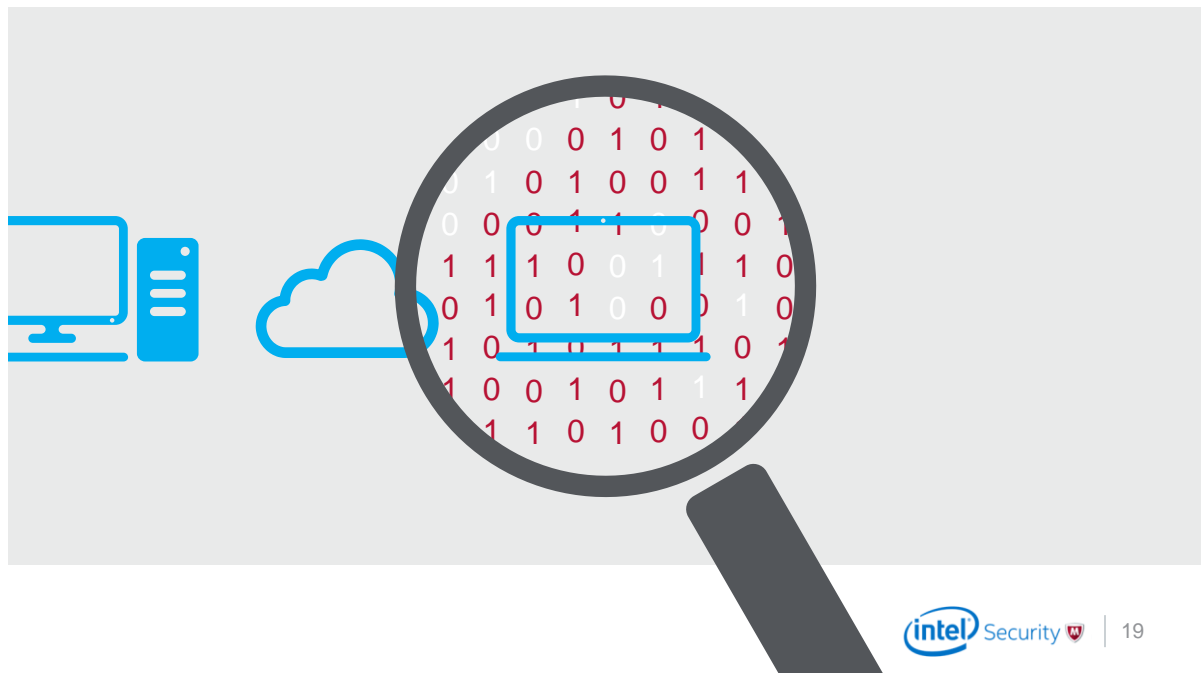
Odchylenia i korelacja oparta o reguły by wychwycić nawet pozornie mało istotne sygnały.



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.



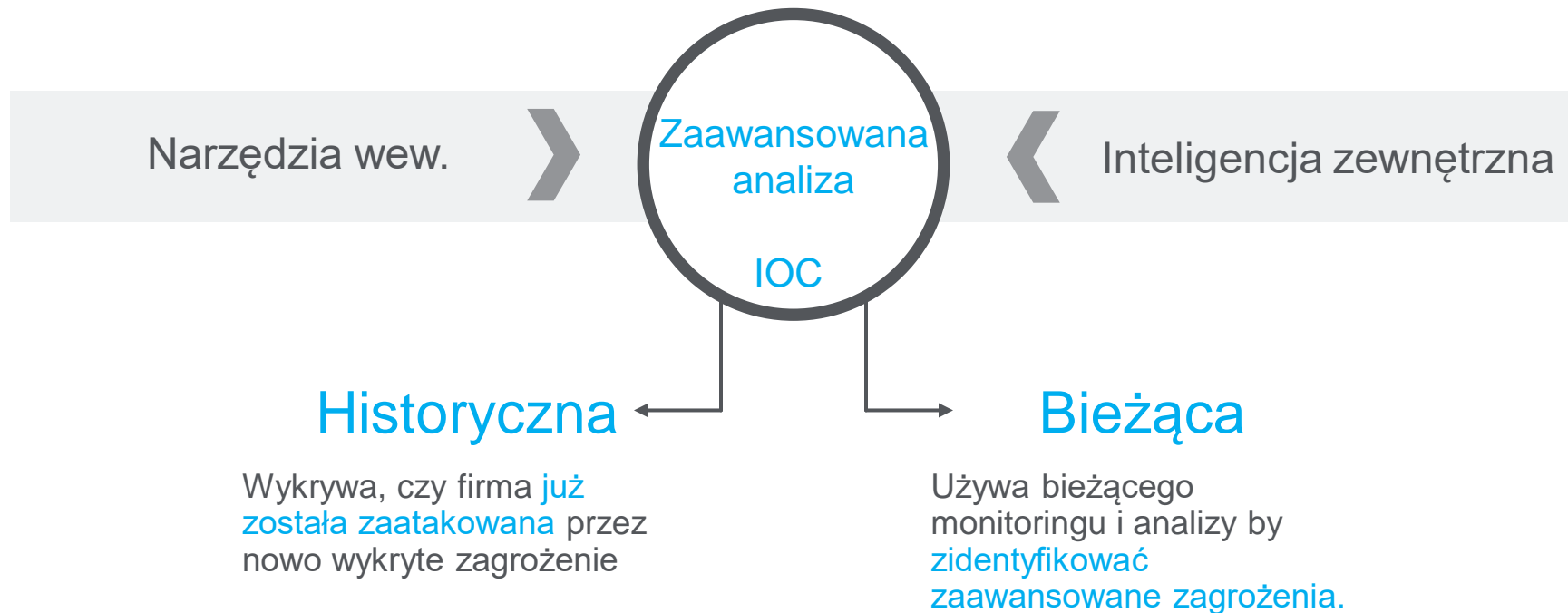
Analityka odchyleń i korelacji.

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.



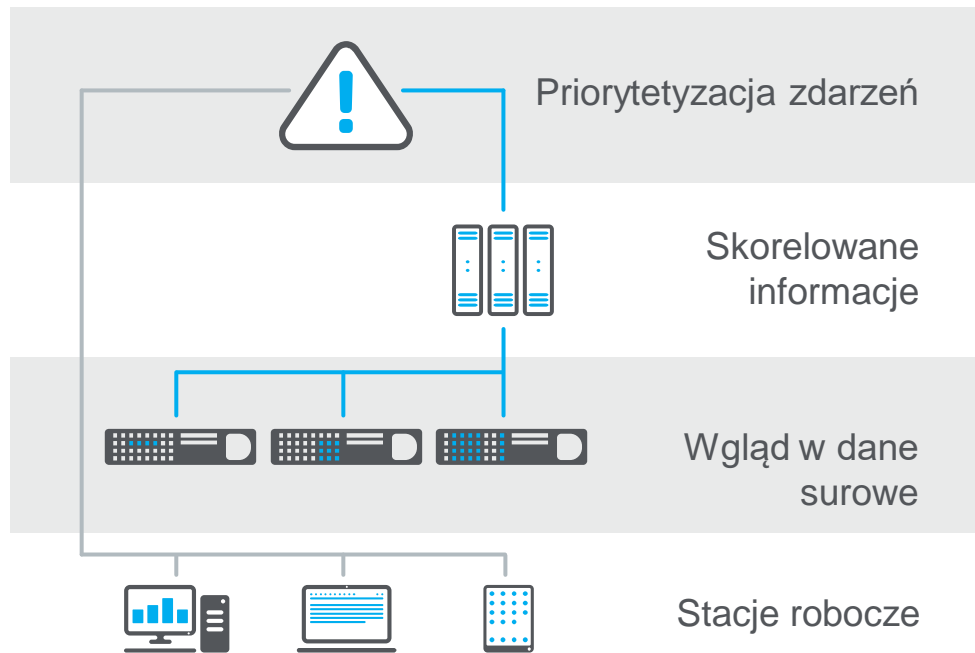
Płynne śledztwo z zaawansowanymi widokami, drażeniem danych oraz rzeczywistym wykrywaniem i odpowiedzią.



Automatyczna i rzeczywista odpowiedź w reakcji na incydenty bez przestoju 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

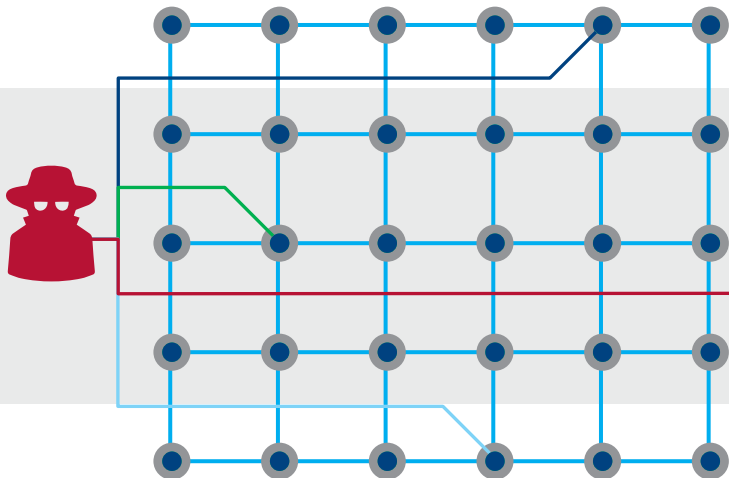
Report

Deploy

Chroń, Wykrywaj, Naprawiaj, Dostosuj

Chroń

Współpracująca architektura wykrywa bieżące zagrożenia.



Przed włamaniem

Po włamaniu

Wykrywaj

Stały wgląd w sytuację wykrywa historyczne i bieżące zagrożenia.



Naprawiaj

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



Adapt

Security Connected – Kompresja czasu odpowiedzi

