

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



Prowadzący:

Specjalista do sp. Informatyki

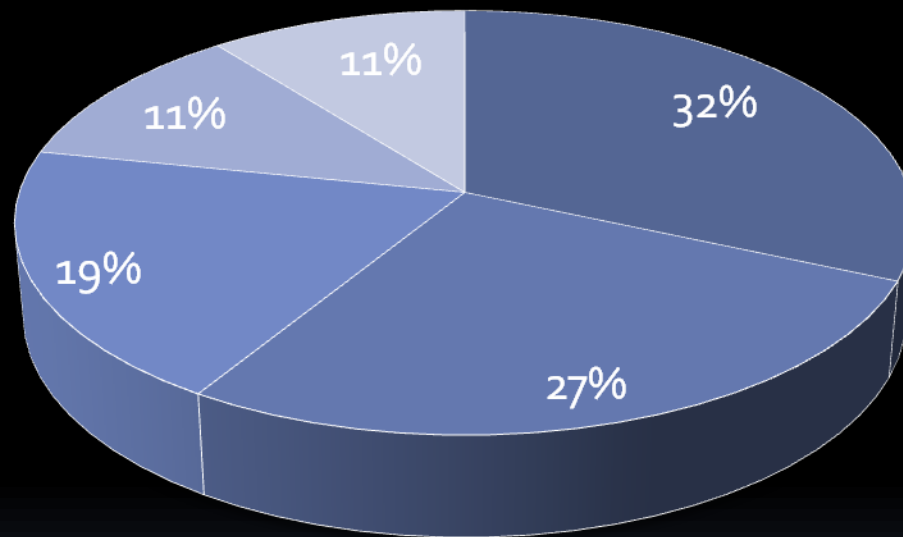
Śledczej

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.

Zagrożenia w sieciach komputerowych



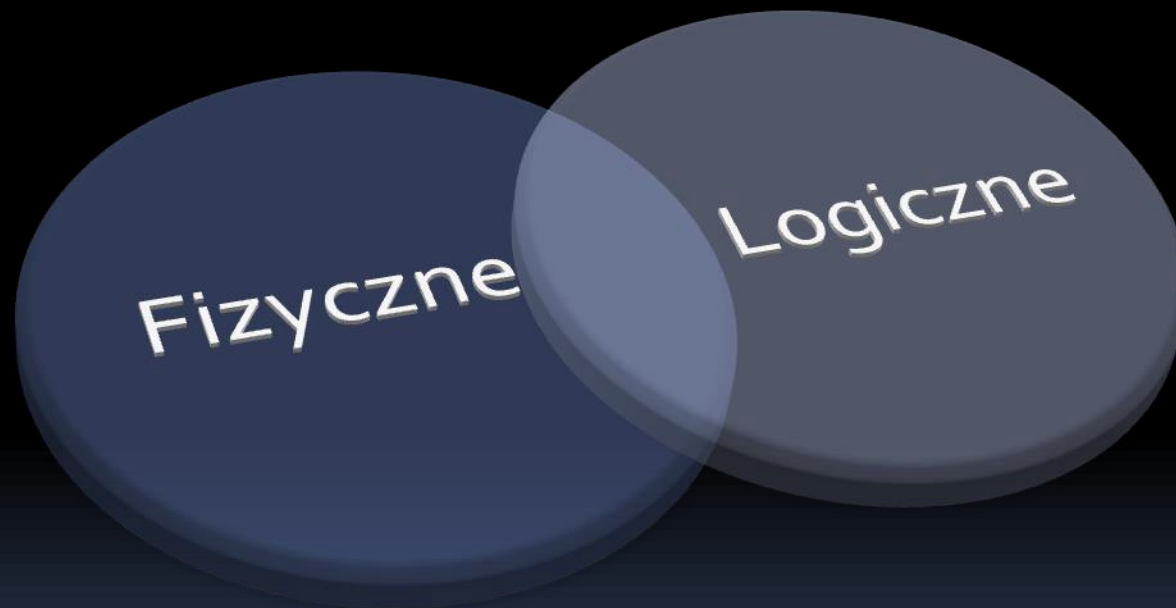
- 1. ogień oraz fizyczne uszkodzenia sprzętu
- 2. wirusy
- 3. ataki hakerskie
- 4. błędy ludzkie
- 5. przestoje

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.

Amat victoria curam.

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

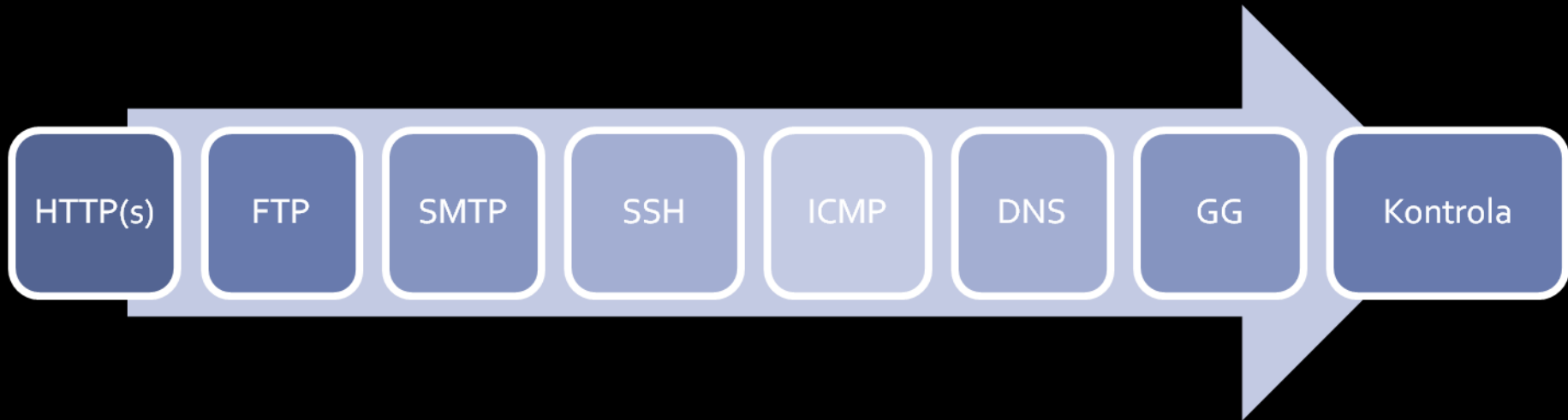
Typy wycieku informacji:



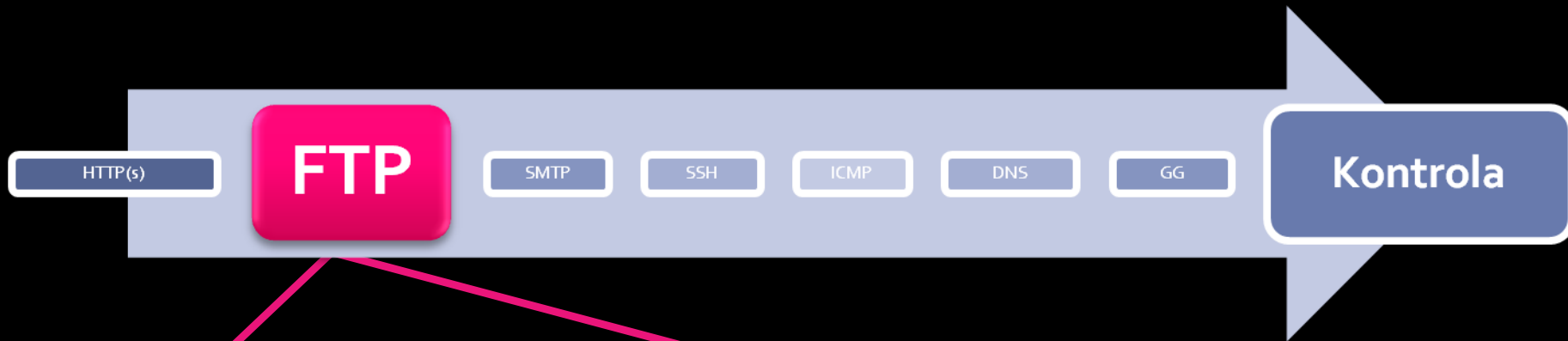
Logiczne typy wycieku informacji:



Typy wycieku informacji:



Ryzyko wycieku poufnych informacji - 4/10



Określenie puli dostępnych adresów

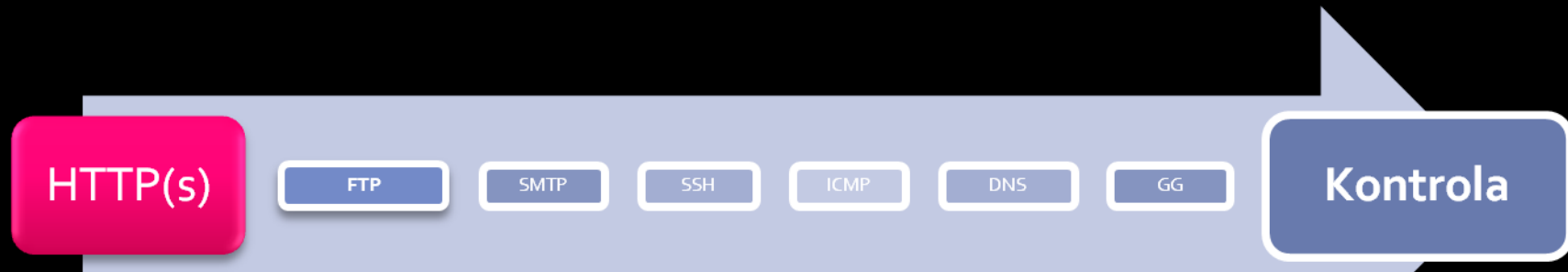
Blokowanie wgrzywania plików na serwer

==> PUT
==> STORE

FTP- PROXY



Ryzyko wycieku poufnych informacji - 5/10



Określenie puli dostępnych adresów

Np. www.youtube.com

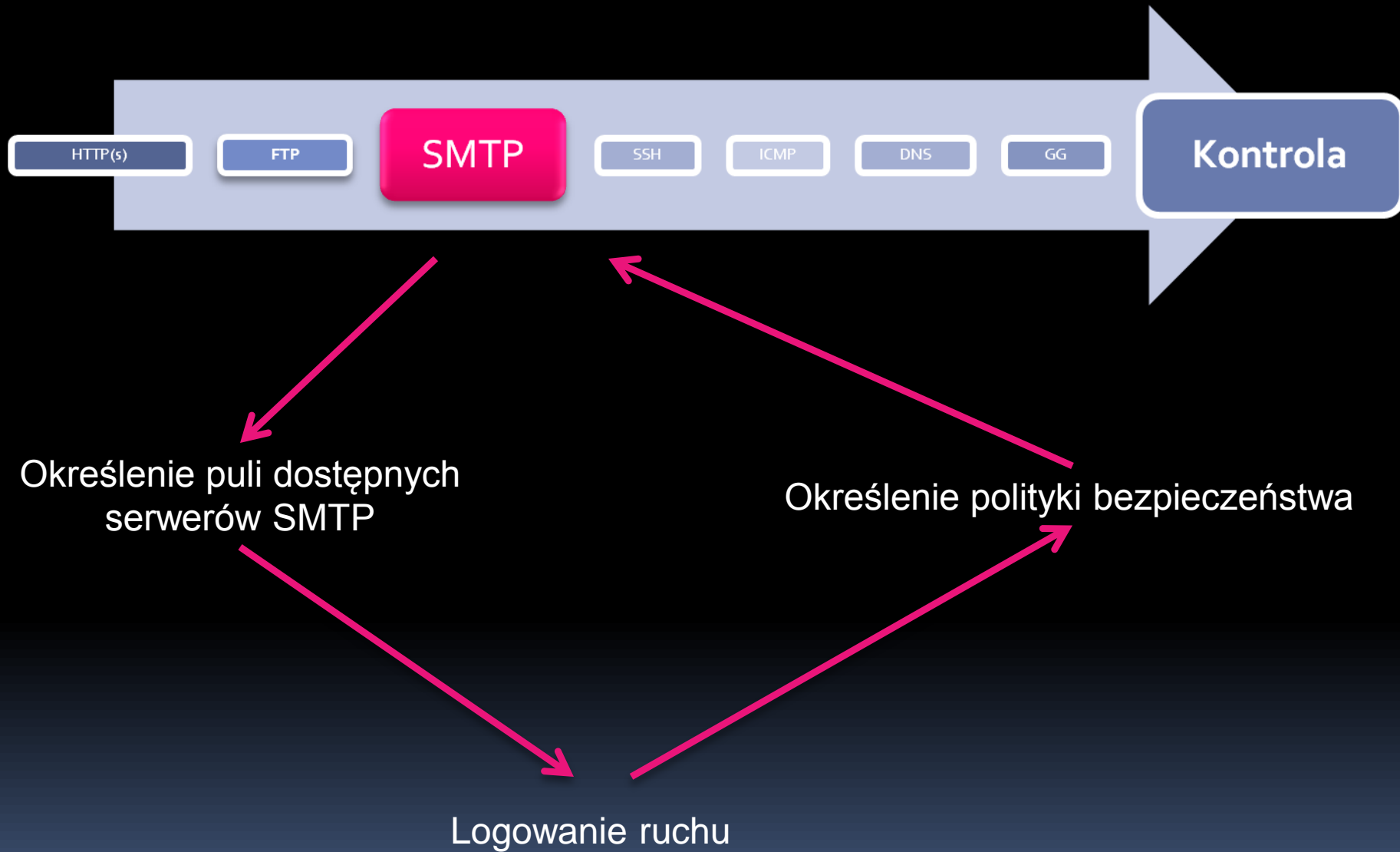
Blokowanie kontentu

Np. „nasza klasa”

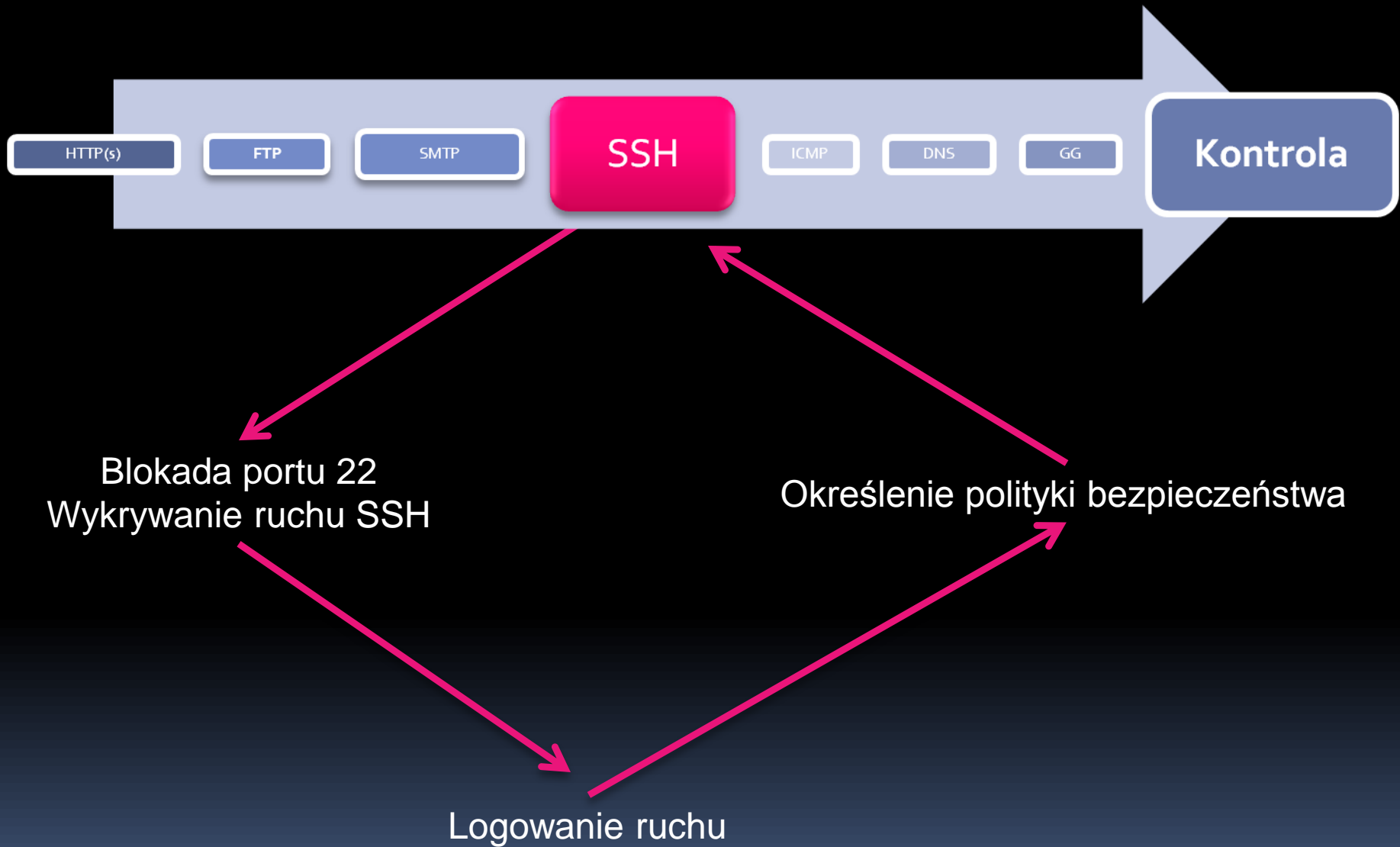
DANSGUARDIAN, SQUID ; WATCH GUARD
(free) (comercial)



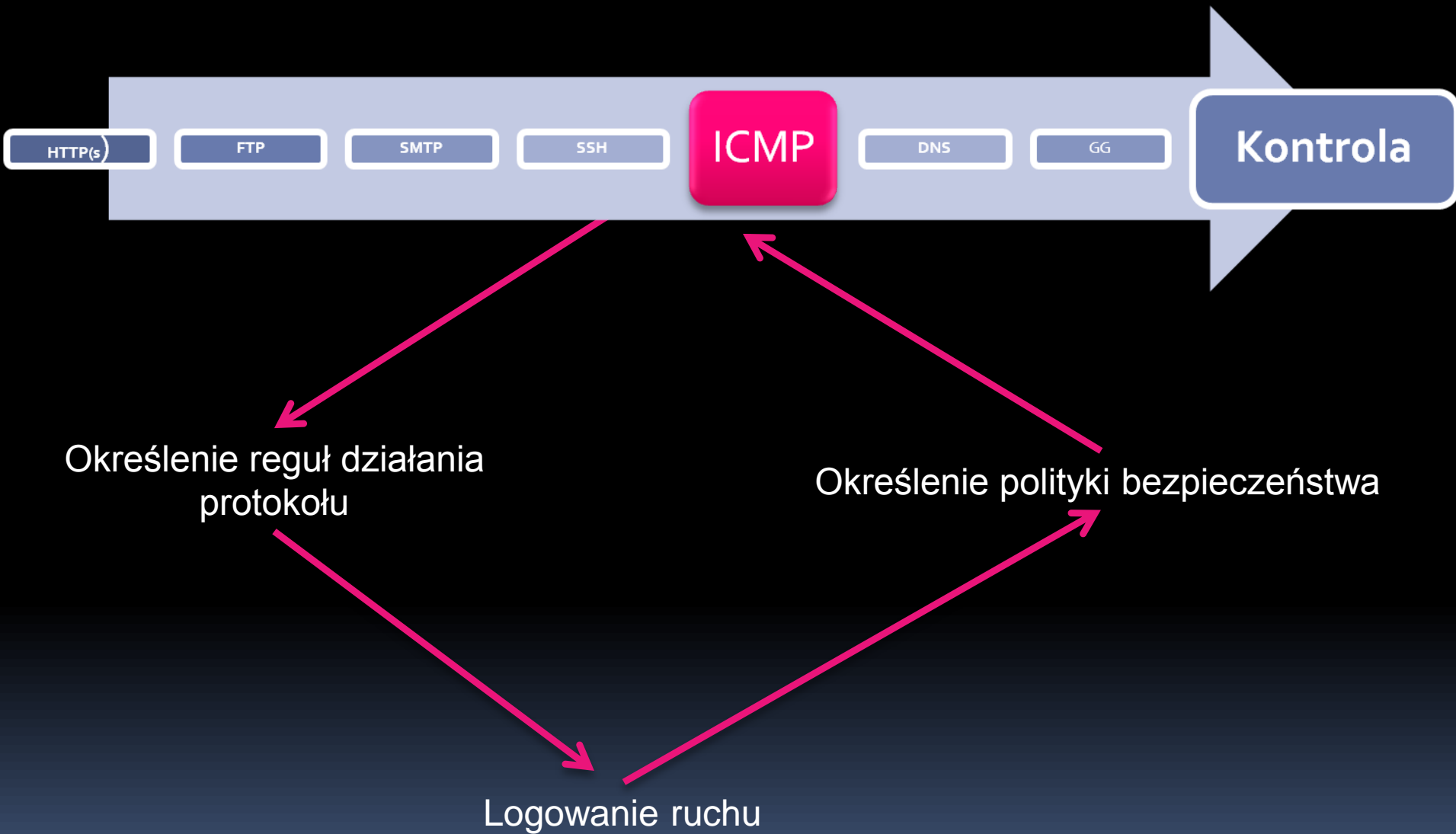
Ryzyko wycieku poufnych informacji - 6/10



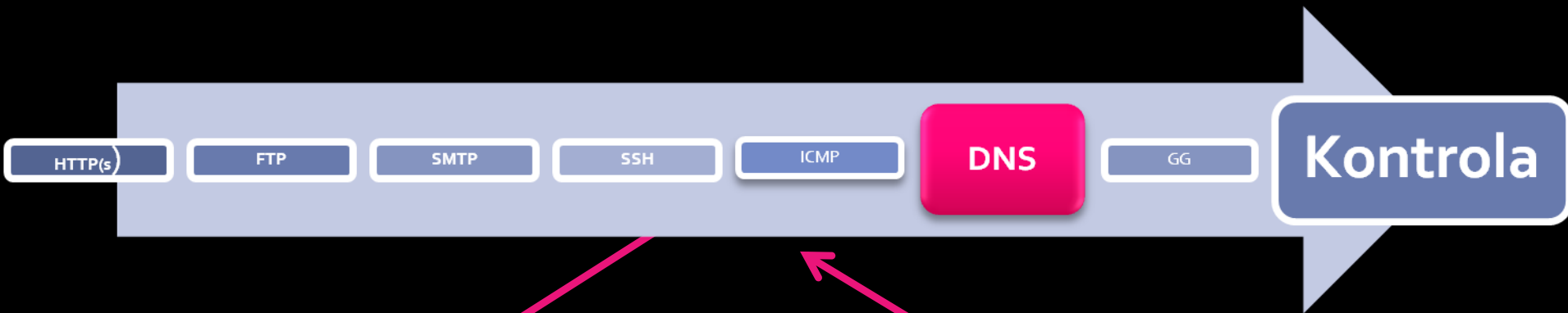
Ryzyko wycieku poufnych informacji - 7/10



Ryzyko wycieku poufnych informacji - 8/10



Ryzyko wycieku poufnych informacji - 9/10



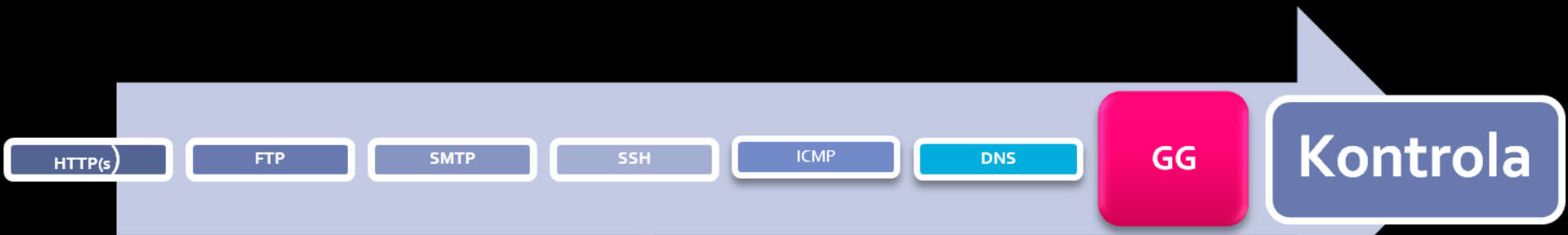
Zestawienie tunelu na porcie DNS 53 np. poprzez: iodine lub NSTX

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”
```

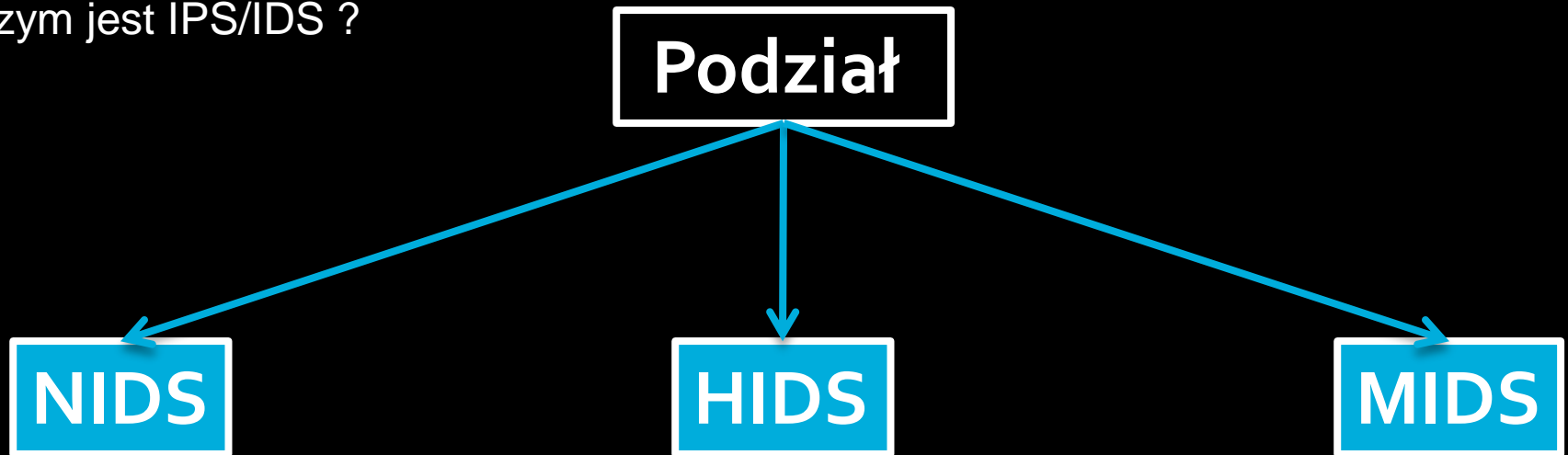


Czym jest IPS/IDS ?

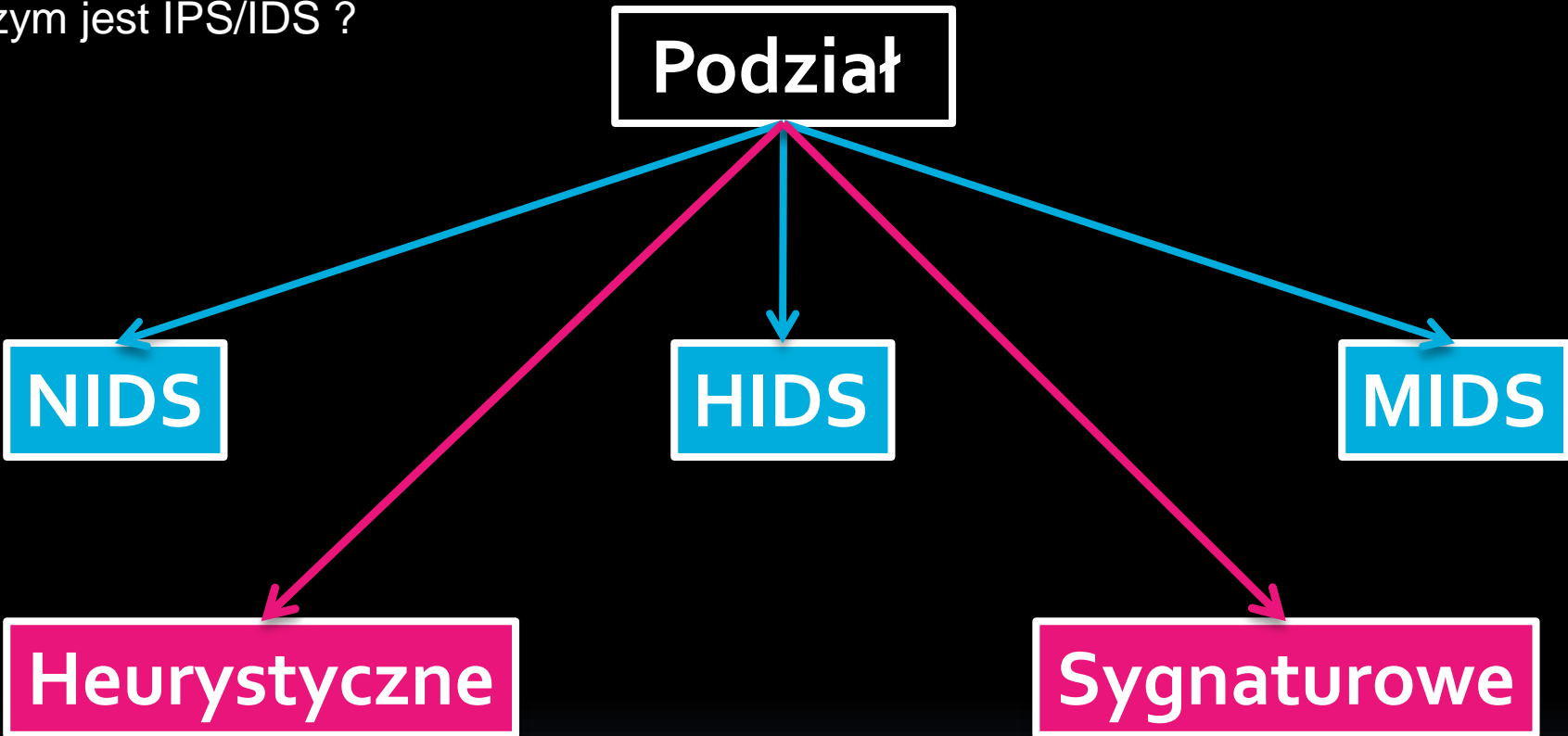
Czym jest IPS/IDS ?

Podział

Czym jest IPS/IDS ?



Czym jest IPS/IDS ?



IDS

VS.

IPS



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 attacks,
- Systemy IPS muszą być drogie.

```
-----
# http://www.snort.org snort 2.7.0 ruleset
# Opracowano na potrzeby wewnętrznej firmy _____
# Opracował: Maciej Wisniewski mwisniewski@btc.com.pl
#-----

#####
# 1) the network variables:
# -----
var HOME_NET [192.168.1.0/24]
var EXTERNAL_NET Any <var EXTERNAL_NET !$HOME_NET>
var DNS_SERVERS [192.168.1. ,192.168.1. ]
var SMTP_SERVERS [ _____ ]
var HTTP_SERVERS [192.168.1. ,192.168.1. ,192.168. .30,192.168.1. ,192.168.1. ,192.168.1.
,192.168.1. ,192.168.1. ,192.168.1. ,192.168.1. ,192.168.1. ,192.168.1.
,192.168.1. ,192.168.1. ,192.168.1. ,192.168.1. ,192.168.1. ,192.168.1.
,192.168.1. ]
var SQL_SERVERS [192.168.1. ,192.168.1. ]
var TELNET_SERVERS [192.168.1. ,192.168.1. ,192.168.1. , 192.168.1. ,192.168.1. ,192.
168.1. ,192.168.1. ,192.168.1. ]
var SNMP_SERVERS none;
var SSH_SERVERS [192.168.1. ,192.168.1. ,192.168.1. ]
var HTTP_PORTS 80 2 _____
var SHELLCODE_PORTS 80 443
var SSH_PORTS 22
var RULE_PATH /etc/snort/rules
#####
# 2) The snort dekodery
# -----

#####
# 3) Silnik wykrywania właman
-- INSERT --
```





„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?



„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?



„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?



„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?



„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?



„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 |

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).

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

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



Przeгляд 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®

The screenshot displays the e-Audytor software interface. On the left, there is a navigation pane with buttons for 'Zarządzanie', 'Zmiany', 'Komputery', 'Aplikacje', 'Klucze produkt.', 'Pliki', 'Procesy', 'Rejestry', 'Sprzęt komputerowy', and 'System operacyjny'. Below these are buttons for 'Urządzenia', 'Dokumenty', 'Magazyn', 'Raporty', 'Serwer zadań', 'Serwer wiadomości', and 'Różne'. The main window is divided into three panes: 'Obiekty' (Objects) with a tree view of license types (ENTERPRISE, Free, Licensed concurrent, etc.), 'Drzewa' (Trees) with a hierarchical organizational chart (2009, 2008, Budżet, Struktura organizacyjna, etc.), and a large table of installed software licenses.

Pakiet	Producent	Wersja pakiet	Zainstalowane	Licencj
<input type="checkbox"/> HTML Help	Microsoft Corporation	4.x	1	1
<input type="checkbox"/> IrfanView	irfan skljan	3.x	1	0
<input type="checkbox"/> IrfanView	irfan skljan	4.x	1	0
<input type="checkbox"/> Java Platform Standard Edition 6	Sun Microsystems, Inc.	1.6	1	1
<input type="checkbox"/> LogMeIn	LogMeIn, Inc.	2.30	1	0
<input type="checkbox"/> Microsoft Baseline Security Analyzer	Microsoft Corporation	2.0	1	1
<input type="checkbox"/> Microsoft Internet Explorer	Microsoft Corporation	6	2	2
<input type="checkbox"/> Microsoft Internet Explorer	Microsoft Corporation	7	3	3
<input type="checkbox"/> Microsoft MSN Messenger	Microsoft Corporation	4.x	3	3
<input type="checkbox"/> Microsoft Office Groove 2007	Microsoft Corporation	12.x	1	0
<input type="checkbox"/> Microsoft Office Professional / Enter	Microsoft Corporation	11.x	3	0
<input type="checkbox"/> Microsoft OneNote 2003	Microsoft Corporation	11.0	1	0
<input type="checkbox"/> Microsoft OneNote 2007	Microsoft Corporation	12.0	1	0
<input type="checkbox"/> Microsoft PowerPoint Viewer 2003	Microsoft Corporation	11.0	3	3
<input type="checkbox"/> Microsoft PowerPoint Viewer 2007	Microsoft Corporation	12.0	1	1
<input type="checkbox"/> Microsoft SQL Server	Microsoft Corporation	9	5	5
<input type="checkbox"/> Microsoft Visio	Microsoft Corporation	11.0	2	0
<input type="checkbox"/> Microsoft Visual Studio 2005	Microsoft Corporation	8.00	1	0
<input type="checkbox"/> Neostrada TP	TP S.A.	5.6	2	2
<input type="checkbox"/> Novell Client for Windows	Novell	4.x	2	2
<input type="checkbox"/> Outlook Express	Microsoft Corporation	6.00	4	4
<input type="checkbox"/> PCInfo Desktop	FairNet Distribution, spol. s r.o.	3.0	1	0
<input type="checkbox"/> Pervasive.SQL 9	Pervasive Software	9.10	1	0
<input type="checkbox"/> PITY 2006	IP5 Przedsiębiorstwo Informatyc	1.0	1	0
<input type="checkbox"/> PrimoPDF	activePDF, Inc.	3.x	1	1
<input type="checkbox"/> Skype	Skype Limited	2.x	2	2
<input type="checkbox"/> Sonic DLA	Sonic Solutions	1.4	1	0
<input type="checkbox"/> Sonic RecordNow	Sonic Solutions	7.x	3	0
<input type="checkbox"/> TCPView	Microsoft Corporation	2.x	1	1
<input type="checkbox"/> Total Commander	Christian Ghisler, C. Ghisler & Co	6.x	1	0
<input type="checkbox"/> WinDirStat	Oliver Schneider	1.1	1	1
<input type="checkbox"/> Windows Defender	Microsoft Corporation	1.1	2	2
<input type="checkbox"/> Windows Mail	Microsoft Corporation	6.x	1	1
<input type="checkbox"/> Windows Media Player	Microsoft Corporation	10	3	3
<input type="checkbox"/> Windows Media Player	Microsoft Corporation	11	1	1
<input type="checkbox"/> Windows Movie Maker	Microsoft Corporation	2.x	3	3
<input type="checkbox"/> Windows Movie Maker	Microsoft Corporation	6.x	1	1
<input type="checkbox"/> Windows NetMeeting	Microsoft Corporation	5.x	1	1
<input type="checkbox"/> Windows NetMeeting	Microsoft Corporation	4.x	3	3
<input type="checkbox"/> WinDVD Application	InterVideo, Inc.	5.x	1	0
<input type="checkbox"/> WinDVD Creator	InterVideo, Inc.	3.x	1	0
<input type="checkbox"/> WinRAR	win.rar GmbH		2	0
<input type="checkbox"/> Zone.com	Microsoft Corporation	1.x	3	3
			117	78

Zarządzanie licencjami

Zdalne zarządzanie

Inwentaryzacja

Pytania ????????

