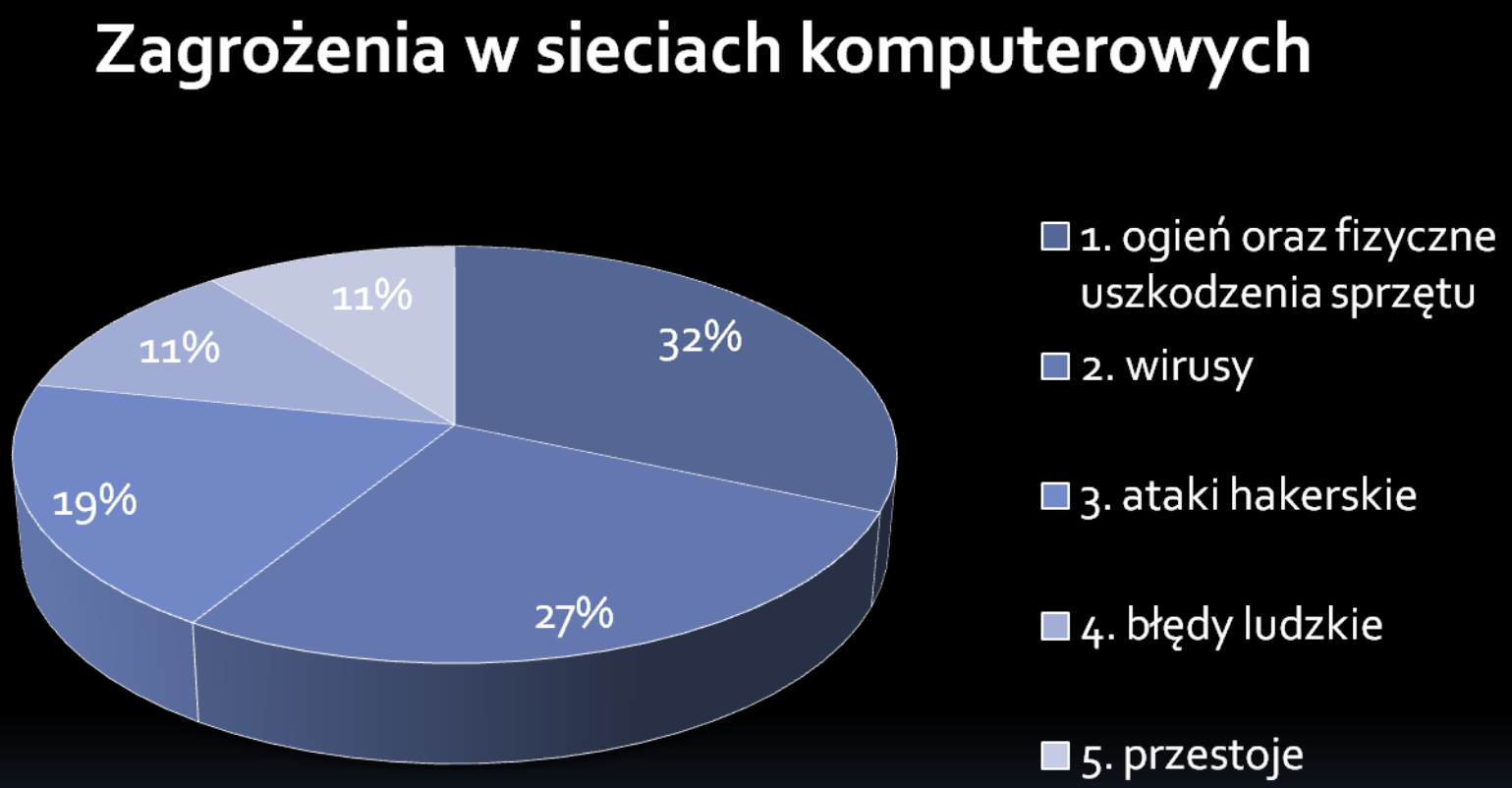
MODELOWANIE BEZPIECZEŃSTWA INFRASTRUKTURY IT NA BAZIE DOŚWIADCZEŃ Z WŁAMAŃ I WYKRYTYCH PODATNOŚCI

Prowadzący:
Specjalista do sp. Informatyki Śledczej
Maciej Wiśniewski

Tytułem wstępu:

- Podatności i zagrożenia w sieciach komputerowych, w kontekście realiów polskich,
- Ryzyko wycieku tajnych informacji,
- Fakty i mity o systemach IPS,
- Ochrona danych i zasobów IT.

Stan faktyczny bezpieczeństwa w polskich przedsiębiorstwach- 1/3



Stan faktyczny bezpieczeństwa w polskich przedsiębiorstwach- 2/3

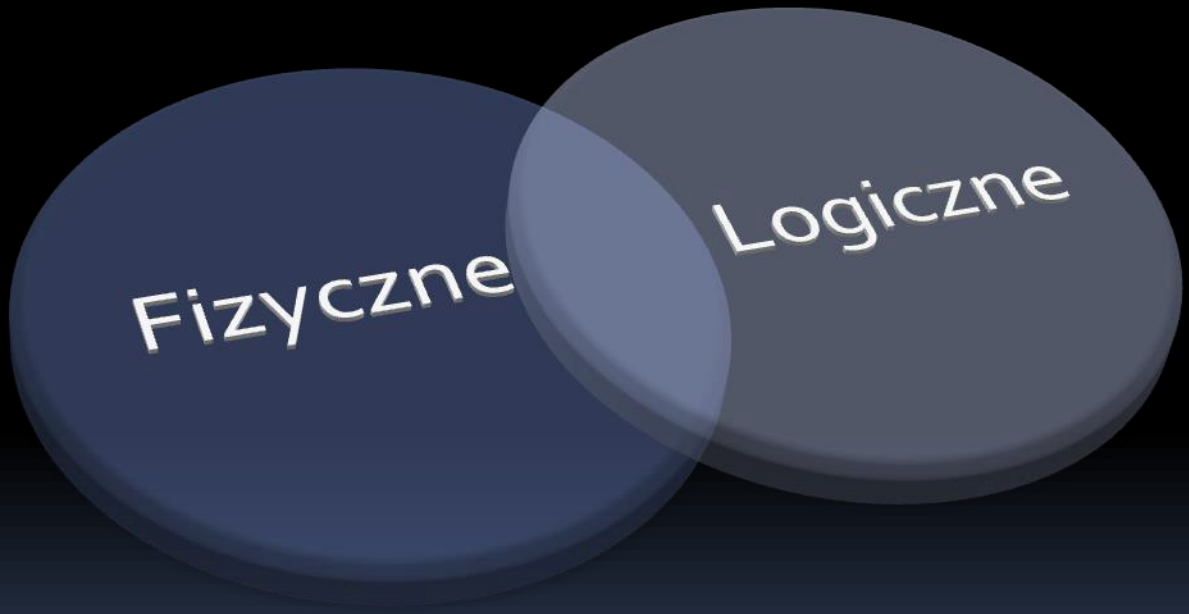
Według danych pochodzących z firmy analitycznej Forrester Research, firma która w ciągu 72 godzin nie zlikwiduje awarii systemu informatycznego, może liczyć się z odpływem nawet 22,5 proc. swoich klientów.

Stan faktyczny bezpieczeństwa w polskich przedsiębiorstwach- 3/3

Amat victoria curam.

Nie ma zwycięstwa bez troski, bez trudu (kosztów).

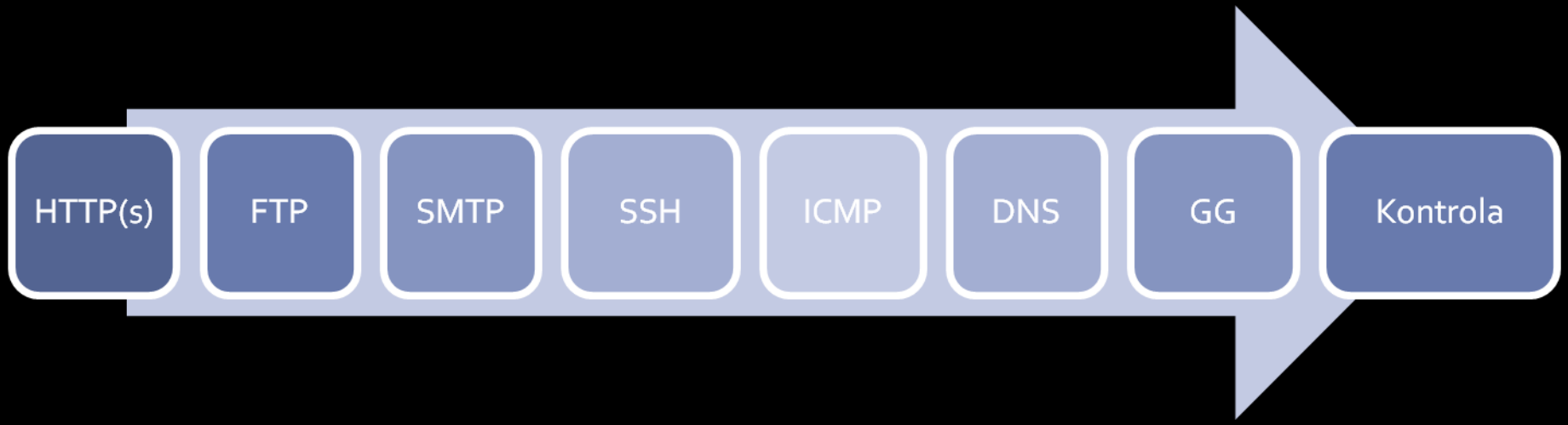
Typy wycieku informacji:



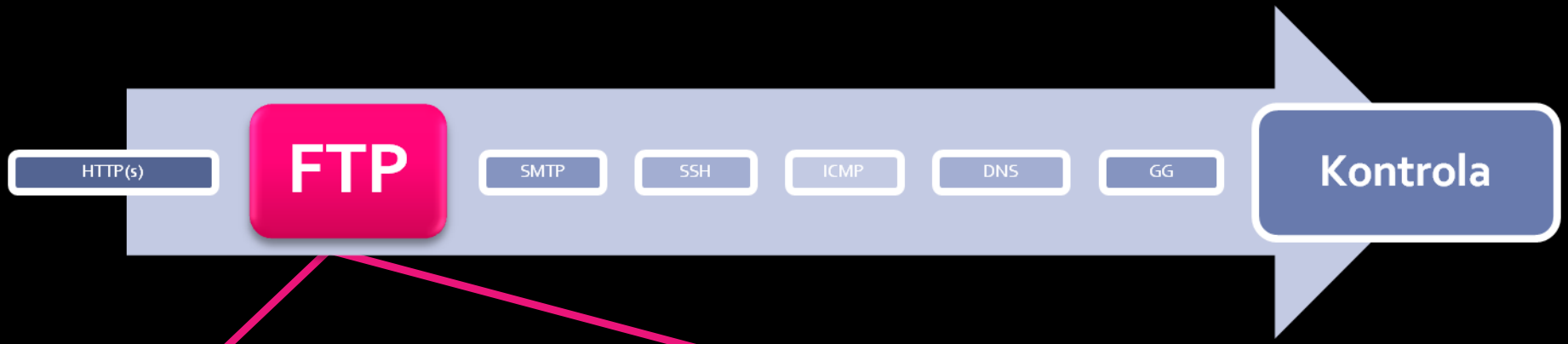
Logiczne typy wycieku informacji:

Ryzyko wycieku poufnych informacji - 3/10

Typy wycieku informacji:



Ryzyko wycieku poufnych informacji - 4/10



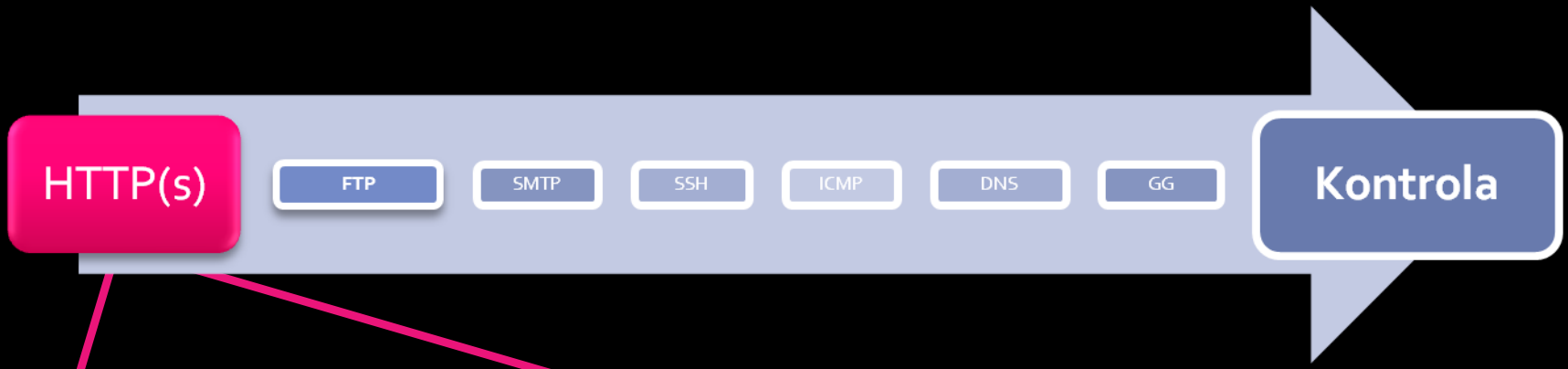
Określenie puli dostępnych adresów

Blokowanie wgrywania plików na serwer

==> PUT
==> STORE

FTP- PROXY

Ryzyko wycieku poufnych informacji - 5/10



Określenie puli dostępnych adresów

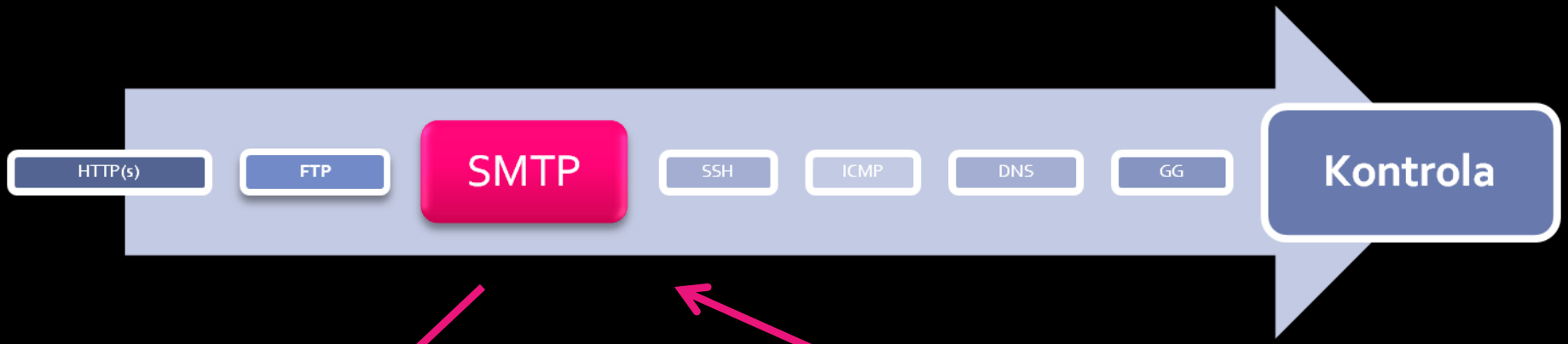
Np. www.youtube.com

Blokowanie kontentu

Np. „nasza klasa”

DANSGUARDIAN, SQUID (free) ; WATCH GUARD (comercial)

Ryzyko wycieku poufnych informacji - 6/10

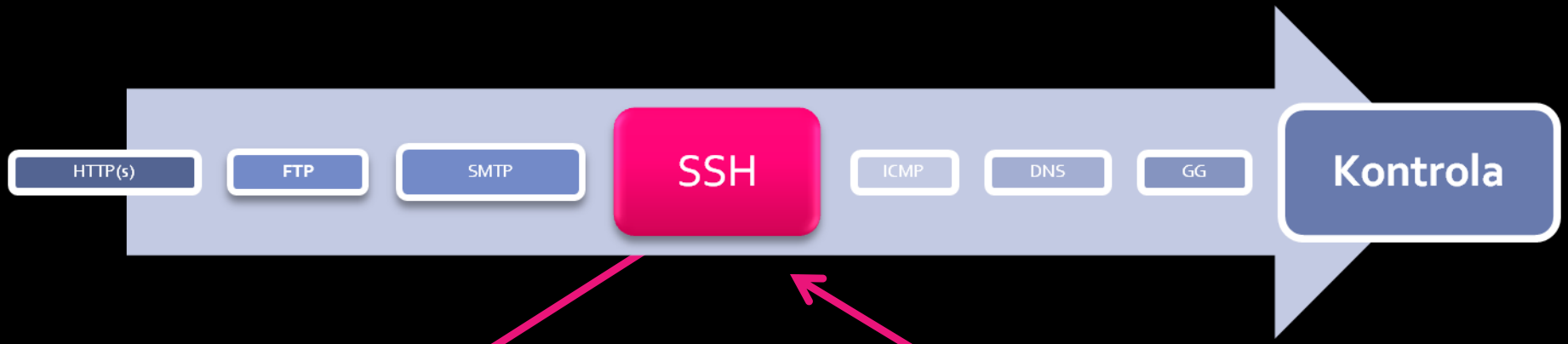


Określenie puli dostępnych serwerów SMTP

Określenie polityki bezpieczeństwa

Logowanie ruchu

Ryzyko wycieku poufnych informacji - 7/10

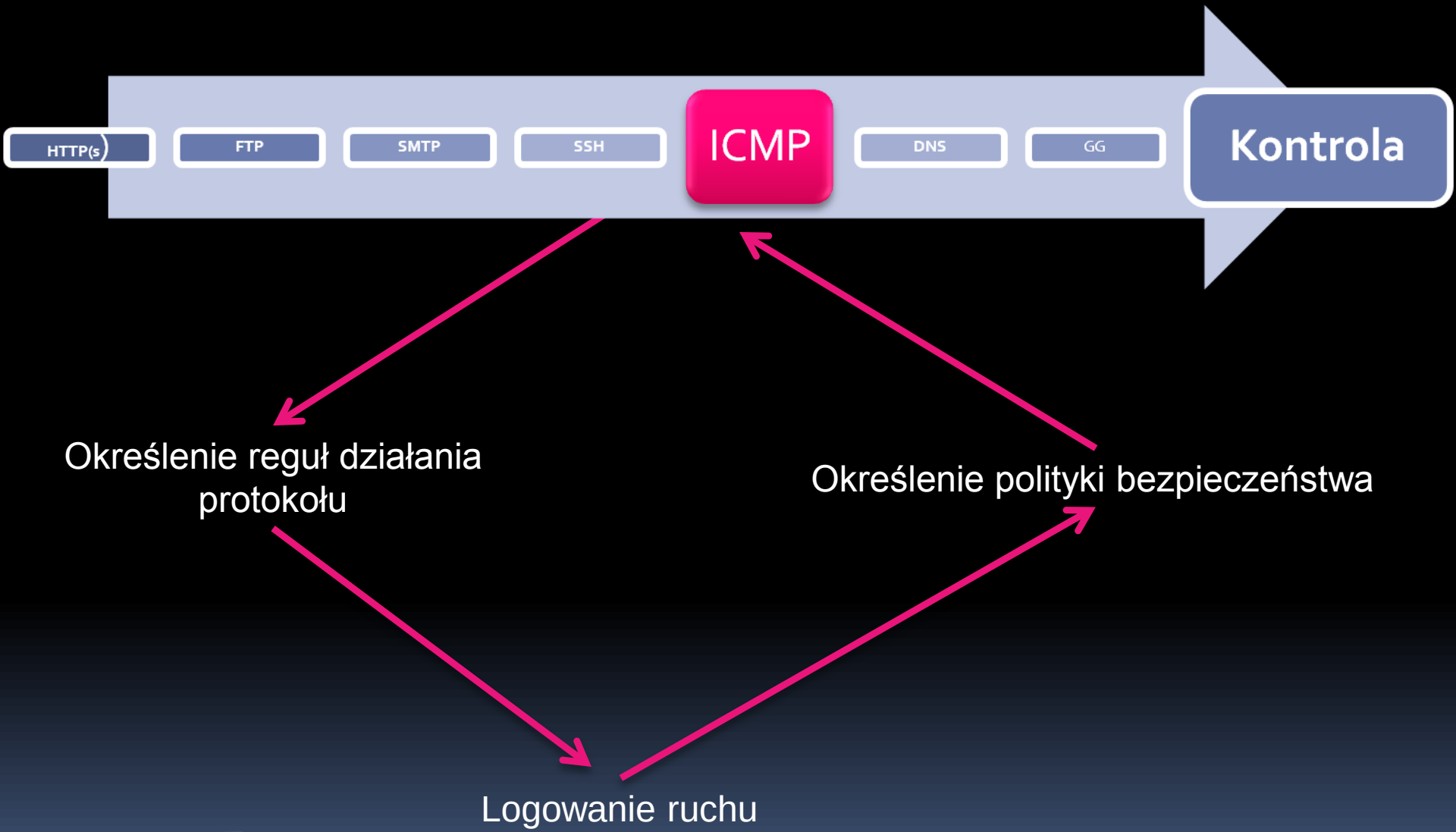


Blokada portu 22
Wykrywanie ruchu SSH

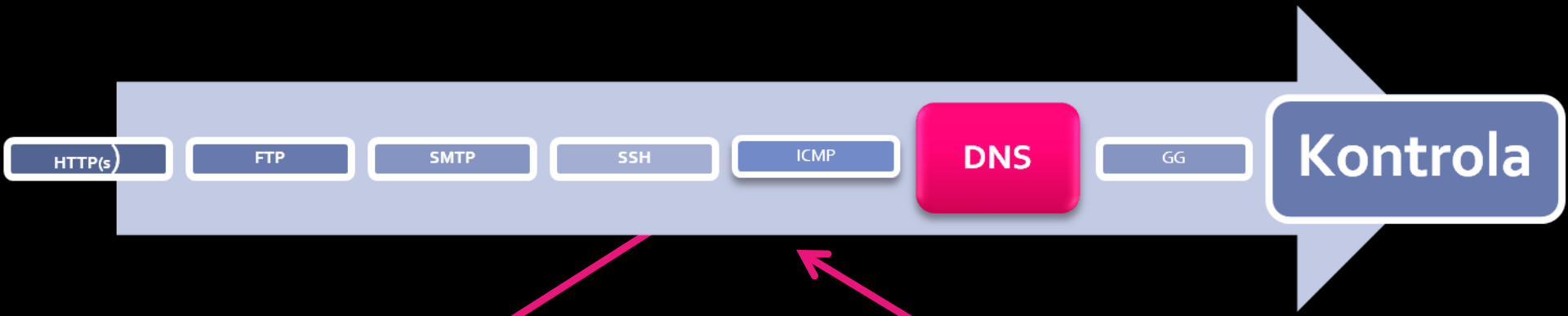
Określenie polityki bezpieczeństwa

Logowanie ruchu

Ryzyko wycieku poufnych informacji - 8/10



Ryzyko wycieku poufnych informacji - 9/10

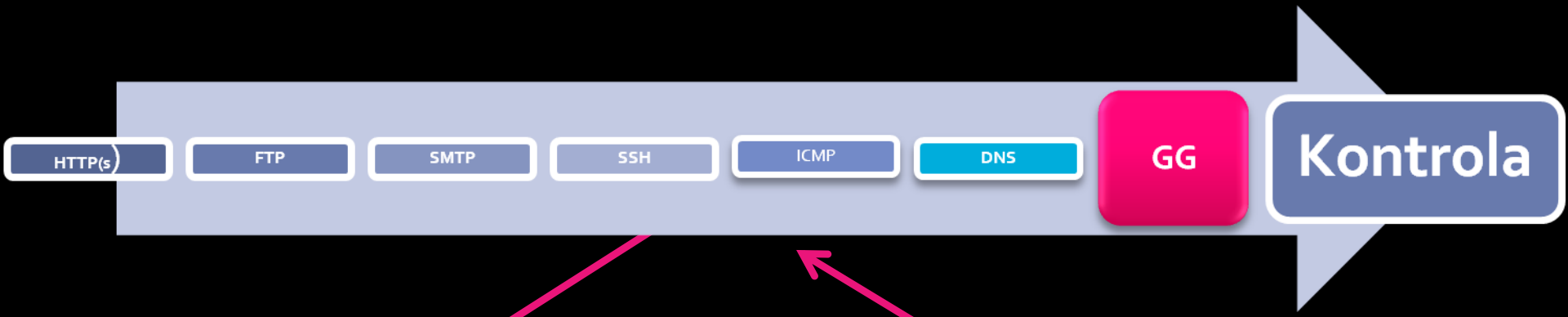


Zestawienie tunelu na porcie DNS 53 np. poprzez: iodine lub NSTX

Określenie polityki bezpieczeństwa

Monitorowanie DNS (np. DNS Proxy)

Ryzyko wycieku poufnych informacji - 10/10



Blokada portu (nie zawsze możliwa)

Blokada hostów np.:
http://www.kadu.net/monitor/

Określenie polityki bezpieczeństwa

„iptables -A OUTPUT -d 91.197.13.24 -j DROP”

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS/IDS - 1/6

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS/IDS - 1/6

Czym jest IPS/IDS ?

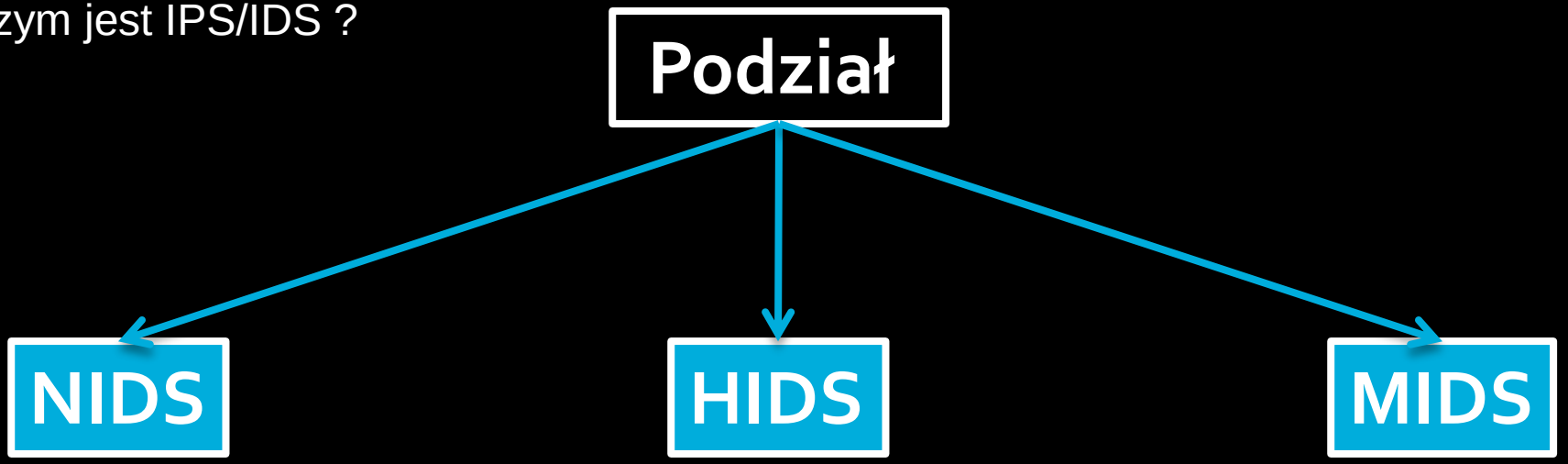
Fakty i mity o bezpieczeństwie systemów chronionych przez IPS/IDS - 1/6

Czym jest IPS/IDS ?

Podział

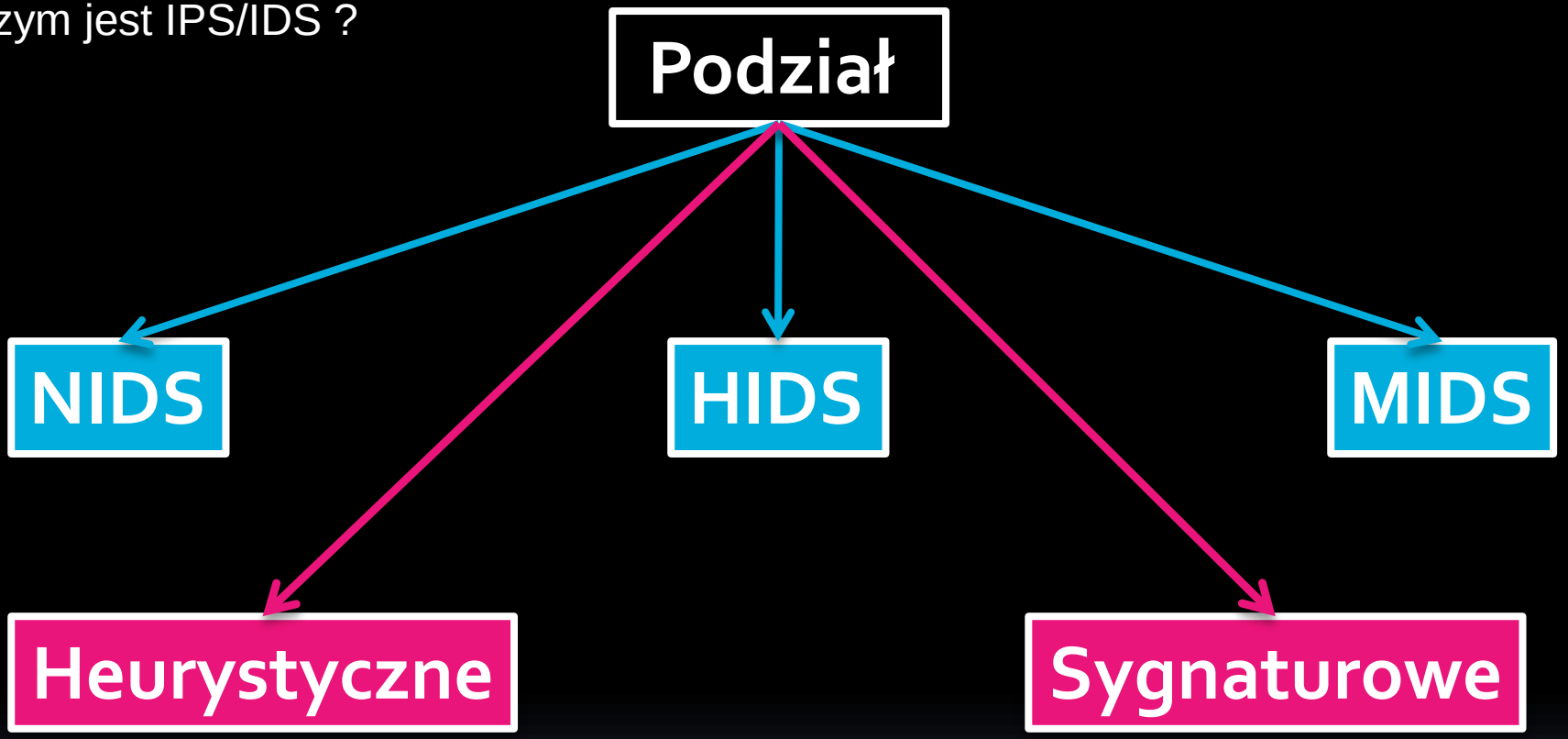
Fakty i mity o bezpieczeństwie systemów chronionych przez IPS/IDS - 1/6

Czym jest IPS/IDS ?



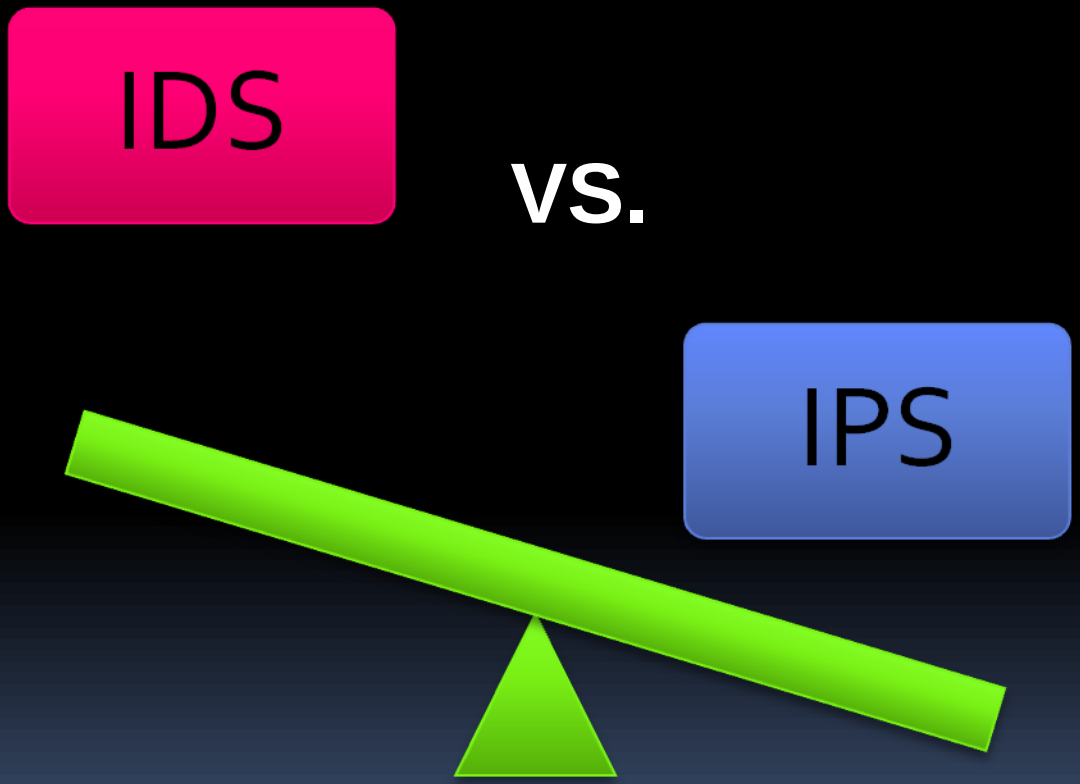
Fakty i mity o bezpieczeństwie systemów chronionych przez IPS/IDS - 1/6

Czym jest IPS/IDS ?



BUSINESS & TECHNOLOGY CONSULTING

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 2/6



btc BUSINESS & TECHNOLOGY CONSULTING

Problemy z wykrywaniem włamań:

- poprawne alarmy (ang. true positives)

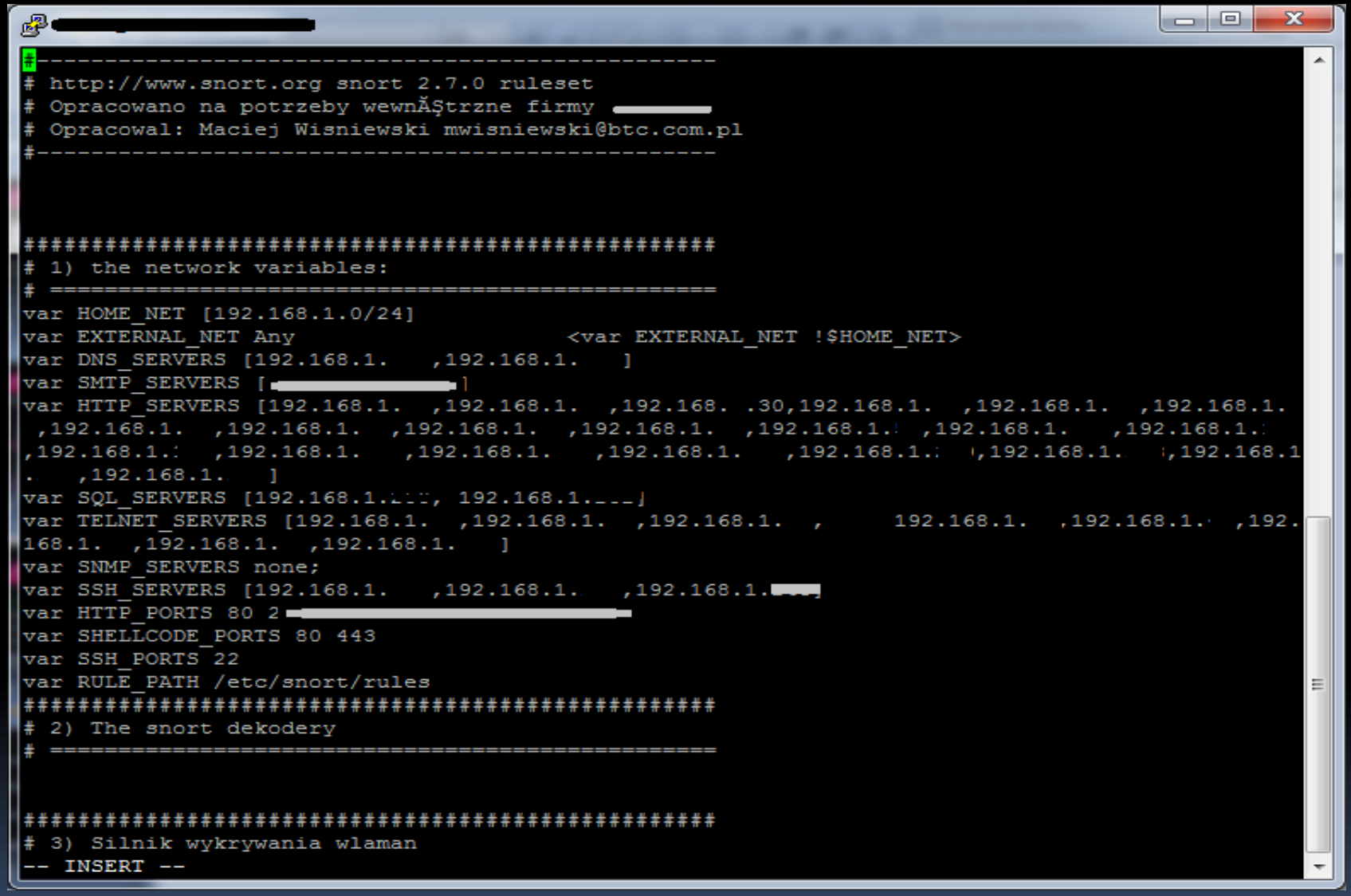
- fałszywe alarmy (ang. false positive)

- brak wykrycia (ang. false negative)

Mity:

- IPS jest nową technologią,
- IPS jest skomplikowany,
- IPS wyeliminuje zapory ogniowe,
- IPS jest remedium na zero-day atacks,
- Systemy IPS muszą być drogie.

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 5/6



Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 6/6

„de facto standard for intrusion detection / prevention”

Typowy atak z ukierunkowaniem na konkretną podatność:

Czy atak był anonimowy ?

Czy atak pozostawił po sobie ślady ?

Czy była szansa udaremnienia ataku ?

Czy istnieje możliwość zabezpieczenia dowodów ?

Czy istnieje możliwość szybkiego przywrócenia systemu?

btc BUSINESS & TECHNOLOGY CONSULTING

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 6/6

„de facto standard for intrusion detection / prevention”

Typowy atak z ukierunkowaniem na konkretną podatność:

TAK / NIE

Czy atak był anonimowy ?

Czy atak pozostawił po sobie ślady ?

Czy była szansa udaremnienia ataku ?

Czy istnieje możliwość zabezpieczenia dowodów ?

Czy istnieje możliwość szybkiego przywrócenia systemu?

btc BUSINESS & TECHNOLOGY CONSULTING

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 6/6

„de facto standard for intrusion detection / prevention”

Typowy atak z ukierunkowaniem na konkretną podatność:

Czy atak był anonimowy ? **TAK / NIE**

Czy atak pozostawił po sobie ślady ? **TAK**

Czy była szansa udaremnienia ataku ?

Czy istnieje możliwość zabezpieczenia dowodów ?

Czy istnieje możliwość szybkiego przywrócenia systemu?

btc BUSINESS & TECHNOLOGY CONSULTING

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 6/6

„de facto standard for intrusion detection / prevention”

Typowy atak z ukierunkowaniem na konkretną podatność:

Czy atak był anonimowy ?	**TAK / NIE**
Czy atak pozostawił po sobie ślady ?	**TAK**
Czy była szansa udaremnienia ataku ?	**TAK**
Czy istnieje możliwość zabezpieczenia dowodów ?	
Czy istnieje możliwość szybkiego przywrócenia systemu?	

btc BUSINESS & TECHNOLOGY CONSULTING

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 6/6

„de facto standard for intrusion detection / prevention”

Typowy atak z ukierunkowaniem na konkretną podatność:

Czy atak był anonimowy ?	**TAK / NIE**
Czy atak pozostawił po sobie ślady ?	**TAK**
Czy była szansa udaremnienia ataku ?	**TAK**
Czy istnieje możliwość zabezpieczenia dowodów ?	**TAK**
Czy istnieje możliwość szybkiego przywrócenia systemu?	

btc BUSINESS & TECHNOLOGY CONSULTING

Fakty i mity o bezpieczeństwie systemów chronionych przez IPS\IDS - 6/6

„de facto standard for intrusion detection / prevention”

Typowy atak z ukierunkowaniem na konkretną podatność:

Czy atak był anonimowy ?	**TAK / NIE**
Czy atak pozostawił po sobie ślady ?	**TAK**
Czy była szansa udaremnienia ataku ?	**TAK**
Czy istnieje możliwość zabezpieczenia dowodów ?	**TAK**
Czy istnieje możliwość szybkiego przywrócenia systemu?	**TAK / NIE**

btc BUSINESS & TECHNOLOGY CONSULTING

Nowoczesne audyty infrastruktury informatycznej - 1/4

Tworząc konstrukcję sieci należy stosować zasadę KISS - “niech to będzie proste” - podział dużego problemu na mniejsze, łatwiejsze do utrzymania. Każda sieć jest inna i powstaje pod naciskiem różnych uwarunkowań (np. finansowych).

Nowoczesne audyty infrastruktury informatycznej - 2/4

„Naszym wrogiem nie jest już ignorancja – jest nim brak czujności”

- Audyt bezpieczeństwa Teleinformatycznego
- Czy standardowe zabezpieczenia wystarczą ?
- Dlaczego BTC Sp. z o.o. ?

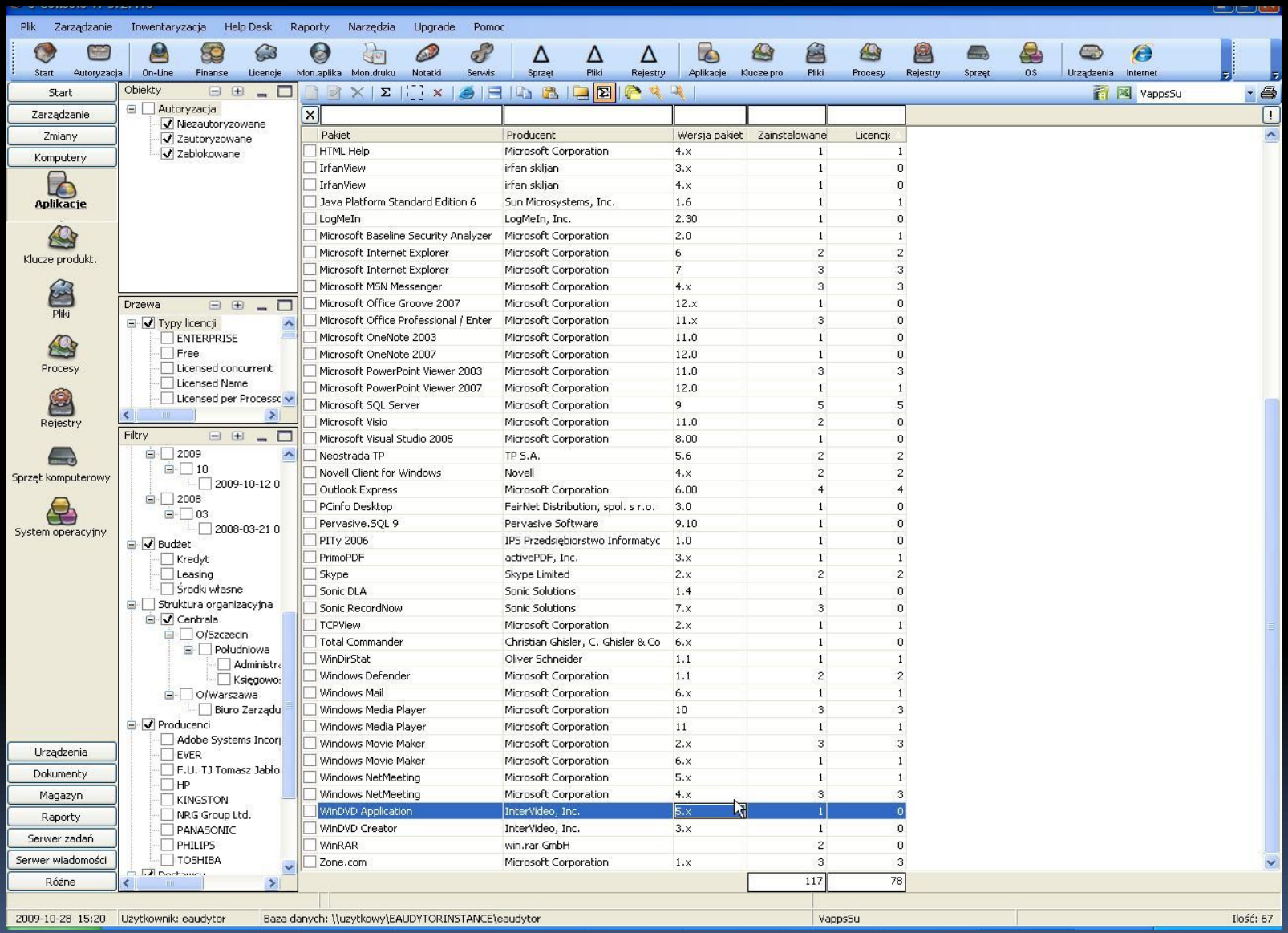
Nowoczesne audyty infrastruktury informatycznej - 3/4

Przegląd naszych produktów i usług z zakresu audytów teleinformatycznych:

- **Audyty bezpieczeństwa technologii sieciowych**
- **Audyty bezpieczeństwa sieci bezprzewodowych (WIFI)**
- **Audyty legalności oprogramowania**
- **Audyty polityki bezpieczeństwa**

- **System E-Audytor®**

System e-Audytor®



Zarządzanie licencjami Zdalne zarządzanie Inwentaryzacja

Pytania ???????