#Security

Cyberzagrożenia w działalności ubezpieczeniowej

Warszawa, 09.2018
Obszar Ryzyka i Bezpieczeństwa IT

POPEŁNIANIE PRZESTĘPSTWA UBEZPIECZENIOWEGO

np. zmiana konta uposażonego

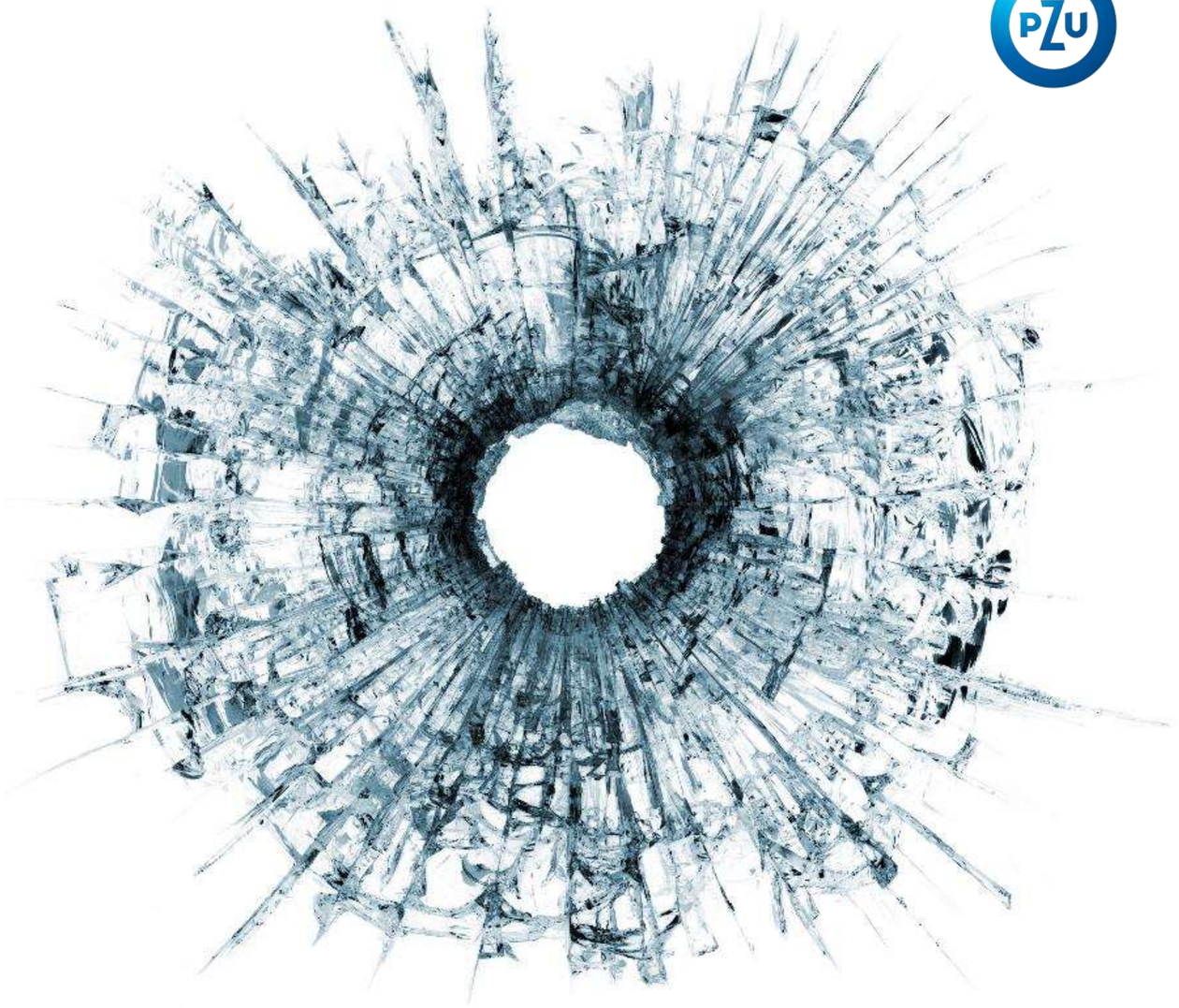
UKRYCIE PRZESTĘPSTWA UBEZPIECZENIOWEGO

np. modyfikacja danych dot. szkody

PRZESTĘPSTWO PRZECIWKO PRYWATNOŚCI

np. kradzież informacji

INNE



DANE

- dane osobowe
- dane o ubezpieczeniach
- dane o szkodach
- dane medyczne
- dane finansowe

SYSTEMY

- Systemy – krwioobieg
- Ingerencja w celu dokonania przestępstwa
- Ingerencja w celu ukrycia przestępstwa

INFORMACJA

- Szpiegostwo gospodarcze
  - Wyniki finansowe
  - Strategia
  - Plany
  - Kontrakty

To przygotowani przestępcy, którzy *nie są „samotnymi wilkami”.*

Dysponują pokaźnymi funduszami

Zatrudniają wysoko wykwalifikowanych specjalistów

Korzystają z zaawansowanych narzędzi hackerskich

Sprzedają swoje usługi i narzędzia *(CaaS – Crime as a Service)*

70-80% to:

- **Przestępczość zorganizowana**
- **Organizacje, w tym terrorystyczne**
- **Państwa**
  - **USA – NSA**
  - **Chiny – armia**
  - **Korea Pn**
  - **Rosja – armia + Kaspersky ;-)**
  - **inni…**

Phishing e-mail lub www

- Przesyłanie wiadomości, które rzekomo pochodzą z godnych zaufania źródeł np. banków
- Fałszywe witryny www, które wyglądem przypominają witryny znanych firm

Wyciek danych

- Główne przyczyny to słabe hasła, klikanie w przypadkowe załączniki do e-mail-i jak również wysyłanie poufnych plików służbowych na prywatne skrzynki e-mail

Zagrożenie platformy Android

- Wzrost ilości szkodliwego oprogramowania dedykowanego do oszustw w bankowości internetowej

Ataki APT (Advanced Persistent Threats)

- Wieloetapowe, bardzo zaawansowane
- Ataki ukierunkowane na konkretne organizacje lub osoby, posiadają charakter cyberszpiegostwa

Akcje cyberszpiegowskie na tle politycznym

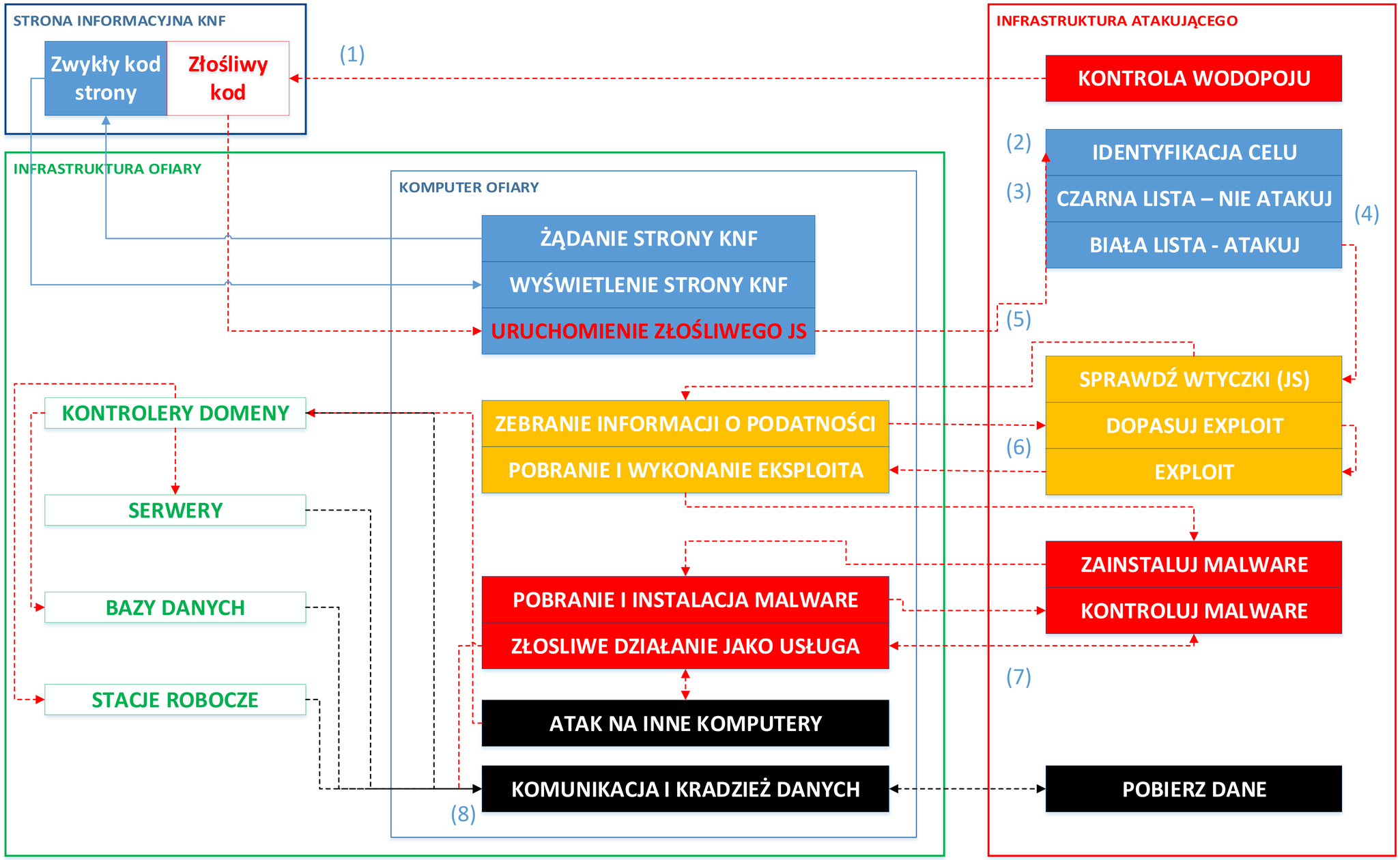
- Możliwość sparaliżowania funkcjonowania instytucji rządowych, mediów czy instytucji finansowych

Ransomware

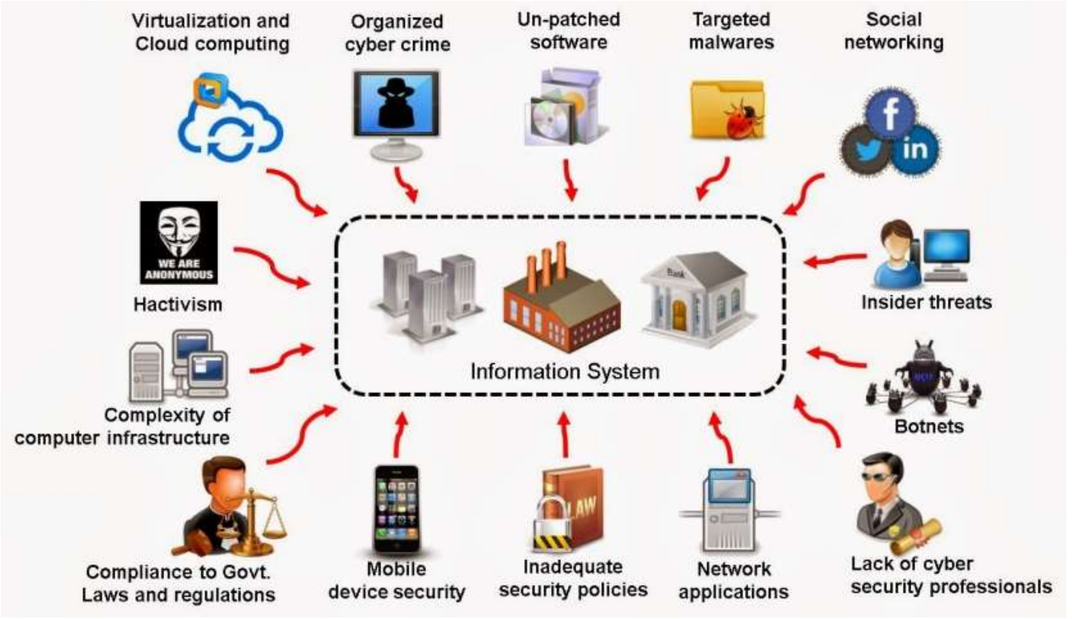
- Ogranicza dostęp do zasobów poprzez szyfrowanie i wymaga zapłacenia okupu, aby ograniczenie zostało usunięte

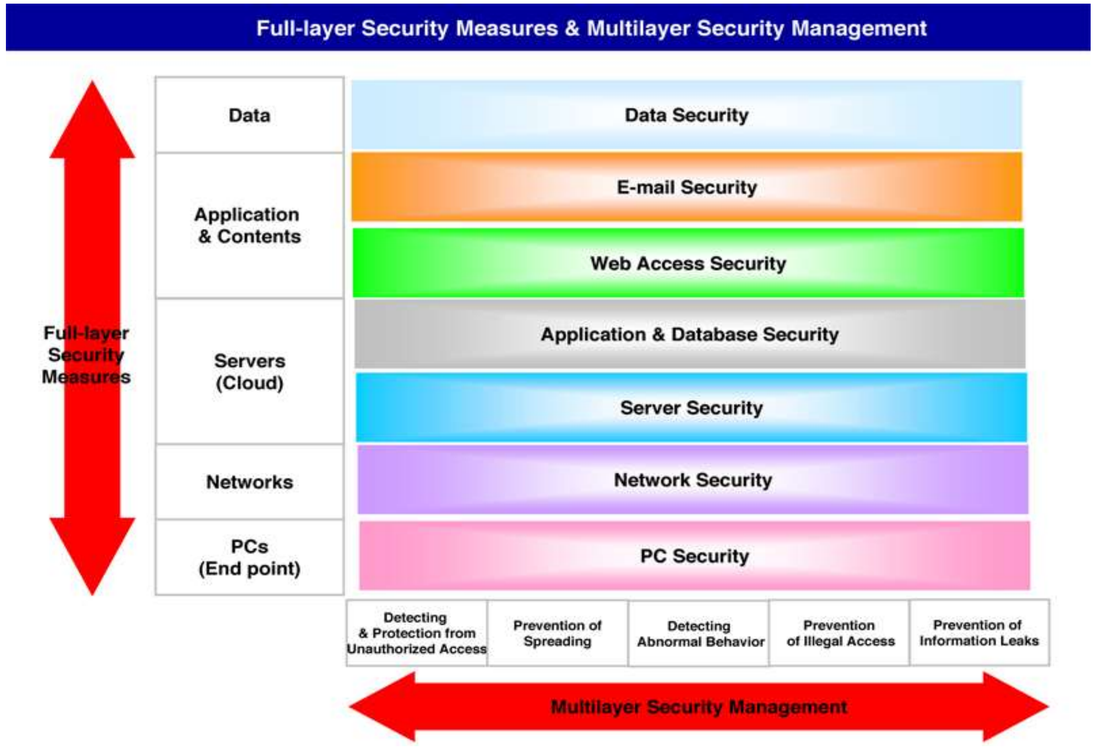
DoS (Denail of service) DDoS (Distributed Denail of service)

- Atak na infrastrukturę informatyczną lub sieć w celu uniemożliwienia jego działania


STRONA INFORMACYJNA KNF
Zwykły kod strony
Złośliwy kod
(1)
INFRASTRUKTURA ATAKUJĄCEGO
KONTROLA WODOPOJU
(2)
IDENTYFIKACJA CELU
(3)
CZARNA LISTA – NIE ATAKUJ
BIAŁA LISTA - ATAKUJ
(4)
INFRASTRUKTURA OFIARY
KOMPUTER OFIARY
ŻĄDANIE STRONY KNF
WYŚWIETLENIE STRONY KNF
URUCHOMIENIE ZŁOŚLIWEGO JS
(5)
SPRAWDŹ WTYCZKI (JS)
DOPASUJ EXPLOIT
EXPLOIT
(6)
KONTROLERY DOMENY
SERWERY
BAZY DANYCH
STACJE ROBOCZE
ZEBRANIE INFORMACJI O PODATNOŚCI
POBRANIE I WYKONANIE EKSPLOITA
ZAINSTALUJ MALWARE
KONTROLUJ MALWARE
POBRANIE I INSTALACJA MALWARE
ZŁOSLIWE DZIAŁANIE JAKO USŁUGA
(7)
ATAK NA INNE KOMPUTERY
KOMUNIKACJA I KRADZIEŻ DANYCH
POBIERZ DANE
(8)

Wiele potencjalnych wektorów ataku





Obrona musi być wielowarstwowa, umieszczona w wielu punktach

SIEM

SIEĆ

- Firewall
- Systemy IPS/IDS

SERWERY

- Firewalle aplikacyjne (WAF)
- Database firewall (DAM/DAF)
- Oprogramowanie do inspekcji kodu
- PIM

LUDZIE

- Systemy AV i AM
- Personal firewall
- Antyspam
- Antymalwere pocztowy
- Sandbox
- Webgateway

WYCIEK

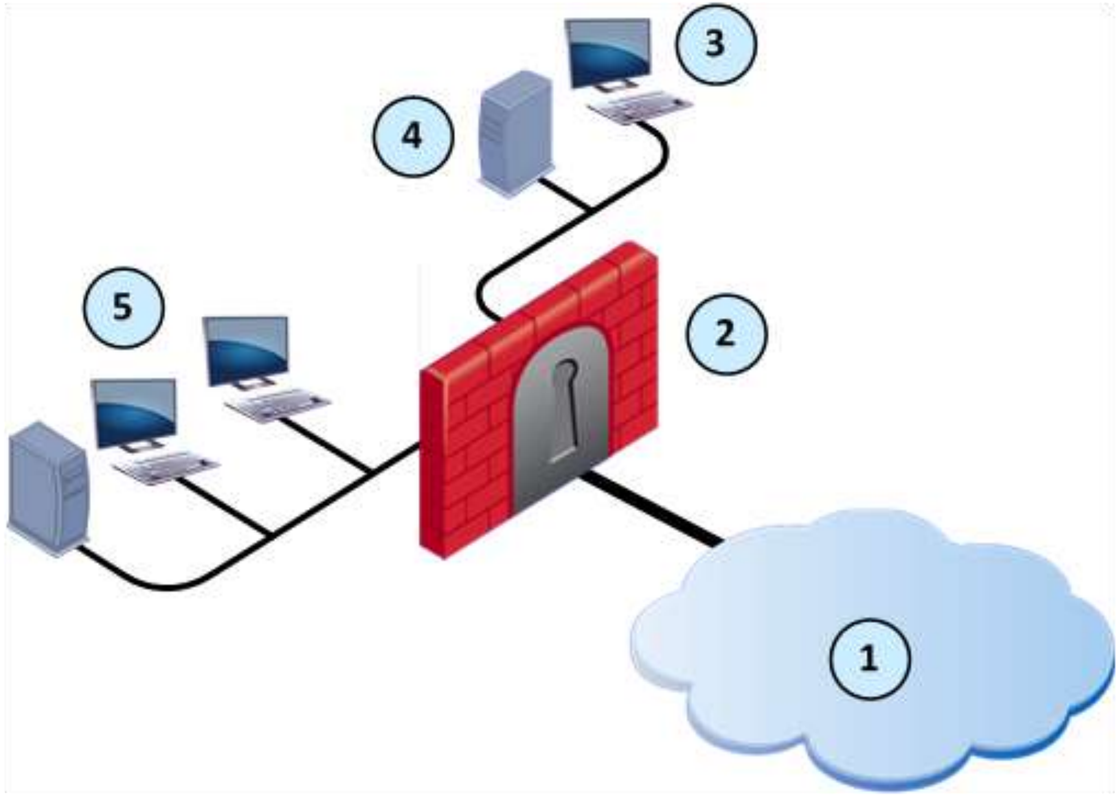
- DLP

Firewall (zapora sieciowa)

- Ochrona sieci wewnętrznej LAN przed dostępem z zewnątrz, tzn. sieci publicznych, Internetu,

- Ochrona przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz.

- Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.

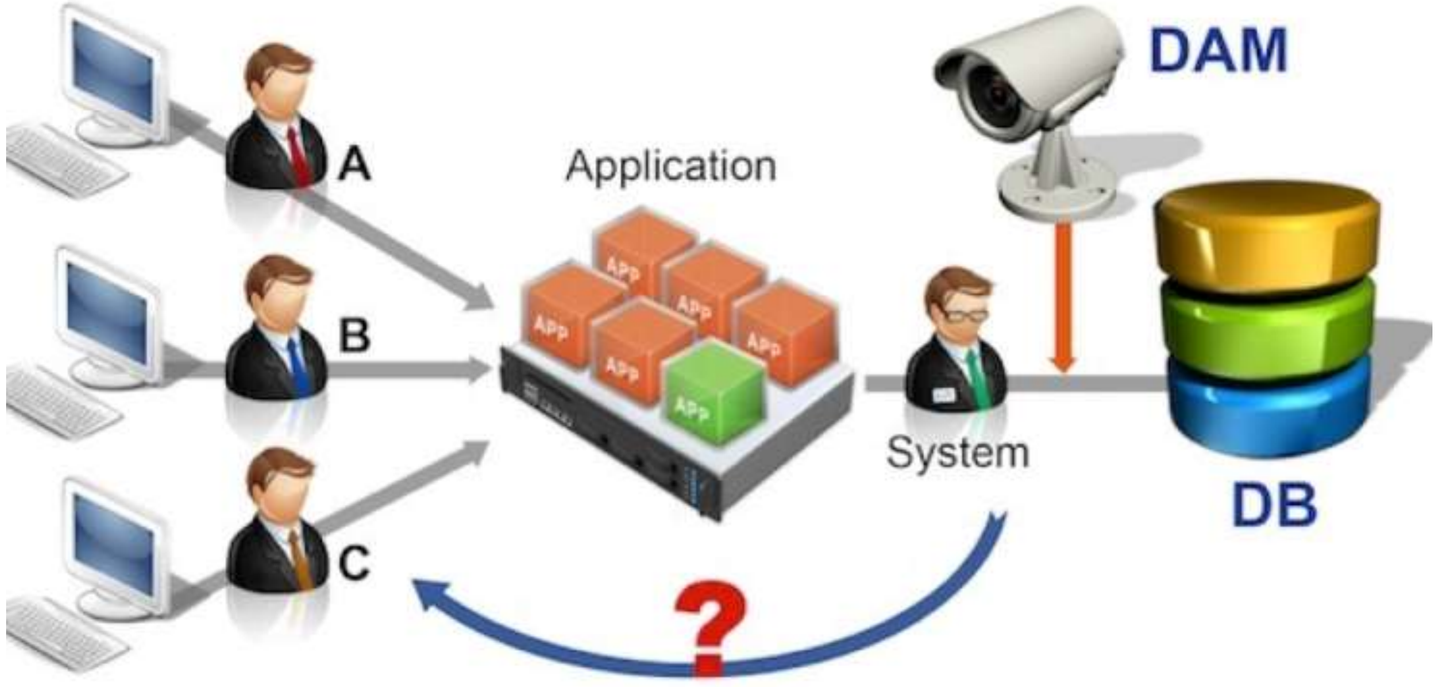


WAF (Web Application Firewall)

- Analizuje i filtruje zawartość ruchu
- Ochrona aplikacji WWW
- Ochrona przed zaawansowanymi atakami na poziomie logiki aplikacji

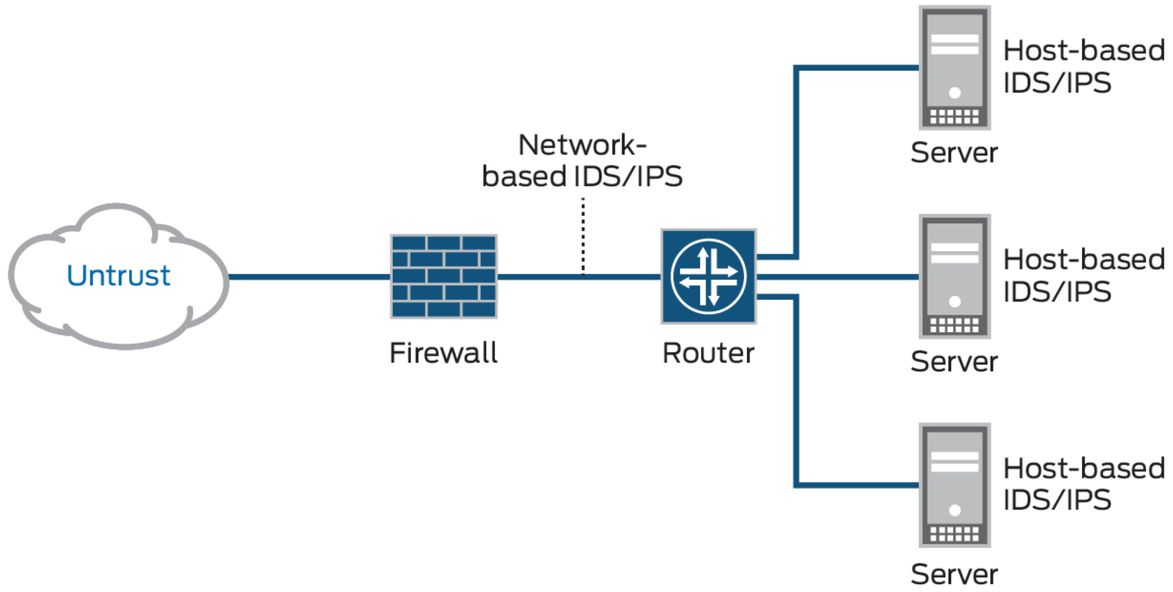
DAM/DAF (Database Activity Monitor)

- Ochrona ruchu do bazy danych
- Monitorowanie działań użytkowników uprzywilejowanych
- Monitorowanie działań aplikacji
- Ochrona przed atakami na bazy, przed nieautoryzowanym dostępem do danych



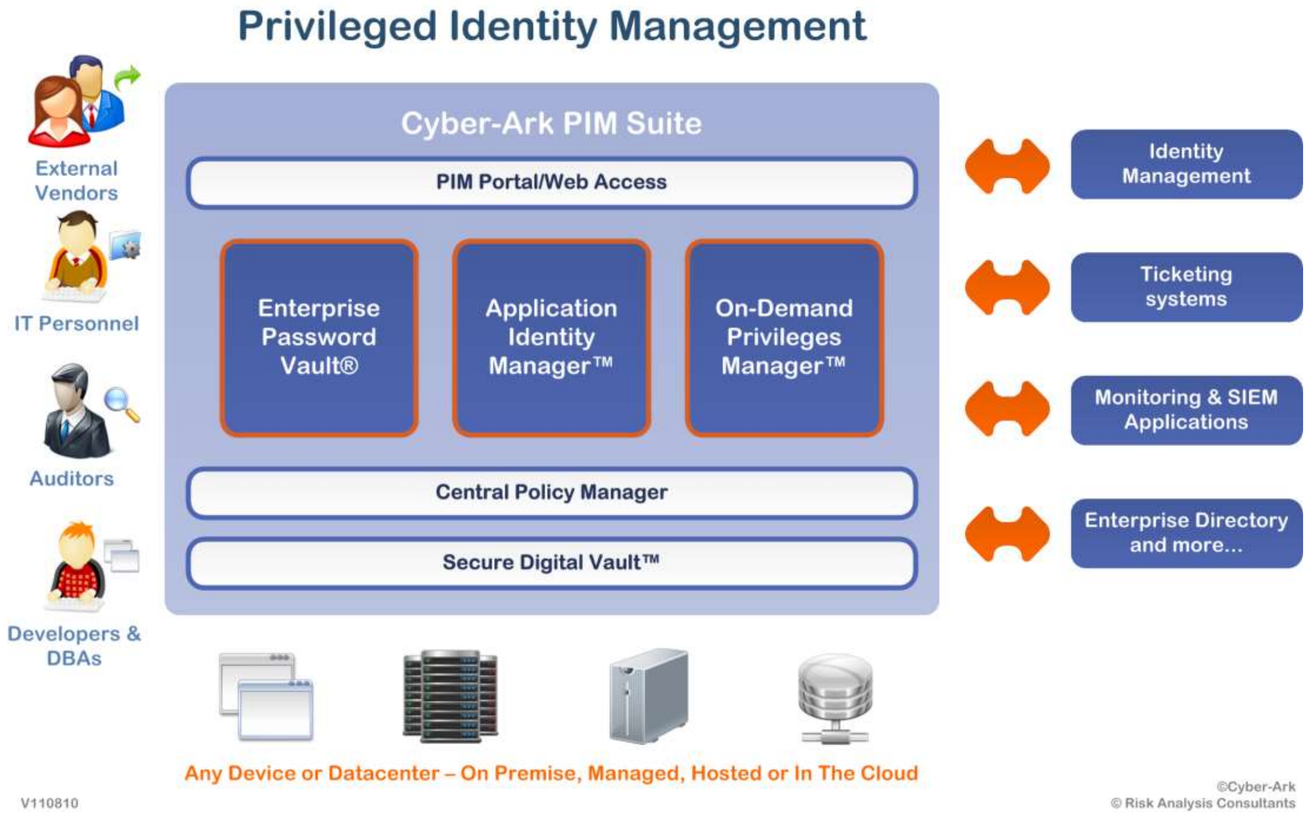
IDS/IPS (Intrusion Detection System/Intrusion Prevention System)

- Ochrona ruchu w sieci
- Wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym
- Anomalie i sygnatury



PIM (Privileged Identity Management)

- Zarządzanie tożsamością uprzywilejowaną
- Zarządzanie prawami dostępu do zasobów
- SSO
- Nagrywanie działań użytkowników (uprzywilejowanych, zewnętrznych itp.)



Systemy antywirusowe i antymalware

- Malware (złośliwe oprogramowanie) - wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze, groźne lub destrukcyjne działanie w stosunku do użytkownika komputera
- Systemy wykrywania i likwidacji malware
- Na komputerach użytkowników, serwerach, w sieci komputerowej

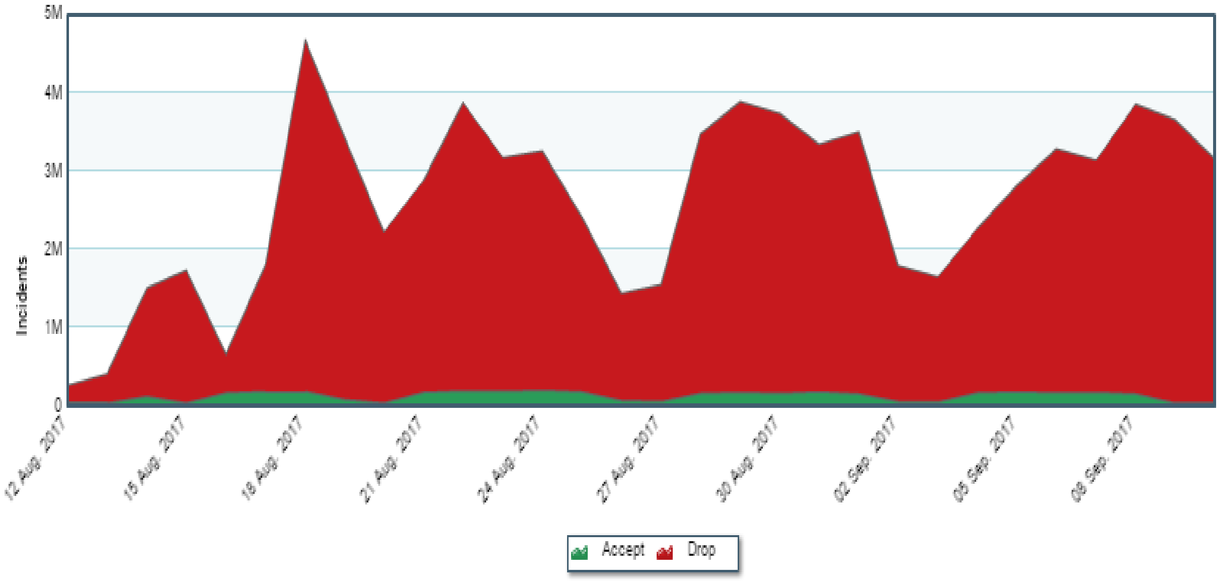
Symantec

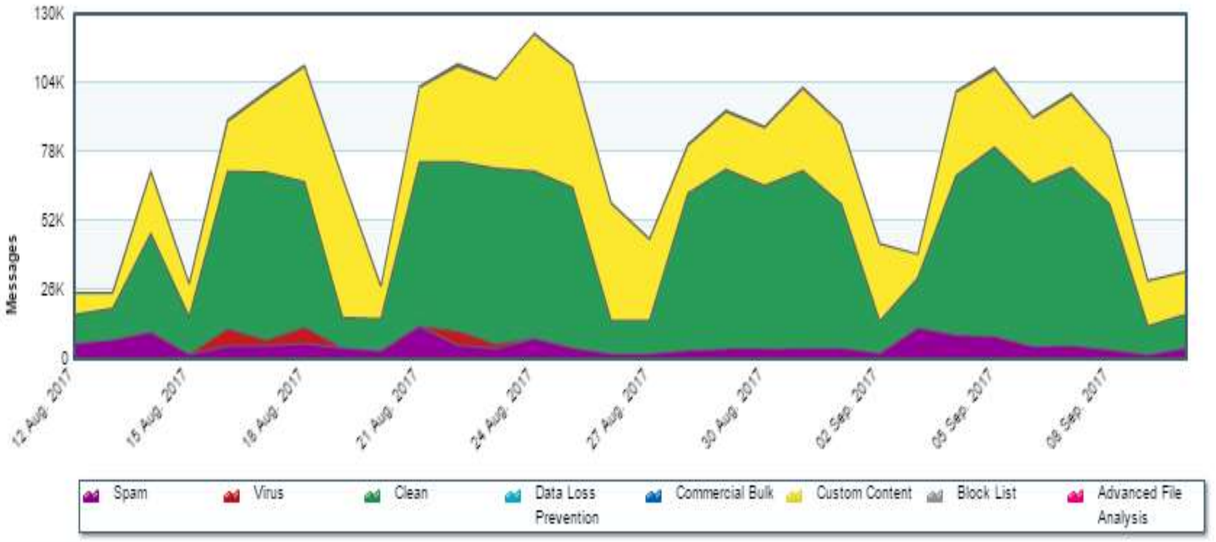
KASPERSKY lab

Malwarebytes ANTI-MALWARE

Antyspam/antymalware (system antyspamowy)

- Spam - niechciane lub niepotrzebne wiadomości elektroniczne
- Często pierwszy krok w ataku na firmę
- Większość poczty wpływającej do ZU to SPAM!!!
- Ochrona przed niechcianą lub szkodliwą pocztą



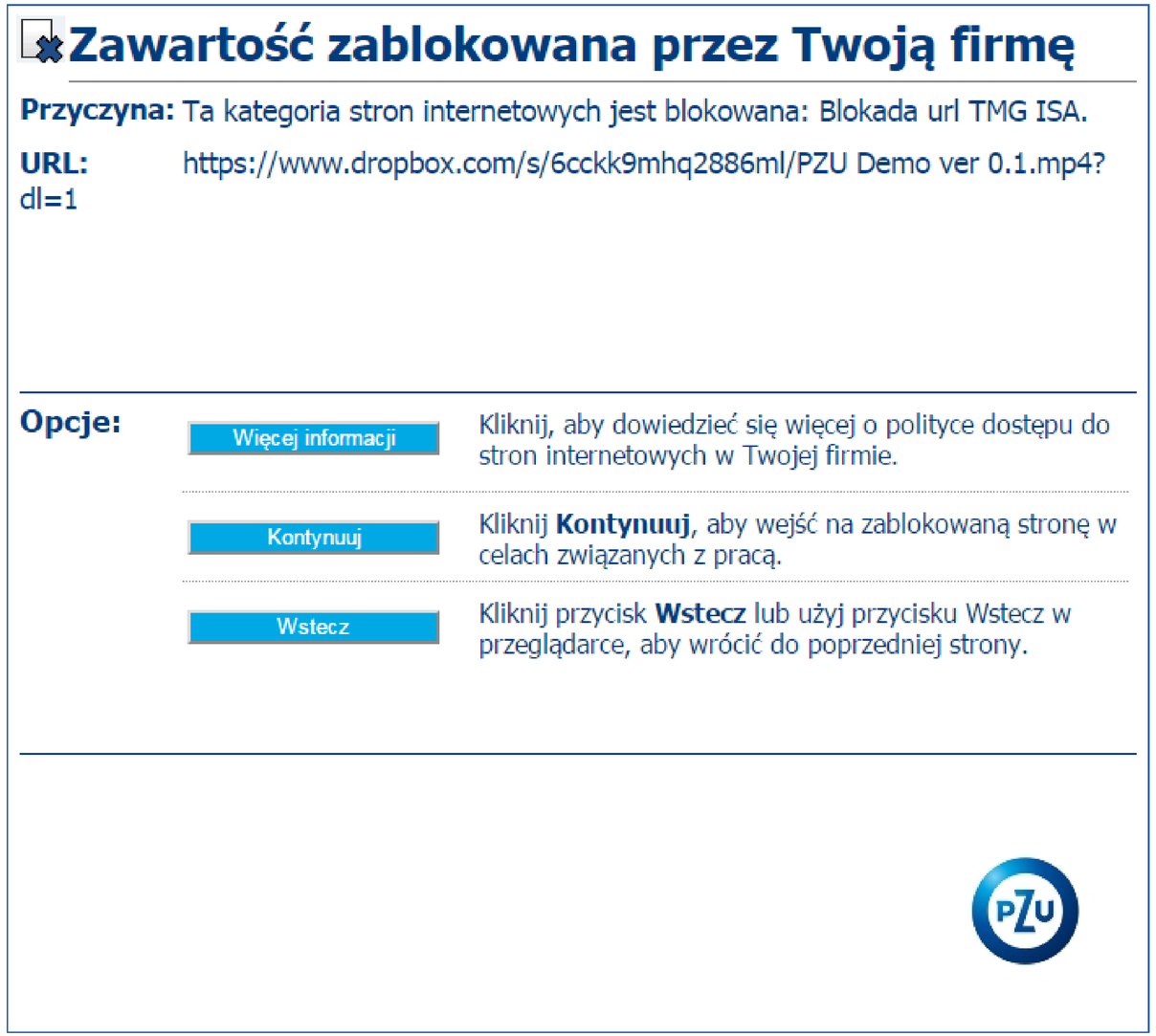


Sandbox (Piaskownica)

- Wydzielona, dedykowana część systemu informatycznego przeznaczona, ze względów bezpieczeństwa, do uruchamiania programów, które są nieprzetestowane lub niezaufane lub pochodzą od niezaufanych stron trzecich.
- Jeśli zawiodły AV, AM, MG – masz jeszcze sandbox.

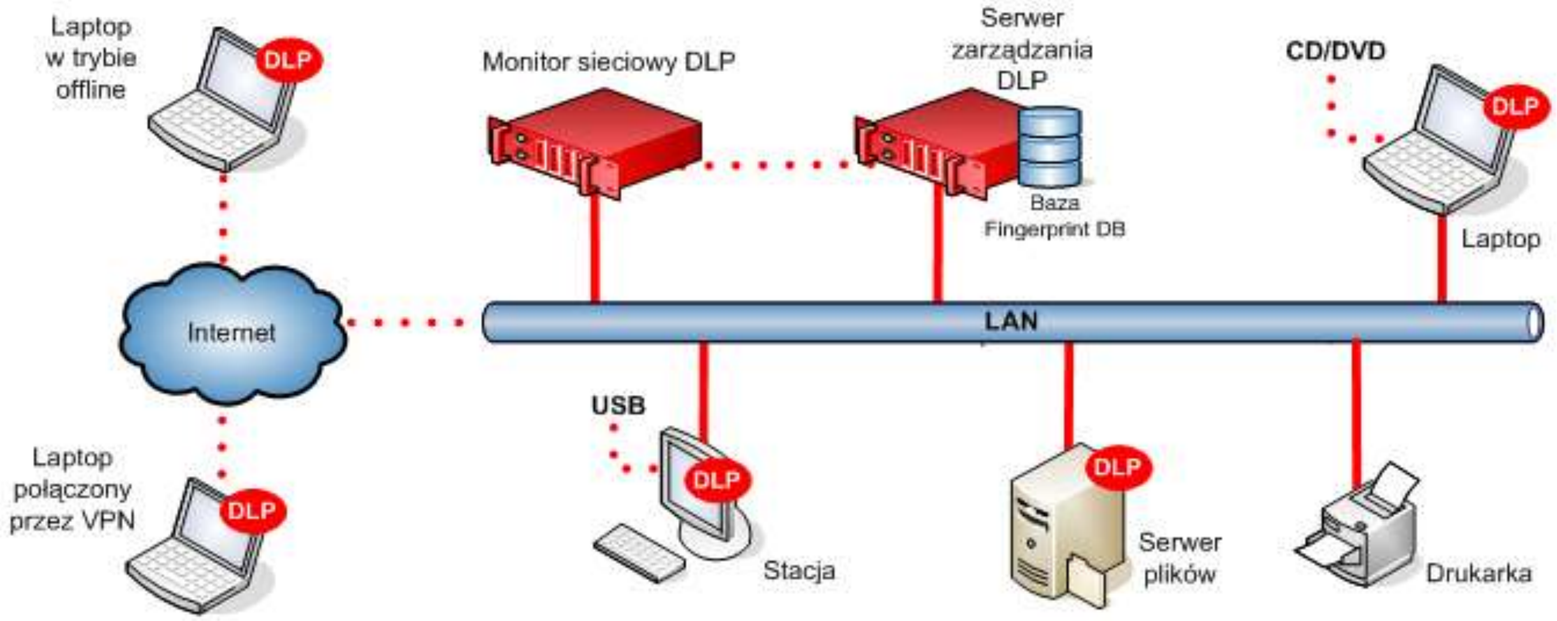
Webgateway

- Ochrona użytkowników przed infekcją z podejrzanych stron
- Filtrowanie dostępu do niebezpiecznych, niepożądanych stron WWW



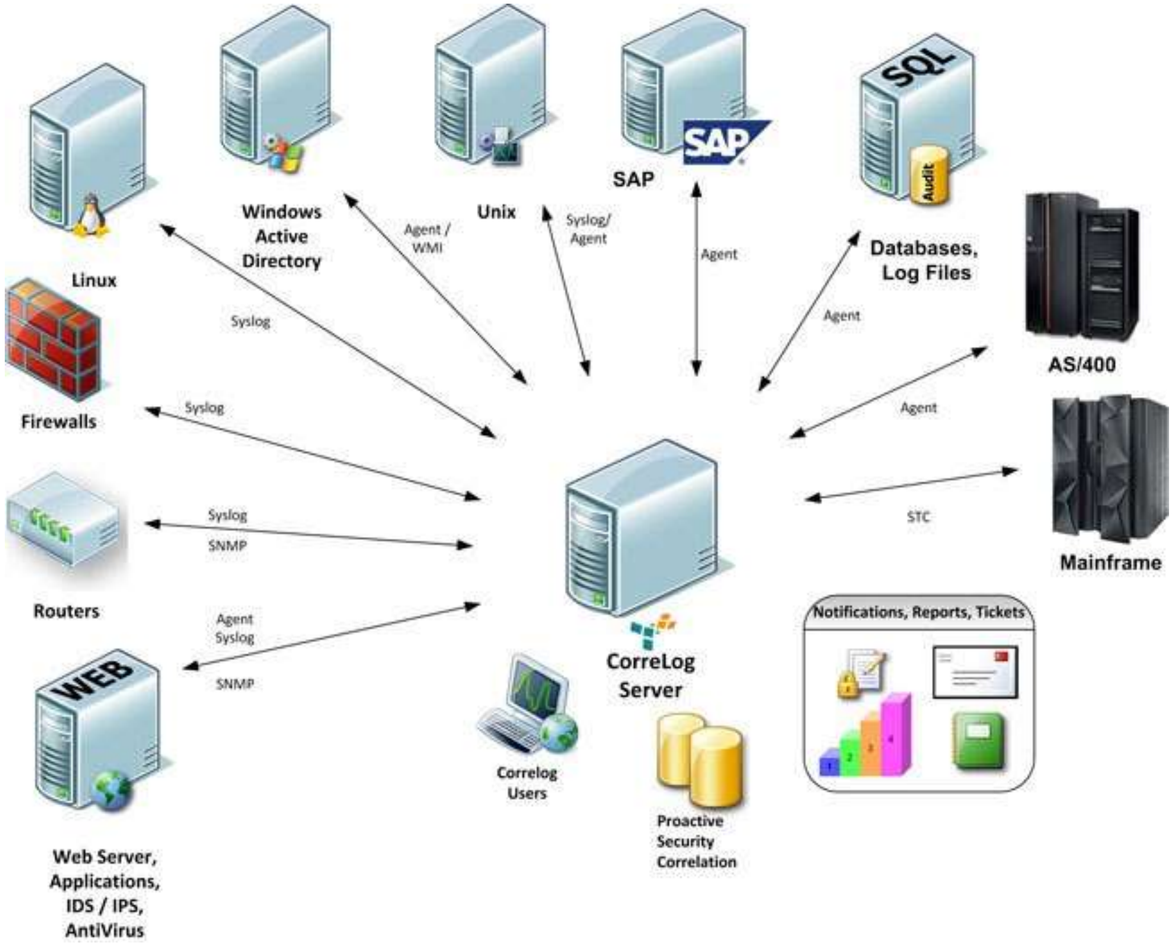
DLP (Data Loss Prevention)

- Ochrona przed utratą wrażliwych danych
- Zapobieganie przypadkowym i intencjonalnym wyciekom istotnych danych
- Ochrona na poziomie poczty, dysków USB, stron www



SIEM (Security Information and Event Management)

- System zarządzania informacją związaną z bezpieczeństwem i zdarzeniami
- Zbiera, analizuje, koreluje informacje z wielu źródeł
- Alarmuje w czasie rzeczywistym o próbach ataku
- Niezbędny w dużych firmach
- Bez tego nie wykryjemy APT



Pytania

Dziękujemy za uwagę