KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

09 Manažment bezpečnostných informácií a udalostí

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Manažment bezpečnostných informácií a udalostí

- manažment bezpečnostných informácií a udalostí
- analýza a agregácia sieťových údajov

Manažment udalostí

- počítačové siete a systémy generujú obrovské množstvo logov a udalostí
- kybernetické hrozby sa prejavujú v dátach roztrúsene a v súvislostiach
- manuálna analýza nestíha pokryť objem a rýchlosť útokov
- cieľ: včasná detekcia, vyšetrovanie a reakcia na incidenty
- riešenie: centralizovaný zber a korelácia – SIEM

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SIEM (I.)

- **SIM** - Security Information Management (dlhodobé uchovanie, reporty)
- **SEM** - Security Event Management (real-time monitoring, alerty)

- SIEM spája obe oblasti do jedného systému
  - poskytuje prehľad o bezpečnostnom stave organizácie
  - podporuje súlad s reguláciami a audity

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SIEM (II.)

- zber a normalizácia logov z rôznych zdrojov
- agregácia a korelácia udalostí
- detekcia hrozieb a generovanie výstrah
- dlhodobé uchovávanie a reporting
- podpora forenznej analýzy a vyšetrovania incidentov

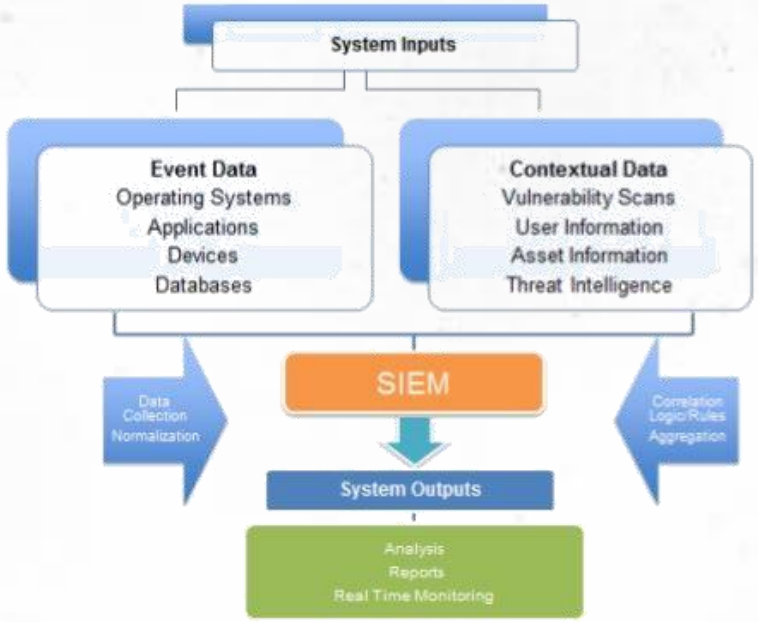
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SIEM (III.)

Zdroj: Claude Opus, spracované podľa RFC 4303 (IETF) – https://datatracker.ietf.org/doc/html/rfc4303

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SIEM (IV.)



Zdroj: https://www.logsign.com/blog/security-information-and-event-management-architecture/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Zdroje údajov

- firewally, smerovače a prepínače
- IDS/IPS senzory a antivírusové systémy
- servery, operačné systémy a aplikácie
- koncové stanice (EDR) a autentizačné systémy
- sieťové toky (NetFlow/IPFIX) a DNS/proxy logy

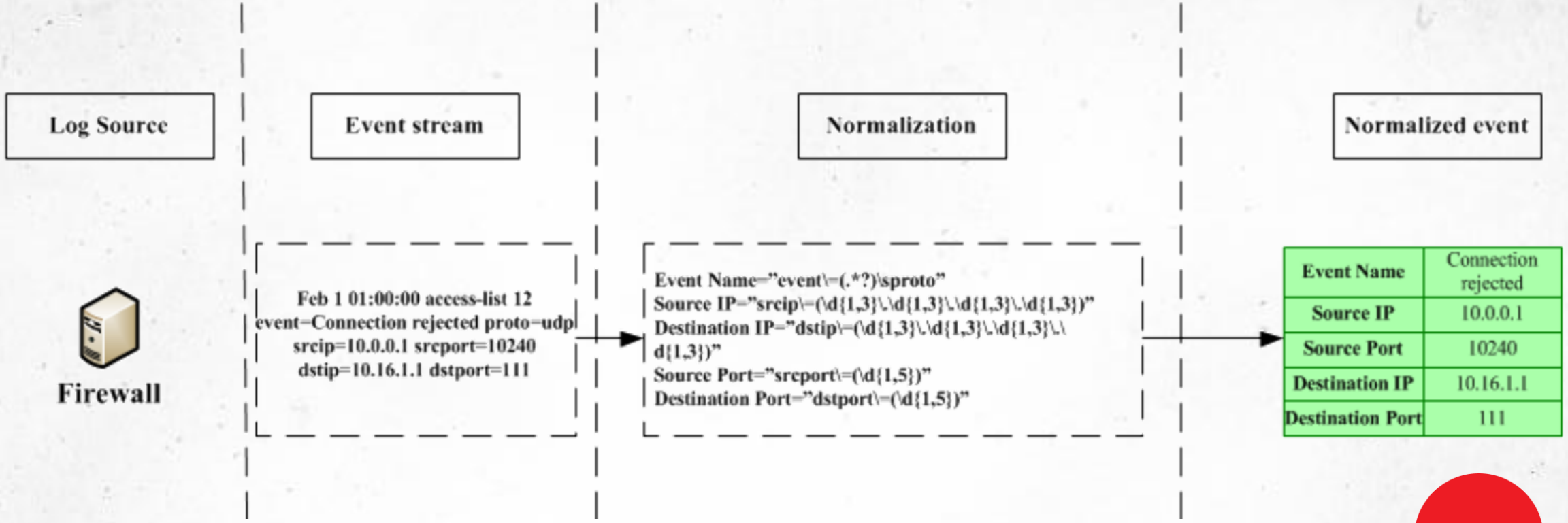
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Zber a normalizácia (I.)

- agenti alebo bezagentový zber (syslog, API)
- rôzne formáty logov → jednotná štruktúra
- časová synchronizácia (NTP) je nevyhnutná
- obohatenie údajov o kontext (geolokácia, aktíva)
- spoľahlivé a bezpečné doručenie do SIEM

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Zber a normalizácia (II.)



Zdroj: https://vpotapov.wordpress.com/2017/02/13/event-normalization/

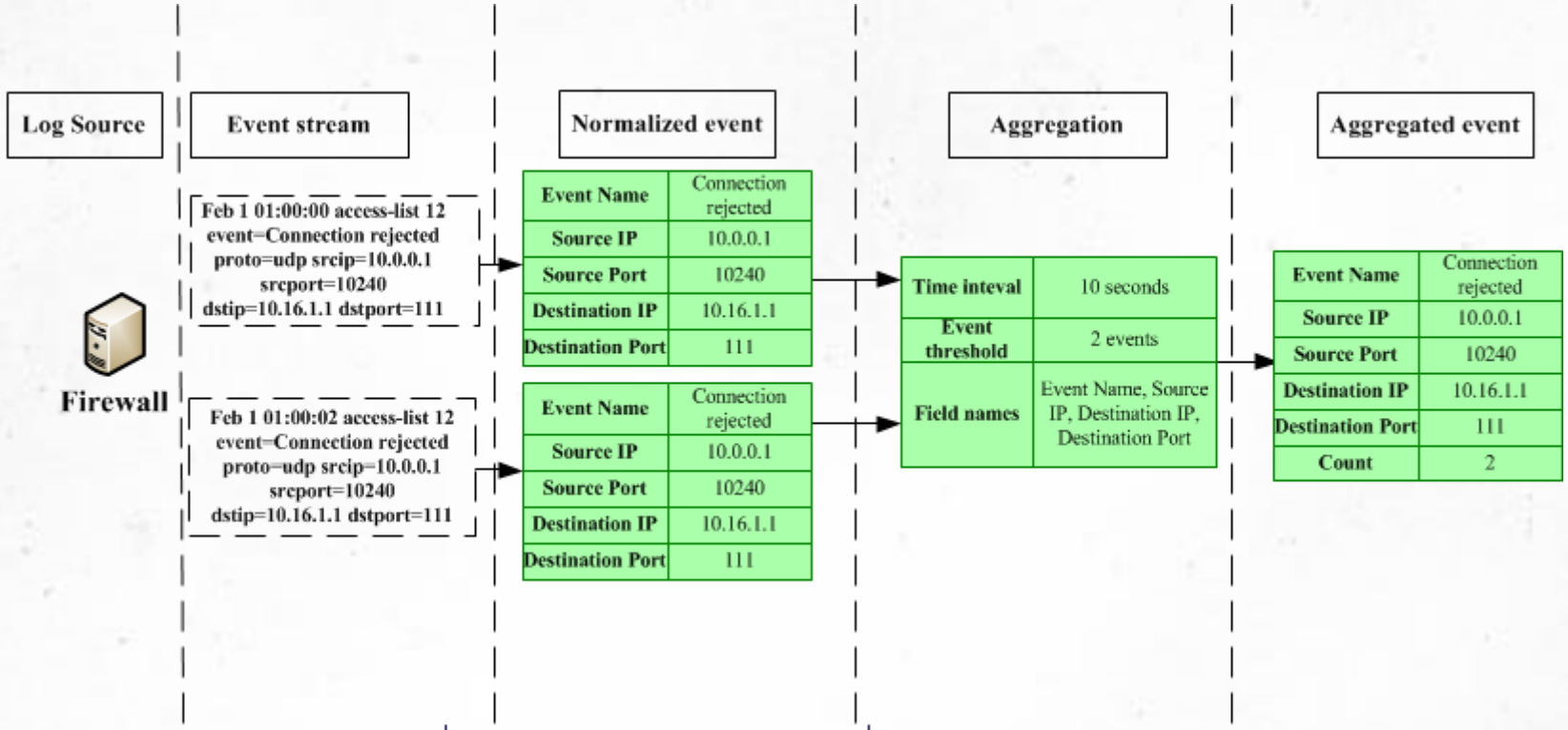
Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Analýza a agregácia sieťových údajov (I.)

- **agregácia**
  - zlúčenie podobných a opakujúcich sa udalostí
  - znižuje šum a objem dát na spracovanie
- **korelácia**
  - hľadanie súvislostí medzi udalosťami
  - pravidlá, prahy a sekvencie udalostí odhaľujú útok
- výsledok: menej, ale významnejších bezpečnostných výstrah

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Analýza a agregácia sieťových údajov (II.)



Zdroj: https://vpotapov.wordpress.com/2017/03/20/event-aggregation/

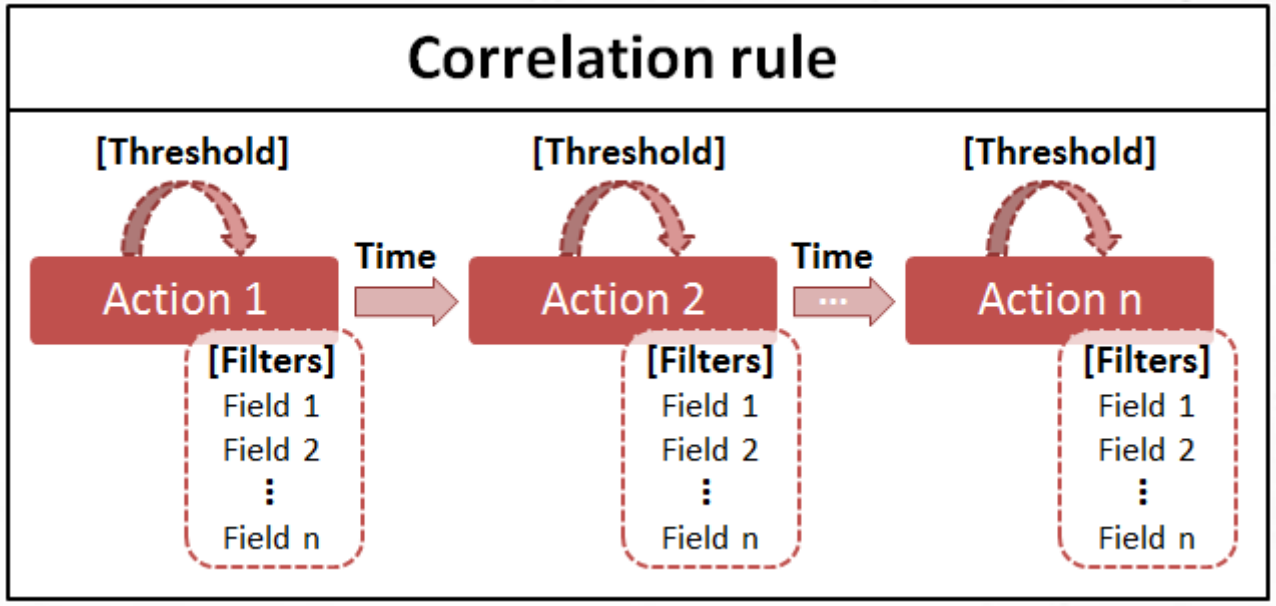
Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Korelačné pravidlá (I.)

- príklad: viacero neúspešných prihlásení + úspešné = brute force
- časové okná a postupnosti udalostí
- kombinácia údajov z viacerých zdrojov
- statické pravidlá vs. detekcia anomálií (UEBA)
- ladenie pravidiel proti falošným poplachom

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Korelačné pravidlá (II.)



Zdroj: https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/Real-timeEventCorrelation/correlation-concepts.html

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vyhodnotenie

- false positive - falošný poplach (nadbytočná práca analytika)
- false negative - nezachytený reálny incident (vážne riziko)
- priorizácia výstrah podľa rizika a kontextu
- ladenie pravidiel znižuje šum
- cieľ: presné a akcieschopné výstrahy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SIEM a SOC

- SOC (Security Operations Center) - tím a procesy reakcie
- SIEM je hlavný technologický nástroj SOC
- doplnenie o SOAR – automatizácia a orchestrácia reakcie
- threat intelligence obohacuje detekciu o aktuálne hrozby
- nepretržitý monitoring (24/7) kritických prostredí

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť