



*short term has no future*

**DEXIA**

# Identifikácia falošných hlásení IDS

Ivan Makatura

IDC IT Security, Virtualization and Datacenter Efficiency Roadshow, Bratislava 2009

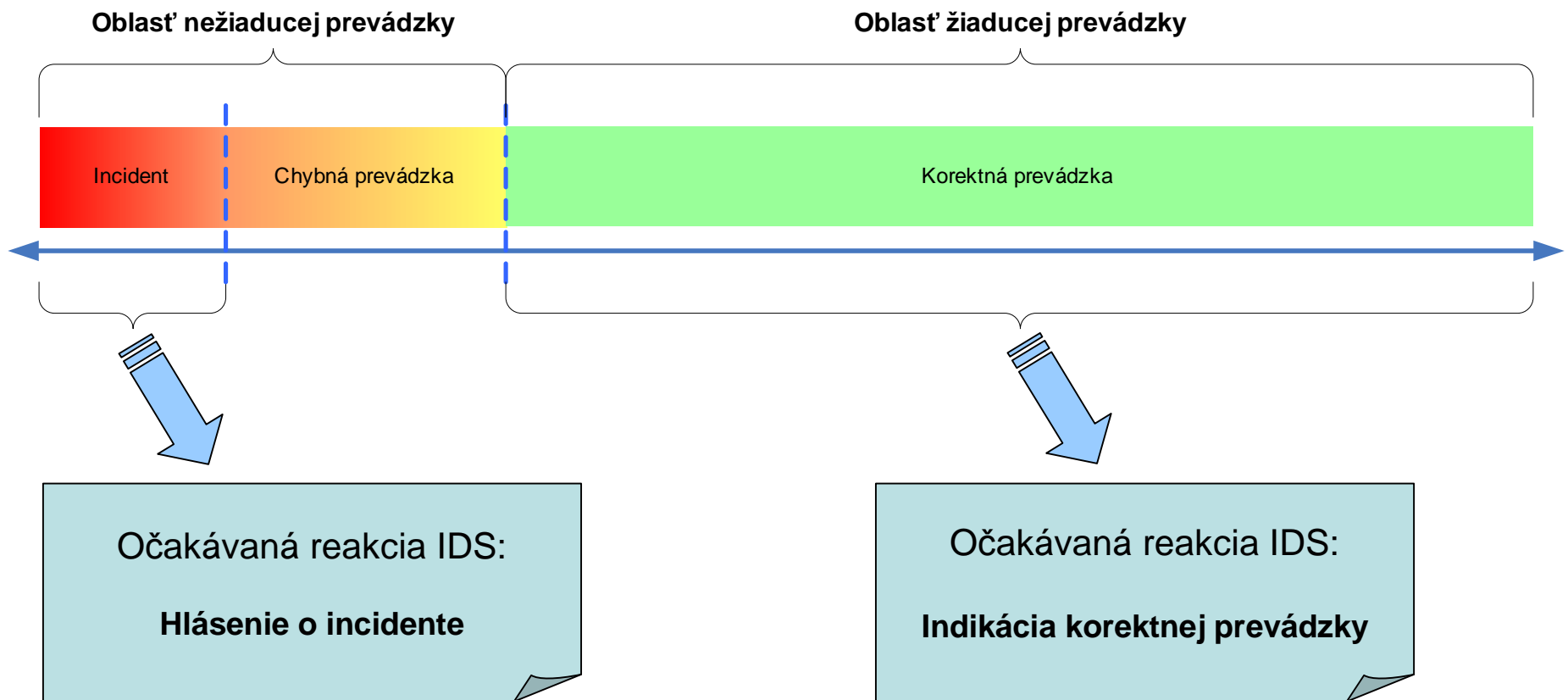
# Cieľ prezentácie

- Sieťové systémy pre detekciu prienikov (NIDS) sú považované za jednu z hlavných technológií pre zvýšenie úrovne informačnej bezpečnosti
- Očakávaný prínos IDS:
  - tvorba odôvodnených alarmov
    - v prípade výskytu incidentu
    - v prípade podozrenia na incident
- Reálne nevýhody IDS:
  - existencia falošných poplachov (tj. prípadov, keď alarm bol vygenerovaný - ale nemal byť)
  - existencia neodhalených prienikov (tj. prípadov, keď alarm nebol vygenerovaný - a mal byť)
- Prezentácia rieši:
  - Návrh rámca pre kategorizáciu hlásení IDS
  - Návrh prístupu k detekcii falošne pozitívnych a falošne negatívnych hlásení

# Základné pojmy

- **IDS** - Intrusion Detection System (systém pre detekciu prienikov)
  - softvérový alebo hardvérový nástroj (eventuálne ich kombinácia) určený na odhaľovanie neoprávnenej alebo nezvyklej aktivity počítačového systému, alebo siete
- **SIM** - (Security Information Management)
  - Systém, ktorý centralizuje a analyzuje informácie o udalostiach v sieti s možnosťou zistiť a reagovať na bezpečnostné udalosti vo chvíli ich vzniku.
  - Úloha SIM: kategorizácia, normalizácia, agregácia, korelačná analýza, vizualizácia zozbieraných udalostí
- **Očakávaný prínos IDS:**
  - generovanie odôvodnených alarmov
- **Nevýhoda IDS:**
  - existencia falošných alarmov

# Očakávané reakcie IDS



# Zdroje hlásení pre IDS

- **LOG:**

- riadkový referenčný záznam o udalostiach a aktivitách systému, aplikácie alebo užívateľa, obvykle kategorizovaný z hľadiska typu aktivity

- **Zdroje logov:**

- Logy sú produkované rôznymi informačnými zdrojmi
- Najčastejšie zdroje logov pre použitie v detekcii incidentov:
  - router, switch, firewall, sonda network-based IDS, agentová služba host-based IDS, IPS, Paketové sniffery, analyzátory protokolov, systémy pre manažment siete a sieťových zariadení, servery, pracovné stanice, produkčné systémy a produkčné aplikácie, autorizačné zariadenia a autentifikačné servery, systémy vstupovej kontroly, dochádzkové systémy, vírusové scannery, content filtre, e-mailové systémy, stand-alone aplikácie, zálohovacie systémy, monitorovacie systémy prostredia, elektronické distribučné kanály (napr. ATM, POS)

- Čím vyšší počet prispievajúcich zariadení, tým vyššia presnosť následnej analýzy

# Model reprezentácie hlásení

- Vo vyhodnocovacích systémoch sa využíva model reprezentácie znalostí klasifikáciou
- Klasifikačný problém:
  - Nech existuje množina údajov  $D=\{d_1, \dots, d_n\}$  a množina tried  $C=\{C_1, \dots, C_m\}$ . Potom **klasifikačný problém** je definovať zobrazenie  $f:D \rightarrow C$ , kde pre každé  $d_i$  je definovaná práve jedna **trieda**.
  - Trieda  $C_j$  obsahuje práve tie prvky, ktoré sa pomocou funkcie  $f$  zobrazia do tejto triedy, t.j.:  
$$C_j = \{d_i \mid f(d_i) = C_j, \text{ pre všetky } d_i \in D\}$$
- V závislosti na pozitívnom, alebo negatívnom výsledku detekcie prieniku sú možné dve akcie systému (t.j. dve triedy):
  - systém vygeneruje alarm / systém nevygeneruje alarm
  - t.j. miera chybovosti sa môže nachádzať len v dvoch triedach:



# Klasifikácia hlásení

- možné je vykonať klasifikáciu alarmov na jednotlivé triedy podľa odchýlky výsledku detekcie od reálnej existencie incidentu:

		Správnosť riešenia	
		True	False
Výsledok detekcie	Positive	<b>True positive</b> Alarm bol vygenerovaný – a aj mal byť	<b>False positive</b> Alarm bol vygenerovaný – ale nemal byť
	Negative	<b>True negative</b> Alarm nebol vygenerovaný – a ani nemal byť	<b>False negative</b> Alarm nebol vygenerovaný – a mal byť

# Kvalita prevádzky vs. klasifikácia hlásení

- **TP** - incident sa stal
- **TN** - incident sa nestal

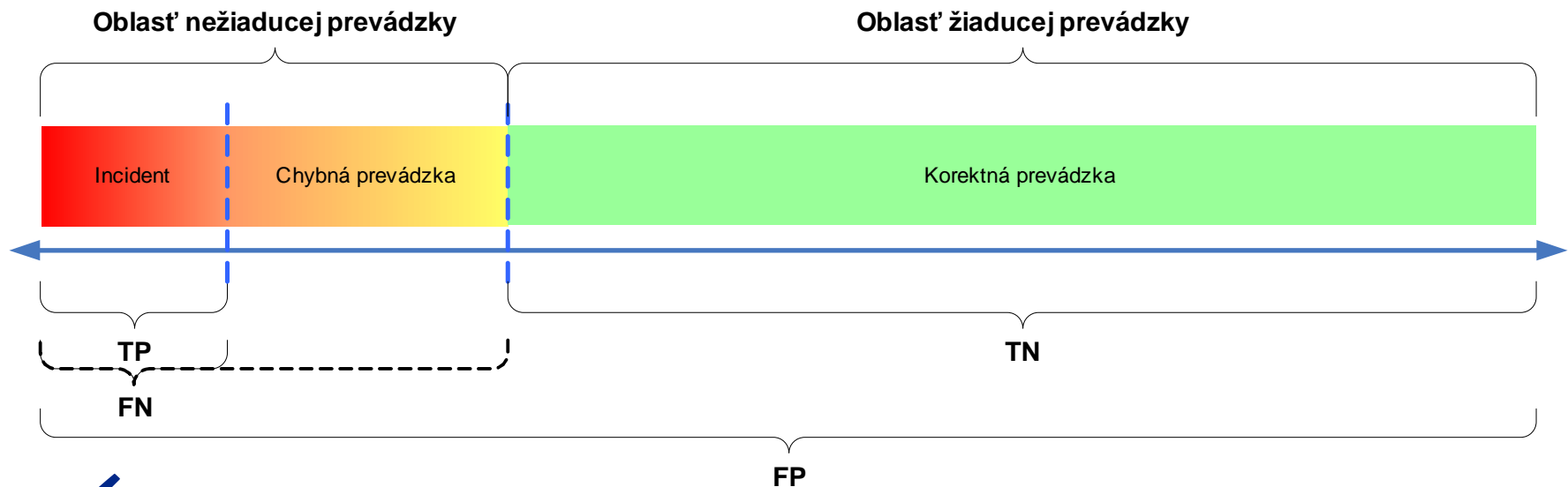
-> alarm bol vygenerovaný  
-> alarm nebol vygenerovaný

Odôvodnené  
reakcie IDS

- **FP** - incident sa nestal
- **FN** - incident sa stal

-> alarm bol vygenerovaný  
-> alarm nebol vygenerovaný

Falošné  
reakcie IDS





**Falošne negatívne hlásenia  
(False negatives)**

# Dôsledky false negative hlásení

- Nežiaduca sieťová prevádzka nie je korektne detekovaná
- Reálne prebiehajúci útok nevygeneruje žiadne hlásenie systému
- Incident je úspešný
- Znižuje sa dôveryhodnosť systému na detekciu prienikov
  
- False negative je **pasívny stav**,
  - t.j. false negative sa neprejavuje konkrétnym hlásením
- Pre identifikáciu FN je potrebné zvoliť taký prístup, v ktorom sa systematicky posúdia detekčné schopnosti NIDS v kontexte prostredia v ktorom je NIDS nasadený

# Identifikačné faktory FN hlásení

- **Rozsah monitorovanej prevádzky**
  - množina "viditeľného" toku údajov
- **Priepustnosť NIDS**
  - objem údajov, ktoré je NIDS schopné spracovať v reálnom čase
- **Účinnosť detekčných mechanizmov**
  - kvalitatívne parametre detekčných mechanizmov
- **Účinnosť reportovacích mechanizmov**
  - kvalitatívne parametre mechanizmov pre hlásenie a zobrazovanie odhalených incidentov (napr. vizualizačné schopnosti SIM)

# Identifikácia false negative hlásení

Oblasť	Spôsob identifikácie
Rozsah monitorovanej prevádzky	<ul style="list-style-type: none"><li>• identifikovať reálny rozsah monitorovanej prevádzky a porovnať ho s optimálnym rozsahom (test s predvolenými signatúrami)</li></ul>
Priepustnosť NIDS	<ul style="list-style-type: none"><li>• identifikovať výkonnostné problémy NIDS (test v hraničných hodnotách IDS)</li></ul>
Účinnosť detekčných mechanizmov	<ul style="list-style-type: none"><li>• identifikovať množinu realizovateľných útokov (emulácia útokov)</li><li>• preveriť účinnosť detekčných mechanizmov (analýza konfigurácie „choke points“)</li></ul>
Účinnosť reportovacích mechanizmov	<ul style="list-style-type: none"><li>• preveriť použiteľnosť analytického rozhrania SIM pomocou testovacích útokov („stress“ test)</li></ul>

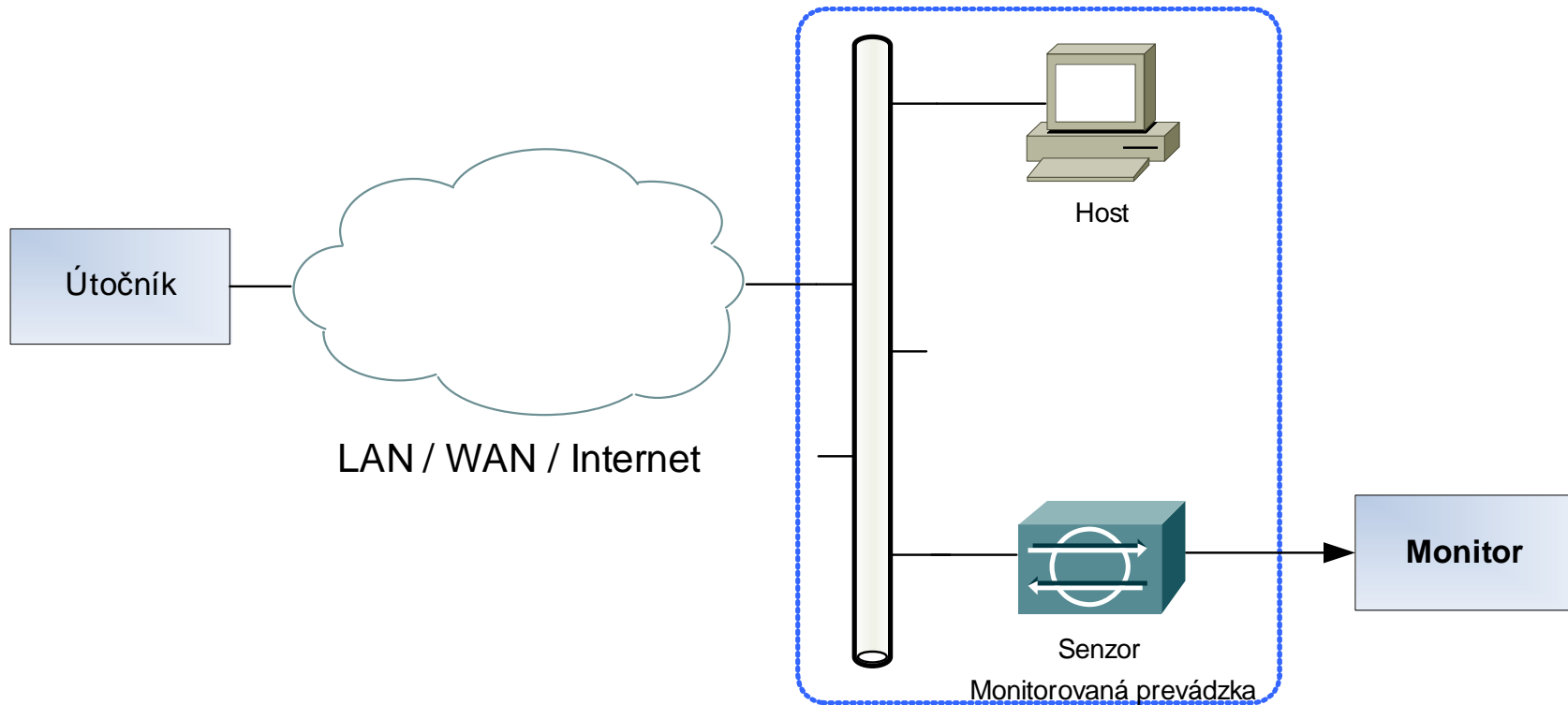
**Falošne pozitívne hlásenia  
(False positives)**

# Dôsledky false positive hlásení

- **Falošný poplach**
  - zbytočná aktivácia obranných mechanizmov a vnútorných reakčných procesov organizácie (tzv. incident response, resp. incident handling)
- **Zníženie priepustnosti NIDS**
  - zbytočne aktivované vnútorné mechanizmy NIDS, ktoré zabezpečujú zber, agregáciu a uchovanie hlásení
  - môže nastať zvýšenie objemu toku údajov a zníženie priepustnosti NIDS
- **Zahltenie obsluhy**
  - FP sú neužitočné, tzv. balastné informácie.
  - V množstve neužitočných informácií môže nastať zahltenie obsluhy NIDS
  - Zvyšuje sa potenciálne riziko neúmyselného nepovšimnutia reálne prebiehajúcich incidentov

# Scenáre NIDS:

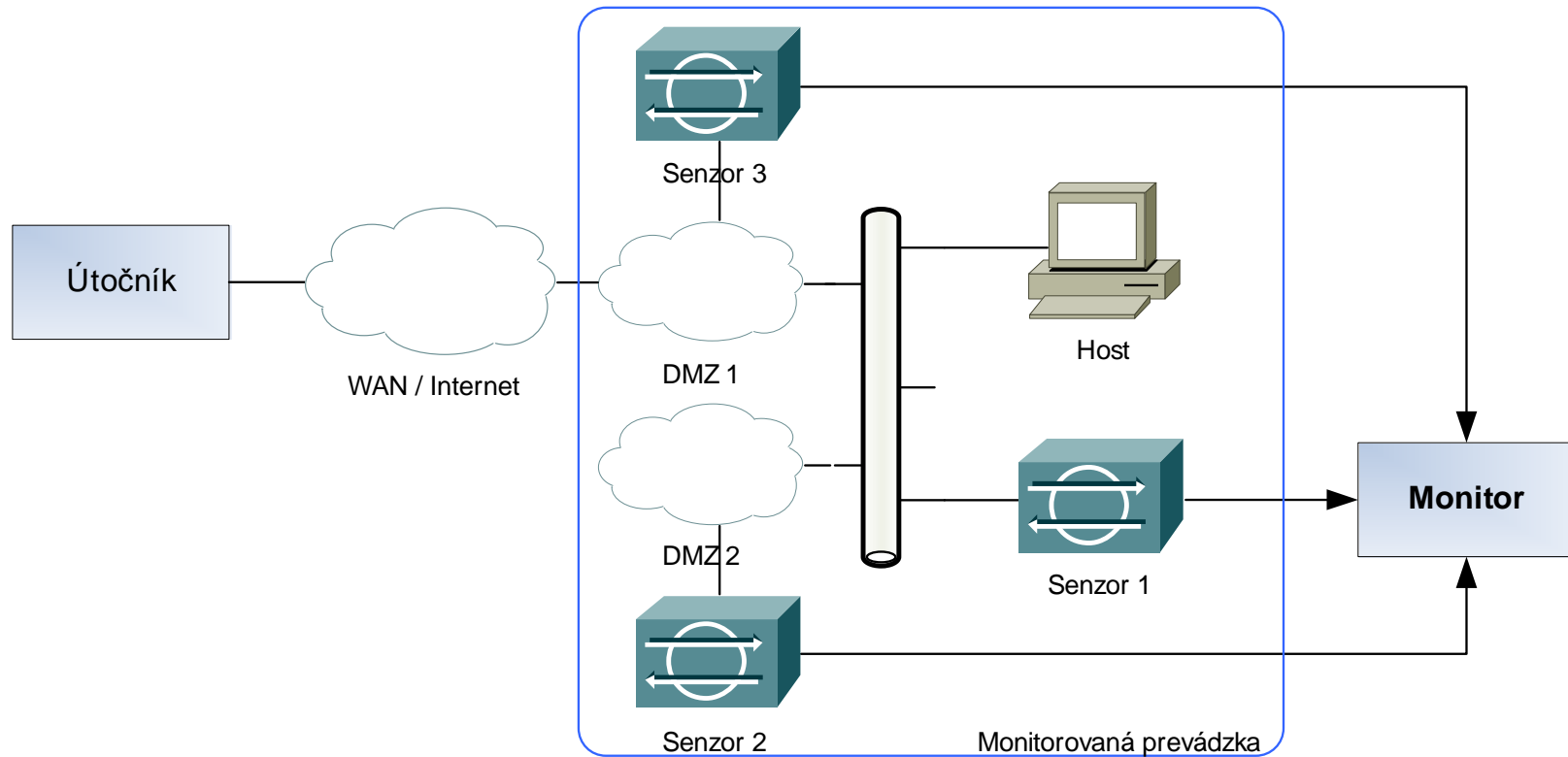
## 1. Samostatný senzor



- využíva sa iba hlásenie NIDS a známe charakteristiky prostredia:
  - informácie o pakete/streame, informácie o datových tokoch, informácie o používaných protokoloch a komponentoch prostredia, charakteristika signatúry, informácie o detekčnom mechanizme NIDS, frekvencia výskytu hlásenia, kontext ostatných hlásení NIDS, atď.

# Scenáre NIDS:

## 2. Viac senzorov a vzorka prevádzky

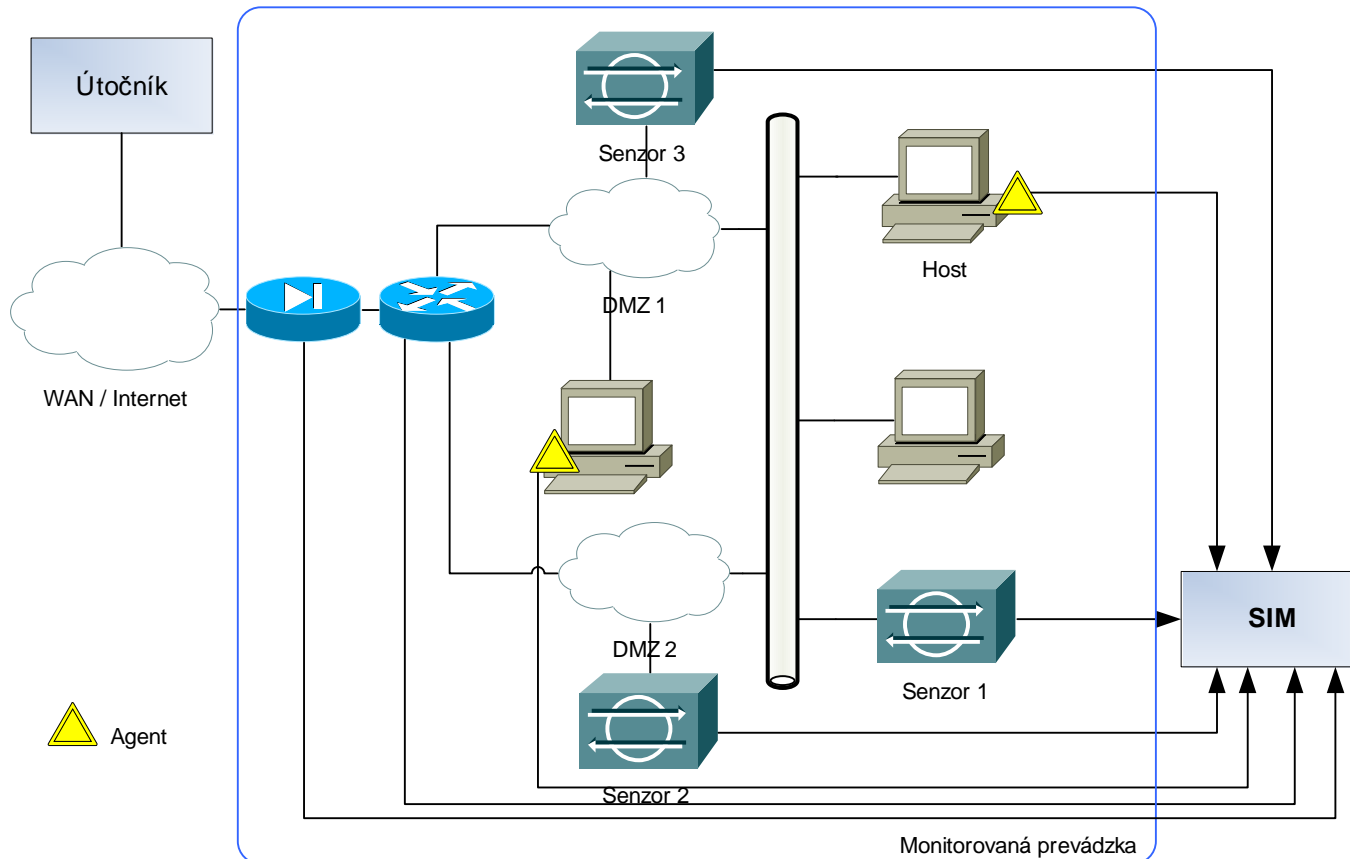


- využívajú sa rovnaké informácie ako v metodike 1,
- navyše je pre forenznú analýzu k dispozícii vzorka toku údajov resp. časť vzorky toku údajov, ktorá spôsobila alarm



# Scenáre NIDS:

## 2. Viac senzorov a SIM



- využívajú sa rovnaké informácie ako v metodike 2,
- navyše je použitý SIM, v ktorom sú k dispozícii informácie aj z ďalších zdrojov:
  - firewally, AV ochrana logy OS, úplný záznam prevádzky a pod.

# Identifikácia false positive hlásení

- **Samostatný senzor**
  - najrýchlejšia metóda detekcie
  - nízka objektivnosť (berú sa do úvahy iba sprostredkované informácie, ktoré navyiac môžu byť skreslené, alebo ovplyvnené)
- **Viac senzorov a vzorka prevádzky**
  - k dispozícii je aj pôvodný, neupravený blok údajov
  - potrebná analýza a odborná interpretácia zachytených údajov
- **Viac senzorov a SIM**
  - je možné použiť úplný archívny záznam prevádzky sniffera (bez zaťaženia NIDS) a tým zvýšiť objektivitu aj oproti metóde 2
  - v prípade, že doplnkové hlásenia iných systémov majú dostatočnú výpovednú hodnotu, nie je potrebné analyzovať zachytenú prevádzku
  - nevýhodou je vysoká náročnosť implementácie a následného prevádzkovania NIDS oproti predchádzajúcim metódam
  - pri plnom snifovaní prevádzky sú kladené enormné nároky na hardvér a skladovaciu kapacitu

- **Cieľ prevádzky IDS:**
  - presná tvorba odôvodnených hlásení v prípade výskytu incidentu
  - minimalizácia počtu falošných hlásení
- **Možné prístupy k eliminácii FP/FN hlásení:**
  - Zhrnuté v predchádzajúcej prezentácii
- **Otvorené otázky a okruhy tém súvisiacich s NIDS:**
  - hodnotenia kvality a výkonnosti IDS
  - vplyv rekonfigurácie monitorovanej sieťovej infraštruktúry na korektnú prevádzku NIDS
  - otázky architektúry a spolupráce sieťových systémov pre detekciu prienikov (NIDS) a lokálnych systémov pre detekciu prienikov (tzv. „Host-Based IDS“)
  - sémantika jazykov pre špecifikáciu incidentov
  - metodika analýza používaných formátov logov a formátov správ pre výmenu informácií a ich syntaktická normalizácia
  - agregáčné algoritmy
  - metodika pre vykonávanie záťažového testovania IDS („stress testing“)
  - analýza možných prístupov ku kategorizácii hlásení



**Ing. Ivan Makatura**  
Chief security officer  
Dexia banka Slovensko a.s.  
makatura@dexia.sk