Zarządzanie bezpieczeństwem systemów informatycznych

Zagadnienia

1. **Narzędzia**
   - kontrola dostępu
   - systemy NAC
   - systemy IDS / IPS / ATP
   - przynęty (*honey-pot, honey-net*)
2. **Zarządzanie polityką – Web Services**
3. **Aktualizacja systemów**
4. **Archiwizacja danych i kopie bezpieczeństwa**
5. **Monitorowanie zabezpieczeń i incydentów**
6. **Kompleksowe systemy nadzoru**

Narzędzia

Ochrona

Klasy narzędzi

- kontrola zdalnego dostępu – filtracja ruchu sieciowego
- kontrola lokalnego dostępu na poziomie poszczególnych użytkowników i zasobów
- kontrola stanu systemu operacyjnego / aplikacji (weryfikacja stanu aktualizacji itp.)
- kontrola występowania innych znanych słabości w konfiguracji

Narzędzia

Filtracja ruchu sieciowego

adresy IP

- ruch przychodzący z sieci publicznej (i wychodzący do niej) z adresami należącymi do puli prywatnych (RFC 1918) lub testowych (RFC 5737, np. 192.0.2.0/24)
- ruch przychodzący z sieci publicznej z adresów należących do sieci wewnętrznej
- localhost
- ruch multicast (224.0.0.0/4), o ile właściwe (uwaga na protokoły routingu!)
- adresy nieprzydzielone przez IANA (Internet Assigned Numbers Authority) (tzw. bogons, np. 1.0.0.0/8 czy 169.254.0.0/16)

https://ipgeolocation.io/resources/bogon.html

Narzędzia

Filtracja ruchu sieciowego

szczególnie newralgiczne usługi

Internet:	systat	11 / tcp / udp
	chargen	19 / tcp / udp
	TFTP	69 / tcp / udp
	...	
Windows:	SMB	135–139 / tcp i 445 / tcp
	UPnP	1900 / tcp / udp
	SSDP	5000 / tcp / udp

Narzędzia

Filtracja ruchu sieciowego

znane niebezpieczne porty

C&C (bots):	NetBus	12345 / tcp i 12346 / tcp
	BackOrifrice	31337 / tcp / udp
	...	
DDoS:	trin00	27665 / tcp, 27444 / udp, 31335 / udp
	trinity v3	33270 / tcp i 39168 / tcp
	stacheldracht	16660 / tcp i 65000 / tcp
	subseven	2222, 6711, 6712, 6776, 6669, 7000 / tcp
	...	

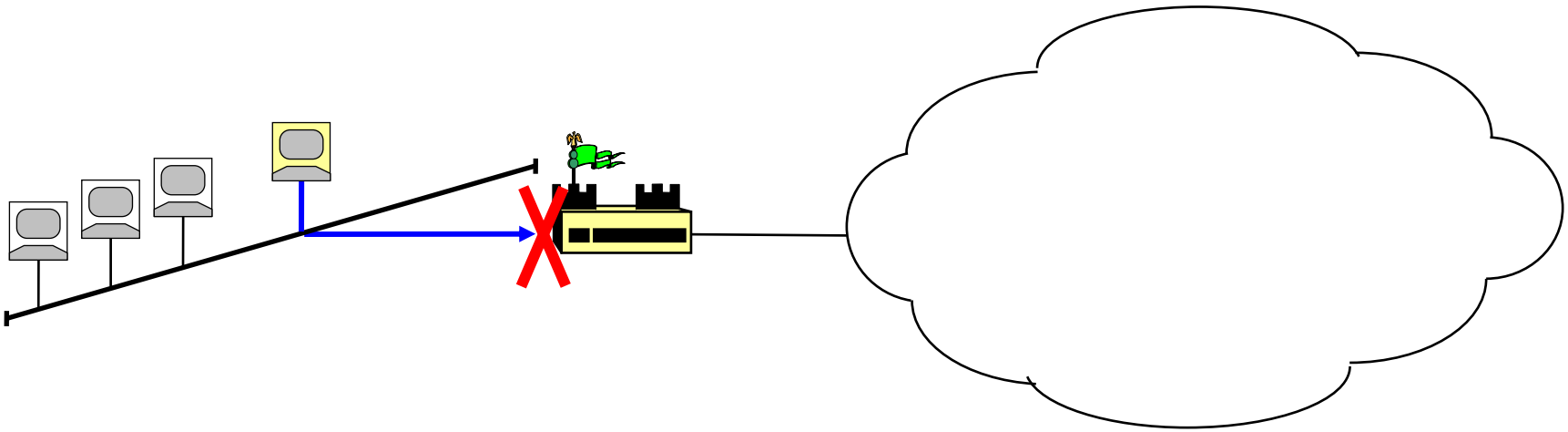
Narzędzia

Kontrola dostępu

metoda „zamka i klucza” (*lock-and-key*)

- wykorzystywana w sytuacji, gdy normalnie dostęp jest blokowany

  (np. wychodzące w sieć publiczną pakiety traceroute: 33400, 34400 / udp):

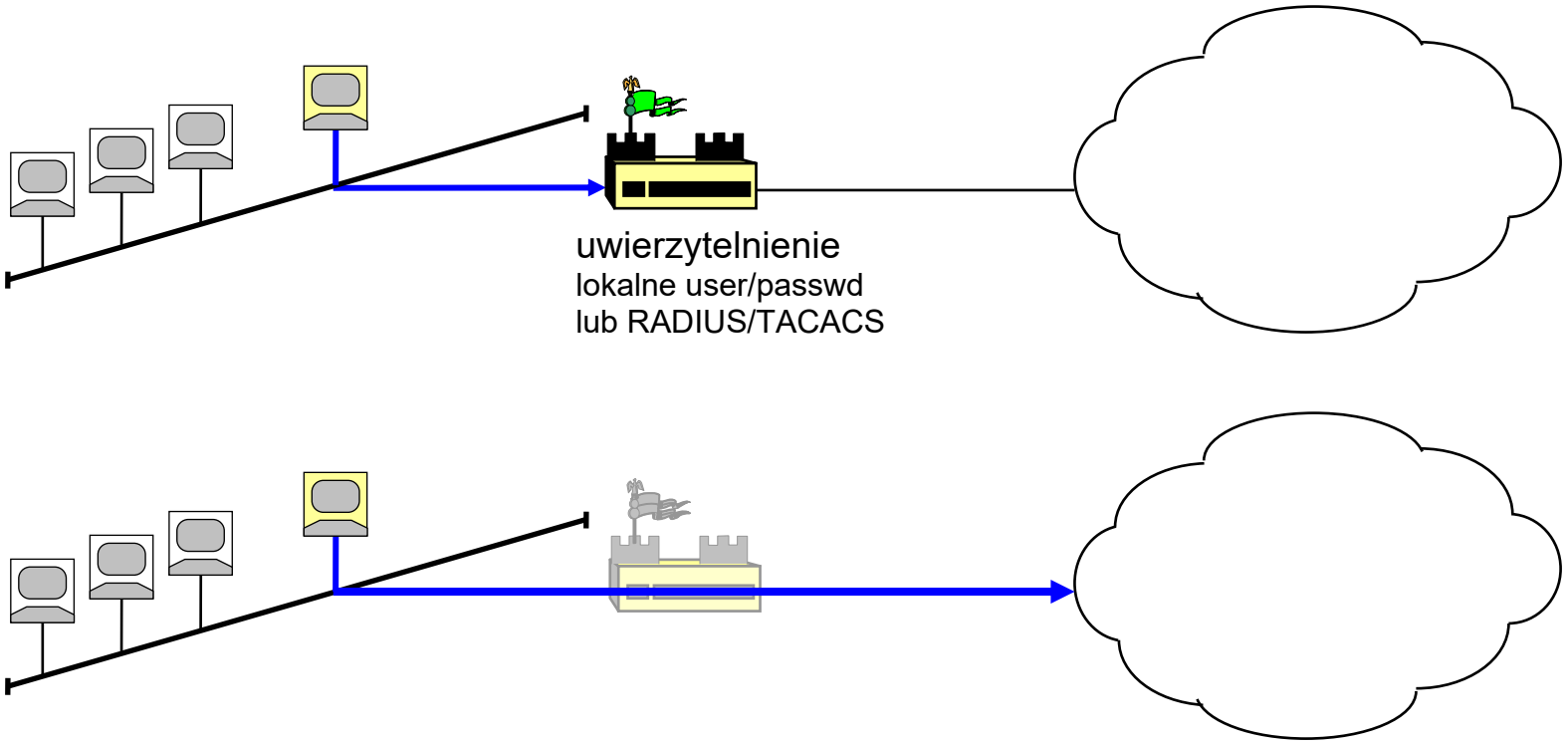


Narzędzia

Kontrola dostępu

metoda „zamka i klucza” (*lock-and-key*)

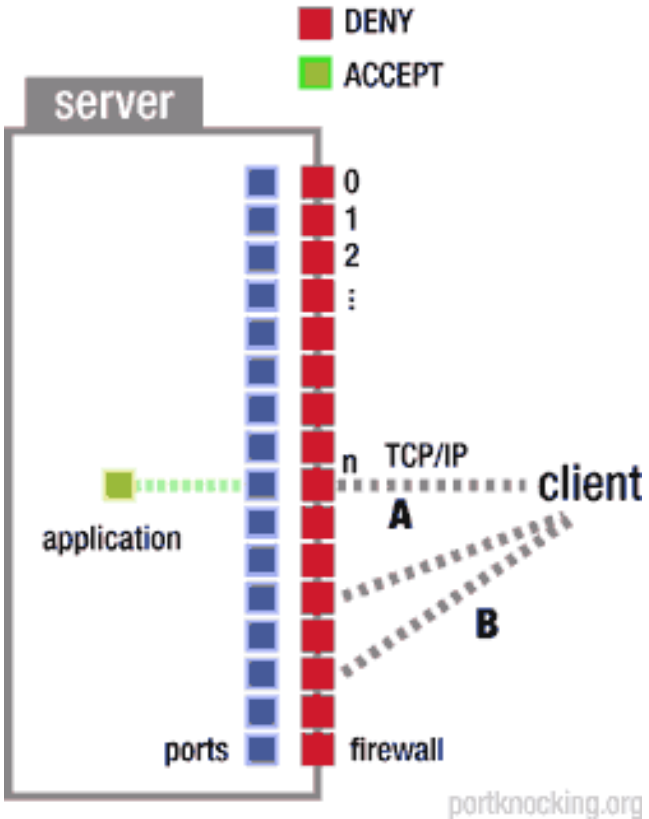
- jednak uwierzytelnione sesje są uprawnione do obejścia blokady:

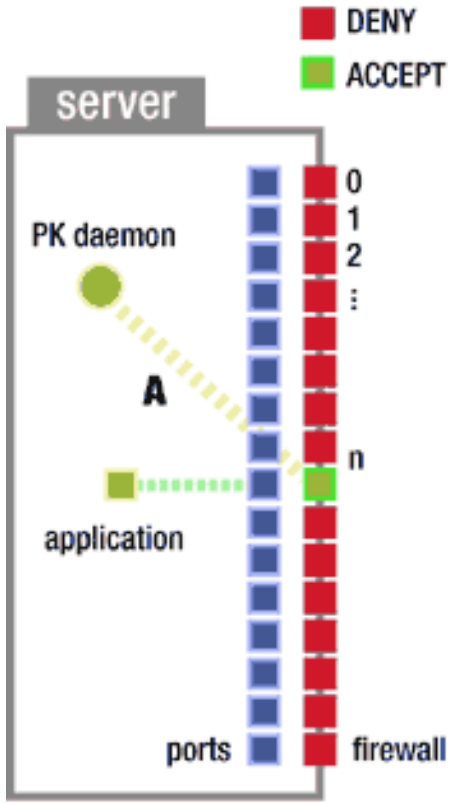


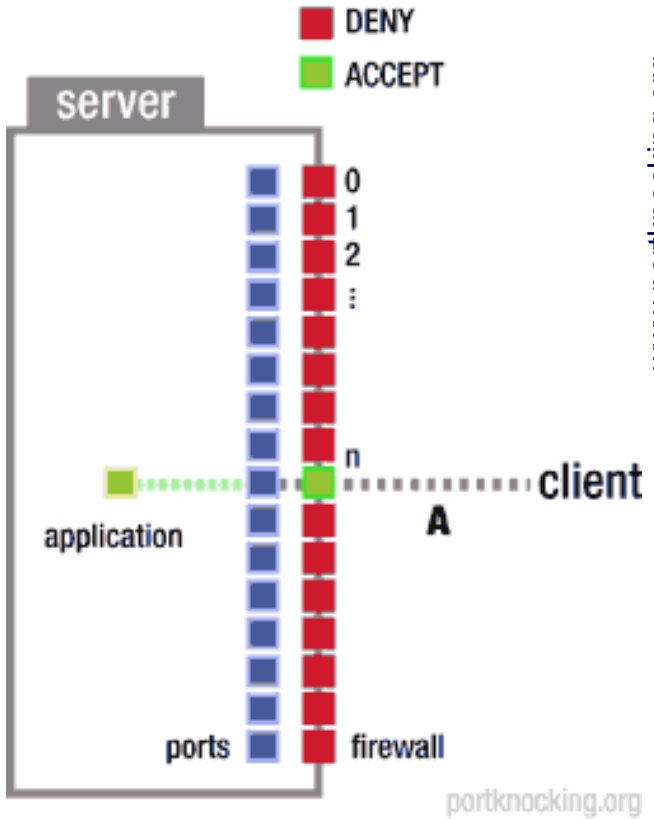
Narzędzia

Kontrola dostępu

port-knocking







www.portknocking.org

Systemy nadzoru stanowisk sieciowych

Network Access Control

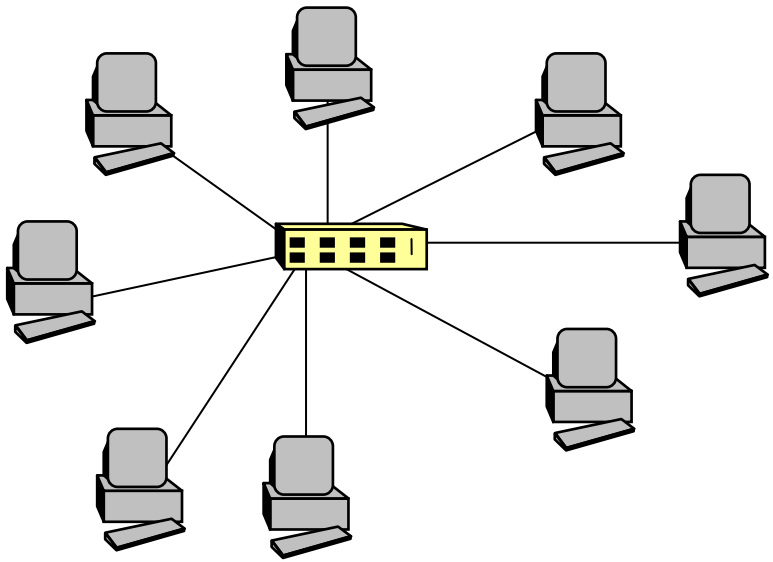
Cel:

- zdalna weryfikacja w sieci lokalnej / korporacyjnej, czy poszczególne stanowiska sieciowe spełniają wymagania polityki bezpieczeństwa, np. w zakresie kontroli antywirusowej czy uaktualnień systemu operacyjnego
- stanowiska niespełniające wymagań są odcinane od sieci rozległej lub kręgosłupowej, ewentualnie otrzymują możliwość ograniczonej komunikacji z innymi segmentami / podsieciami

Uwierzytelnianie stanowisk

Standard IEEE 802.1X

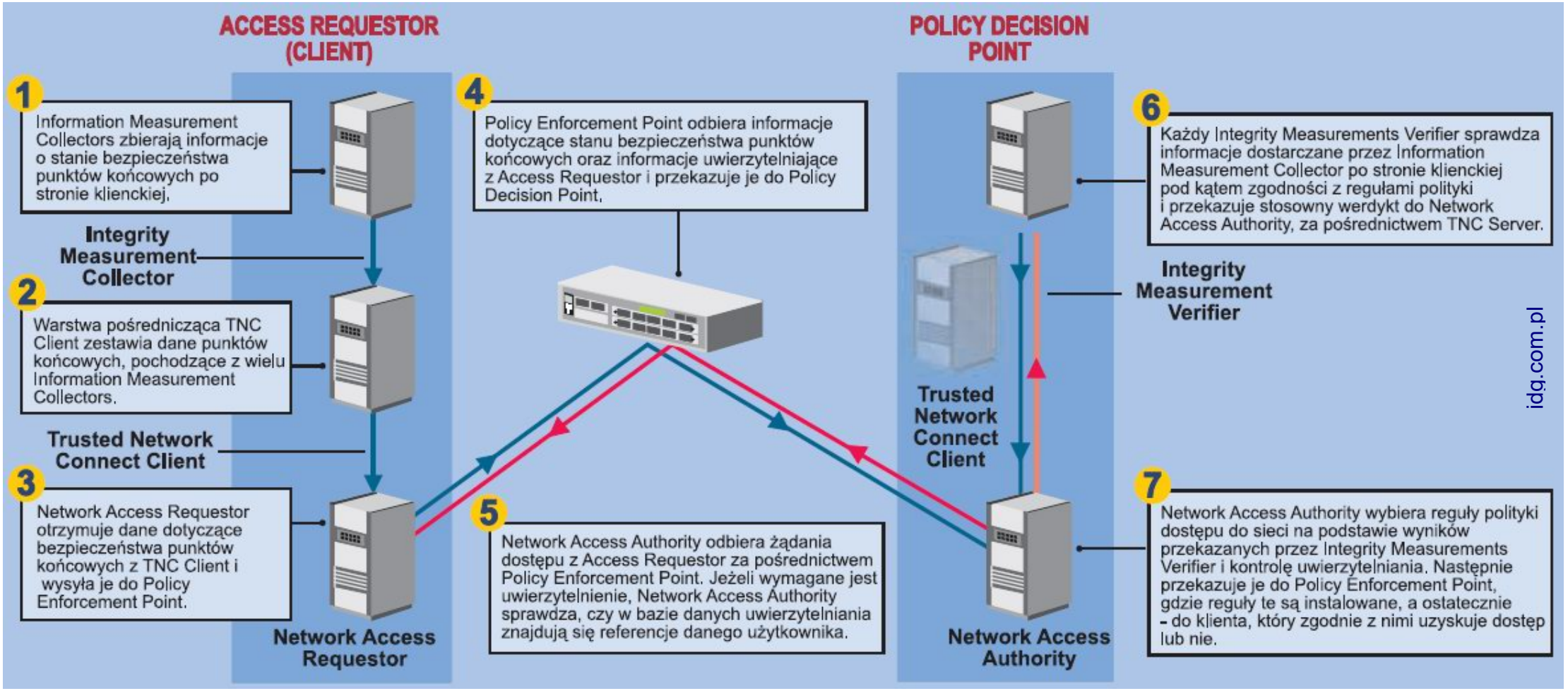
- ochrona infrastruktury sieciowej przed nieautoryzowanym dostępem
- poprzez centralne uwierzytelnianie stacji sieciowych
- np. przełącznik lub punkt dostępowy wymusza uwierzytelnienie stacji



Systemy nadzoru stanowisk sieciowych

Network Access Control

Model Trusted Network Connect (specyfikacja Trusted Computing Group)



Systemy nadzoru stanowisk sieciowych

Komponenty systemu NAC:

Serwer Kontroli Dostępu (Policy Decision Point, Secure Access Control Server)

- instalowany na stacji administracyjnej, analizuje informacje o stanie bezpieczeństwa pobrane ze stacji sieciowych i podejmuje decyzje o dopuszczeniu ich do sieci

Lokalny agent nadzoru (Client Trust Agent, System Health Agent)

- instalowany na stacjach sieciowych, zbiera informacje o stanie bezpieczeństwa systemu od innych modułów programowych (np. aplikacji antywirusowych)

Policy Enforcement Points

- przełączniki, węzły międzysieciowe lub zapory sieciowe – pośredniczą w przekazywaniu tych informacji do Serwera Kontroli Dostępu
- na podstawie jego decyzji blokują/ograniczają ruch

Systemy nadzoru stanowisk sieciowych

Przykłady:

- Network Admission Control (Cisco)
- Network Access Protection (Microsoft)
- Checkpoint Integrity
- Policy Enforcer (McAfee)
- Sygate Enterprise Protection (Symantec)
- OESIS (OPSWAT)

open source:

- FreeNAC (freenac.net)
- PacketFence (www.packetfence.org)

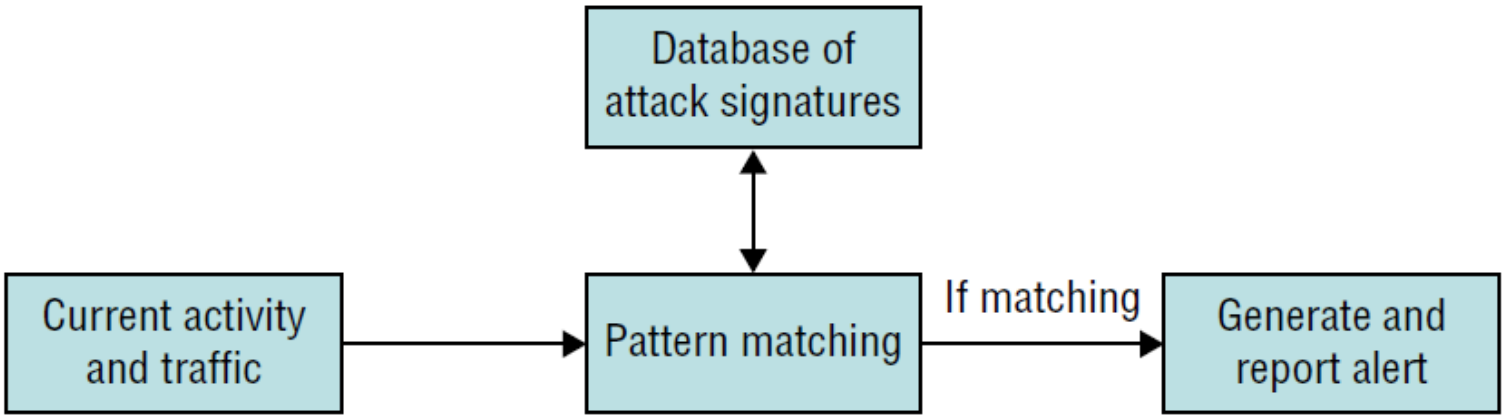
IDS

(*Intrusion Detection Systems*)

Systemy IDS

- monitorowanie ruchu sieciowego w celu wykrycia zagrożeń:
  - podejrzanej aktywności (skanowania portów, adresów sieciowych)
  - podejrzanej zawartości pakietów (wirusów)
  - dostępu do usług informacyjnych i katalogowych
  - ataków DoS

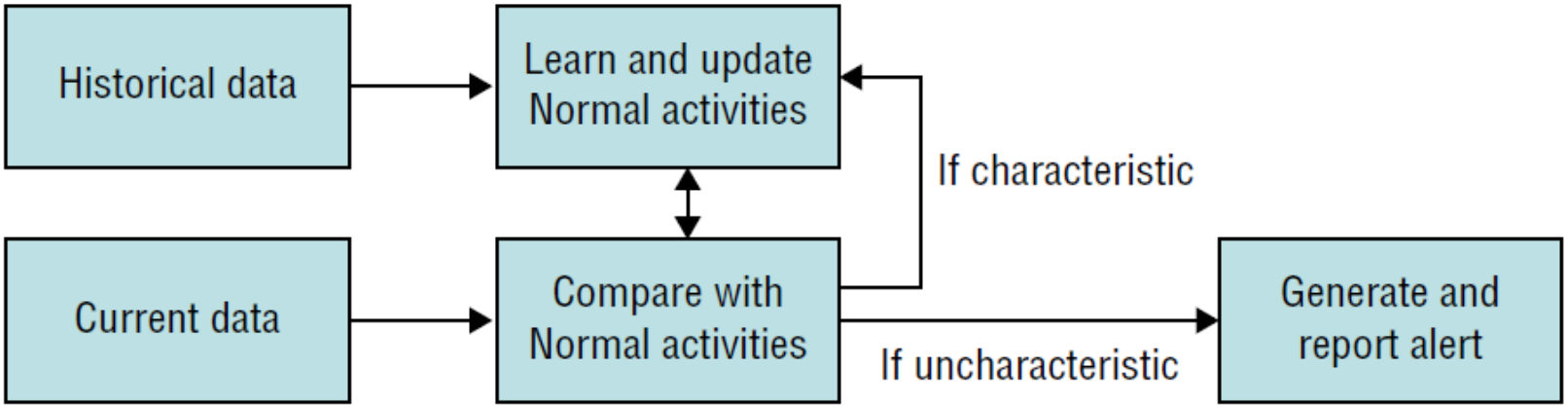
  na podstawie bazy wzorców zagrożeń



signature-based IDS

Systemy IDS

- analiza statystyczna ruchu (wykrywanie anomalii)



statistical anomaly-based IDS

Systemy IDS

- raportowanie

+ reagowanie (zapora) → IPS (*Intrusion Prevention Systems*)

- pułapki / przynęty:
  - mają za zadanie skierować intruza w „ślepy zaułek” (fałszywe usługi) odwodząc go od usług właściwych
  - dając administratorowi czas na reakcję

Systemy IDS

Systemy IDS / IPS mogą pracować jako:

Network IDS/IPS

- wydzielone stacje sieciowe w sieci lokalnej
- moduły urządzeń sieciowych (np. Cisco Catalyst 6000 IDS Module)
- niekiedy zestaw wielokomponentowy obejmujący m.in.:
  - monitory ruchu sieciowego (NSM = Network Security Monitoring)
  - agentów nadzoru stanowisk sieciowych
  - centralnego zarządcę

Host IDS/IPS (HIDS/HIPS)

- analiza logów systemowych, integralności systemu plików itp. (np. Samhain)
- ochrona lokalnego systemu operacyjnego / aplikacji (np. przed RCE)

Systemy IDS

Problem wydajności systemów IDS / IPS

- ponad 40 000 (!) wzorców ataków (sygnatur) i rośnie
- na ogół wymagana jest analiza całego pakietu (*deep packet inspection*)
- do tego może być niezbędna analiza stanu sesji
- problem zwłaszcza specjalizowanych modułów routerów filtrujących
  - np. sensor IDS Cisco serii 4200 ma nominalną wydajność rzędu Gb/s

Systemy IDS

Zagrożenia

Techniki Anti-IDS (AIDS):

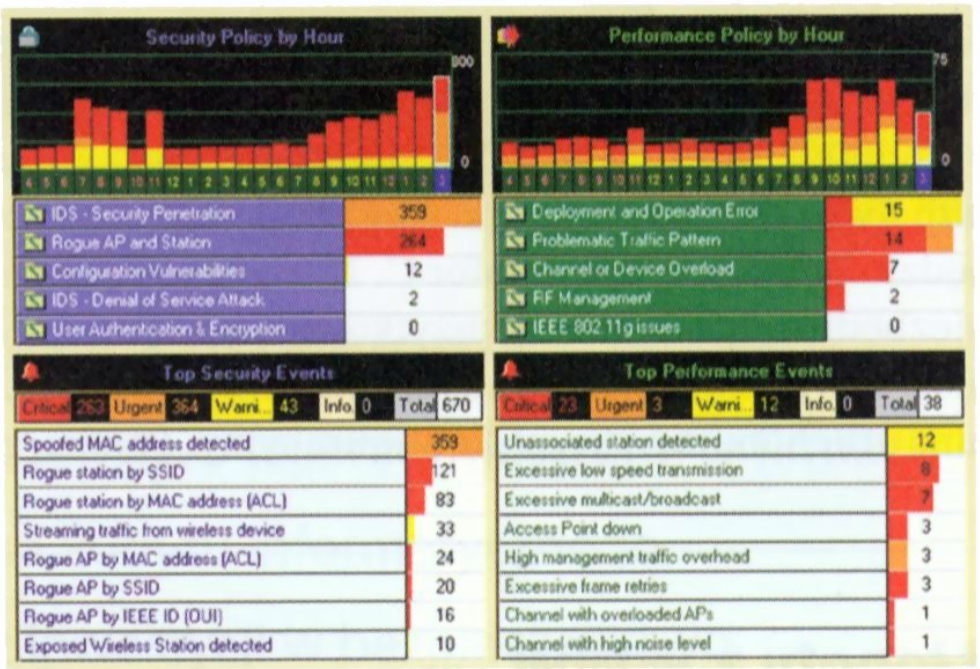
- ukrywanie cech charakterystycznych (modyfikacja sygnatur)
- fragmentacja
- ataki DoS na systemy IDS
- przykład: Whisker (ataki na WWW z predefiniowanymi sposobami obejścia IDS)

Łączność bezprzewodowa

Systemy WIDP (*Wireless Intrusion Detection & Prevention*)

- skanowanie pasma częstotliwości przez wszystkie kanały
- w celu wykrycia:
  - nieautoryzowanych punktów dostępowych przyłączonych do chronionej sieci
  - nieautoryzowanych stacji klienckich przyłączonych do chronionej sieci
  - autoryzowanych stacji klienckich przyłączonych do nieautoryzowanej sieci
- przykłady:

  AirDefense, AirMagnet, Nzyme, ...



Detekcja sniffingu

Popularne metody

- metoda DNS
- metoda ARP
- metoda ARP cache
- metoda PING
- metoda ICMP delta (*latency test*)

Detekcja sniffingu

Metoda DNS

Idea

- monitorowanie ruchu w sieci pod kątem zapytań o adresy IP kierowane do serwera DNS (*reverse DNS lookup*)
- często wykonywanych przez sniffery w celu zapisania informacji o nazwach stacji w przechwyconych pakietach

Ograniczenia

- konieczny dostęp do całości ruchu w naszej sieci lokalnej – bez mostowania / przełączania (w przypadku przełącznika – wpięcie do portu monitorującego)

Detekcja sniffingu

Metoda ARP

Idea

- normalne zapytania ARP kieruje się pod rozgłoszeniowy adres MAC
- ale karta sieciowa pracująca w trybie promiscuous będzie odbierać również ramki skierowane pod inne adresy i przekazywać wyżej (np. do stacji protokołu ARP)
- i stacja ARP na nie odpowie

Ograniczenia

- musimy wiedzieć o czyj adres IP pytamy – kogoś podejrzewamy
- aby stacja ARP odpowiedziała, trzeba spreparować zapytanie na nietypowy adres multicast: FF:FF:FF:FF:FF:FE, FF:FF:00:00:00:00, FF:00:00:00:00:00, 01:00:5E:00:00:01
- nie wszystkie implementacje jednakowo reagują (nie na każdy adres odpowiadają)

Detekcja sniffingu

Metoda ARP cache

Idea

- podobnie: karta sieciowa w trybie promiscuous przechwyci ramki skierowane pod adresy inne niż rozgłoszeniowe (np. FF:FF:FF:FF:FF:FE)
- np. ramkę ARP z ogłoszeniem nowego adresu IP, którego faktycznie nie przydzielono żadnemu stanowisku, np. "192.168.0.254, o adresie MAC AA:AA:AA:AA:AA:AA"
- stacja ARP na komputerze sniffera odbierze ramkę i zachowa te adresy w cache
- następne zapytanie ICMP *echo request* z adresem źródłowym (!) 192.168.0.254 spowoduje pojawienie się odpowiedzi *echo reply* bez uprzedniego zapytania ARP o ten adres

Ograniczenia

- musimy wiedzieć dokąd skierować zapytanie ICMP – kogoś podejrzewamy
- odpytujemy podejrzane lub wszystkie adresy IP w sieci

Detekcja sniffingu

Metoda PING

Idea

- normalne zapytanie ICMP *echo request* do określonego adresu IP wysyłane jest w ramce MAC skierowanej pod adres MAC odpowiadający temu adresowi IP
- karta sieciowa w trybie promiscuous odbierze ramkę nawet jeśli adres MAC nie będzie odpowiadać odpytywanemu IP
- i ostatecznie pojawi się odpowiedź *echo reply*

Ograniczenia

- odpytujemy podejrzane lub wszystkie adresy IP w sieci

Detekcja sniffingu

Metoda ICMP delta

Idea

- porównanie różnic w czasach odpowiedzi ICMP (lub dowolnych innych) w przypadku obciążenia karty odpytywanego stanowiska
- kartę sieciową pracującą w trybie promiscuous łatwo obciążyć generując w sieci dużo ramek skierowanych pod fałszywe adresy MAC
- i porównać czas odpowiedzi z przypadkiem znikomego ruchu w sieci

Ograniczenia

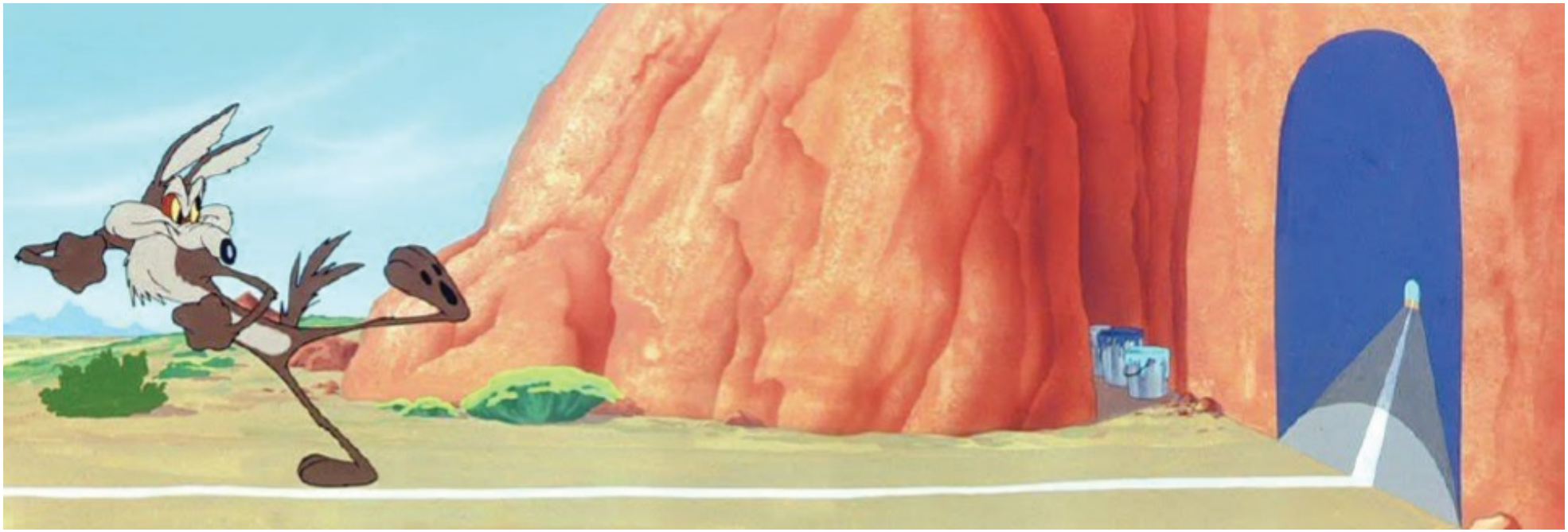
- zakładamy, że uda się szumem komunikacyjnym dostatecznie obciążyć stację podsłuchującą
- nieskuteczne, gdy sieć pasmo sieci normalnie jest już znacząco wykorzystane

Detektory snifferów

Przykłady

- Antisniff: http://packetstorm.linuxsecurity.com/sniffers/antisniff/
- Anasil: http://www.anasil.net
- Sentinel: http://www.mirrors.wiretapped.net/security/network-monitoring/sentinel
- Neped: http://www.securiteam.com/tools/Neped
- Promiscan: http://www.securityfriday.com
- Hunt: http://packetstormsecurity.nl/sniffers/hunt/
- Sniffdet: http://sniffdet.sourceforge.net/
- L0pht Antisniff (http://www.l0pht.com/antisniff/ – bogaty zestaw metod, ale podatny na ataki: por. http://www.iss.net/security_center/advice/Intrusions/2000418/)
- `nmap -sV --script=sniffer-detect.nse 192.0.0.0/24`

Przynęty



Przynęty

System wabiący

- dedykowany niezabezpieczony system, którego celem jest zebranie informacji o ataku i atakującym oraz odciągnięcie jego uwagi od rzeczywistego chronionego systemu
- fake services,
  honey-nets (podsieci, np. rzekomych urządzeń IoT),
  honey-patches (fake unpatched system)
- gromadzą relatywnie małe ilości danych, które mają zwykle bardzo dużą wartość

Przykłady:

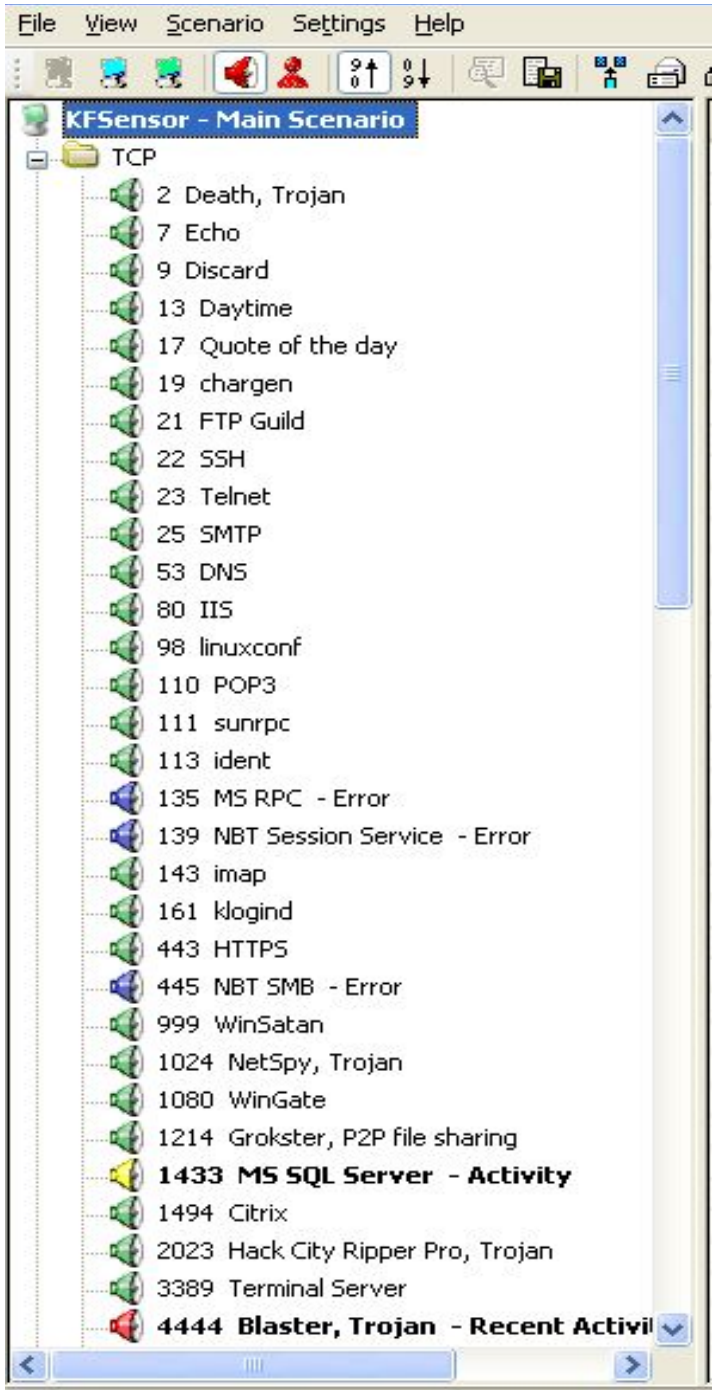
- KFSensor, SmallPot, Tiny Honeypot, Kippo, Cowrie, Glutton, …

www.honeynet.org

Przynęty

KFSensor

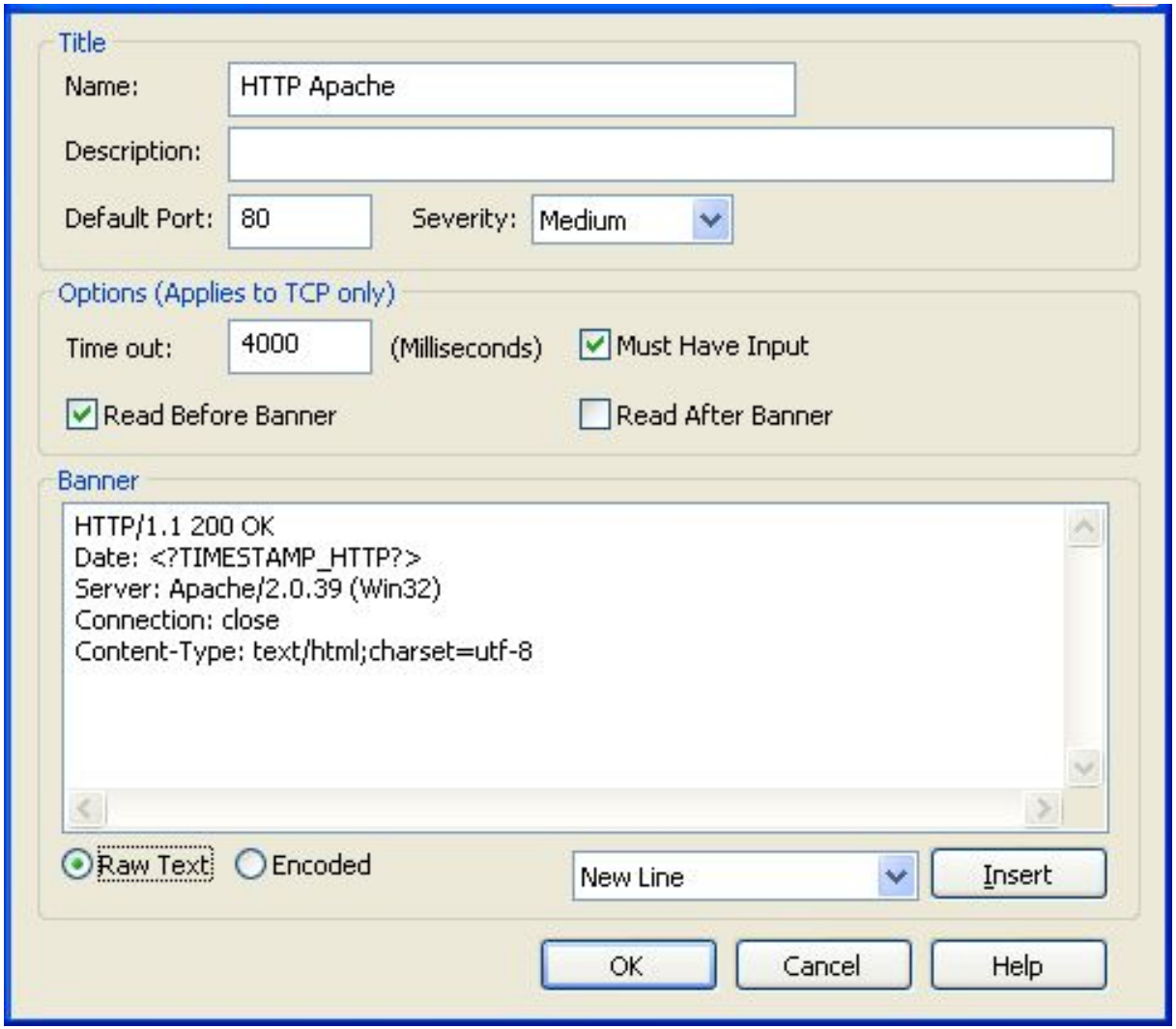
- wiele symulowanych usług
- z predefiniowanym zachowaniem (reakcją na połączenie)



Przynęty

KFSensor

- możliwe własne definicje usług

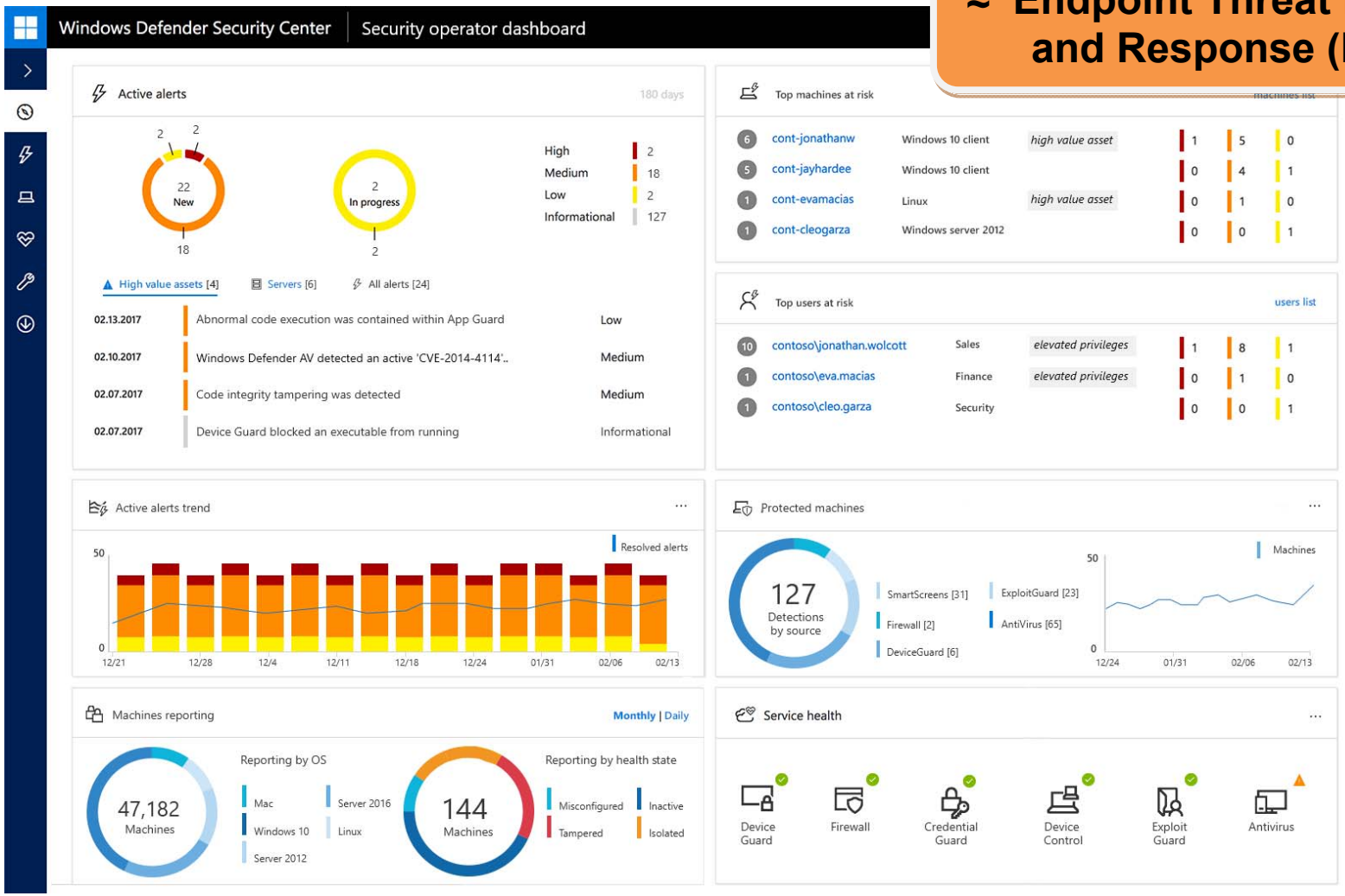


Systemy ATP

(*Advanced Threat Protection*)

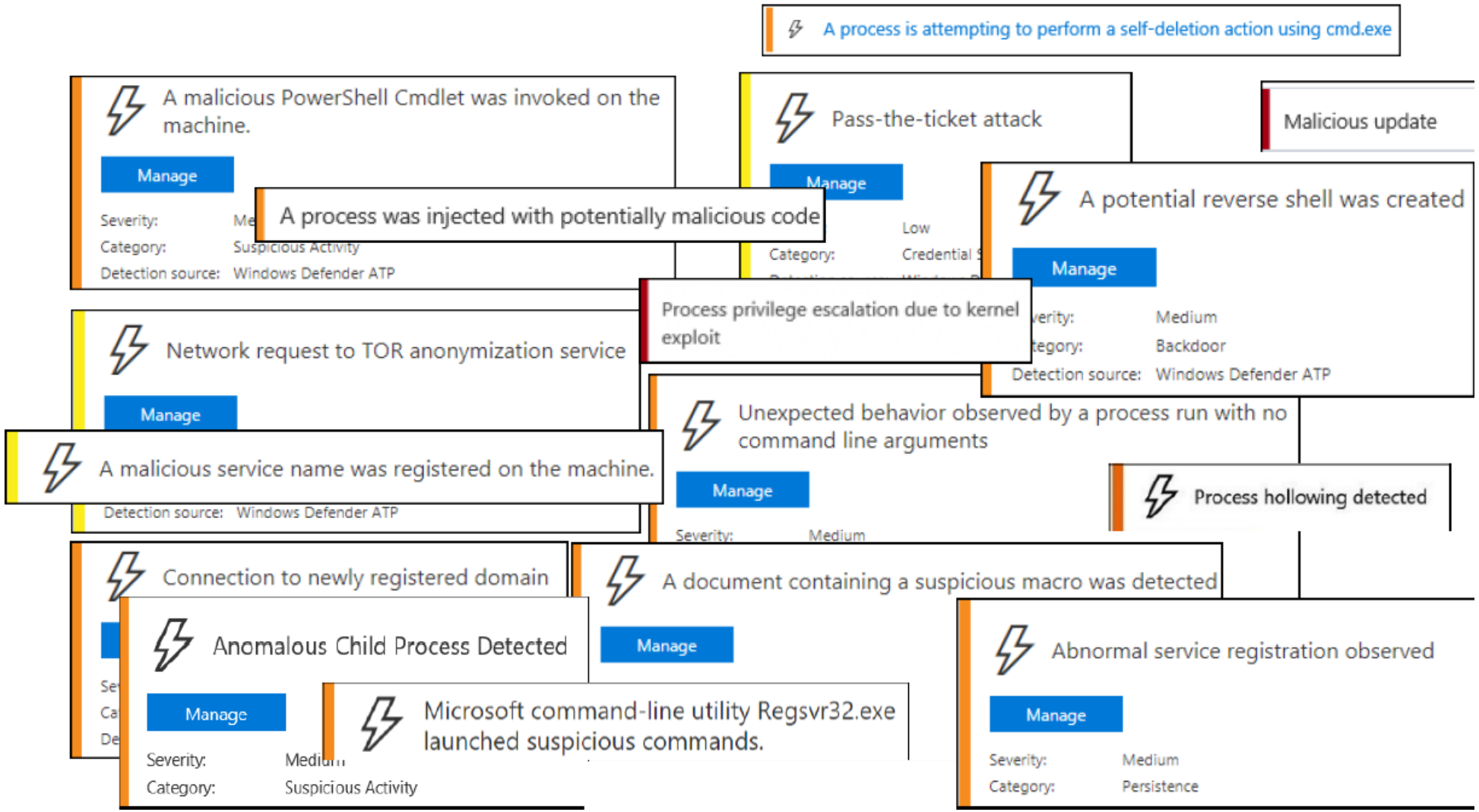
All-in-one: IDS / IPS / A-V / ...

≈ Endpoint Threat Detection and Response (ETDR)



Systemy ATP

All-in-one: IDS / IPS / A-V / ...



Web Services

Web Services

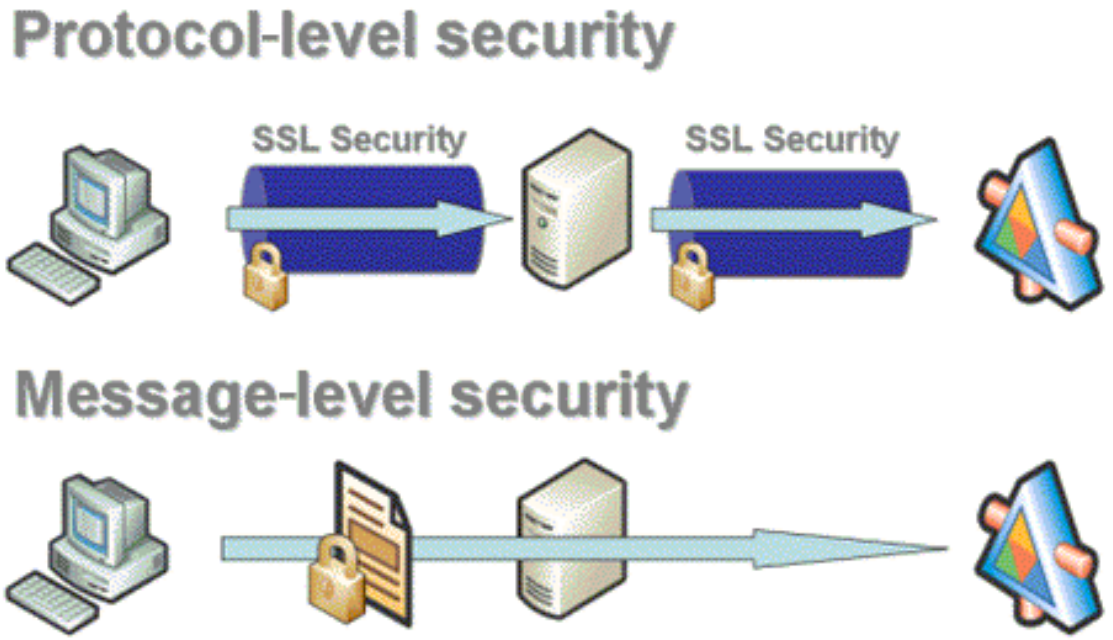
Web Service Architecture (WSA)

- SOA – Service Oriented Architecture
- SOAP – pierwotnie Simple Object Access Protocol – XML envelope
- typowo SOAP over HTTP
- WSDL + UDDI

```
1  <soap:Envelope xmlns:soap="http://..." xmlns:wsu="http://...">
2      <soap:Body>
3          <!-- The goal is to sign only the candidates that will actually be promoted -->
4          <promotion_candidates>
5              <manager wsu:Id="WWID46464">John</manager>
6              <engineer wsu:Id="WWID34396">Mike</engineer>
7              <manager wsu:Id="WWID34364">Joe</manager>
8              <engineer wsu:Id="WWID32896">Tom</engineer>
9          </promotion_candidates>
10     </soap:Body>
11 </soap:Envelope>
```

Web Services

- HTTP tunneling
- XML firewalls
- transport-level vs. message-level protection



Web Services

XML security extensions

- XML Signature

```
<Signature Id="SampleSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
     <CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
     <DigestValue>  ...  </DigestValue>
  </SignedInfo>
  <SignatureValue>  ...  </SignatureValue>
  <KeyInfo>
      <KeyValue>
         <DSAKeyValue>  ...  </DSAKeyValue>
      </KeyValue>
  </KeyInfo>
</Signature>
```

Web Services

XML security extensions

- XML Signature recommendation

  Base64 – `http://www.w3.org/2000/09/xmldsig#base64`

  Canonical XML 1.0 – `http://www.w3.org/TR/2001/REC-xml-c14n-20010315`

  HMAC-SHA1 – `http://www.w3.org/2000/09/xmldsig#hmac-sha1`

  RSA-SHA1 – `http://www.w3.org/2000/09/xmldsig#rsa-sha1`

  DSS (DSA-SHA1) – `http://www.w3.org/2000/09/xmldsig#dsa-sha1`

- XML Encryption recommendation

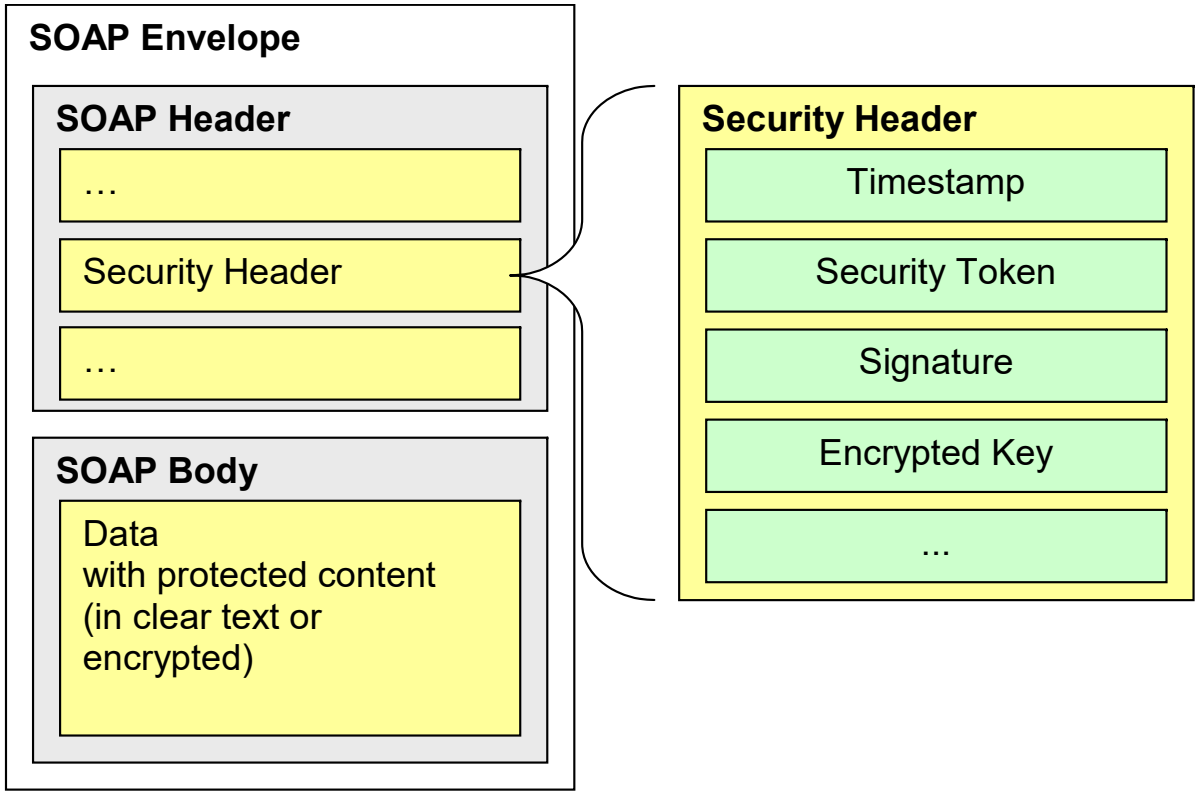
- XML Key Management Specification (XKMS)

  - using PKI (XML req for issuing, retrieving, or revoking certificates)

Web Services

WS Security specifications

- WS-Security – SOAP Message Security
  - security tokens
  - message integrity
  - message confidentiality



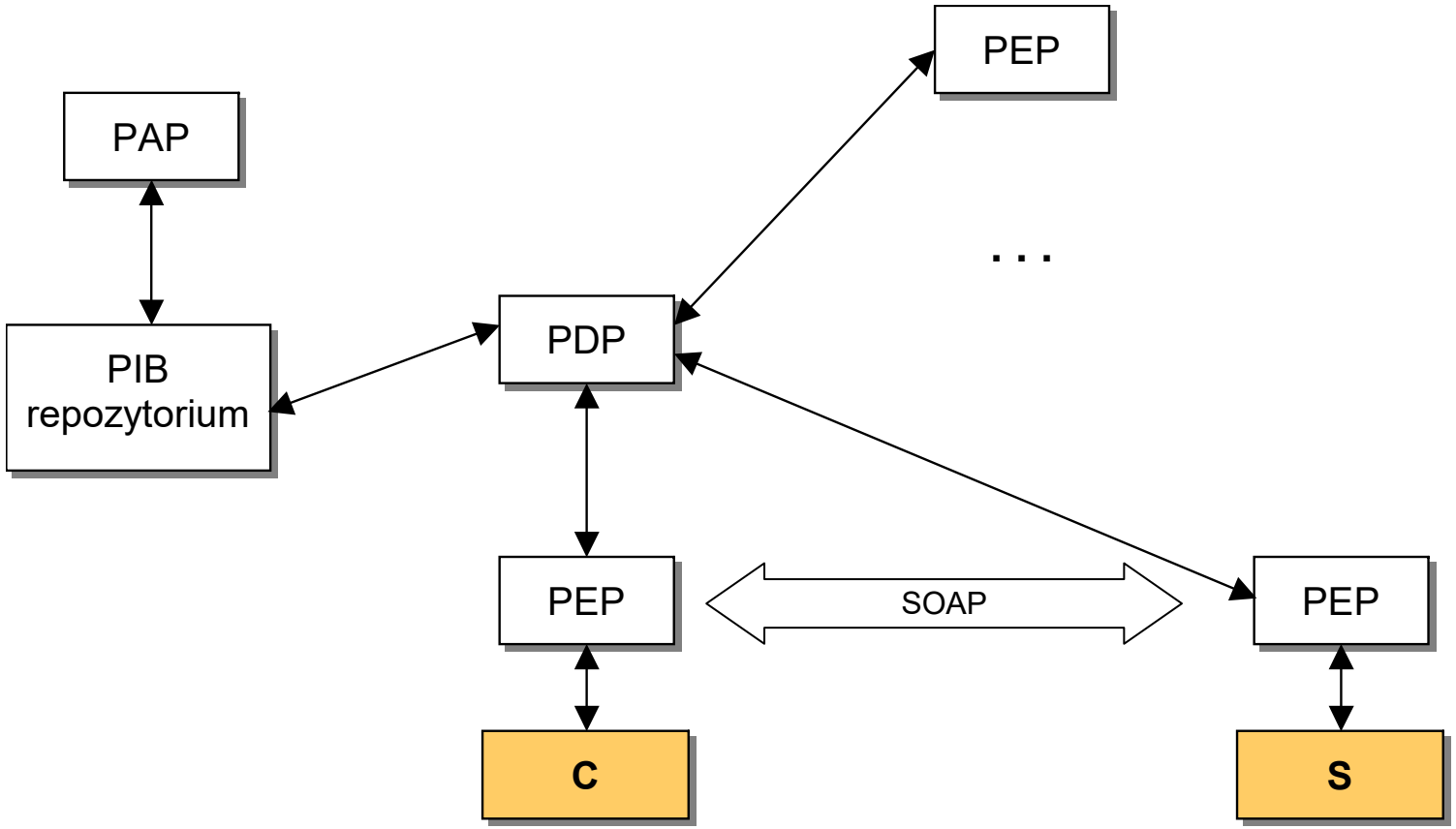
Web Services

Policies

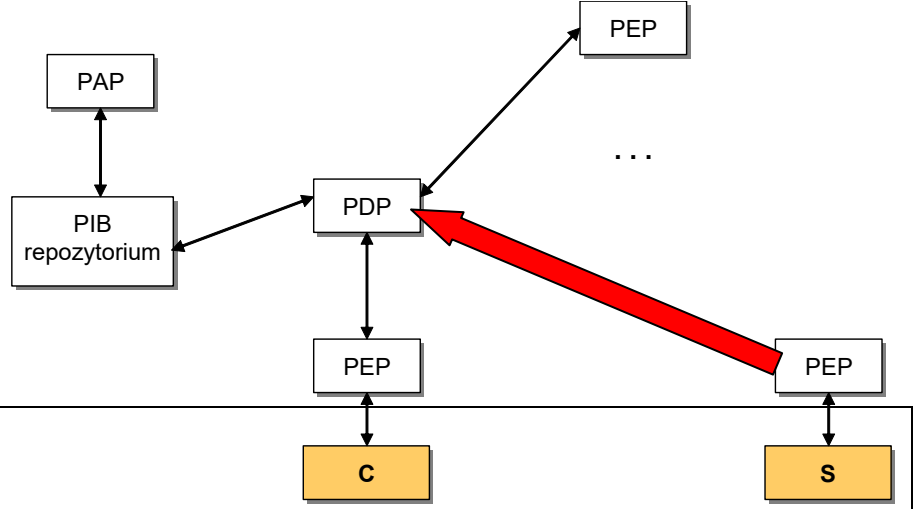
- WS-Policy / WS-PolicyAttachment
  - general model and syntax for describing the security policies
  - how to find or attach policy rules to Web Services applications
- Web Services Security Policy Language (WS-SecurityPolicy)
  - how to specify and interchange policies
- SAML (Security Assertion Markup Language)
  - acquirement and exchange of policy assertions with SOAP messages
  - authentication, attribute, authorization assertions
- XACML (eXtensible Access Control Markup Language)
  - local policy definition language

Web Services

Distributed policy model



Web Services



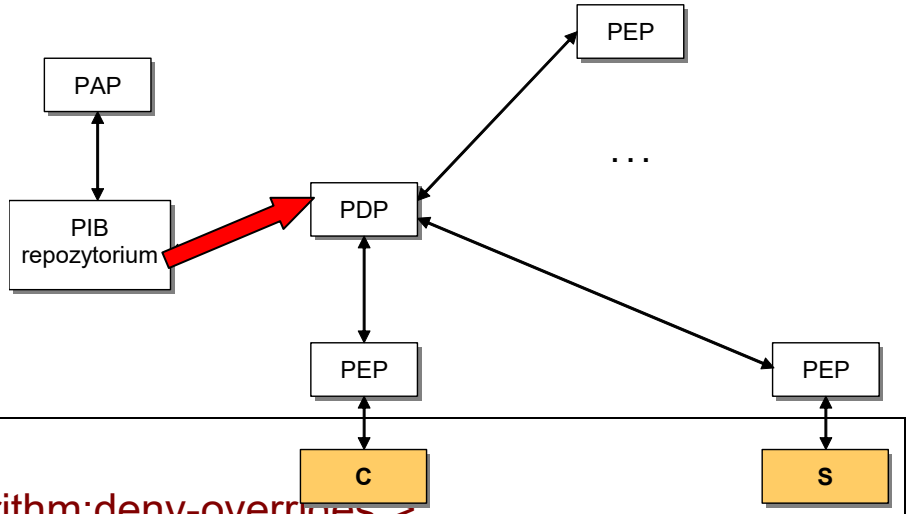
XACML request

```
<Request  xmlns=…">
 <Subject>
  <Attribute AttributeId="users_username" DataType="http://www.w3.org/XMLSchema#string">
    <AttributeValue>    root     </AttributeValue>
  </Attribute>
 </Subject>

 <Resource>
  <Attribute  AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
    <AttributeValue>      file://etc/passwd      </AttributeValue>
  </Attribute>
 </Resource>

 <Action>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
    <AttributeValue>       read     </AttributeValue>
  </Attribute>
 </Action>
</Request>
```

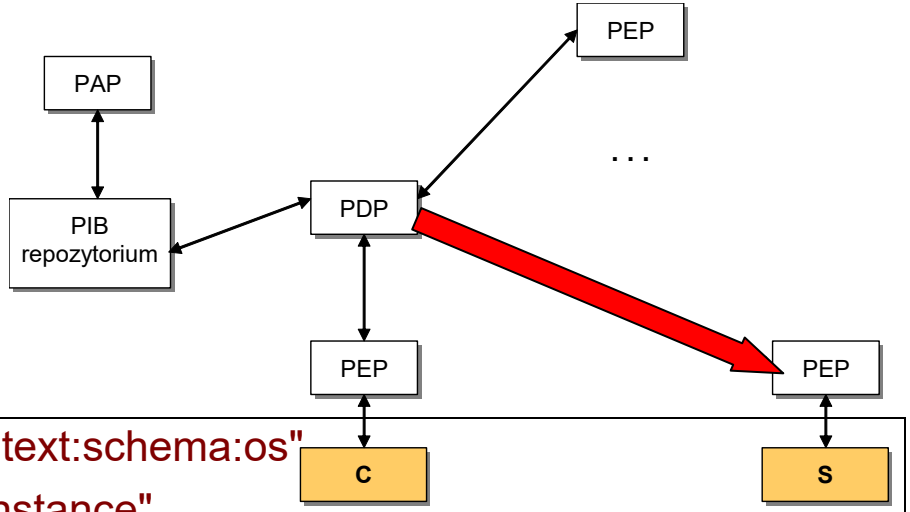
Web Services



XACML policy rule

```
<Policy xmlns=…  PolicyID=…
 RuleCombiningAlgId="identifier:rule-combining-algorithm:deny-overrides" >
  <Rule  RuleId="Rule1"   Effect="Permit">
    <Description>Użytkownik o nazwie "root" na prawo dowolnej akcji na dowolnym zasobie.</D…>
    <Subject>
      <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <SubjectAttributeDesignator  AttributeId="users_username"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
          root
        </AttributeValue>
      </SubjectMatch>
    <Subject>
    <Target/>
   …
</Policy>
```

Web Services



XACML response

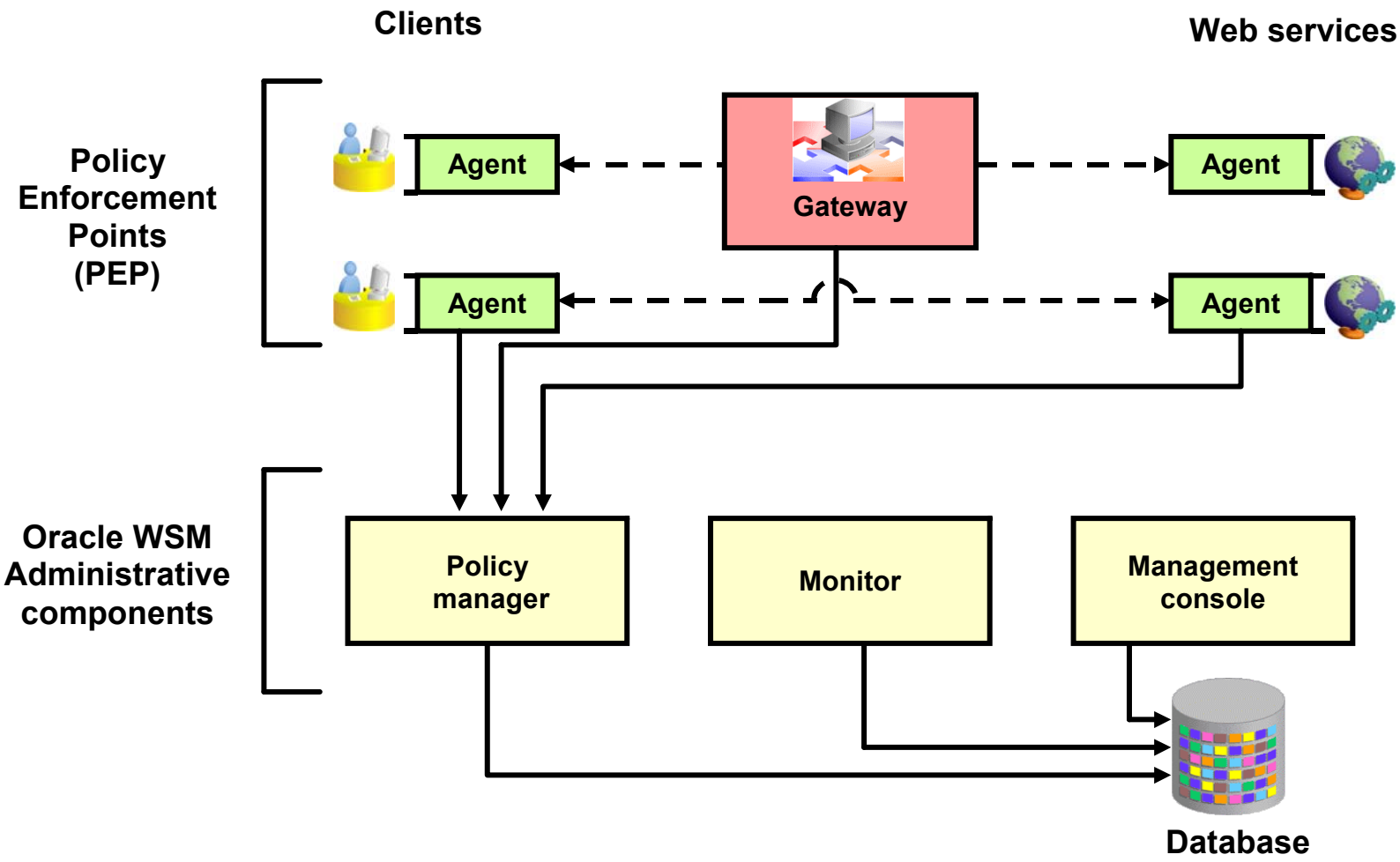
```
<Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
    http://docs.oasis-open.org/xacml/xacml-core-2.0-context-schema-os.xsd">

   <Result>
     <Decision>   Permit   </Decision>
   </Result>

</Response>
```

Web Services

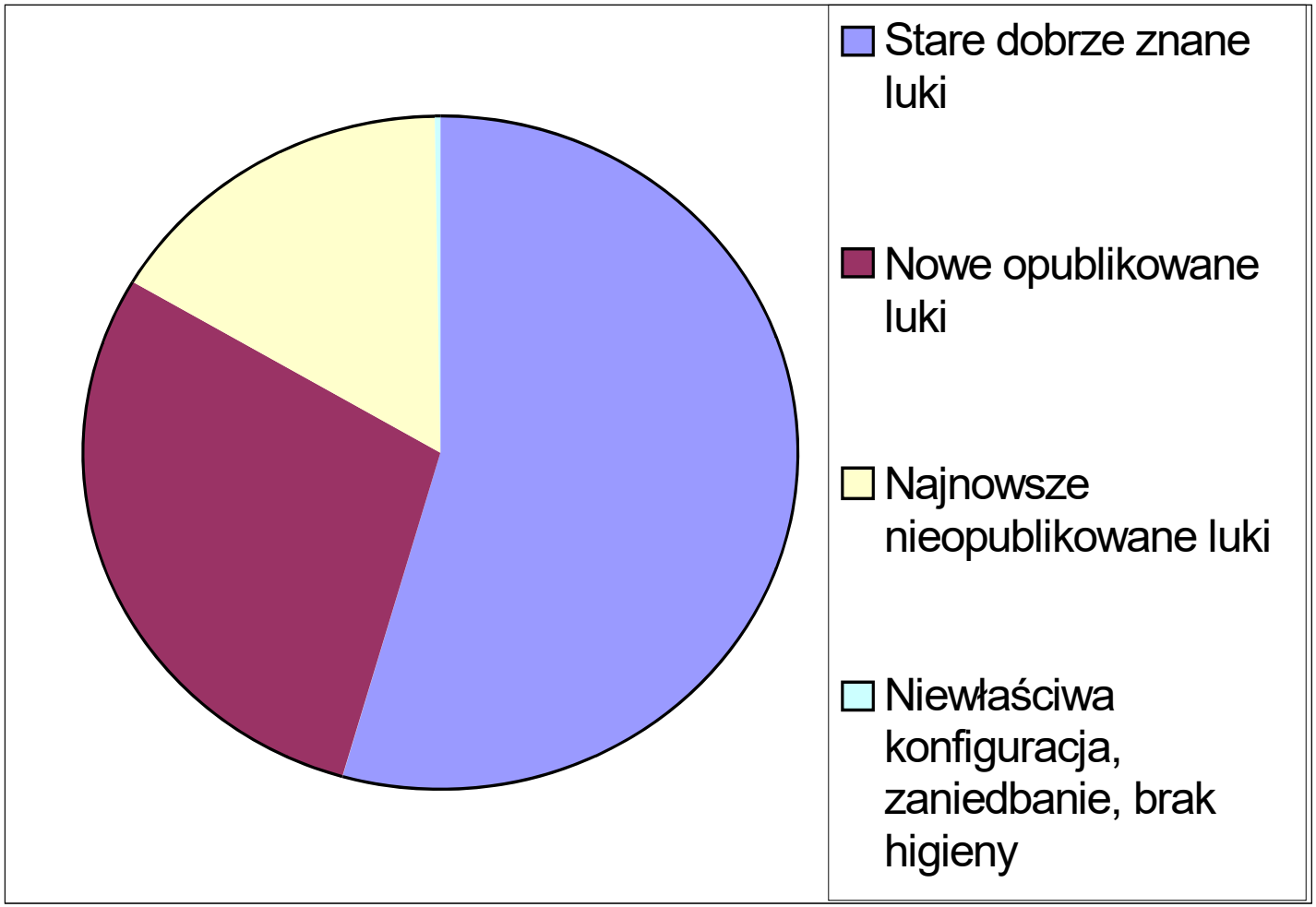
Przykład: Oracle Web Services Manager



Aktualizacja systemów

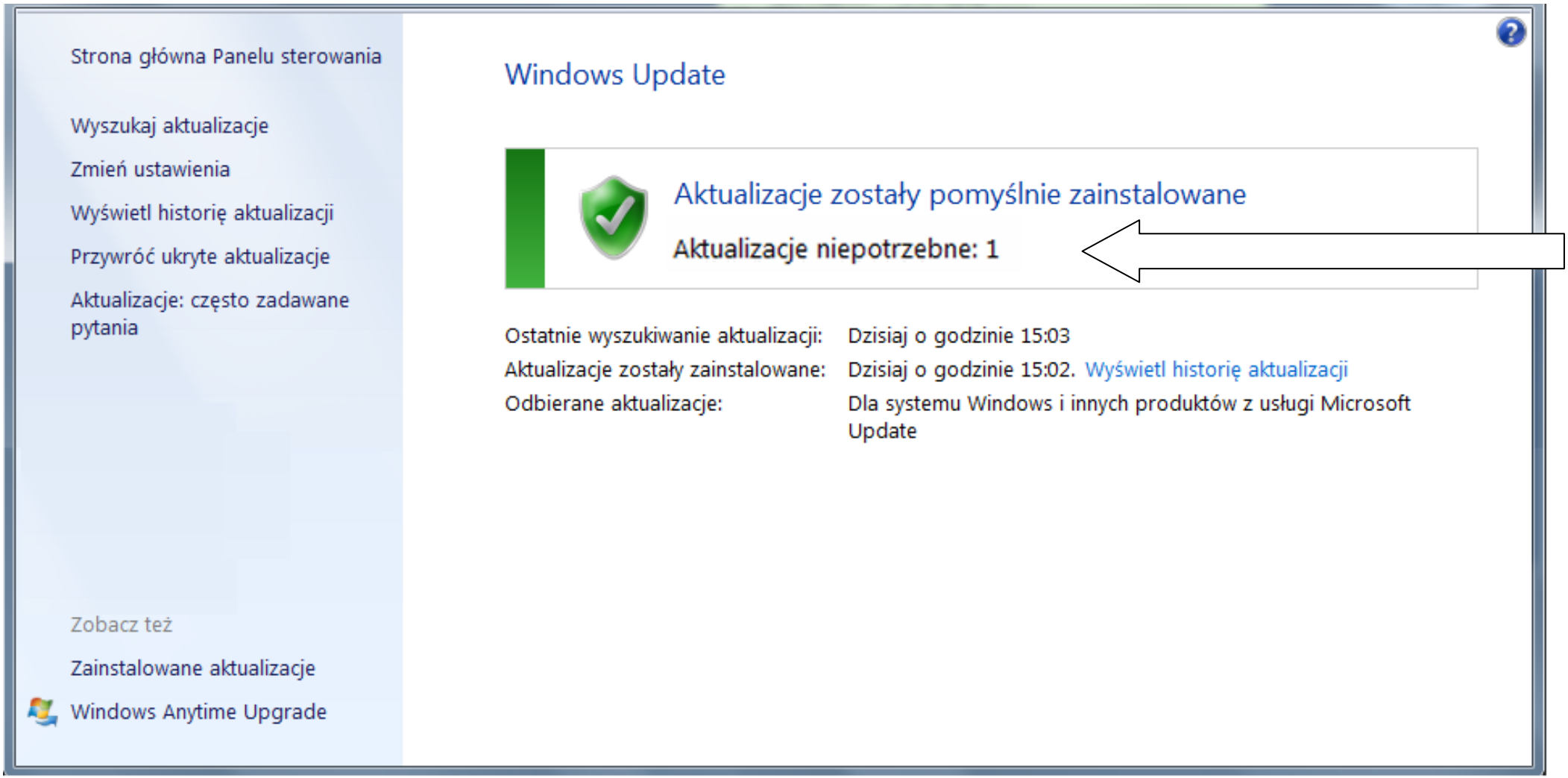
Aktualizacja systemów

Przyczyny udanych włamań:



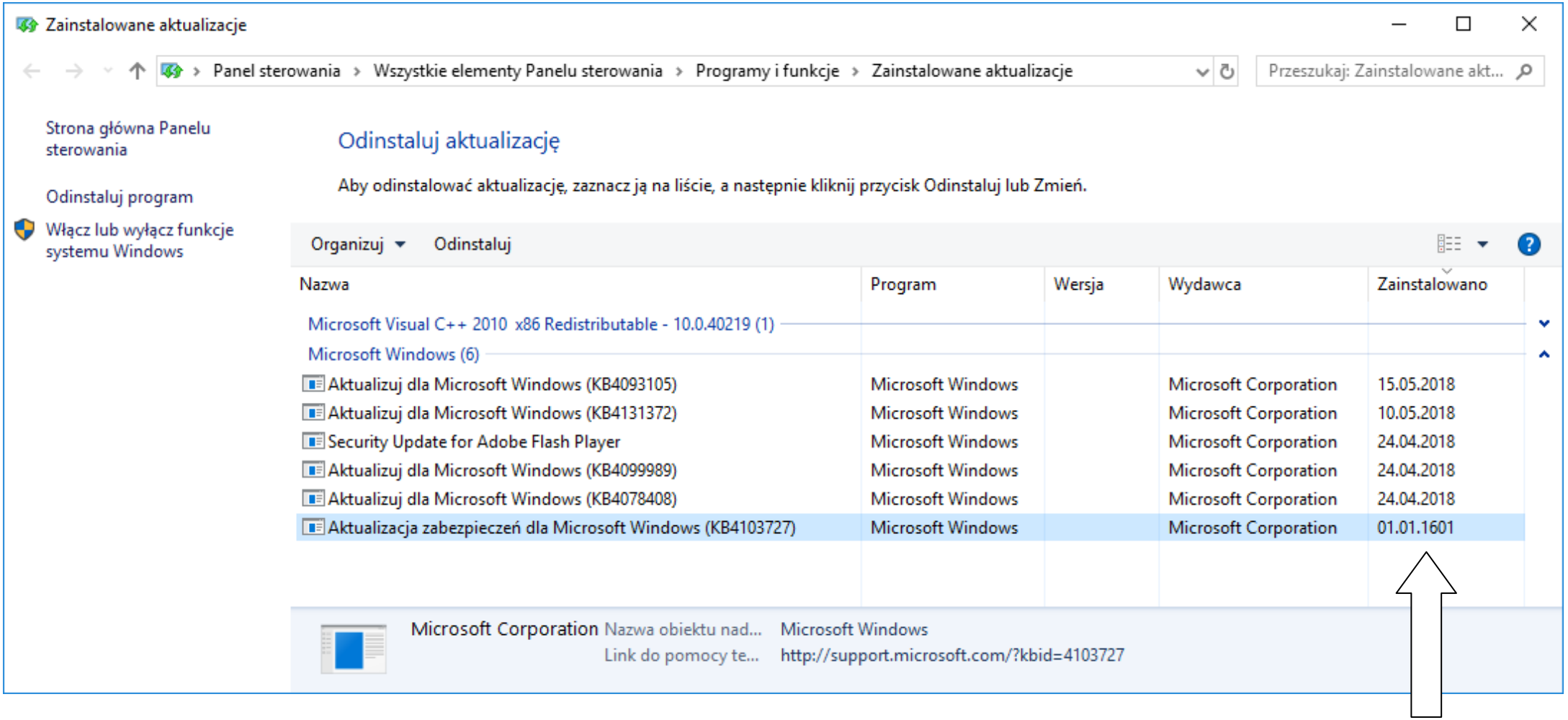
Aktualizacja systemów

Windows



Aktualizacja systemów

Windows



Zarządzanie przepływem danych, archiwizacja i kopie bezpieczeństwa

Archiwizacja danych i kopie zapasowe (backup)

Podstawowe modele archiwizacji:

- **bezpośrednio z serwera (*server-based backup*)**
  - bezpośrednio do serwera aplikacyjnego (bazy danych) dołączone są urządzenia archiwizujące (napędy pamięci masowej)
  - zapewniona spójna ochrona archiwizowanych danych
  - duża szybkość procesu archiwizacji
  - obciążenie serwera

Archiwizacja danych i kopie zapasowe (backup)

Podstawowe modele archiwizacji:

- **ze stacji sieciowej (*workstation-based backup*)**
  - urządzenia archiwizujące dołączone są do stacji sieciowej i na niej pracuje program archiwizujący
  - konieczność zapewnienia stacji archiwizującej odpowiednich przywilejów
  - możliwość archiwizowania danych z kilku serwerów, również zdalnych (a nawet innych stacji sieciowych)
  - mniejsza szybkość procesu archiwizacji przy współdzielonym ruchu sieciowym (ograniczona przepustowością sieci)
  - obciążenie sieci

Archiwizacja danych i kopie zapasowe (backup)

Podstawowe modele archiwizacji:

- **dedykowany serwer archiwizacji (*backup-server*)**
  - własny – rozwiązanie najwydajniejsze, ale i najkosztowniejsze
  - możliwe wykorzystanie usług data-store w chmurze (np. Amazon S3)

Archiwizacja danych i kopie zapasowe (backup)

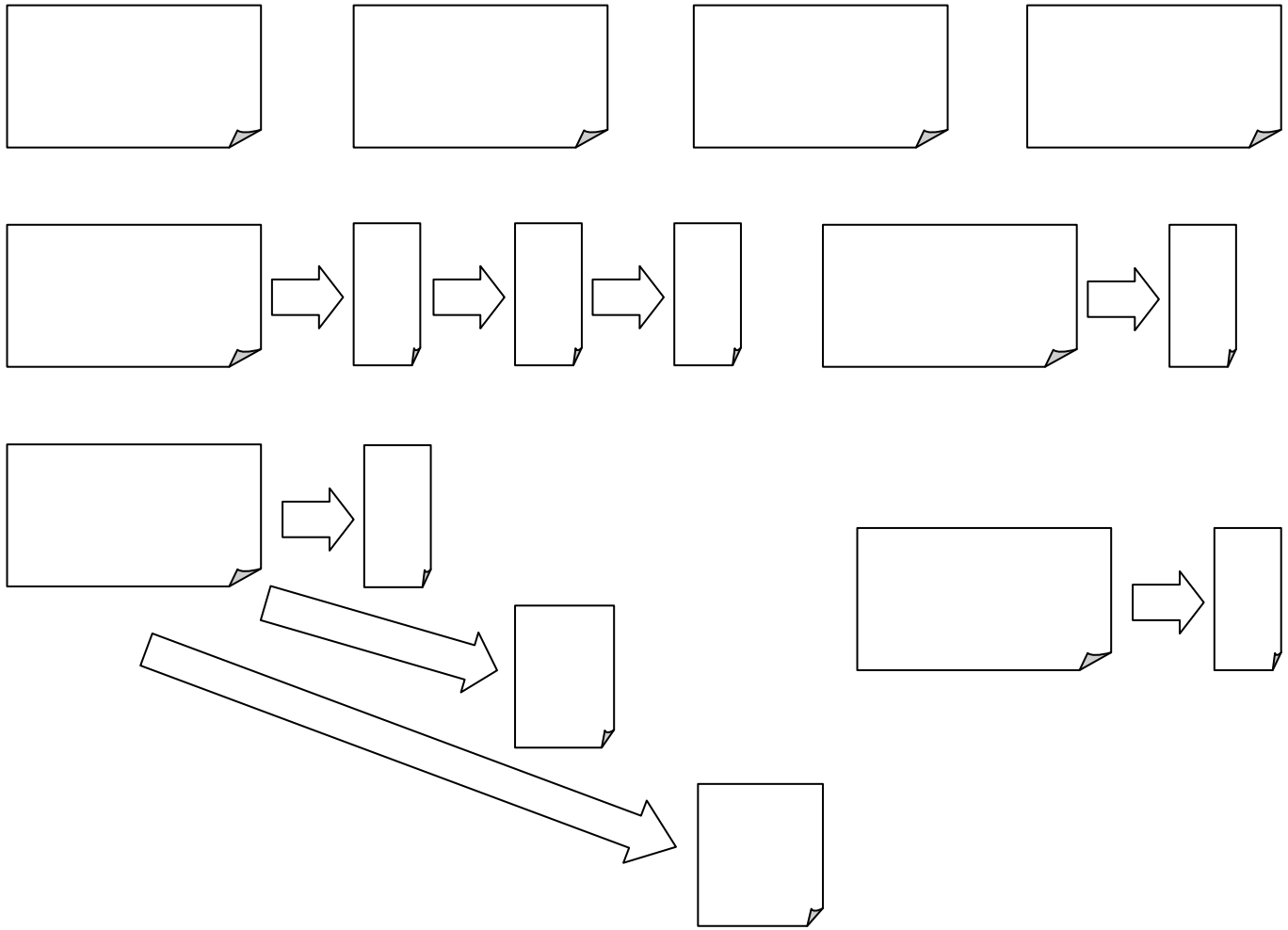
Strategie backupu:

1) pełny

2) przyrostowy

3) różnicowy

4) delta



Archiwizacja danych i kopie zapasowe (backup)

Przykładowe nośniki archiwizacji:

Streamery (dostęp sekwencyjny):

- DDS (*Digital Data Storage*) do 20GB
- DLT (*Digital Linear Tape*) do 800GB
- LTO (*Linear Tape Open*) do 12 TB

niezawodność: kody ECC

prawdopodobieństwo błędnej korekcji dla CRC-64 1 : 18 446 744 070

Dyski (dostęp bezpośredni):

- przenośne napędy dysków magnetycznych JAZ
- dyski optyczne i magnetooptyczne
  (DVD 4.7GB, DVD DL 9GB, DVD QL 17GB, BD 25GB, BD 8L 400 GB)
- pamięci flash CF 100GB, SD 2TB

Archiwizacja danych i kopie zapasowe (backup)

ILM – Information Lifecycle Management

Strategie rotacji nośników

Schemat rotacji wieża Hanoi z 5 nośnikami

Nośnik	Dzień															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	A		A		A		A		A		A		A		A	
		B				B				B				B		
				C								C				
								D								
																E

za: Przemysław Jatkiewicz „Ochrona danych osobowych”, Wyd. PTI, 2015

Archiwizacja danych i kopie zapasowe (backup)

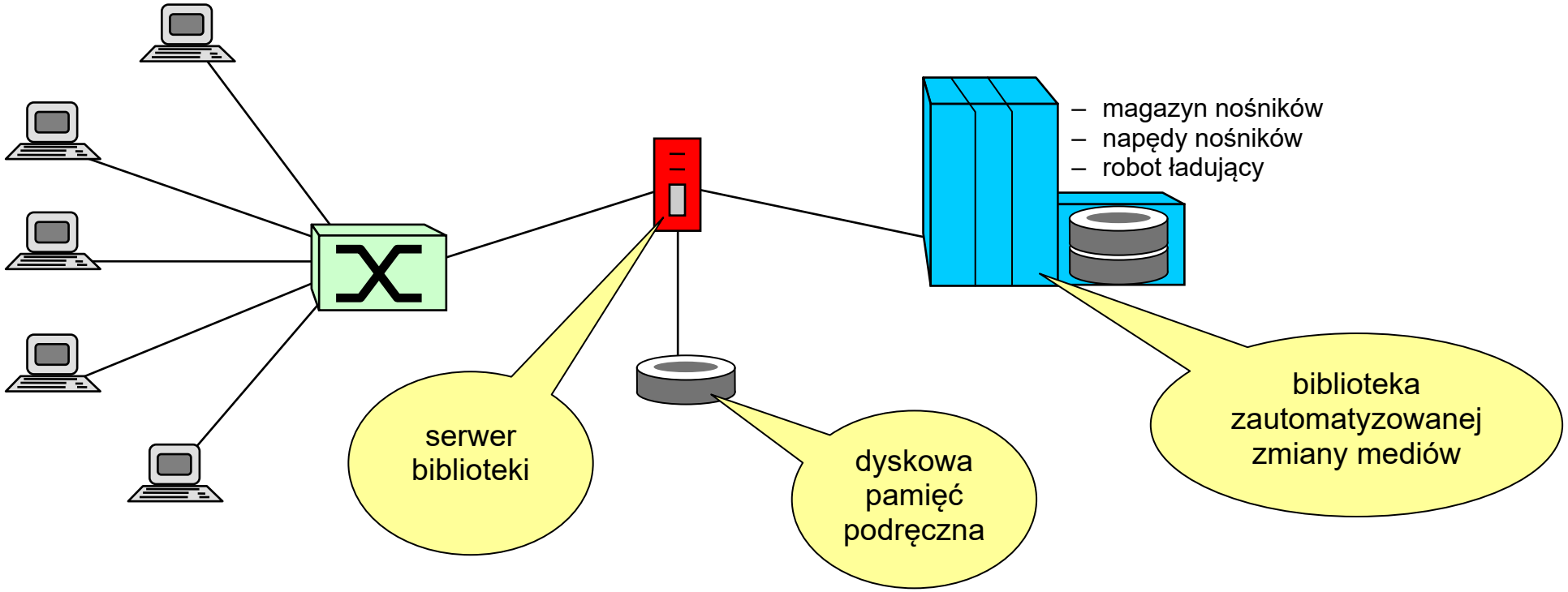
Najczęstsze błędy w procesie archiwizacji:

- brak weryfikacji poprawności sporządzanych kopii archiwalnych / zapasowych
- przechowywanie kopii w bezpośrednim sąsiedztwie archiwizowanych danych
- podłączanie nośników na stałe do backupowanego systemu ($\rightarrow$ ransomware!)

Archiwizacja danych i kopie zapasowe (backup)

Hierarchiczne systemy archiwizacji (HSM – *Hierarchical Storage Management*)

- wybór klasy nośnika w funkcji częstotliwości wykorzystania (lub ważności) danych

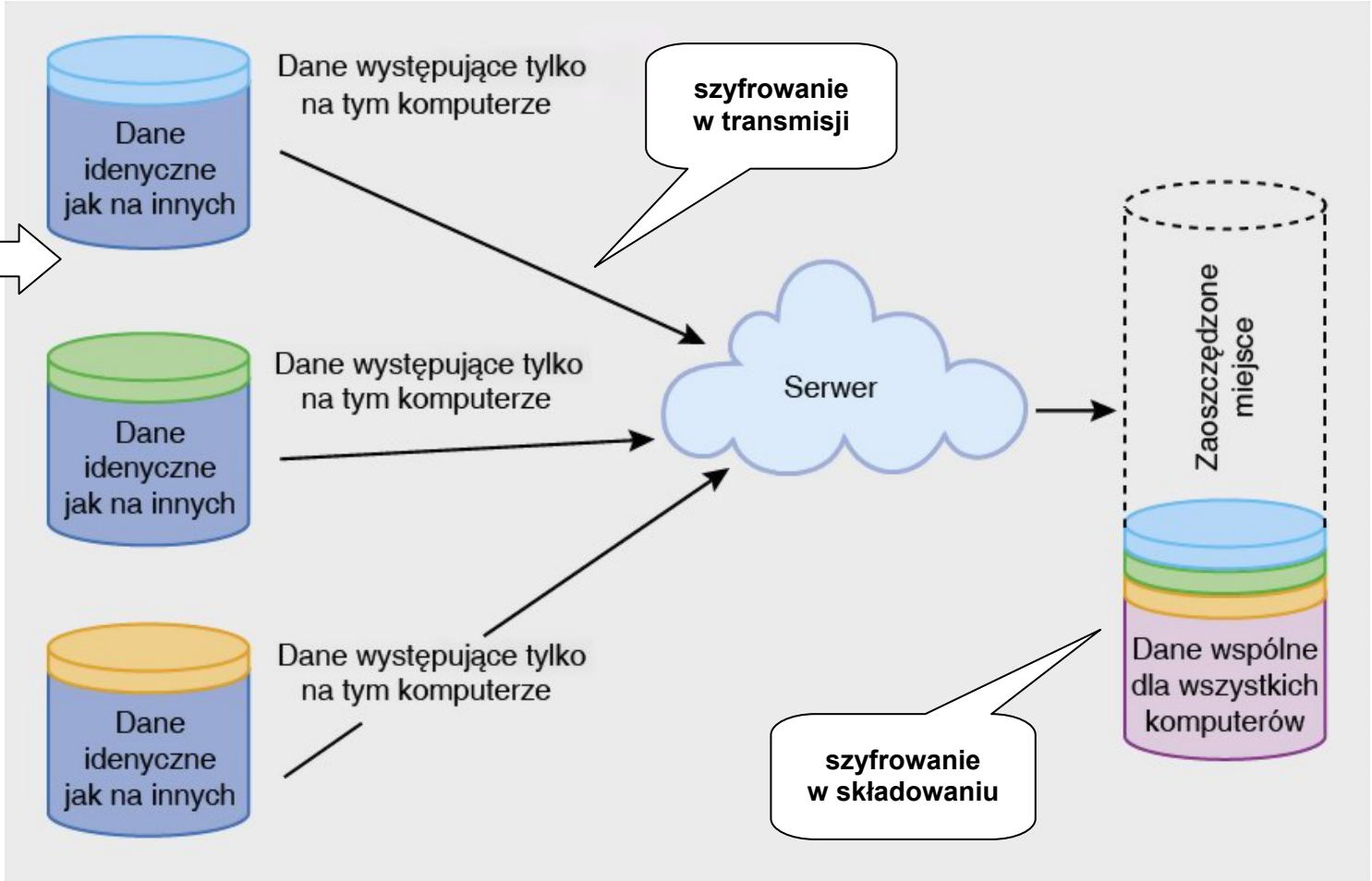


CDP

(*Continuous Data Protection*)

Ochrona danych na stanowiskach przenośnych

- kontrola dostępu
- inkrementalna archiwizacja z deduplikacją i wersjonowaniem (specyfikacja pasma sieci i ilości wersji)
- lokalny cache CDP (specyfikacja przestrzeni)

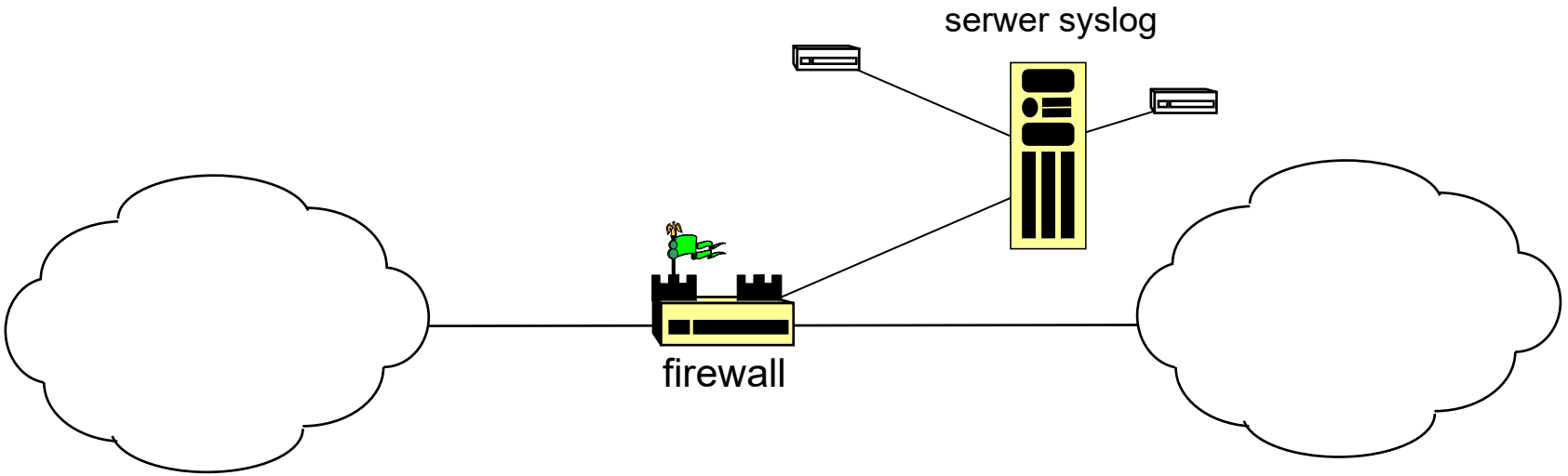


Monitorowanie bezpieczeństwa

Monitorowanie bezpieczeństwa

Alerty i rejestry zdarzeń

- wewnętrzne repozytorium (*audit-trail*) lub konsola urządzenia (np. routera, zapory)
- zewnętrzny serwer usługi syslog
- zewnętrzny monitor SNMP, NetFlow, …



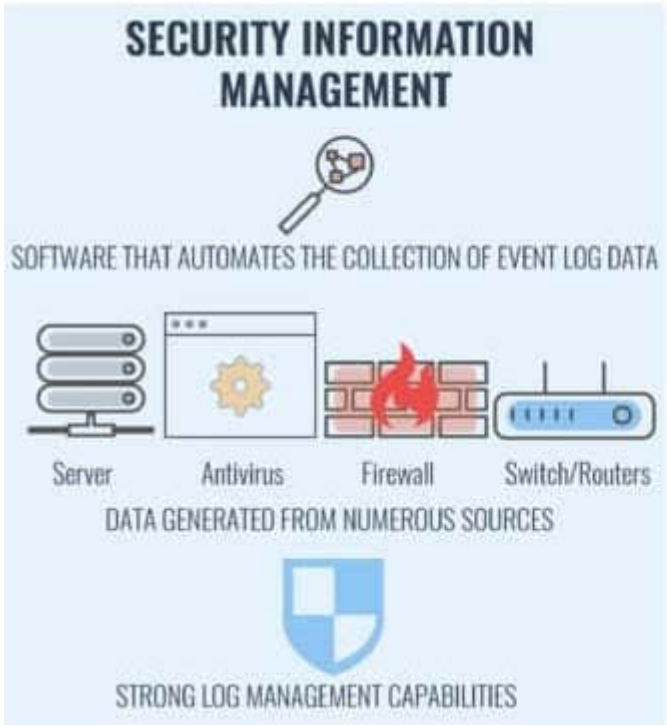
Monitorowanie bezpieczeństwa

Audyt

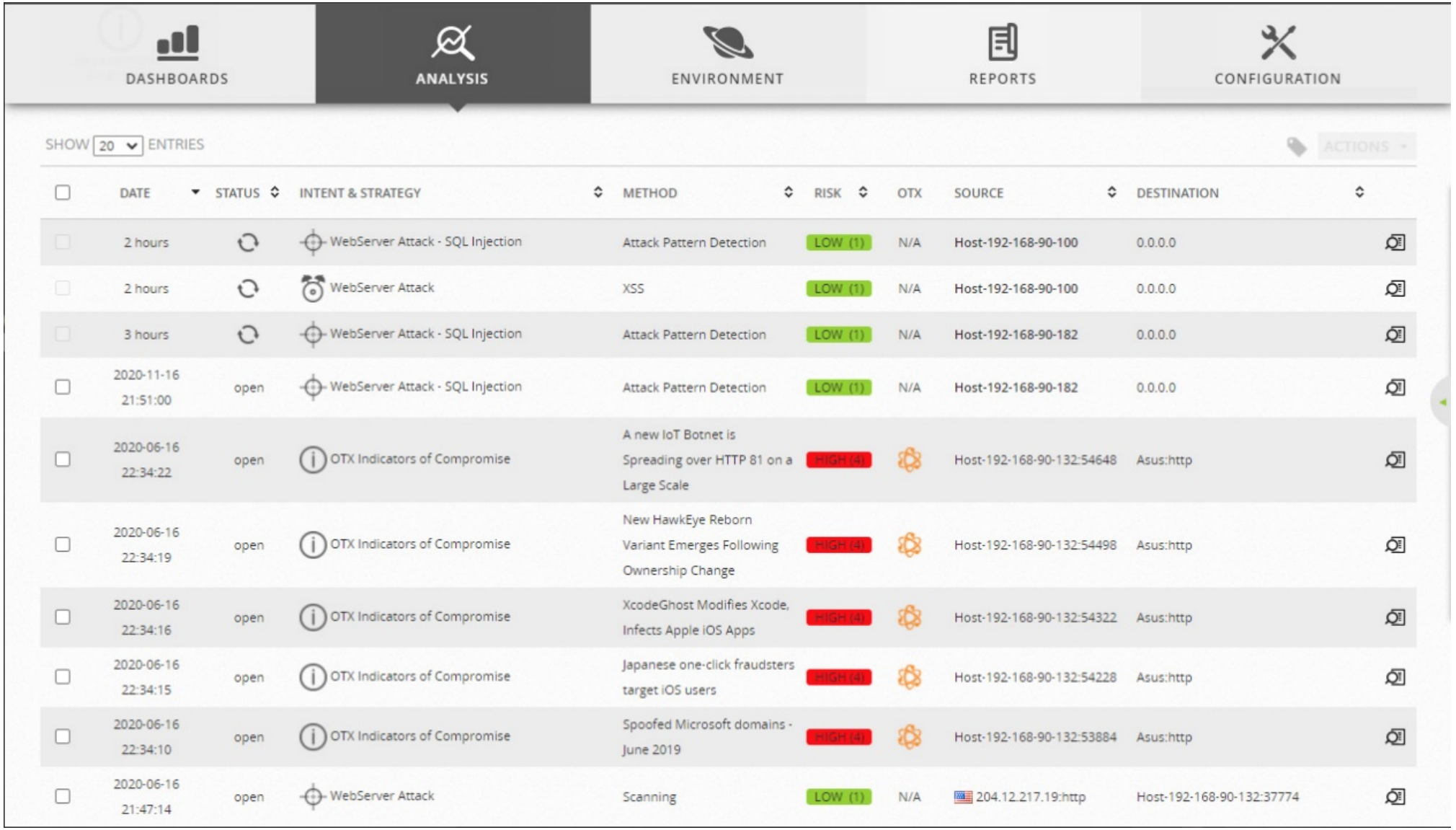
- okresowy – zlecany wyspecjalizowanym firmom zewnętrznym (brygady tygrysa)
- samodzielny – wsparcie narzędziami programowymi
- skanery logów wyszukujące luki bezpieczeństwa (*Vulnerability Assessment*)
- SIEM (*Security Information & Event Management*)
  - zbieranie rozproszonych logów
  - selekcja, katalogowanie, agregowanie
  - analiza i wychwytywanie sytuacji istotnych (powyżej zadanego progu zagrożenia)
  - wykrywanie ataków wolno rozwijających się, uczenie się
  - przykłady: IBM QRadar (pierwotnie firma Q1 Labs), NetIQ Sentinel, HP ArcSight, LogRhythm, …

Monitorowanie bezpieczeństwa

SIEM (*Security Information & Event Management*)



Monitorowanie bezpieczeństwa



DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
2 hours		WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	Host-192-168-90-100	0.0.0.0
2 hours		WebServer Attack	XSS	LOW (1)	N/A	Host-192-168-90-100	0.0.0.0
3 hours		WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	Host-192-168-90-182	0.0.0.0
2020-11-16 21:51:00	open	WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	Host-192-168-90-182	0.0.0.0
2020-06-16 22:34:22	open	OTX Indicators of Compromise	A new IoT Botnet is Spreading over HTTP 81 on a Large Scale	HIGH (4)		Host-192-168-90-132:54648	Asus:http
2020-06-16 22:34:19	open	OTX Indicators of Compromise	New HawkEye Reborn Variant Emerges Following Ownership Change	HIGH (4)		Host-192-168-90-132:54498	Asus:http
2020-06-16 22:34:16	open	OTX Indicators of Compromise	XcodeGhost Modifies Xcode, Infects Apple iOS Apps	HIGH (4)		Host-192-168-90-132:54322	Asus:http
2020-06-16 22:34:15	open	OTX Indicators of Compromise	Japanese one-click fraudsters target iOS users	HIGH (4)		Host-192-168-90-132:54228	Asus:http
2020-06-16 22:34:10	open	OTX Indicators of Compromise	Spoofed Microsoft domains - June 2019	HIGH (4)		Host-192-168-90-132:53884	Asus:http
2020-06-16 21:47:14	open	WebServer Attack	Scanning	LOW (1)	N/A	204.12.217.19:http	Host-192-168-90-132:37774

Monitorowanie bezpieczeństwa

Problemy

- m.in. zamaskowane kanały komunikacyjne:

  np. narzędzie RCovert pozwala na „podpinanie” danych pod ramki ACK protokołu 802.11 (WiFi) na ogół uważane za nieszkodliwe i pomijane przez IDS