Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Monitorovanie, zaznamenávanie a hlásenie udalostí

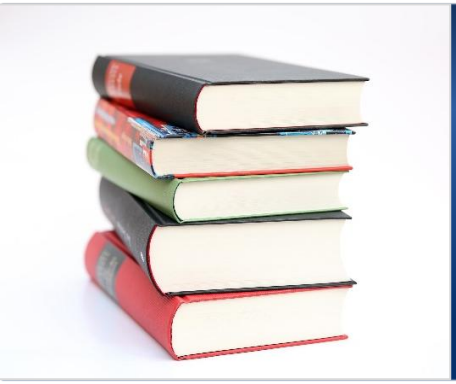
Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk



Ciele

- pochopiť, prečo sú logy a monitorovanie kľúčové pre KB vo VS,
- poznať základné princípy kvalitného logovania (čo zbierať, ako ukladať, ako zabezpečiť),
- rozumieť procesu bezpečnostného monitorovania (architektúra, nástroje, alerting, prevádzka),
- pochopiť princípy korelácie udalostí a ako z nich získať signály pre detekciu incidentov,
- získať praktický checklist a návrh jednoduchých korelačných pravidiel.

Zopár faktov na úvod

„Monitorovanie, zaznamenávanie a hlásenie bezpečnostných udalostí je kľúčovým prvkom efektívneho riadenia KB.“

Fakty:

- denne sa spracúvajú tisíce až milióny udalostí v IT infraštruktúre.
- z nich len malá časť môže znamenať KBI
- bez správneho monitorovania ich nikdy nezachytíme včas

Úlohou manažéra KB nie je tieto udalosti priamo vyhodnocovať, ale **rozumieť** **systému**, ktorý ich zhromažďuje, analyzuje a transformuje na zrozumiteľné informácie pre rozhodovanie.

Kontext a dôležitosť

- Prečo sú logy kritické:
  - forenzika,
  - audit,
  - detekcia anomálií,
  - zodpovednosť (accountability),
  - splnenie zákonných požiadaviek/súlad s normami.
- Špecifikum verejnej správy:
  - vyššie nároky na:
    - auditovateľnosť,
    - ochranu osobných údajov,
    - transparentnosť,
  - často heterogénne IT prostredie,
  - pôvodné (legacy) systémy, ktorým chýbajú funkcie moderných systémov + moderné služby.
- Výzvy:
  - množstvo dát
  - rôznorodosť formátov
  - nedostatočné retenčné politiky
  - zlé vyhľadávanie
  - únava z výstrah v rámci reakcie na incidenty (alert fatigue).

Prečo logovanie často zlyháva

- Manažéri často predpokladajú, že „***logy sa ukladajú, tak to funguje***“. Problém je, že:
  - logy sú nekompletné alebo sa prepíšu po pár dňoch,
  - nie sú centralizované,
  - chýba im korelácia,
  - nie sú chránené pred úpravou,
  - nikto ich pravidelne nevyhodnocuje.
- Výsledok: logy existujú, ale **nikto ich nečíta**.
- Až po incidente sa zisťuje, že chýbajú kľúčové údaje.

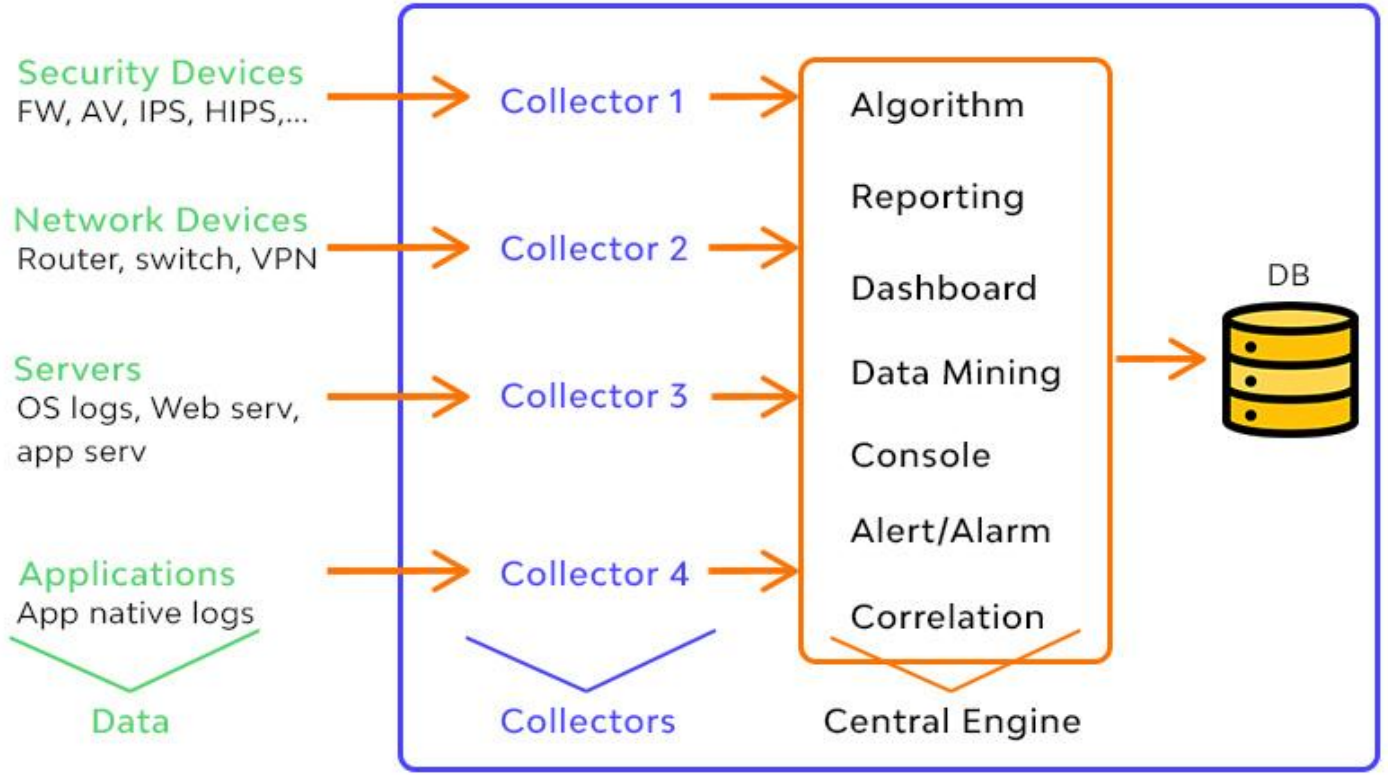
- Manažér KB nemusí nastavovať logy technicky, ale musí:
  - zabezpečiť existenciu **politiky logovania**,
  - vyžadovať **denné alebo týždenné prehľady**,
  - rozumieť **zdrojom logov** a **kto ich spravuje**,
  - poznať **proces reakcie**, ak log indikuje anomáliu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Logovanie

= systematické zaznamenávanie udalostí do log súborov

- Logy vznikajú na:
  - serveroch,
  - sieťových zariadeniach (firewally, routery, IDS/IPS),
  - aplikáciách,cloude,
  - databázach,
  - bezpečnostných systémoch (antivírusy, EDR, FW, IPS, ...).

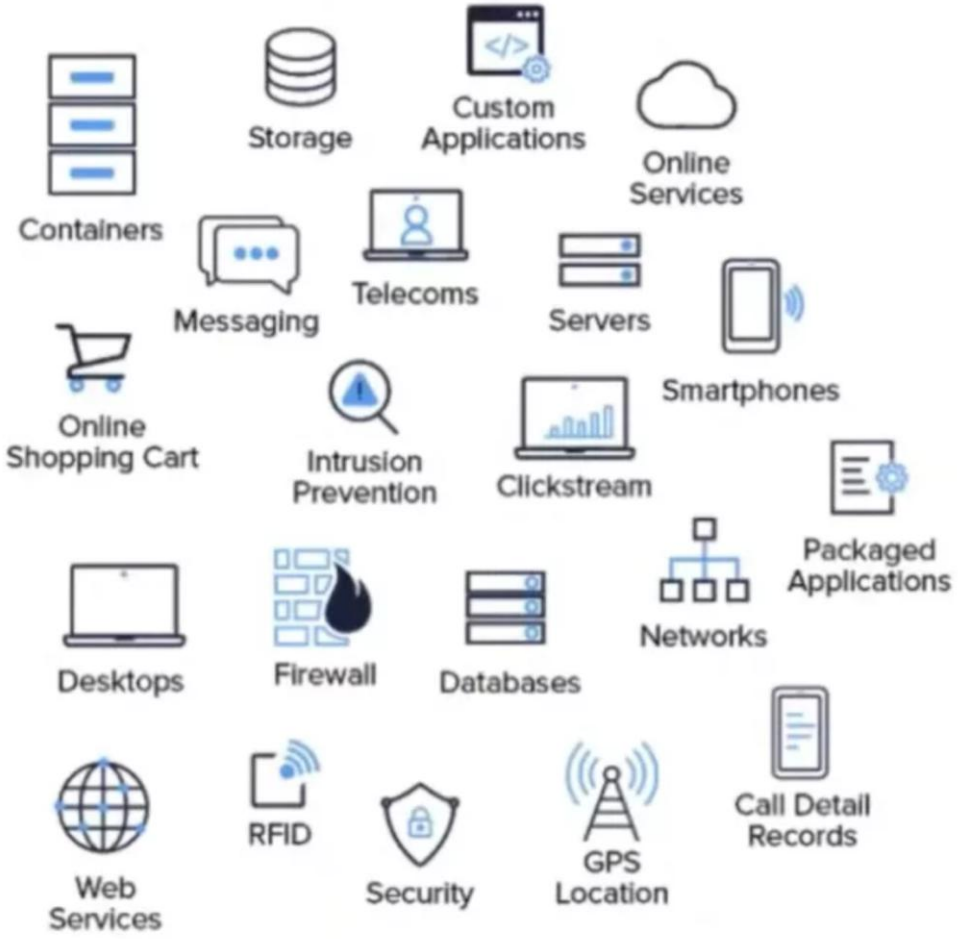


Základná myšlienka:
„Bez záznamov neexistuje dôkaz.“

- Bez logov nemožno:
  - spätne analyzovať, čo sa v systéme stalo,
  - ani dokázať, že k útoku vôbec došlo.

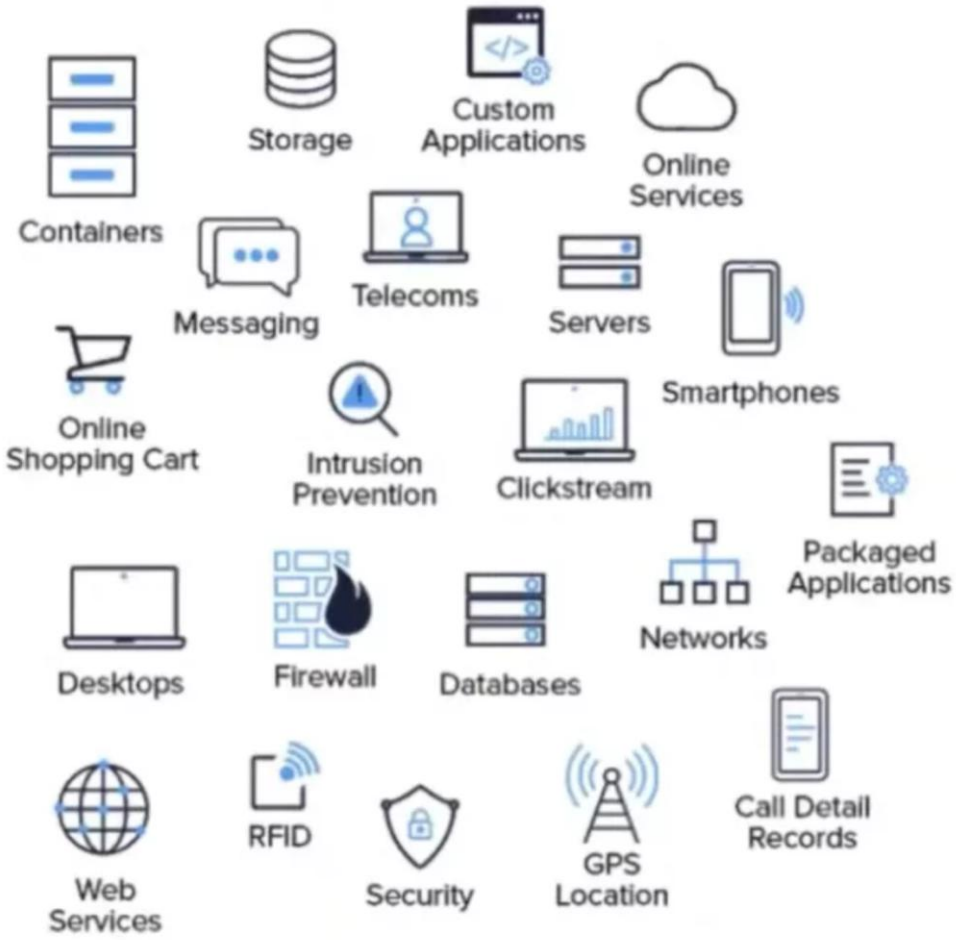
Čo logovať? (minimálne)

- Autentifikačné udalosti:
  - prihlásenia, neúspešné pokusy,
  - zmeny hesla, MFA udalosti.
- Autorizácia a prístup k citlivým zdrojom:
  - prístup k dokumentom, správam,
  - zmeny rolí.
- Zmeny v konfigurácii a správe:
  - nasadenia, zmeny konfigurácie firewallu, SIEM/IDS pravidlá.
- Sieťové udalosti:
  - začiatky/konce relácií, firewall accept/deny, DNS query (pri podozrení).
- Systémové udalosti:
  - reštarty, chyby, procesy s vysokými privilégiami.
- Aplikačné logy:
  - chyby, transakcie so záznamom identifikátora užívateľa.
- Bezpečnostné zariadenia:
  - IDS/IPS, EDR, WAF, CASB.
- Integrita a antivírus:
  - súbory karantény, hash zmeny.



Formát a štruktúra logov

- Odporúčania:
  - Preferovať štruktúrované logy (JSON, key=value, syslog, ...) pred voľným textom.
  - Základné polia: timestamp (UTC), host, service, severity/level, event_type, user_id, src_ip/dst_ip, session_id, message, correlation_id.
- Timestamp:
  - vždy v UTC + presný formát (ISO 8601 s časovou zónou).
  - Dôležité pre koreláciu medzi systémami.
- Používať konzistentné úrovne závažnosti (severity)
  - (INFO, WARN, ERROR, CRITICAL).



NSM (Network Security Monitoring)

- je koncept a proces
- predstavuje systematický prístup k **zberu, korelácii a analýze bezpečnostne relevantných údajov** zo siete a IT infraštruktúry, s cieľom:
  - získať **prehľad** o dianí v sieti,
  - včas **odhaliť** bezpečnostné incidenty,
  - podporiť **rozhodovanie** a **reakciu** na incidenty.
- **NSM pracuje s dátami ako:**
  - sieťová prevádzka (PCAP, NetFlow),
  - bezpečnostné a systémové logy,
  - alerty z IDS/IPS a ďalších bezpečnostných nástrojov.
- **NSM spája technické údaje do kontextu**, ktorý umožňuje porozumieť tomu, *čo sa v systéme skutočne deje* – nielen to, že vznikla udalosť.

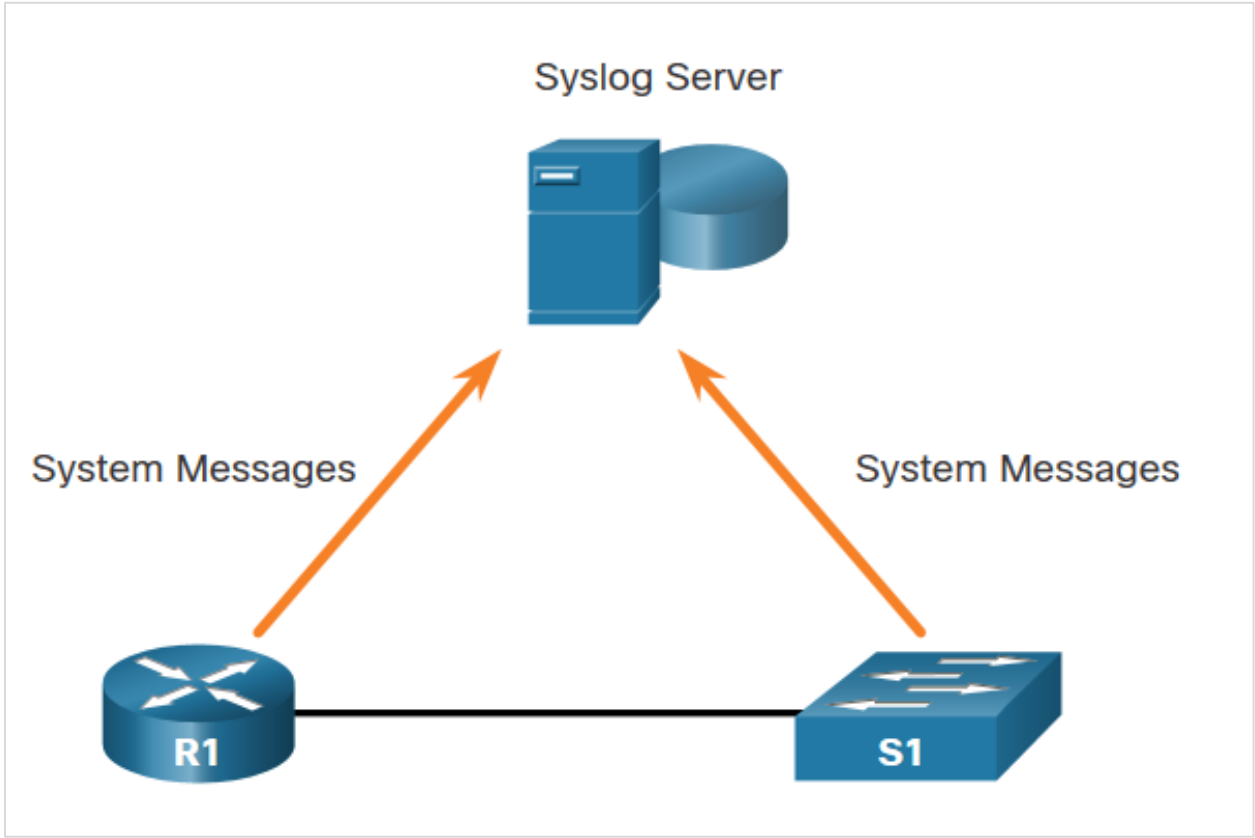
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Syslog

Logovanie

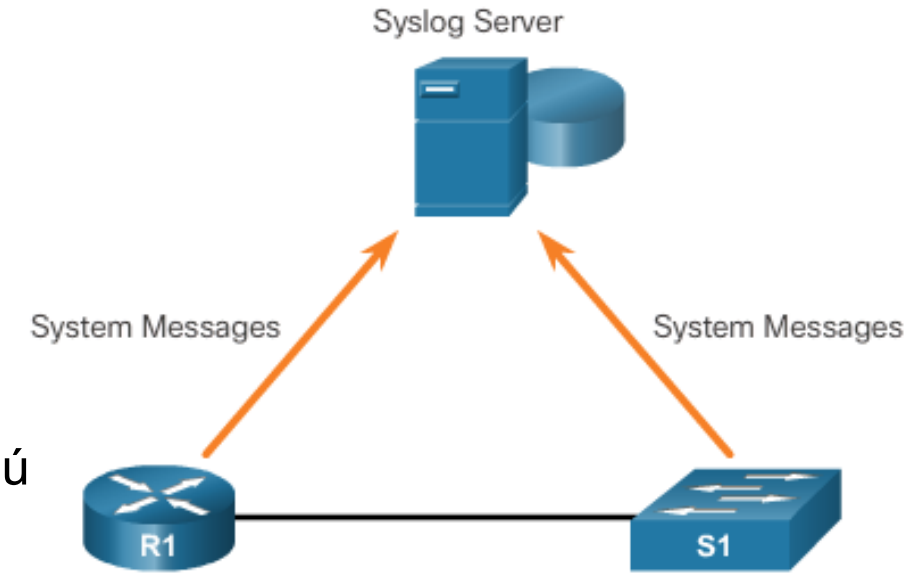
Syslog protokol

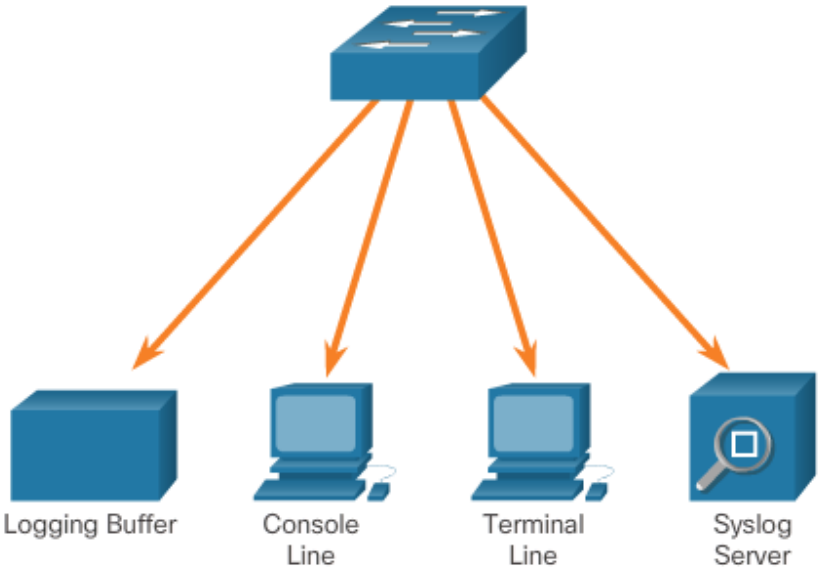
- Najbežnejšou metódou prístupu k systémovým správam
- Umožňuje sieťovým zariadeniam posielať systémové správy cez sieť na syslogové servery
- Zabezpečuje tri hlavné funkcie:
  - Schopnosť zhromažďovať logovacie informácie na účely **monitorovania** a **riešenia problémov**
  - Schopnosť **vybrať typ** zaznamenaných informácií
  - Schopnosť **určiť miesto**, na ktoré sa systémové správy majú odosielať



Syslog

- Popip protokolu Syslog (UDP/514, RFC 3164)
  - Umožňuje zariadeniam posielať správy na syslog server
  - Podporovaný väčšinou sieťových zariadení
  - Hlavné funkcie:
    - **Zber informácií** pre monitorovanie a riešenie problémov
    - Výber **typu** zapisovaných informácií ktoré sa zaznamenajú
    - Určenie **cieľa** zaznamenaných syslog správ
- Formát Syslog správy
  - Stupeň závažnosti od 0 po 7
  - Facility – identifikácia služby
- Časová pečiatka služby
  - Vylepšuje ladenie a správu v reálnom čase
  - Protokoly môžu byť označené časovou pečiatkou a je možné nastaviť zdrojovú adresu správ syslog.
  - `service timestamps log datetime msec`

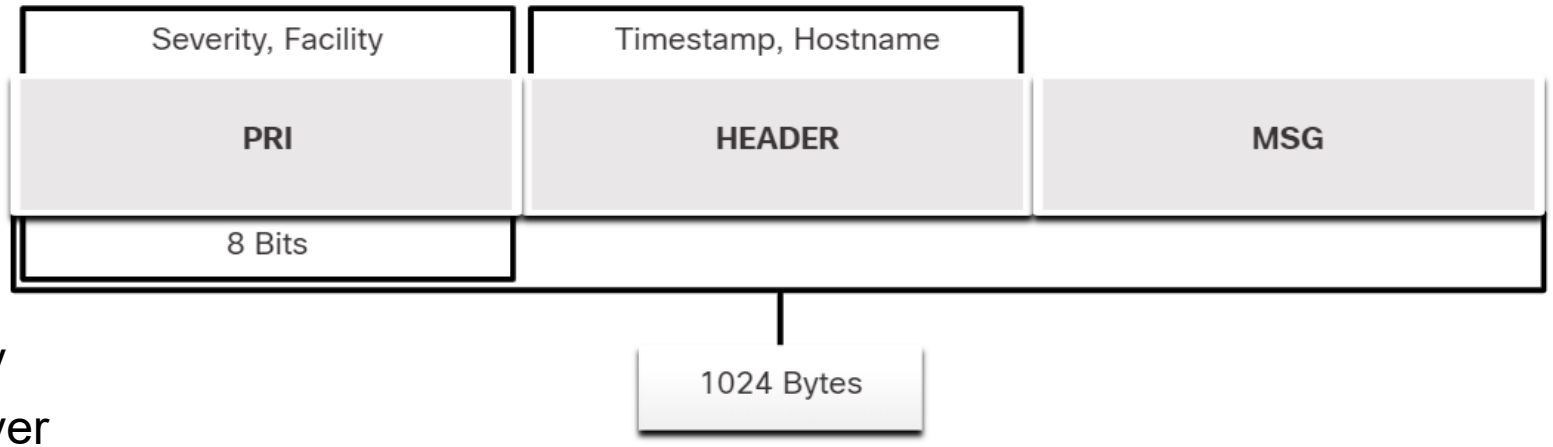




Cieľ pre syslog správy

Logy koncových zariadení

Syslog



- Syslog zahŕňa
  - špecifikácie pre formáty správ
  - aplikačnú štruktúru klient-server
  - a sieťový protokol
- Mnoho rôznych typov sieťových zariadení je možné nakonfigurovať na používanie štandardu syslog na logovanie udalostí na centralizované servery syslog. Je to protokol klient/server
- Úplný formát správy Syslog má tri odlišné časti:
  - PRI (priorita)
    - pozostáva z dvoch prvkov, Facility a Severity (Závažnosť) správy, pričom obe sú celočíselnými hodnotami
      - Facility pozostáva zo zdrojov, ktoré správu vygenerovali, ako je systém, proces alebo aplikácia
      - Severity je hodnota od 0 do 7, ktorá definuje závažnosť správy
  - HEADER
  - MSG (text správy)

Syslog (Pokr.)

Facility

- Facility kódy medzi 15 a 23 (local0-local7) nemajú priradené kľúčové slovo ani názov
  - Môžu byť priradené k rôznym významom v závislosti od kontextu použitia
- Zistilo sa, že rôzne operačné systémy využívajú obe Facility 9 a 15 na správy hodín

Facility Number	Facility Description	Facility Number	Facility Description
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	**security/authorization messages	16	local use 0 (local0)
5	messages generated internally by Syslog	17	local use 1 (local1)
6	line printer subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 3 (local3)
8	UUCP subsystem	20	local use 4 (local4)
9	clock daemon	21	local use 5 (local5)
10	security/authorization messages	22	local use 6 (local6)
11	FTP daemon	23	local use 7 (local7)

Syslog (Pokr.)

Severity

Hodnota	Severity
0	**Emergency**: systém je nepoužiteľný
1	**Alert**: akcia sa musí vykonať okamžite
2	**Critical**: kritické stavy, ktoré by mali byť okamžite napravené a signalizujú poruchu v systéme
3	**Error**: porucha, ktorá nie je naliehavá, by mala byť vyriešená v danom čase
4	**Warning**: chyba momentálne neexistuje; ale v budúcnosti sa vyskytne chyba, ak sa daný stav nevyrieši
5	**Notice**: udalosť, ktorá nie je chybou, ale považuje sa za neobvyklú. Nevyžaduje okamžitú akciu.
6	**Informational**: správy týkajúce sa bežnej prevádzky
7	**Debug**: správy zaujímavé pre vývojárov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Syslog (Pokr.)

Priority

- Hodnota Priority (PRI) sa vypočíta vynásobením hodnoty Facility číslom 8, a jej pripočítaním k hodnote Severity, ako je uvedené nižšie

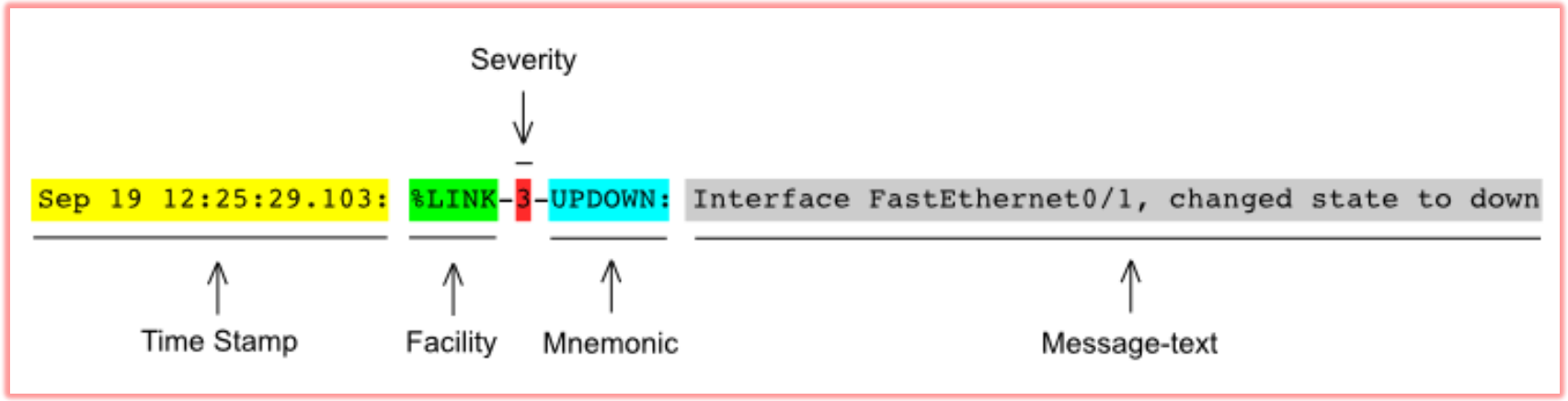
Priority = (Facility * 8) + Severity

- Hodnota Priority je prvou hodnotou v pakete a nachádza sa v zátvorkách <>

Nižšie je uvedený zoznam RFC, ktoré definujú protokol Syslog:

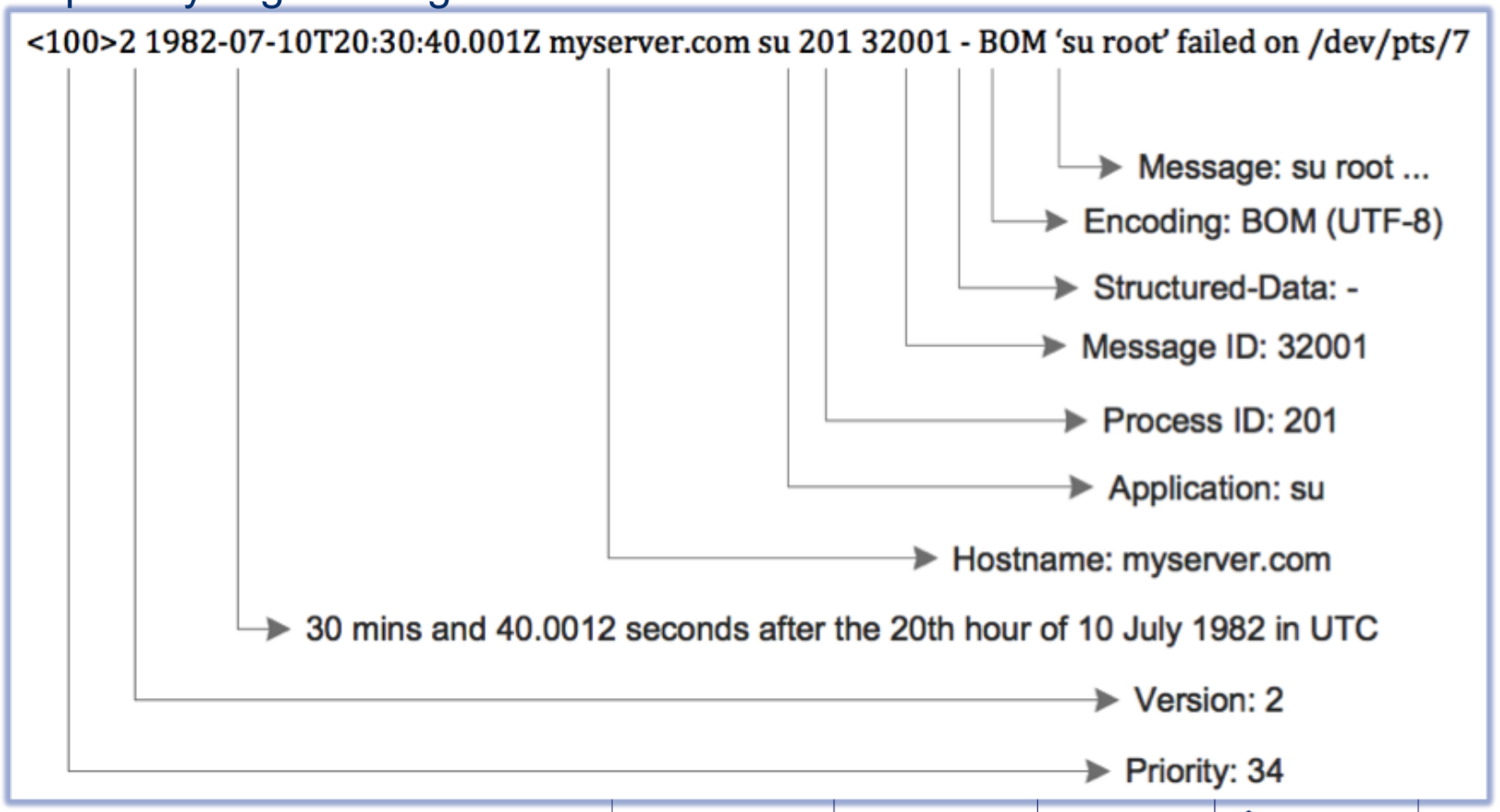
- RFC 3195 *Reliable Delivery for Syslog*
- RFC 5424 *The Syslog Protocol*
- RFC 5425 *TLS Transport Mapping for Syslog*
- RFC 5426 *Transmission of Syslog Messages over UDP*
- RFC 5427 *Textual Conventions for Syslog Management*
- RFC 5848 *Signed Syslog Messages*
- RFC 6012 Datagram Transport Layer Security (DTLS) *Transport Mapping for Syslog*

Syslog



Cisco IOS syslog message

Rapid7 syslog message



Rôzne projekty: syslog, rsyslog, syslog-ng

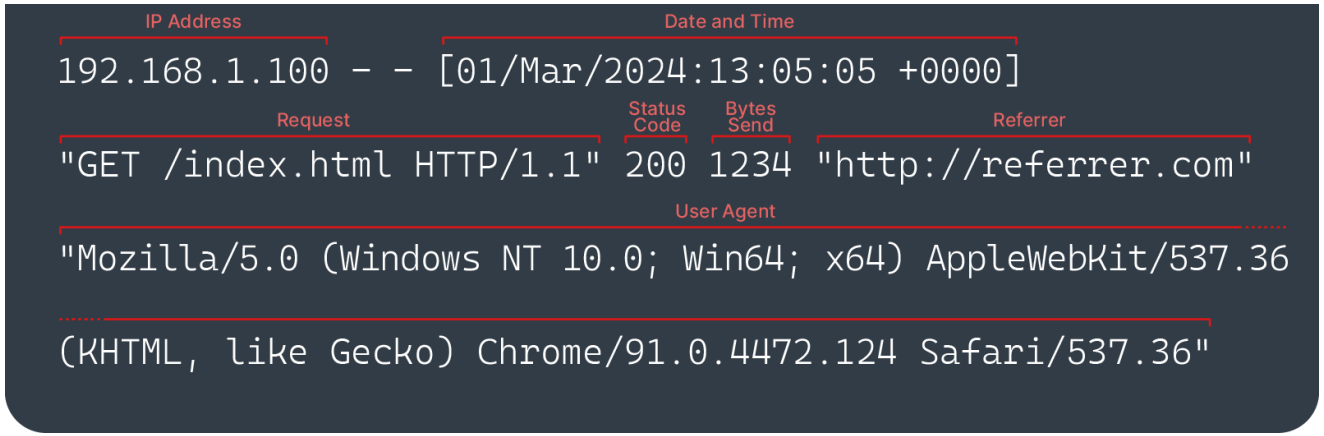
- všetky umožňujú získavanie údajov z rôznych typov systémov do centrálneho úložiska
- **Syslog**
  - Prvý (root) projekt, 1980, jednoduchý protokol, podporuje iba UDP = nezaručuje doručenie správ
- **Syslogng** (dnes asi najvyspelejší projekt)
  - 1998, rozšíril syslog o nové funkcie:
    - filtrovanie na základe obsahu
    - logovanie priamo do databázy
    - TCP pre transport
    - TLS šifrovanie
- **Rsyslog**
  - 2004, rozšíril syslog o nové funkcie:
    - Podpora protokolu RELP (application-level ACK)
    - Podpora prevádzky vo vyrovnávacej pamäti

Logy koncových zariadení

Logy servera

- základným zdrojom údajov pre NSM
- Príklady:
  - **logy servera DNS proxy**, ktoré dokumentujú všetky dotazy a odpovede DNS, ktoré sa vyskytujú v sieti
  - **Apache webserver access logs**
  - **Microsoft Internet Information Server (IIS) access logs**

Apache Access Log



IIS Access Log

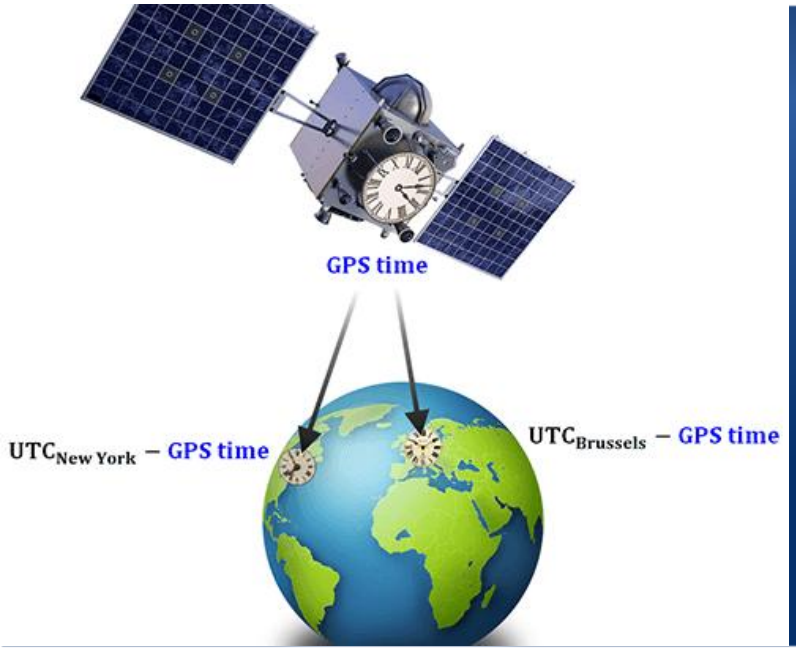
01/09/2025, 09:18:34, 198.51.100.42, -, W3SVC1, WEB-PROD-01, 203.0.113.10, 443, GET, /dashboard, -, 200, 0, 48762, 84, 0, HTTP/2, Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.94 Safari/537.36, -, https://portal.example.com

Logy koncových zariadení

Logy servera

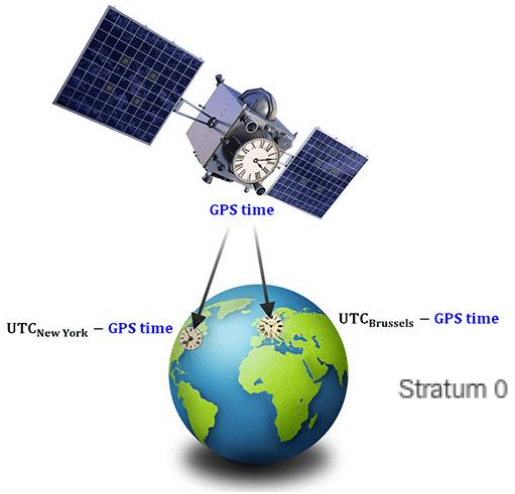
```
01/09/2025, 09:18:34, 198.51.100.42, -, W3SVC1, WEB-PROD-01,
203.0.113.10, 443, GET, /dashboard, -, 200, 0, 48762, 84, 0, HTTP/2,
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.94 Safari/537.36, -,
https://portal.example.com
```

Pole	Hodnota	Popis
Date / Time	`01/09/2025 09:18:34`	Dátum a čas spracovania požiadavky
Client IP	`198.51.100.42`	IP adresa klienta
Service	`W3SVC1`	Identifikátor IIS služby
Server name	`WEB-PROD-01`	Názov webového servera
Server IP / Port	`203.0.113.10 : 443`	Cieľová IP adresa a port
HTTP Method	`GET`	Typ HTTP požiadavky
URI Stem	`/dashboard`	Požadovaný zdroj
Status / Substatus	`200 / 0`	Úspešné spracovanie požiadavky
Bytes sent	`48762`	Objem odoslaných dát (v bajtoch)
Time taken	`84 ms`	Čas spracovania požiadavky
Protocol	`HTTP/2`	Použitá verzia protokolu
User-Agent	`Chrome 122 / Windows 10`	Identifikácia klienta
Referrer	`https://portal.example.com`	Predchádzajúca stránka

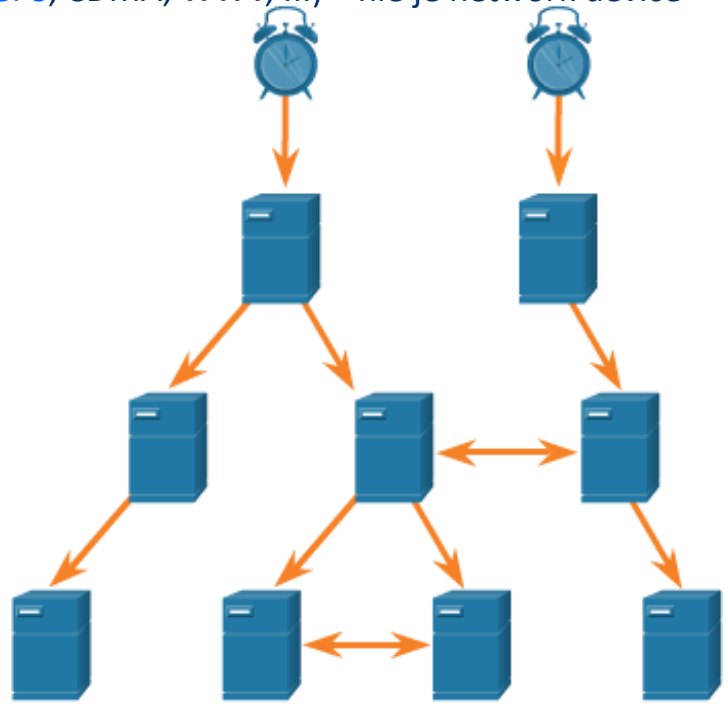


NTP

NTP koncept



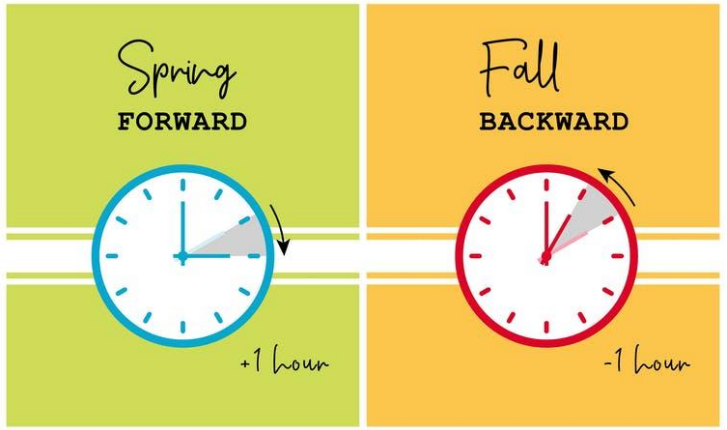
Reference clock (malé, alebo žiadne oneskorenie – GPS, CDMA, WWV, ...) – nie je network device

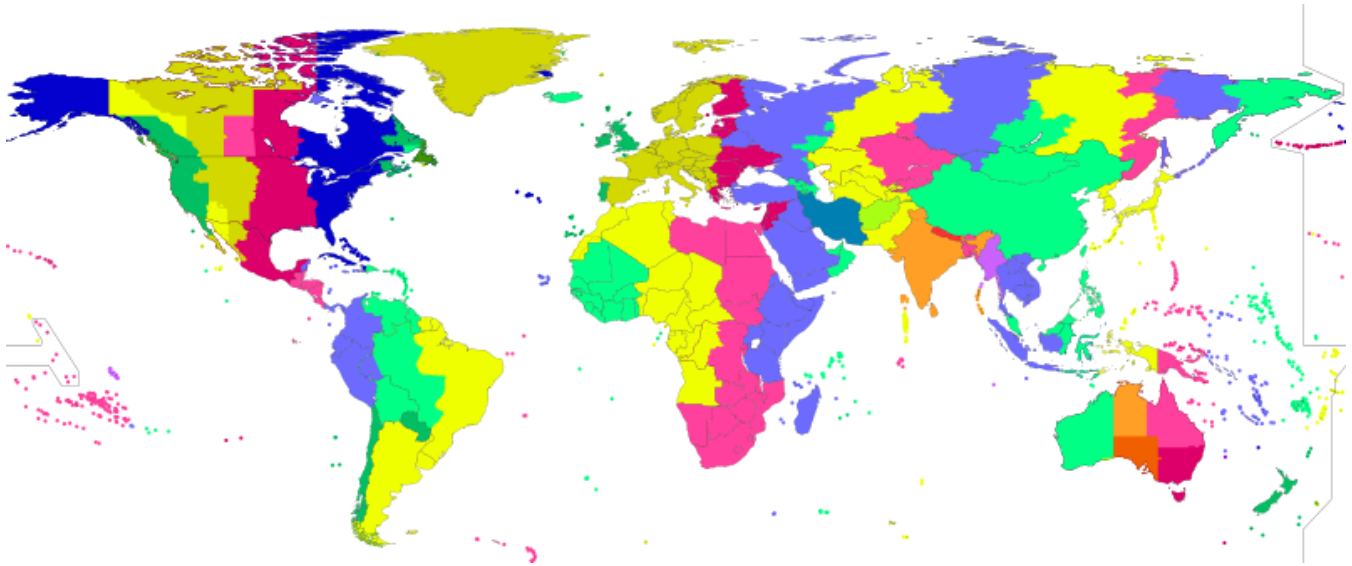


- Reference clock = stratum 0
  - Spoľahlivý zdroj času UTC
  - Malý alebo žiadny delay
  - Nie sú to zriadenia v sieti
    - ale na ne sa napájajú stratum 1 servery
  - Používa
    - GPS
    - CDMA (Code Division Multiple Access)
    - WWV (broadcasting of time signals, Washington, 50W transmission, 500 m wavelength, dnes v: Fort Collins, Colorado)
      - A iné:Irig-B, DCF77, ..
- Stratum 1
  - Server, ktorý je priamo prepojený na stratum 0 zariadenie – nie cez sieťovú linku!
    - Buď má v sebe stratum 0 zariadenie (EndRun time servers)
    - Ale priamu linku – RS 232 prepoj, alebo cez IRIG-B časové kódovanie
  - je základným štandardom sieťového času
  - Presnosť: 10 mikrosekúnd voči UTC
- Stratum 2
  - Pripojený k stratum 1 cez sieťovú linku (čas dostane cez NTP pakety)
  - Presnosť: 0,5 - 100 ms
- Stratum 3...

Ako NTP „zvláda” prechod na letný čas (DST)?

- Daylight saving time (DST)
- Pri NTP nie je potrebné:
  - prepínanie na letný čas
  - nerozlišuje ani časové pásma
- Dôvod:
  - NTP je založený na UTC
  - UTC nemá prechod na letný čas
  - za prechod z/do DST sú výhradne zodpovedné OS serverov a klientov
  - aj za manipuláciu s časovými pásmami

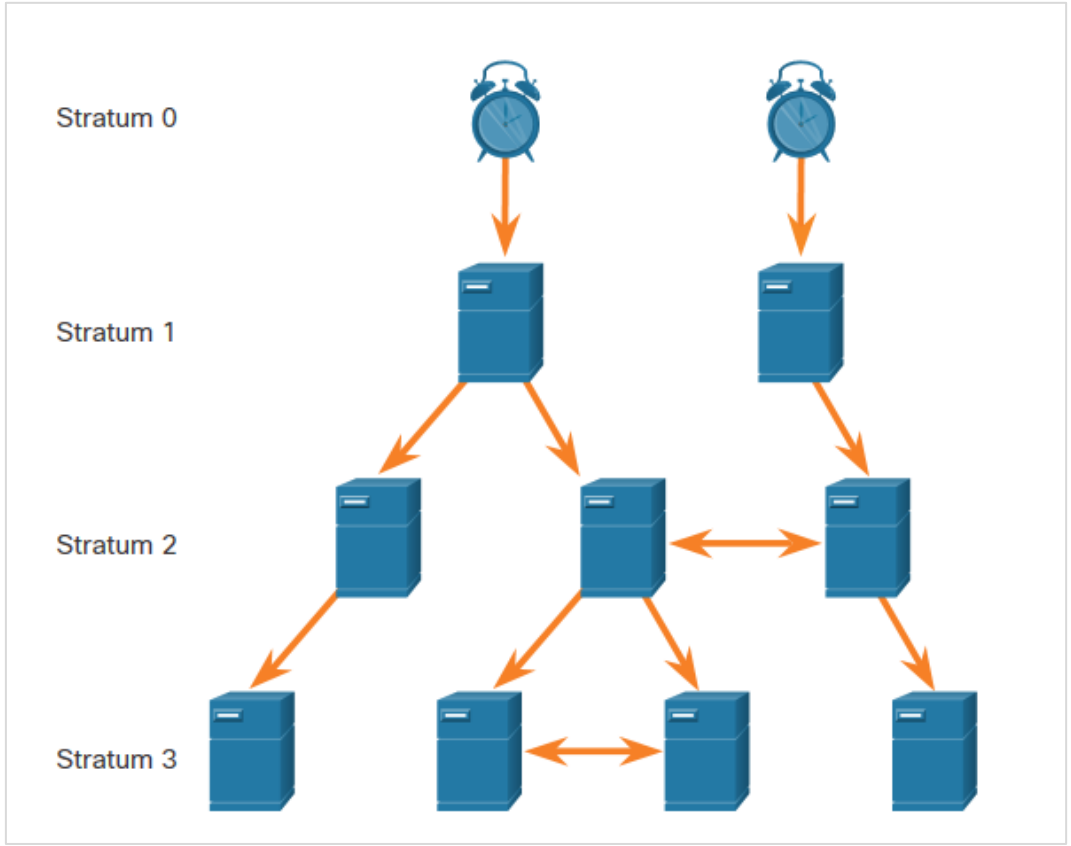




Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

NTP – súhrn vlastností

- Je dôležité synchronizovať čas všetkých zariadení v sieti. Nastavenie dátumu a času na sieťovom zariadení možno vykonať jednou z dvoch metód:
  - Manuálna konfigurácia dátumu a času
  - Konfigurácia pomocou Network Time Protocol (NTP)
- NTP siete používajú hierarchický systém zdrojov času, kde sa každá úroveň v tomto systéme nazýva stratum. Servery NTP sú usporiadané na troch úrovniach známych ako stratum:
  - **Stratum 0**: Sieť NTP získava čas z autoritatívnych zdrojov času.
  - **Stratum 1**: Zariadenia sú priamo pripojené k autoritatívnym časovým zdrojom.
  - **Stratum 2 a vyššie**: Zariadenia stratum 2, ako sú NTP klienti, synchronizujú svoj čas pomocou NTP paketov zo stratum 1 serverov.



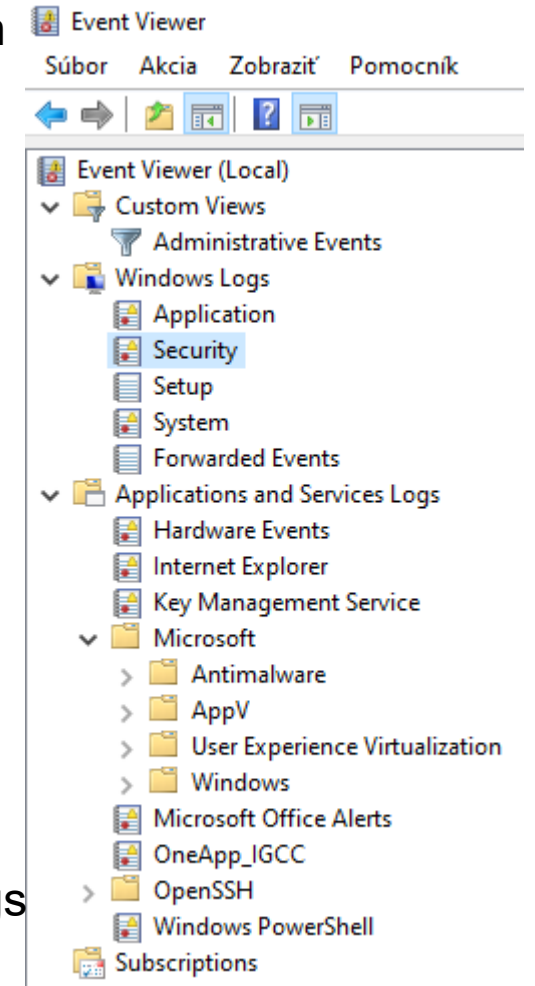
NTP Stratum Levels

Logy koncových zariadení

Používateľské logy

- Systémy detekcie prieniku na koncových zariadeniach (**HIDS**) bežia na zariadeniach používateľov
- Mnohé ochrany založené na používateľoch odosielajú logy na servery **centralizovanej správy logov**, ktoré možno vyhľadávať z centrálneho miesta pomocou **nástrojov**
- Používateľské logy systému **MS Windows** sú viditeľné lokálne cez **Event Viewer**

Kategória logov	Popis
Application	Udalosti generované aplikáciami
Security	Bezpečnostné udalosti (audity, prihlásenia, prístup)
System	Udalosti operačného systému, služieb a ovládačov
Setup	Inštalácia systému a aktualizácie
Forwarded Events	Udalosti prijaté z iných počítačov (WEF). WEF je natívna funkcia Windows, ktorá umožňuje centrálne zbierať logy (udalosti) z viacerých Windows počítačov bez potreby inštalácie agenta



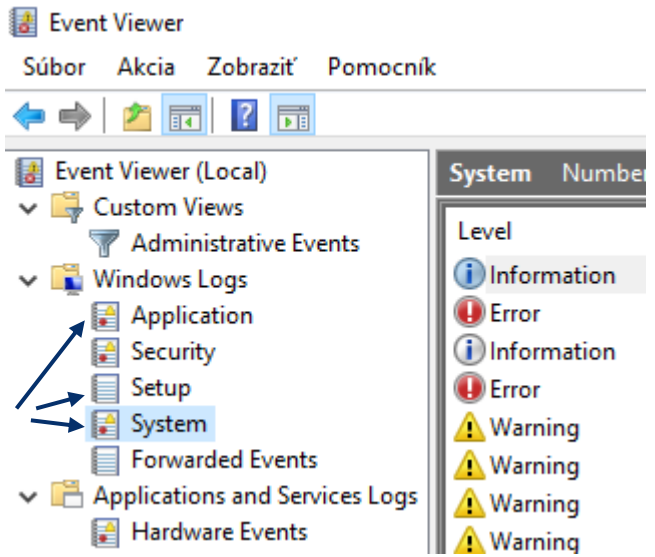
- **Power Shell/ Command-line logs** – súčasťou Security logs, alebo Applications logs
  - Útočníci, ktorí získali prístup k systému a niektorým typom malvéru, vykonávajú príkazy z rozhrania príkazového riadka (CLI) a nie z GUI. Spustenie CLI Logging poskytne **prehľad** o tomto type incidentu

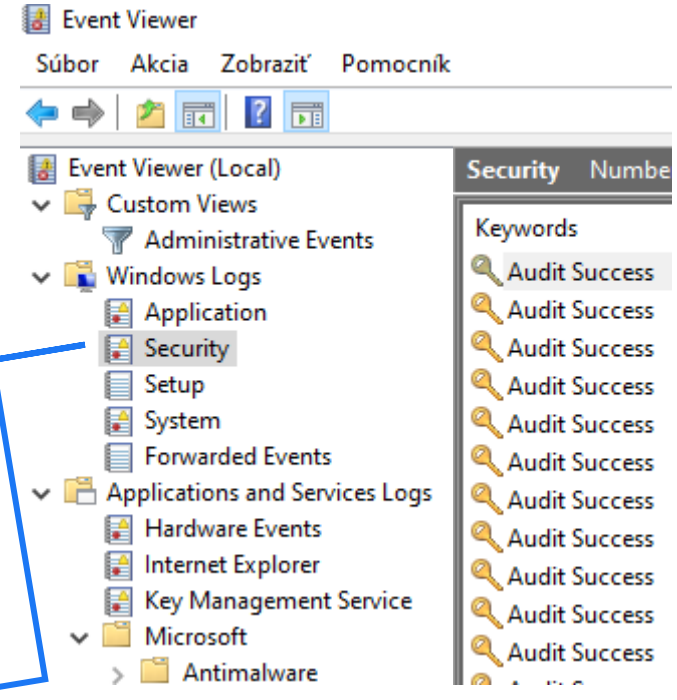
Logy koncových zariadení

Používateľské logy

Levels
– závažnosť udalosti
Keywords
– technické meta-označenia

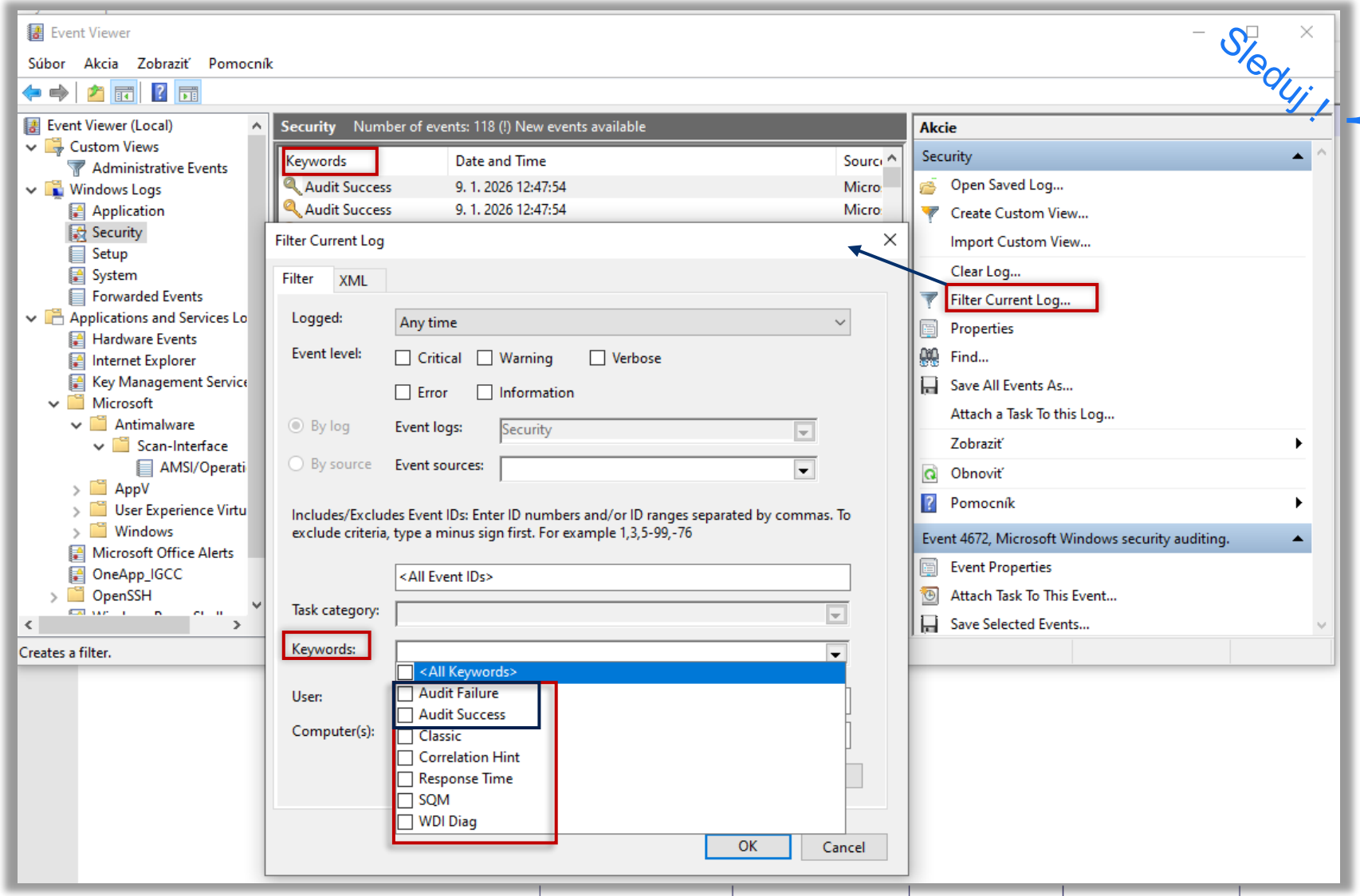
	Keywords / Level	Popis
Levels	Critical (1)	Kritická udalosť, ktorá signalizuje **vážne zlyhanie systému alebo aplikácie**. Často vyžaduje okamžitý zásah (napr. pád systému, zlyhanie kľúčovej služby).
	Error (2)	Chyba, ktorá spôsobila **zlyhanie funkcie alebo služby**, ale systém môže pokračovať v behu. Typické sú chyby aplikácií, služieb alebo ovládačov.
	Warning (3)	Varovanie upozorňujúce na **potenciálny problém**, ktorý zatiaľ nespôsobil zlyhanie, ale môže k nemu viesť (napr. málo miesta na disku).
	Information (4)	Informačná udalosť opisujúca **normálnu a úspešnú činnosť** systému, služby alebo aplikácie (spustenie služby, úspešná operácia).
	Verbose (5)	Veľmi detailná diagnostická udalosť určená najmä na **ladenie a troubleshooting**. Bežne sa nezobrazuje, pokiaľ nie je zapnuté rozšírené logovanie.
Keywords	Success Audit	Je to udalosť, ktorá zaznamenáva **auditovaný pokus o bezpečnostný prístup, ktorý je úspešný**. Napríklad úspešný pokus používateľa o prihlásenie do systému je udalosťou Success Audit.
	Failure Audit	Je to udalosť, ktorá zaznamenáva **auditovaný pokus o bezpečnostný prístup, ktorý zlyhá**. Ak sa napríklad používateľ pokúsi o prístup k sieťovej jednotke a zlyhá, pokus sa loguje ako udalosť Failure Audit.





Meta-značenia logov pomocou Keywords

Ukážka množiny „Keywords“ pre Security Logs vo Win



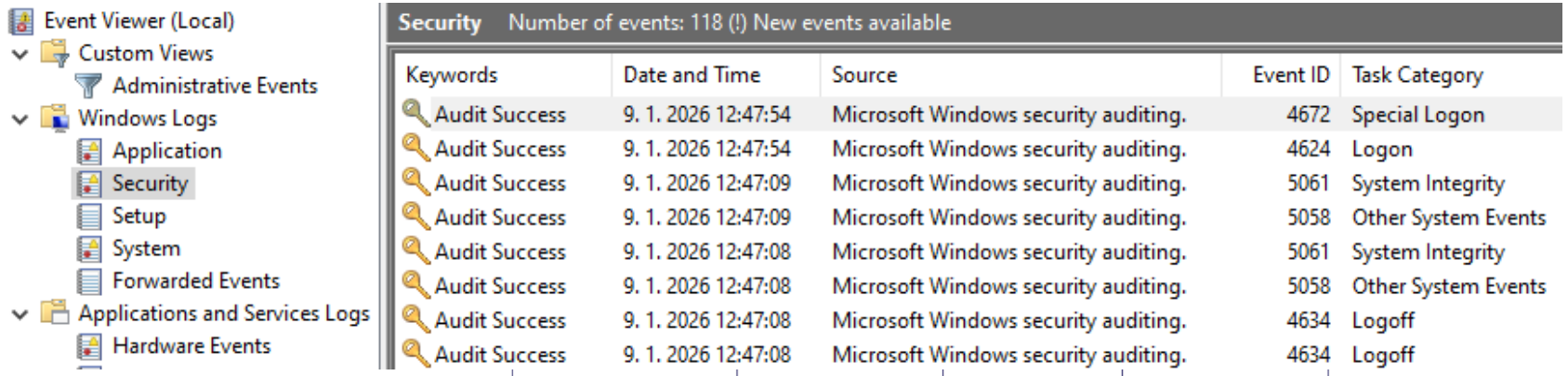
Keyword	Vysvetlenie
Audit Success	**Úspešná** auditovaná bezpečnostná udalosť
Audit Failure	**Neúspešná** auditovaná bezpečnostná udalosť
Classic	Udalosť pochádza zo **starého (legacy) Windows Event Log systému**
Correlation Hint	Pomocná značka na **koreláciu viacerých udalostí** (interné použitie Windows / SIEM)
Response Time	Udalosť obsahuje **informácie o časovej odozve** alebo výkonnosti
SQM	*Software Quality Metrics* – telemetria kvality systému
WDI Diag	*Windows Diagnostic Infrastructure* – diagnostické udalosti systému

Meta-značenia logov pomocou Keywords

Príklady Audit Success / Audit Failure v OS Win

- **Security log používa:**
  - **Keywords → Audit Success / Audit Failure**
  - **Event ID** → identifikátor udalosti (napr. 4624, 4625)
  - **Task Category** → typ bezpečnostnej činnosti (Logon, Account Management…)

Event ID	Keyword	Význam
4624	Audit Success	Úspešné prihlásenie používateľa
4625	Audit Failure	Neúspešný pokus o prihlásenie
4688	Audit Success	Spustenie nového procesu
4720	Audit Success	Vytvorenie používateľského účtu
4769	Audit Failure	Zlyhanie Kerberos autentifikácie



Zber a pipeline

- Zber:
  - lokálni agenti (beats, syslog)
  - bezagentové mechanizmy (API, cloud logging).
- Preprava:
  - zabezpečené kanály (TLS),
  - autentifikácia endpointov.
- Normalizácia/parsing:
  - preklad rôznych formátov do spoločnej schémy.
- Obohacovanie (enrichment):
  - pridanie geografických údajov podľa IP, asset owner, environment tags, ...
- Indexovanie a deduplikácia:
  - priestorovo efektívne ukladanie a rýchle dotazy.

Odporúčané mapovanie pre SIEM - pravidlá prioritizácie

- V reálnej praxi **severity ≠ incident**:
  - Syslog *Error* na smerovači ≠ bezpečnostný incident
  - Syslog *Informational* s Event ID (napr. login admina) **MÔŽE byť High**
- **Severity je len jeden vstup**, rozhoduje:
  - zdroj
  - obsah
  - kontext
  - korelácia

Syslog Severity	Windows Event Level	Vysvetlenie	SOC priorita
Emergency (0)	Critical (1)	Systém nefunkčný	High
Alert (1)	Critical (1)	Vyžaduje okamžitý zásah	
Critical (2)	Critical (1)	Kritické zlyhanie	
Error (3)	Error (2)	Chyba	
Warning (4)	Warning (3)	Varovanie	Medium
Notice (5)	Information (4)	Dôležitá informácia	
Informational (6)	Information (4)	Bežná informácia	Low
Debug (7)	Verbose (5)	Diagnostické údaje	Ignore / Troubleshooting

Normalizácia Windows Event Level a Syslog Severity

- V **ELK stacku (Elasticsearch + Logstash + Kibana)** sa normalizácia robí podľa **Elastic Common Schema (ECS)**.
- Cieľ je, aby **Windows events, syslog, firewall aj EDR** používali **rovnaké polia a rovnakú „závažnosť“**, aby sa dali porovnávať a korelovať
- Základ: Elastic Common Schema (ECS)
  - ECS definuje jednotné polia, napr.:
    - event.kind
    - event.category
    - event.type
    - event.outcome
    - log.level
    - event.severity
  - Kľúčové pole pre závažnosť je event.severity (číselné)

Windows Event Level	event.severity	log.level
Critical	1	critical
Error	3	error
Warning	4	warning
Information	6	info
Verbose	7	debug

Syslog severity	event.severity	log.level
Emergency (0)	0	emergency
Alert (1)	1	alert
Critical (2)	2	critical
Error (3)	3	error
Warning (4)	4	warning
Notice (5)	5	notice
Informational (6)	6	info
Debug (7)	7	debug

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad: ako to robí Logstash / Ingest pipeline (logika)

- **Zjednodušený princíp:**

  IF Windows Event Level == Critical
  → event.severity = 1

  IF Windows Event Level == Information
  → event.severity = 6

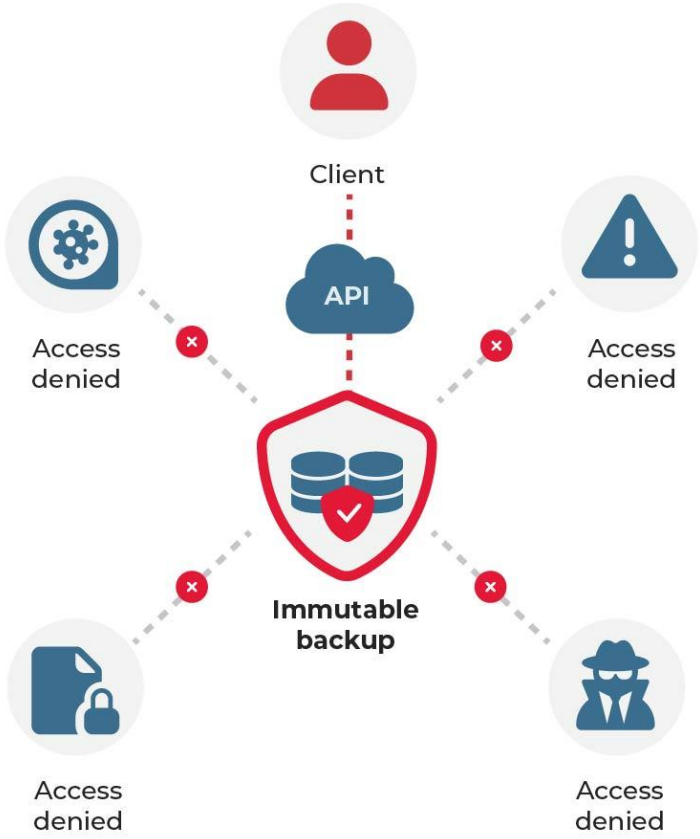
  IF Security + Failure Audit
  → event.outcome = failure
  → event.severity = 3–5 (podľa Event ID)

- **Prečo je to dôležité v SOC**
  - Jeden alerting systém
  - Korelácia Windows ↔ Linux ↔ Network
  - Menej falošných poplachov
  - Jedna priorita incidentu
    - Tu pozor ! V SOC
      - nikdy sa nepoužíva len severity
      - používa sa kombinácia pravidiel
        - Incident Priority = Severity + :
          + Security context
          + Asset criticality
          + Frequency / Correlation / iné...

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Integrita, uchovávanie, ochrana

- Integrita:
  - zabezpečiť, že logy nie sú modifikované (WORM, digitálne podpisy, hash reťazce).
- Retencia:
  - politika retenčného obdobia (napr. krátka na operácie, dlhá na audit) v súlade so zákonmi a internými požiadavkami.
- Prístup:
  - striktne RBAC, audit prístupu k logom.
- Šifrovanie pri prenose aj pri ukladaní.
- Zálohy: off-site/nemenné kópie pre vyššiu odolnosť.



Ochrana osobných údajov, compliance

- Minimalizácia:
  - logovať iba potrebné údaje, anonymizovať/ pseudo-anonymizovať kde sa vyžaduje.
- GDPR/špecifické zákony verejnej správy:
  - uchovávanie, prístup, účel spracovania (logy môžu obsahovať osobné údaje).
- Pravidlá pre zverejňovanie logov internému aj externému tímu.

Bezpečnostné monitorovanie

Architektúra a hlavné komponenty

- Zdroje logov (endpoints, servery, sieťové zariadenia, cloud, aplikácie).
- Agregátor/collector (centralizovaný SIEM alebo cloud logging).
- Analytika/detekcia (korelačné pravidlá, machine learning, behavior analytics).
- Upozorňovanie/alerting (notifikácie, ticketing).
- Dashboardy a reporting.
- Incident response (playbooks, orchestration/SOAR).

Nástroje a technológie (príklady)

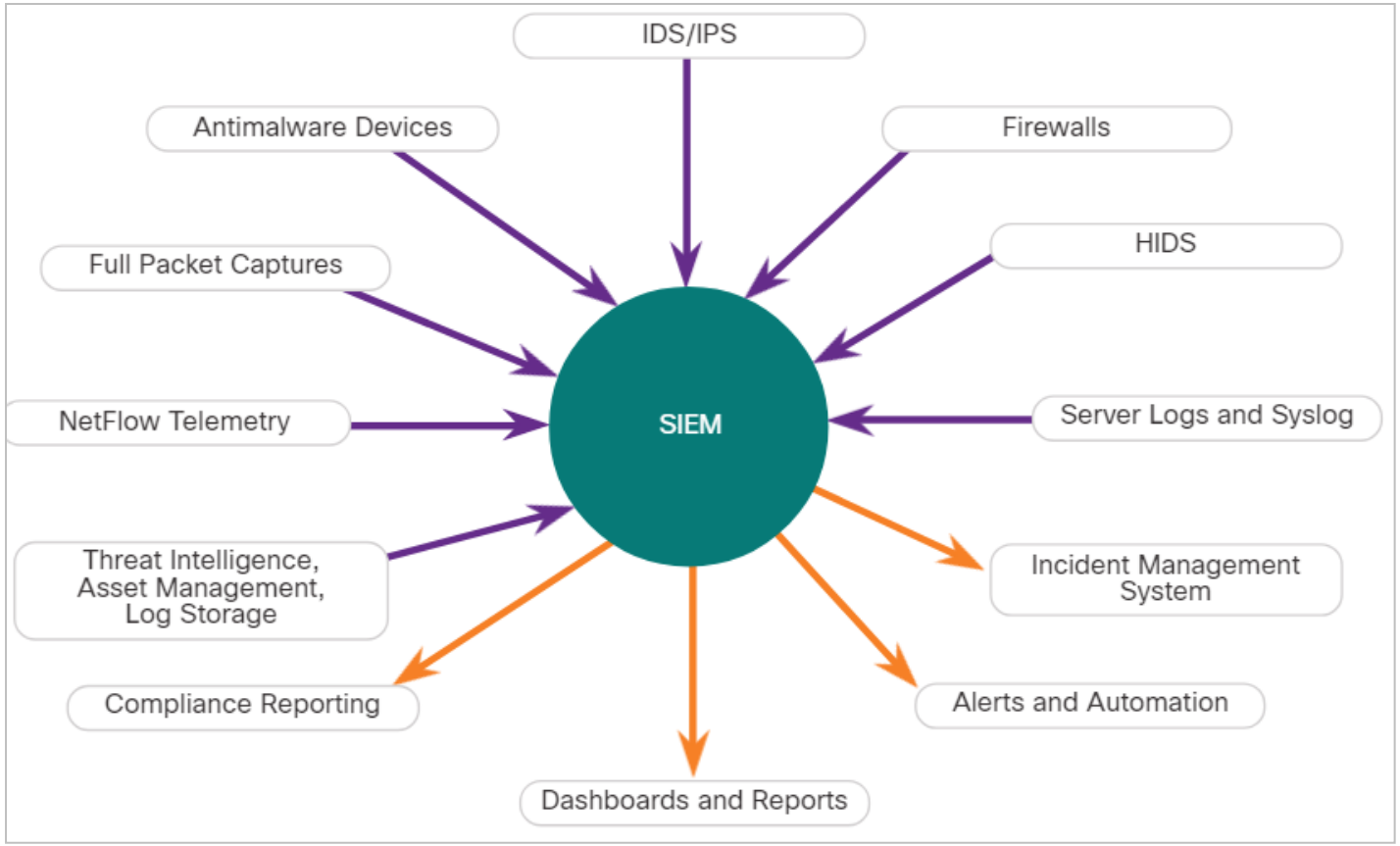
- SIEM (napr. Splunk, Elastic SIEM, Microsoft Sentinel)
  - centralizácia a korelácia.
- EDR/NDR
  - detekcia na endpointoch a v sieti.
- Logstash/Fluentd/Beats
  - zber a transformácia.
- SOAR
  - automatizácia reakcií.

SIEM

SIEM a Log Collection

Technológia Security Information and Event Management (SIEM) sa používa v mnohých organizáciách na poskytovanie správ v reálnom čase a dlhodobú analýzu bezpečnostných udalostí.

SIEM vstupy a výstupy:



SIEM a Log Collection (Pokr.)

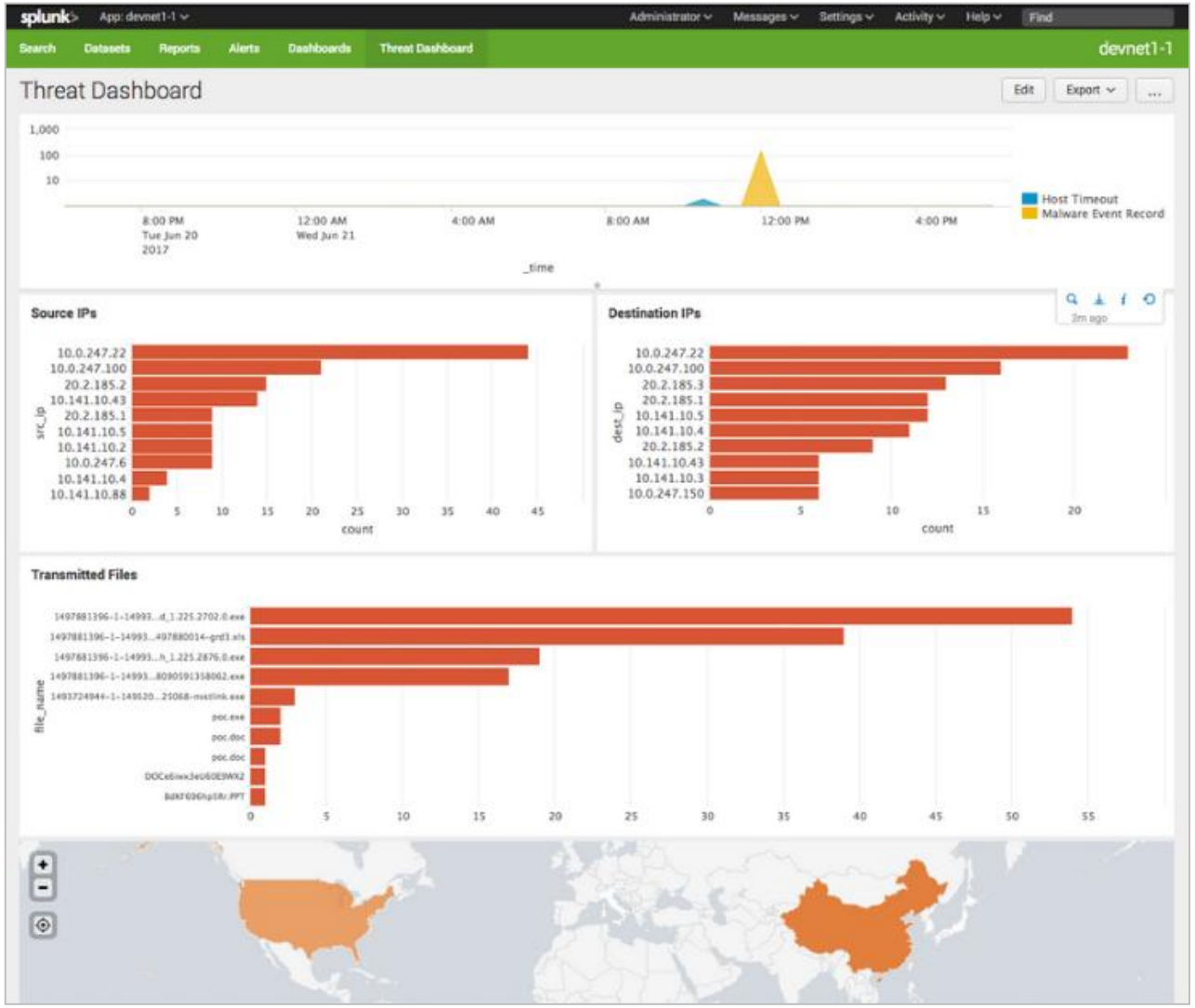
SIEM kombinuje základné funkcie nástrojov SEM a SIM a poskytuje pohľad na podnikovú sieť pomocou nasledujúcich funkcií:

- **Log collection** – záznamy udalostí zo zdrojov v celej organizácii poskytujú dôležité forenzné informácie a pomáhajú riešiť požiadavky na podávanie správ o súlade
- **Normalization** – mapuje logy z rôznych systémov do spoločného dátového modelu, čo umožňuje organizácii pripojiť sa a analyzovať súvisiace udalosti, aj keď sú pôvodne logované v rôznych zdrojových formátoch
- **Correlation** – prepája logy a udalosti z rozdielnych systémov alebo aplikácií, urýchľujúc detekciu a reakciu na bezpečnostné hrozby.
- **Aggregation** – znižuje objem údajov udalostí konsolidáciou duplicitných záznamov udalostí
- **Reporting** – predstavuje korelované agregované údaje o udalostiach v monitorovaní v reálnom čase a dlhodobých súhrnoch vrátane grafických interaktívnych panelov
- **Compliance** – hlásenie na splnenie požiadaviek rôznych nariadení o súlade

SIEM a Log Collection (Pokr.)

- Príklad nástroja SIEM:
  - **Splunk**
    - Splunk je široko používaný v SOC
    - Vzhľadom na nedostatok odborníkov na KB, ktorí by monitorovali a analyzovali veľký objem bezpečnostných údajov, je dôležité, aby **nástroje od viacerých dodávateľov** bolo možné integrovať do jednej platformy
- Integrované bezpečnostné platformy idú **nad rámec SIEM a SOAR**,
  - aby zjednotili viaceré bezpečnostné technológie do jednotnej platformy

Splunk Threat Dashboard

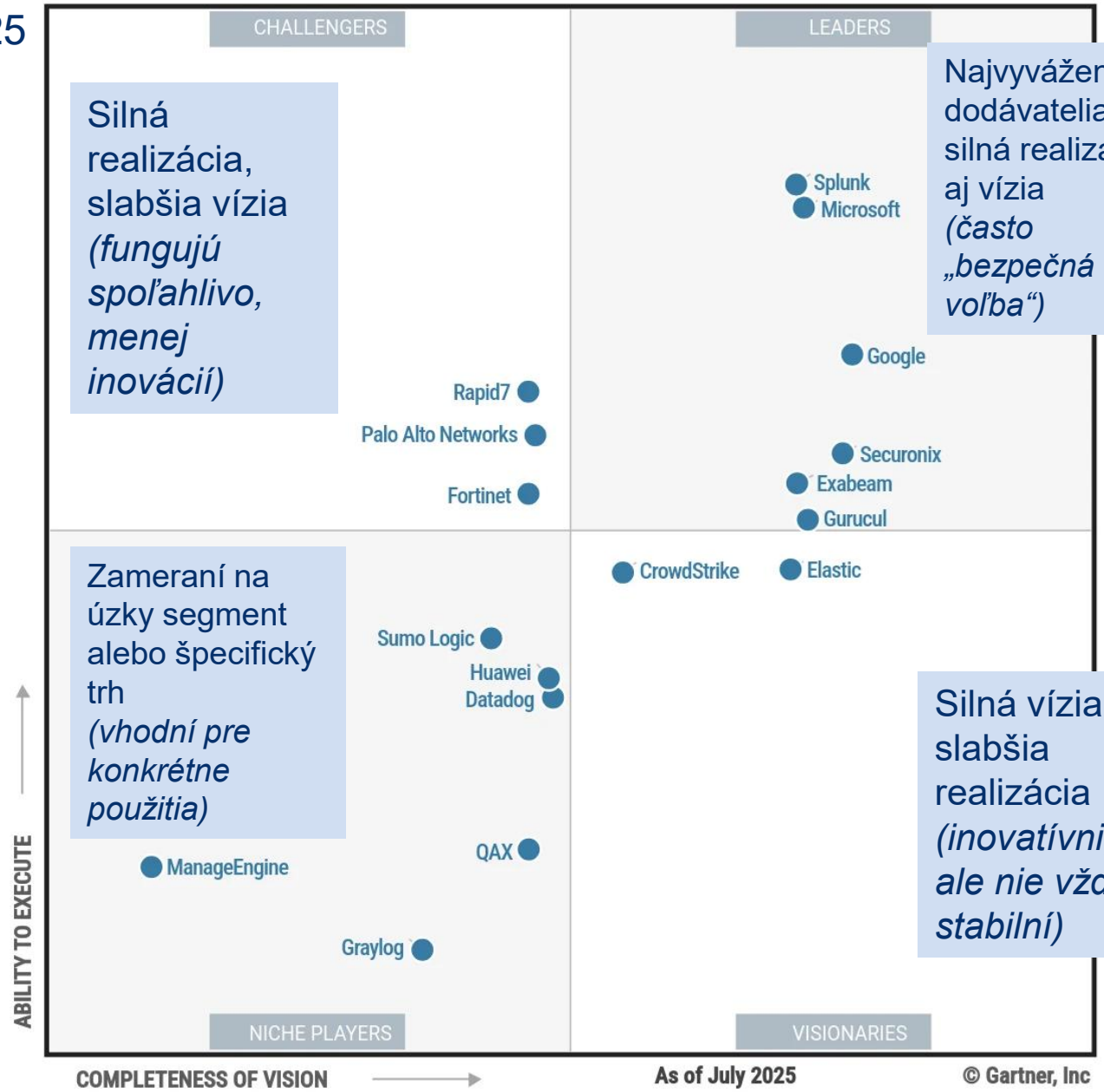


Gartner magic quadrant

SIEM (leaders)

2021

2025



Silná realizácia, slabšia vízia *(fungujú spoľahlivo, menej inovácií)*

Najvyváženejší dodávatelia – silná realizácia aj vízia *(často „bezpečná voľba“)*

Zameraní na úzky segment alebo špecifický trh *(vhodní pre konkrétne použitia)*

Silná vízia, slabšia realizácia *(inovatívni, ale nie vždy stabilní)*

https://www.microsoft.com/en-us/security/blog/2025/10/16/microsoft-named-a-leader-in-the-2025-gartner-magic-quadrant-for-siem

Financované Európskou úniou NextGenerationEU
PLÁN [O]

Gartner

Terminológické okienko

Vzťah medzi NSM a SIEM

- **Network Security Monitoring** predstavuje **koncept** kontinuálneho monitorovania bezpečnostnej aktivity v sieti a systémoch,
- zatiaľ čo SIEM je **technologická platforma** umožňujúca centralizovaný zber, koreláciu a vyhodnocovanie bezpečnostných udalostí.
- Rozdiel medzi nimi spočíva primárne v účele a úrovni abstrakcie, nie v type spracúvaných dát.
- **Ešte jasnejšie:**
  - **SIEM je jedným z technických prostriedkov, prostredníctvom ktorých sa NSM v praxi realizuje.**
  - NSM definuje *čo* a *prečo* monitorujeme
  - SIEM definuje *ako* údaje zbierame, korelujeme a reportujeme
- **Ešte inak:**
  - **NSM - monitorovací a analytický prístup** (process-oriented)
  - **SIEM - konkrétny nástrojový mechanizmus** (tool-oriented)

- SIEM ide nad rámec NSM, podporuje aj ďalšie bezpečnostné a prevádzkové oblasti:
  - Compliance a audit
    - generovanie reportov pre normy (ISO/IEC 27001, PCI DSS, GDPR)
    - dlhodobá archivácia a preukázateľnosť logovania
  - Reporting a manažérsky dohľad
    - prehľadové dashboardy, metriky a trendy
    - podpora strategického rozhodovania
  - Workflow a operatívne riadenie
    - správa incidentov, eskalácie, ticketing
    - integrácia so SOAR a reakčnými procesmi

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Výstrahy (alerts)

Vyhodnocovanie výstrah

Alert Generation

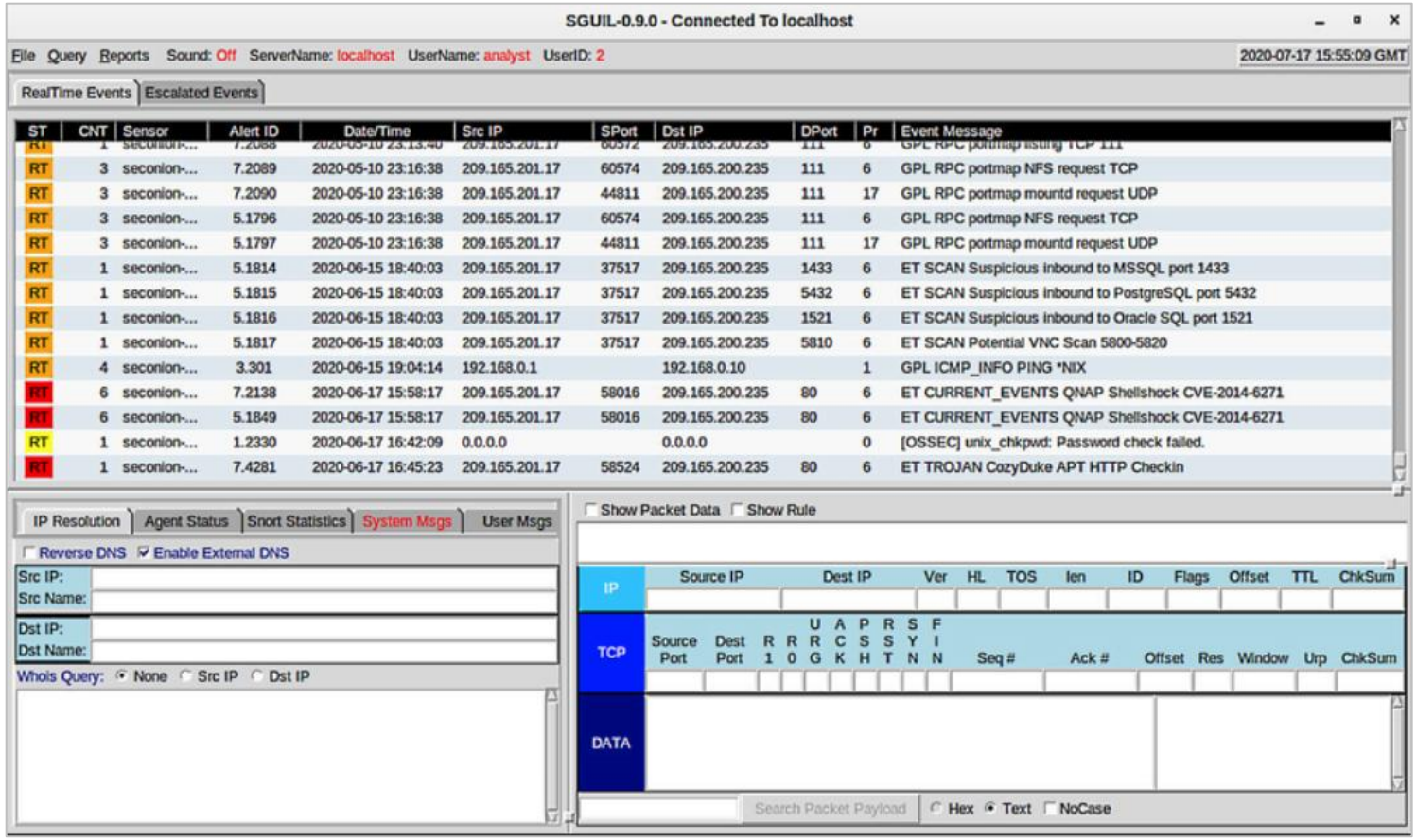
- Bezpečnostné výstrahy sú oznamovacie správy, ktoré sú generované nástrojmi, systémami a bezpečnostnými zariadeniami NSM. Výstrahy môžu mať rôzne podoby v závislosti od zdroja
- V Security Onion, Sguil poskytuje konzolu, ktorá integruje výstrahy z viacerých zdrojov do timestamped queue
- Analytik KB pracuje prostredníctvom **bezpečnostného frontu** a skúma, klasifikuje, zvyšuje (T1, T2, T3, T4) alebo ruší výstrahy
- Výstrahy môžu obsahovať päticu informácií, ako aj časové pečiatky a informácie identifikujúce, ktoré zariadenie alebo systém generoval výstrahu:
  - **SrcIP** - zdrojová IP adresa udalosti
  - **SPort** - zdrojový (lokálny) port Layer 4 udalosti
  - **DstIP** - cieľová IP adresa udalosti
  - **DPort** - cieľový port Layer 4 udalosti
  - **Pr** - číslo IP protokolu udalosti

Vyhodnocovanie výstrah

Alert Generation (Pokr.)

Obrázok ukazuje okno aplikácie Sguil s radom výstrah, ktoré čakajú na preskúmanie v hornej časti rozhrania. Polia dostupné pre udalosti v reálnom čase sú nasledovné:

- ST - stav udalosti.
  - Udalosť je farebne odlíšená podľa priority na základe kategórie výstrahy.
  - Existujú štyri úrovne priority: veľmi nízka, nízka, stredná a vysoká a farby sa pohybujú od svetložltej po červenú, keď sa priorita zvyšuje
- CNT - počet, koľkokrát bola táto udalosť zistená pre rovnakú zdrojovú a cieľovú IP adresu.
  - Systém určil, že tento súbor udalostí je korelovaný
- Sensor - agent hlásiaci udalosť.
  - Dostupné senzory a ich identifikačné čísla sa dajú nájsť na karte Agent Status na paneli, ktorý sa zobrazí pod oknom udalostí vľavo

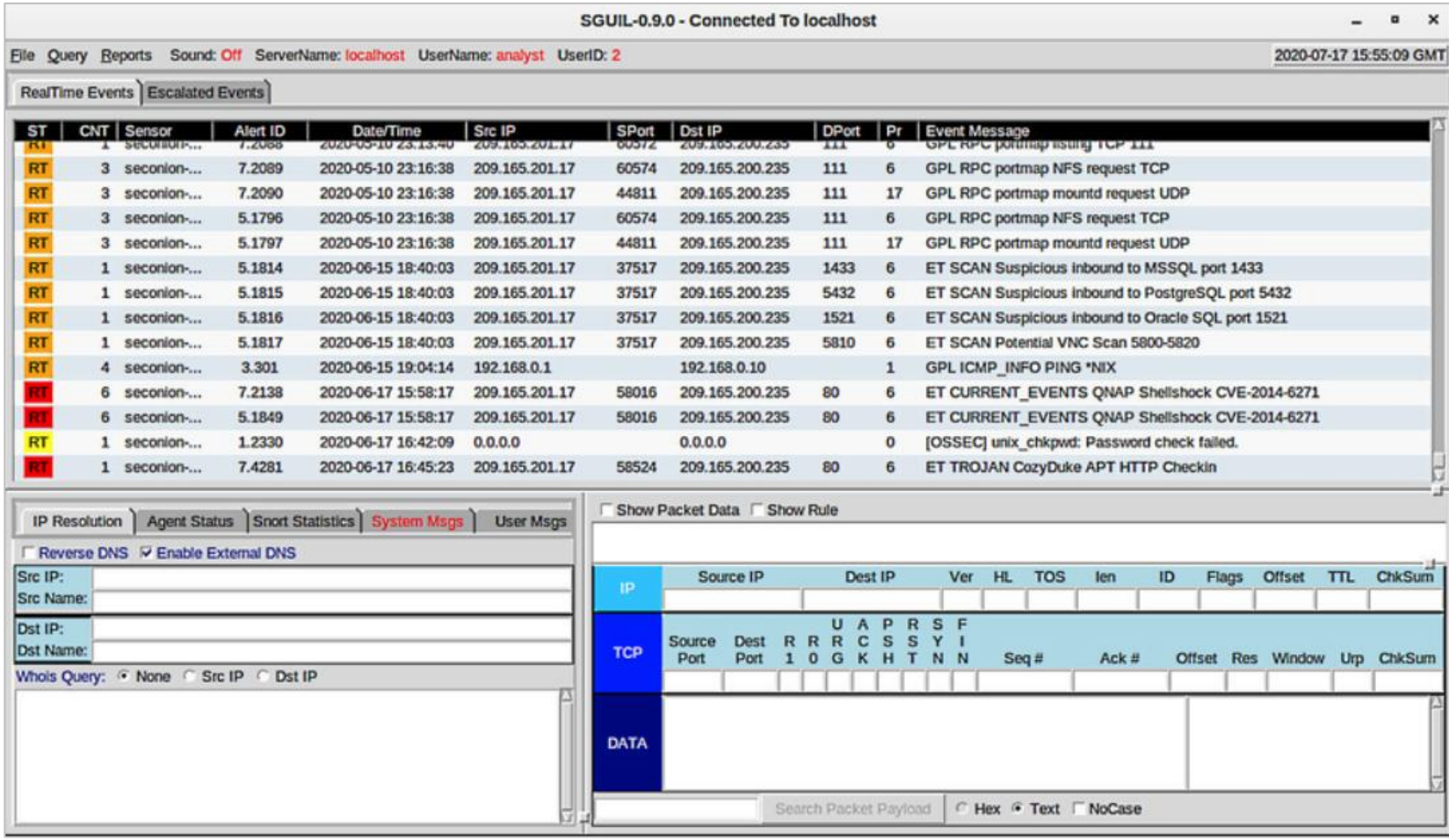


Sguil Window

Vyhodnocovanie výstrah

Alert Generation (Pokr.)

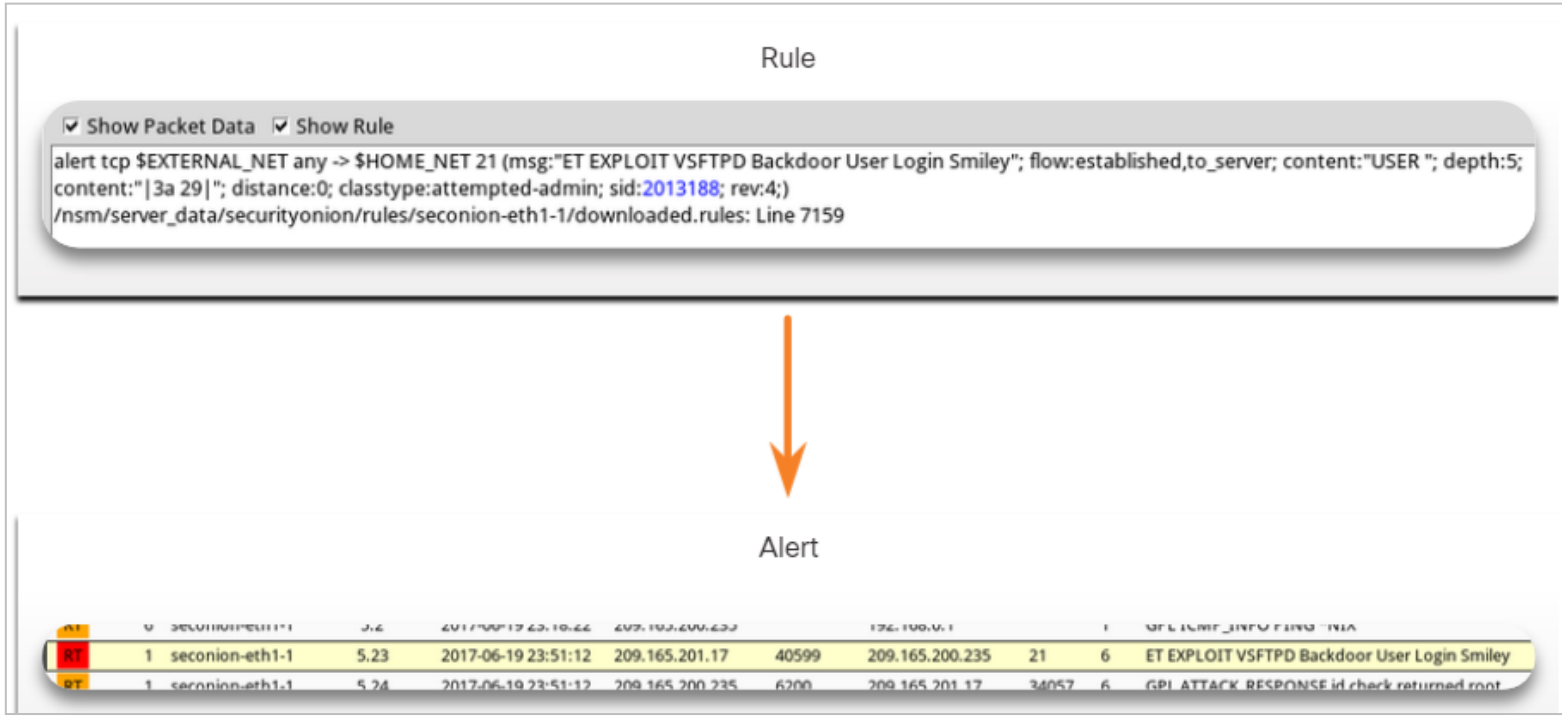
- Alert ID - dve čísla oddelené bodkou, predstavuje senzor, ktorý nahlásil problém, a číslo udalosti pre tento senzor
- Date/Time - časová pečiatka udalosti.
  - V prípade korelovaných udalostí je to časová pečiatka prvej udalosti
- Event Message - identifikačný text udalosti.
  - Je nakonfigurovaný v pravidle, ktoré spustilo výstrahu.
  - Príslušné pravidlo je možné zobraziť vpravo, hneď nad hlavičkami paketov (Show rule)



Sguil Window

Pravidlá a výstrahy

- Výstrahy môžu pochádzať z viacerých zdrojov, v prípade Security Onion:
  - **NIDS** - Snort, Zeek, a Suricata
  - **HIDS** - OSSEC, Wazuh
  - **Asset management and monitoring** - Passive Asset Detection System (PADS)
  - **HTTP, DNS, a TCP transakcie** - zaznamenávané Zeekom a pcaps
  - **Syslog správy** - viacero zdrojov



- Informácie nájdené vo výstrahách, ktoré sa zobrazujú v NSM, sa budú líšiť vo formáte správy, pretože pochádzajú z rôznych zdrojov
- Výstraha Sguil na obrázku bola spustená pravidlom, ktoré bolo nakonfigurované v Snorte

Vyhodnocovanie výstrah

Potreba pre vyhodnocovanie výstrah

- Oblasť hrozieb sa neustále mení s objavovaním nových zraniteľností a hrozieb.
  - Ako sa menia potreby používateľov a organizácie, menia sa aj útoky
- Aktéri hrozieb sa naučili, ako rýchlo meniť vlastnosti svojich exploitov, aby sa vyhli odhaleniu

- Je lepšie mať výstrahy, ktoré sú niekedy generované nevinnou návštevnosťou, ako mať pravidlá, ktoré vynechávajú škodlivú prevádzku
- Je potrebné, aby skúsení analytici kybernetickej bezpečnosti preskúmali výstrahy, aby zistili, či skutočne došlo k zneužitiu
- Analytici kybernetickej bezpečnosti prvej úrovne pracujú s frontou výstrah v nástroji, ako je Sguil, Kibana, a iné dashboardy v iných SIEM
  - Mnohé umožňujú aj pivotovanie do iných nástrojov – napr. z Sguil do IDS Zeek, analyzovať dáta vo Wireshark, v Kibane, a iné

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Vyhodnocovanie výstrah

- Bezpečnostné incidenty sú klasifikované **pomocou schémy** prevzatej z lekárskej diagnostiky.
  - Táto klasifikačná schéma sa používa na usmernenie činností a na vyhodnocovanie diagnostických postupov.
  - Ide o to, že **diagnóza** môže byť presná, pravdivá, nepresná alebo nepravdivá
- Pri analýze bezpečnosti siete sa analytikovi kybernetickej bezpečnosti **zobrazí výstraha**.
  - Analytik kybernetickej bezpečnosti musí **určiť, či je táto „diagnóza“ pravdivá**
- Výstrahy možno klasifikovať nasledovne:
  - **True Positive**: Výstraha bola overená ako skutočný bezpečnostný incident
  - **False Positive**: Výstraha nenaznačuje skutočný bezpečnostný incident.
    - Aktivita, ktorá vedie k falošne pozitívnemu výsledku, sa niekedy označuje ako **benign trigger**
- Alternatívnou situáciou je, že výstraha nebola vygenerovaná. Neprítomnosť výstrahy možno klasifikovať ako:
  - **True Negative**: Nevyskytol sa žiadny bezpečnostný incident. Aktivita je legitímna (*benign activity*)
  - **False Negative**: Došlo k nezistenému incidentu

Prehľad vyhodnocovania výstrah

Vyhodnocovanie výstrah (Pokr.)

Keď sa vydá výstraha, dostane jednu zo štyroch možných klasifikácií:

	True	False
Positive (Výstraha existuje)	**Incident nastal**	**Incident nenastal**
Negative (Výstraha neexistuje)	**Incident nenastal**	**Incident nastal**

- **True positives** sú požadovaným typom upozornenia.
  - Znamená to, že pravidlá, ktoré generujú výstrahy, fungovali správne
- **False positives** nie sú žiaduce.
  - Hoci nenaznačujú, že došlo k nezistenému zneužitiu, sú nákladné, pretože analytici kybernetickej bezpečnosti musia vyšetrovať falošné poplachy
- **True negatives** sú žiaduce.
  - Naznačujú, že legitímna/normálna prevádzka je správne ignorovaná a nevydávajú sa chybné upozornenia
- **False negatives** sú nebezpečné.
  - Naznačujú, že bezpečnostné systémy, ktoré sú v infraštruktúre, nezistili zneužitie

*"**True**" udalosti sú žiaduce. "**False**" sú nežiaduce a potenciálne nebezpečné.*

Vyhodnocovanie výstrah (Pokr.)

- Legitímne udalosti (*benign events*)
  - sú tie, ktoré by nemali spúšťať výstrahy
  - Ich nadmerný počet naznačuje, že niektoré pravidlá alebo detektory je potrebné zlepšiť alebo odstrániť
- V prípade podozrenia na true positives je potrebné:
  - aby analytik KB postúpil varovanie na vyššiu úroveň na účely vyšetrovania.
  - vyšetrovateľ bude pokračovať vo vyšetrovaní s cieľom potvrdiť incident a identifikovať prípadné škody, ktoré mohli byť spôsobené
- Falošné poplachy:
  - Analytik KB je zodpovedný aj za informovanie bezpečnostného personálu o tom, že sa vyskytujú falošné poplachy do takej miery, že to vážne ovplyvňuje jeho čas
- False negatives
  - môžu byť objavené dlho po zneužití.
    - V rámci retrispektívy (retrospective security analysis, RSA).
    - Napr. keď sa na archivované údaje o zabezpečení siete použijú novo získané pravidlá alebo iné informácie o hrozbách
    - Preto je dôležité:
      - monitorovať spravodajstvo o hrozbách,
        - aby sme sa dozvedeli o nových zraniteľnostiach a zneužitiach
        - a vyhodnotili pravdepodobnosť, že sieť bola voči nim zraniteľná niekedy v minulosti

Deterministická analýza a Pravdepodobnostná analýza

Deterministická analýza

- **Ako uvažuje:**
  - Vychádza zo **známych zraniteľností**
  - Hodnotí **najhorší možný scenár**
  - Predpokladá, že útočník má **všetky potrebné informácie**
  - Útok je úspešný **len ak prejdú všetky kroky**
  - Analytik KB **pozná celý postup útoku**
- **Silné stránky:**
  - Jednoduchá a zrozumiteľná
  - Vhodná pre **kritické systémy**
- **Slabiny:**
  - Často **nadhodnocuje riziko**
  - Neberie do úvahy realitu a náhodnosť útokov

Pravdepodobnostná analýza

- **Ako uvažuje:**
  - Riziko vyjadruje ako **pravdepodobnosť úspechu útoku**
  - Každý krok útoku má **svoju šancu na úspech**
  - Úspech ďalšieho kroku **nie je istý**
  - Nie všetky informácie sú presne známe (napr. porty, konfigurácie, ...)
  - Používa **štatistické a historické dáta**
- **Silné stránky:**
  - Realistickejší pohľad na hrozby
  - Umožňuje **prioritizáciu rizík**
- **Slabiny:**
  - Vyžaduje kvalitné dáta
  - Výsledky sú **odhad**, nie istota

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Deterministická a pravdepodobnostná analýza

- **Prečo to má zaujímať manažéra KB?**
  - Nie všetky hrozby majú **rovnakú váhu**
  - Rozpočet KB je **obmedzený**
  - Cieľom je:
    - investovať tam, kde je **najväčšie reálne riziko**
    - znížiť **pravdepodobnosť incidentu**
    - minimalizovať **dopad na biznis**

Pravdepodobnostná analýza

... pomáha **rozhodovať**

Deterministická

... pomáha **chrániť kritické aktíva**

- **Ako pomáha deterministická analýza**
  - Definuje **čo musíme monitorovať za každú cenu**
  - Identifikuje **kritické kroky útoku**
  - Základ pre:
    - detekčné pravidlá
    - alerty typu *Critical / High*
- **Ako pomáha pravdepodobnostná analýza**
  - Využíva **reálne dáta z logov**
  - Sleduje trendy a anomálie
  - Umožňuje:
    - dynamickú prioritu incidentov
    - zníženie „alert fatigue“
- **Zhrnutie**
  - Deterministická analýza = **ochrana najhoršieho prípadu**
  - Pravdepodobnostná analýza = **riadenie reálneho rizika**
- Monitorovanie a logovanie:
  - dodáva **dáta**
  - znižuje neistotu
  - umožňuje **lepšie rozhodovanie**
- **Bez logov neexistuje realistické riadenie rizík.**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prevádzka a procesy pri monitorovaní

Prevádzka a procesy

- Monitoring 24/7 vs. pracovné hodiny
  - stratégiu podľa rizika.
- On-call, eskalácie, SLA pre reakcie.
- Tuning alertov:
  - thresholding, pravidlá, suppression windows (pauza).
- Playbooky:
  - krok-za-krokom reakcia, kto čo robí po alerte.
- Threat hunting:
  - aktívne hľadanie podozrení mimo alertov.
- Reporting:
  - kvartálne/ročné reporty, KPI (MTTD, MTTR, počet false positives)

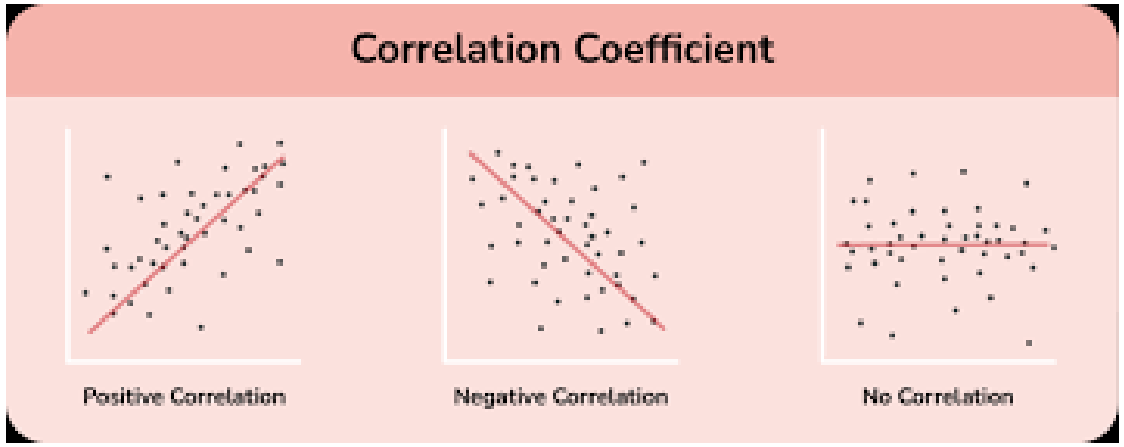
KPI a metriky (čo merať)

- Počet a typy alertov (funkčné vs bezpečnostné).
- False positive rate.
- MTTD (Mean Time to Detect), MTTR (Mean Time to Respond).
- Pokrytie logovaním (percento kritických systémov logovaných).
- Compliance metriky (retencia, prístupnosť).
  - percento údajov, ktoré spĺňajú zásady uchovávania údajov,
  - počet porušení zásad uchovávania údajov
  - priemerný čas potrebný na odstránenie údajov

Princípy korelácie bezpečnostných udalostí

Prečo korelovať?

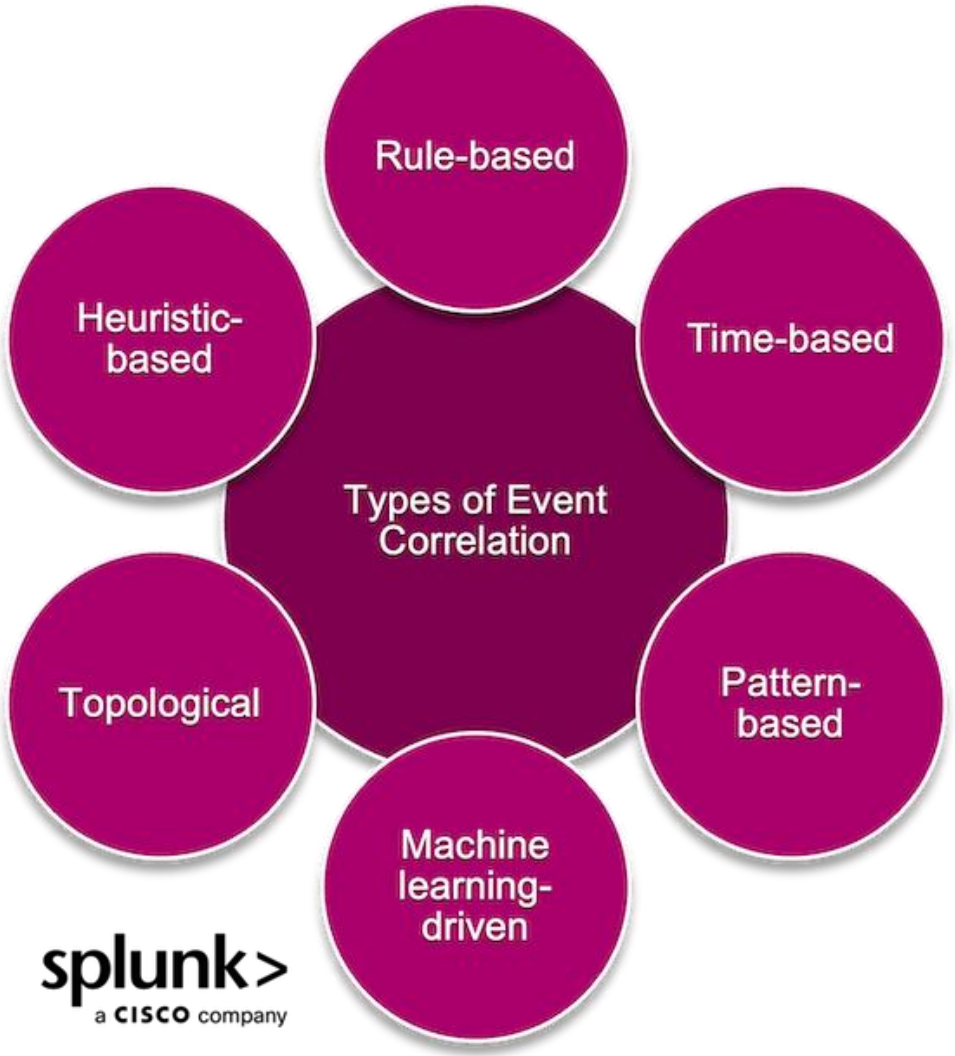
- Jednotlivé udalosti často nie sú škodlivé
  - korelácia umožní zložiť puzzle (multi-step útoky).
- Zníženie hluku:
  - korelácia kombinuje udalosti do významných incidentov.
- Zlepšenie kontextu:
  - obohacovanie a spojenie udalostí dáva úplný obraz.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

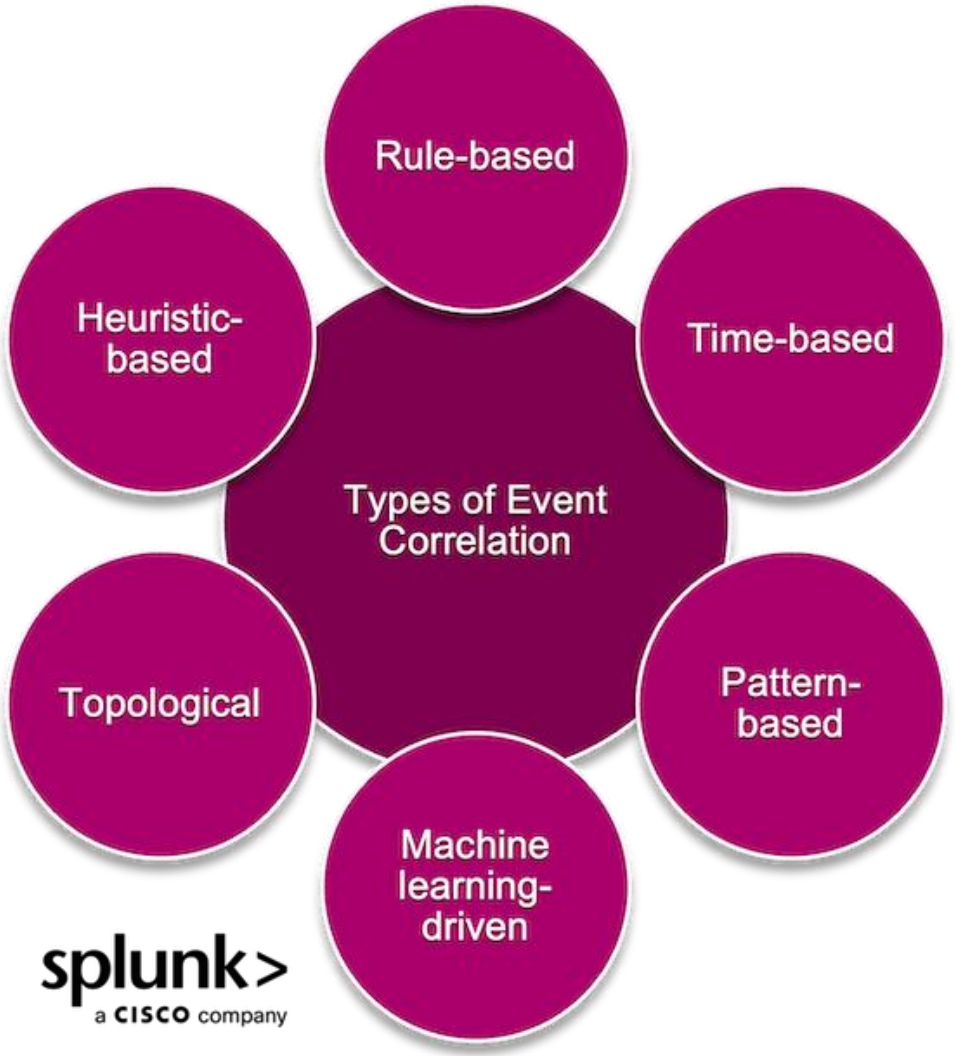
Typy korelácie

- Korelácia založená na pravidlách (rule-based): ak A a B v čase T → alert
- Korelácia na základe časovej sekvencie (sequence detection): napr. scan → prihlásenie → privilege escalation
- Korelácia využívajúca kontext (asset owner, kritickosť)
- Behaviorálna korelácia / anomaly detection: porovnanie súčasného správania s baseline.
- Graph-based korelácia: vytváranie grafu entít (user, host, IP, proces) a hľadanie malých „zhlukov“ neprirodzených spojení.



Kľúčové princípy dobrej korelácie

- Kontext je kráľ: ip→hostname→user→asset owner→risk score.
- Určiť pred- a post-incidentné signály (pre- a po-exfiltrácii).
- Časová okná: definovať vhodné okná (napr. 5 min, 1 hod, 24 hod) podľa typu incidentu.
- Prioritizácia: použiť scoring (váhy udalostí) namiesto binárnych pravidiel.
- Robustnosť proti false positives: pridať prahy, whitelisting, reputačné filtre.
- Auditovateľnosť: korelačné pravidlá by mali byť verziované a dokumentované.
- Testovanie: simulovať útoky (tabletop exercises) a doladiť pravidlá.



Ďalšie vylepšenia korelácie

Scoring a prioritizácia

- Každému eventu priradiť skóre, napr.:
  - failed_login=1,
  - malware_detected=100.
- Aggregovať skóre pre entitu (user/host) v časovom okne.
- Ak skóre prekročí prah → alert vyššej priority.

Mapovanie na tieňové techniky (MITRE ATT&CK)

- **„Tieňové techniky“** = techniky útočníkov, ktoré sú **ťažko viditeľné alebo zle detegovateľné**, pretože sa maskujú za legitímne procesy, používajú systémové nástroje alebo bežia v mene dôveryhodných používateľov.
- Názov teda metaforicky znamená: *„techniky operujúce v tieni viditeľného systému“.*
- **Mapovanie na „tieňové techniky“** v kontexte bezpečnostného monitorovania znamená:
  - priradiť konkrétne korelačné pravidlá, alerty a detekcie k tým technikám, ktoré útočníci často používajú skryto (v „tieni“).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

techniky, ktoré sa ťažko odhaľujú v logoch

„Tieňové techniky“ útokov

Oblasť útoku	Príklad techniky	Prečo sa ťažko odhaľuje
Spúšťanie kódu	PowerShell, WMI	Používajú sa aj na bežnú administráciu, vyzerajú legitímne
Krádež prístupov	LSASS dumping	Prebieha ako systémový proces s vysokými právami
Zotrvanie v systéme	Naplánované úlohy, registry kľúče	Vyzerá ako štandardné správanie systému
Obchádzanie obrany	Obfuskácia skriptov	Kód je úmyselne „zamaskovaný“, ťažko čitateľný
Únik dát	HTTPS, cloudové úložiská	Dáta odchádzajú cez povolené a šifrované kanály
Riadenie útoku	DNS tunneling, ICMP	Využívajú sieťové protokoly, ktoré sa bežne nepodozrievajú

- Útočníci často **nepoužívajú „hackerské nástroje“**
- Zneužívajú **bežné systémové funkcie**
- V logoch sa správajú:
  - **legitímne**
  - **nenápadne**
  - **bez jasného podpisu útoku**
- Preto **nestačí len zbierať logy**, ale je nutné ich **vyhodnocovať v kontexte správania**
- Bez korelácie a behaviorálnej analýzy zostávajú tieto techniky „v tieni“
- Pre každý korelačný scenár je preto vhodné pridať MITRE ATT&CK techniku, napr.:
  - Brute Force=T1110,
  - Data Exfiltration=T1041.
  - To pomáha pri reportovaní a tvorbe playbookov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Problémy a obmedzenia

- Artefakty heterogénnych systémov → ťažké normalizovať.
- Evasive techniques: útočník môže rozložiť akcie v čase (slow and low).
- Alert fatigue: príliš veľa poplachov znefunkční tím.
- Závislosť na kvalite logov — korelácia je len tak dobrá, ako sú logy.

Prečo je vyladďovanie monitorovania zdĺhavé?

- **Každé prostredie je iné**
  - Logy, ktoré sú dôležité v jednej organizácii, môžu byť irelevantné v inej.
  - Tuning si vyžaduje pochopenie konkrétnej infraštruktúry, procesov a správania používateľov.
- **Veľké množstvo dát a šumu**
  - SIEM zbiera obrovské objemy logov – väčšina nie je bezpečnostne významná.
  - Trvá dlho, kým sa odfiltruje „normálny“ šum a zostanú len relevantné udalosti.
- **Iteratívny proces**
  - Ladenie sa robí v cykloch: nasadiť → testovať → analyzovať → upraviť → znovu testovať.
  - Každá zmena pravidla alebo logu môže ovplyvniť iné korelácie.
- **Zmeny v prostredí**
  - Pridávajú sa nové systémy, aktualizujú aplikácie, mení sa sieťová topológia — to všetko mení aj správanie logov, takže tuning nikdy nie je „hotový“.
- **Nedostatok kontextu a kvalitných vzoriek útokov**
  - Aby sa detekcie doladili správne, je potrebné testovať na reálnych dátach a incidentoch, čo si vyžaduje čas aj skúsenosti.

Praktické odporúčania pri logovaní (Checklist)

Na začiatok

- Vypracovať logging policy (kto, čo, prečo, retencia).
- Inventarizovať kritické systémy a definovať minimálny logovací set.
- Zaviesť centralizované ukladanie logov (SIEM/central log store).
- Definovať vlastné korelačné pravidlá pre najkritickejšie use-cases (autentifikácia, administrácia, exfiltrácia).

Prevádzka

- Testovať a dolaďovať pravidlá (pravidelne).
- Merať MTTD/MTTR a ciele zlepšovania.
- Zabezpečiť playbooky a pravidelné školenia.
- Zabezpečiť audit logov a integritu.

Bezpečnosť a compliance

- Minimalizovať osobné údaje v logoch; ak sú, zabezpečiť prístup a retention.
- Dokumentovať všetky pravidlá korelácie a incident response kroky.
- Udržiavať záznamy o prístupe k logom pre audit.

Hlásenie udalostí a incidentov

Hlásenie udalostí a incidentov

Prečo hlásiť

- Hlásenie nie je len interná vec – často ide aj o **povinnosť podľa zákona** (Zákon o KB, GDPR).
- Správne hlásenie umožňuje:
  - rýchle zapojenie reakčných tímov,
  - zdieľanie informácií s CSIRT/SOC,
  - zníženie dopadov incidentu.

Kto hlási a komu

- **Interný používateľ** → lokálny správca / IT oddelenie,
- **IT oddelenie / SOC** → manažér KB,
- **Manažér KB** → vedenie, CSIRT tím, regulačný orgán.

Čo obsahuje hlásenie

- Dátum a čas incidentu,
- Popis udalosti,
- Dotknuté systémy a dáta,
- Pravdepodobná príčina,
- Prijaté opatrenia,
- Odporúčania do budúcna.

- Manažér by mal zabezpečiť:
  - existenciu **procesu eskalácie**,
  - školenie zamestnancov o **povinnosti hlásiť incidenty**,
  - **jasné kanály komunikácie**,
  - následnú **analýzu a spätnú väzbu**.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Legislatíva v SR: Zákon 69/2018 Z. z.

Hlásenie závažného kybernetického bezpečnostného incidentu (KBI)

§ 24 Hlásenia (regulačnému orgánu)

a) do 24 hod. od jeho zistenia - **včasné varovanie**:
   - či závažný KBI
     - mohol byť spôsobený protiprávnym konaním,
     - alebo či môže mať cezhraničný vplyv,
     - a ak ide o PZS, ktorý je poskytovateľom dôveryhodných služieb, uvádza sa tiež vplyv na poskytovanie dôveryhodných služieb,

b) do 72 hodín od jeho zistenia – **oznámenie**:
   - aktualizujú sa a dopĺňajú informácie z včasného varovania,
     - prvotné posúdenie KBI, jeho závažnosti a následkov
     - ak ide o PZS, ktorý je poskytovateľom dôveryhodných služieb bez zbytočného odkladu, avšak najneskôr do 24 hodín od jeho zistenia,

c) na žiadosť toho, kto prevádzkuje jednotku CSIRT, sa v určenej lehote hlásia
   - aktualizované alebo iné **vyžiadané informácie** o priebehu závažného KBI,

d) najneskôr 1 mesiac po nahlásení oznámenia podľa písmena b) sa hlási **záverečná správa**
   - podrobný opis, závažnosť, následky
   - druh kybernetickej hrozby alebo hlavnú príčinu, ktorá pravdepodobne KBI spôsobila,
   - zavedené a prebiehajúce opatrenia a cezhraničný vplyv, ak existuje,

e) ak ide o závažný KBI s cezhraničným vplyvom, ktorý v lehote podľa písmena d) stále trvá, hlási sa do 30 dní odo dňa obnovy riadnej prevádzky siete a informačného systému **aktualizovaná záverečná správa** v rozsahu podľa písmena d);
   - ak v čase predkladania záverečnej správy podľa písmena d) závažný kybernetický bezpečnostný incident ešte prebieha, hlásia sa ďalšie aktualizované alebo iné vyžiadané informácie a aktualizovaná záverečná správa do 30 dní odo dňa, keď sa závažný kybernetický bezpečnostný incident vyriešil.

Legislatíva v SR: Zákon 69/2018 Z. z.

Hlásenie incidentu

- Hlásenie: https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html

Na nahlásenie incidentu vyberte jednu z nasledovných možností:

Hlásenie cez Jednotný informačný systém kybernetickej bezpečnosti

Zvoľte túto možnosť, ak máte pridelený prístup do JISKB, napríklad ak **ste prevádzkovateľom základnej služby** podľa Zákona 69/2018 Z.z. o kybernetickej bezpečnosti.

Nahlásenie incidentu

Zvoľte túto možnosť, ak nemáte pridelený prístup do JISKB, vrátane hlásení od verejnosti.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Monitorovanie, zaznamenávanie a hlásenie udalostí

Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk