Stealthwatch architektúra

Stanislav Smolár, SOITRON, s.r.o. (stanislav.smolar@soitron.com)

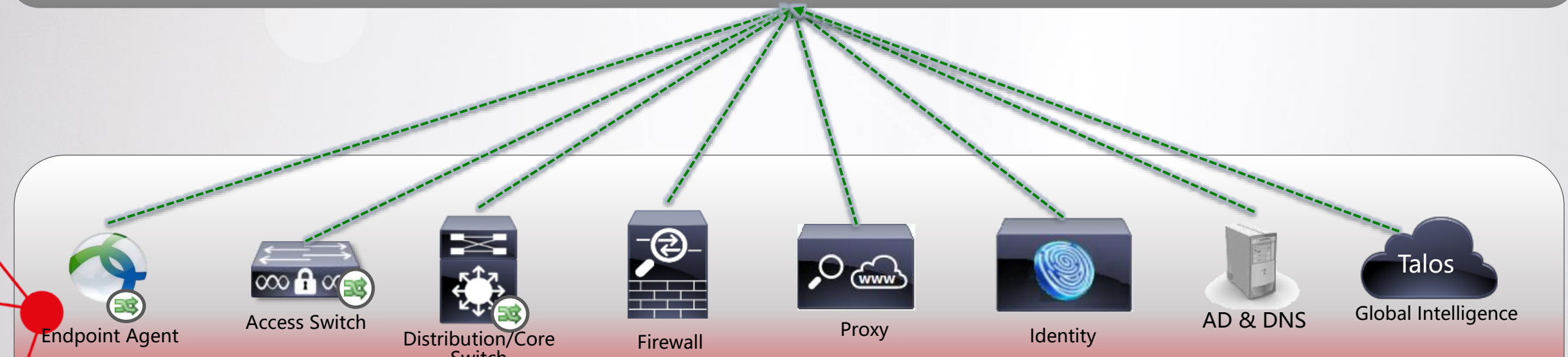
SOITRON

Čo je behaviorálna analýza?

SOITRON

Sieťová telemetria

Telemetria alebo diaľkové meranie alebo meranie na diaľku je metóda prenosu údajov meranej veličiny na diaľku resp. technické prostriedky na takéto meranie.
https://sk.wikipedia.org/wiki/Telemetria



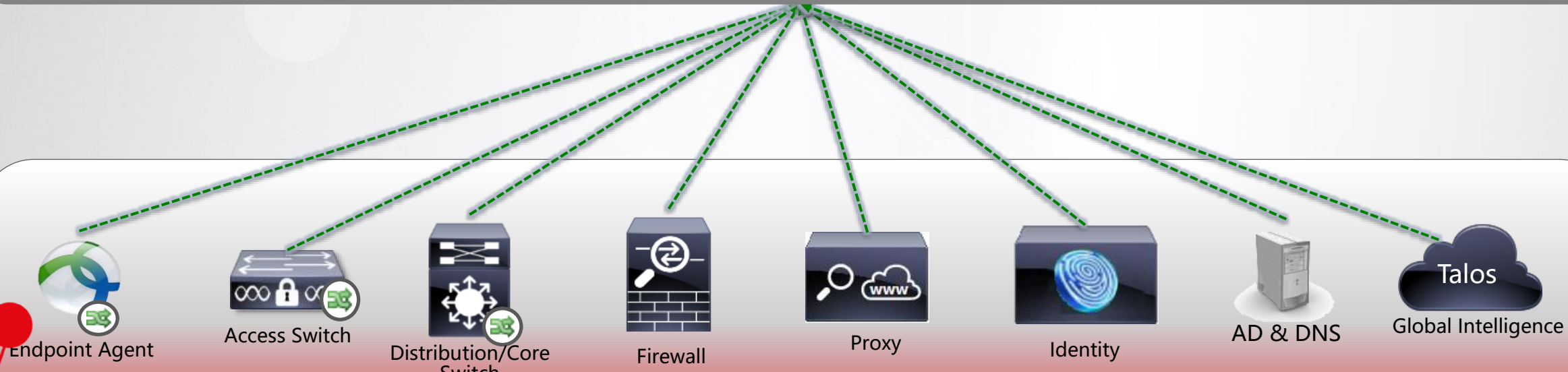
Sieťové zariadenia

Izolované informácie na základe funkcie a polohy

SOITRON

Cisco Stealthwatch

Cisco Stealthwatch: nástroj na zber a agregáciu sieťovej telemetrie na účely bezpečnostnej analýzy a monitorovania.



Sieťové zariadenia

Izolované informácie na základe funkcie a polohy

SOITRON

Stealthwatch komponenty

Stealthwatch Enterprise
- On-premises zariadenia
- On-premises viditeľnosť a kolekcia telemetrie

Stealthwatch Cloud
- Hostovaná v Cloude; SaaS
- Public cloud (IaaS) monitoring
- On-prem viditeľnosť pre malé nasadenia

Stealthwatch Cloud

SOITRON

Stealthwatch Enterprise architektúra

Cognitive Analytics
- Cloud hostované analytika
- Globálna mapa rizík

Cognitive Analytics

Stealthwatch Cloud

Threat Intelligence
- Známe C&C servery
- TOR vstupy & výstupy

Threat Intelligence License

Stealthwatch Host Classifier
- Cloud hosted profiler
- Navrhuje klasifikáciu
- Novinka v 7.0

Stealthwatch Host Classifier

Cisco Security Packet Analyzer
- full packet capture
- 2 physical models

Stealthwatch Management Console
- Manažment a Reporting
- Až 25 Flow Collectorov
- Až 6 000 000 fps na celom svete
- 2 fyzické a virtuálne modely
- Vysoká dostupnosť

FC

Stealthwatch Flow Collector
- Zhromažďuje a analyzuje flow dáta
- Až do 4000 exportérov
- Až do 240,000 fps
- 4 fyzické a 3 virtuálne modely

UDP Director
- UDP Packet Copier
- forward UDP do viacerých destinácií
- Vysoká dostupnosť
- 2 fyzické a virtuálne modely

FR

EC

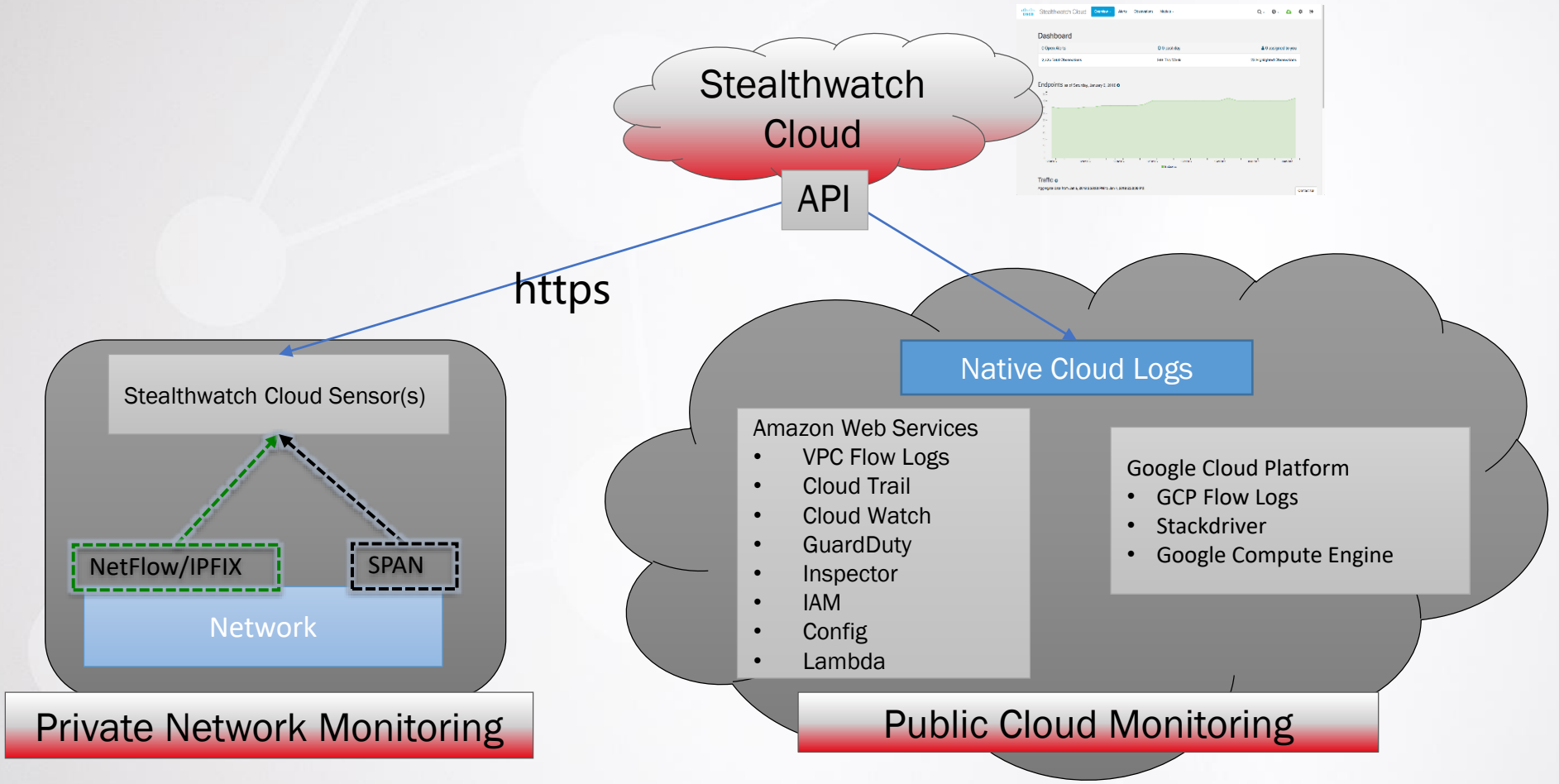
FS

Stealthwatch Flow Sensor
- Generuje IPFIX from SPAN/TAP
- 256 bytes payloadu
- 7.0 ETA EXPORT!!

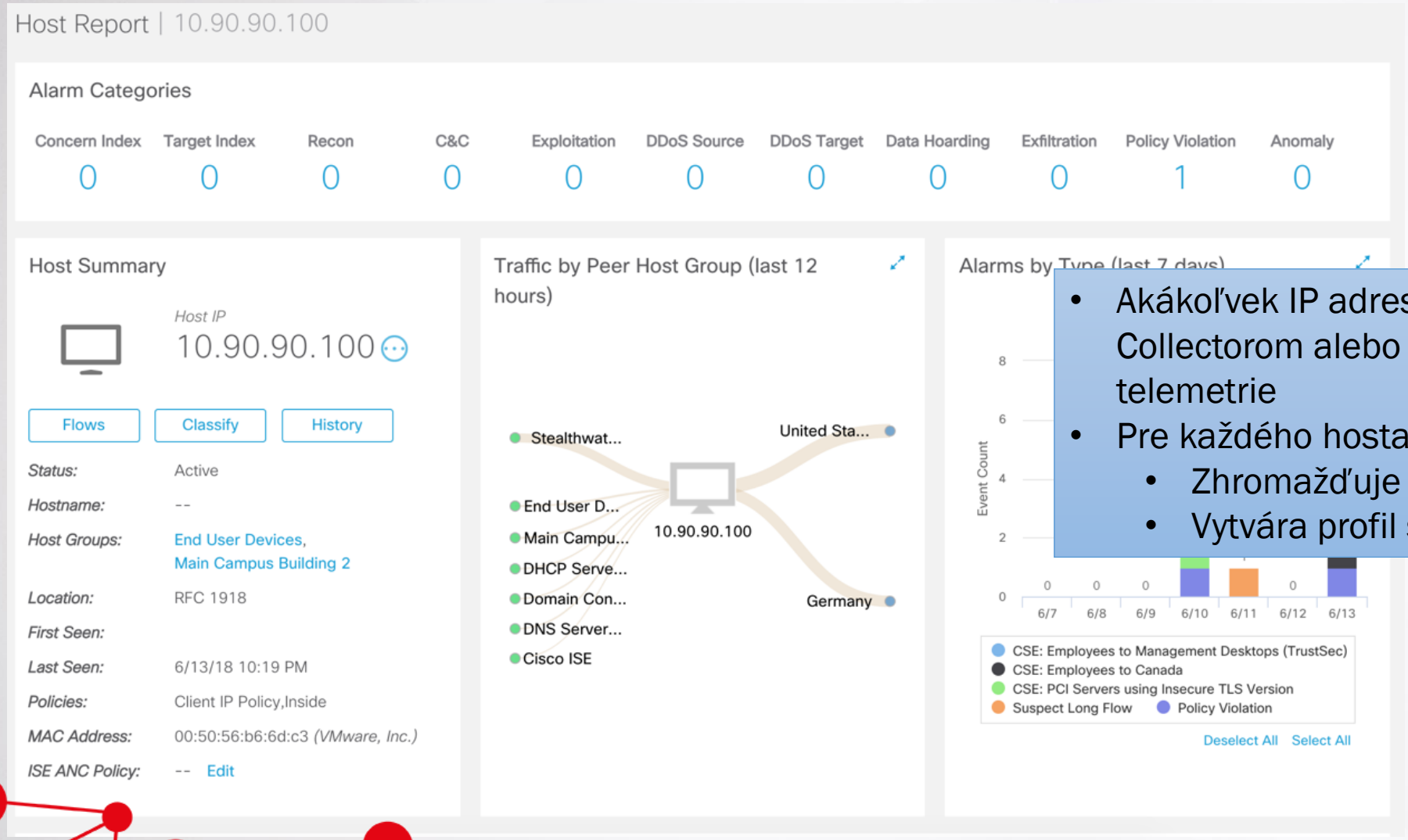
Endpoint License Concentrator
- Zber AnyConect NVM flow dát a preposlanie do Flow Collector
- Virtual Appliance

SOITRON

Stealthwatch Cloud architektúra



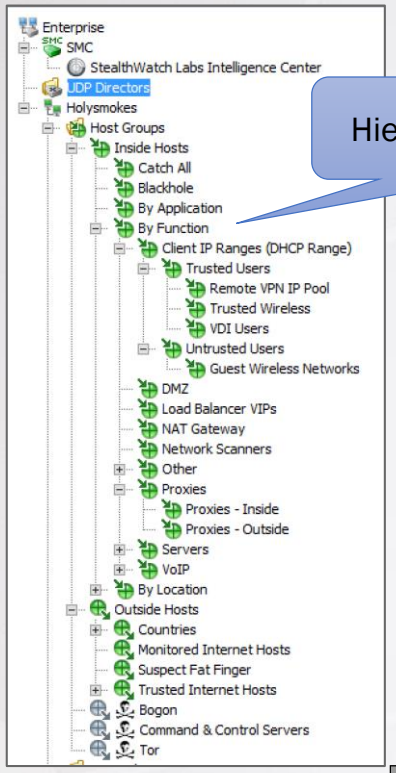
Koncept: Host



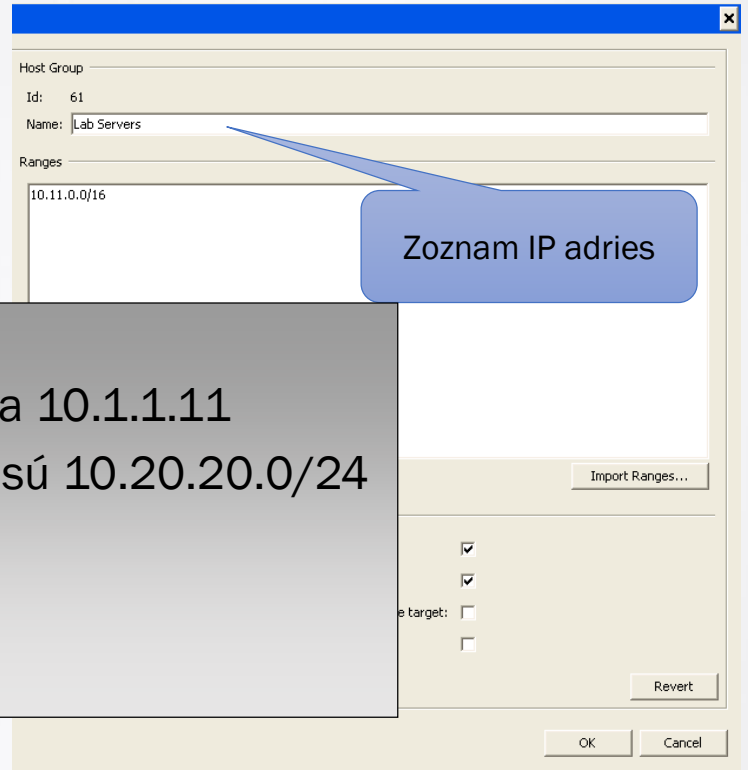
- Akákoľvek IP adresa pozorovaná Flow Collectorom alebo SMC zo zdrojov telemetrie
- Pre každého hosta, Stealthwatch
  - Zhromažďuje metaúdaje
  - Vytvára profil správania

SOITRON

Koncept: Host Groups



Hierarchická štruktúra



Zoznam IP adries

Príklady:

Moje DNS servery sú 10.1.1.10 a 10.1.1.11

Všetky moje platobné terminály sú 10.20.20.0/24

Moje HQ je 10.0.0.0/8

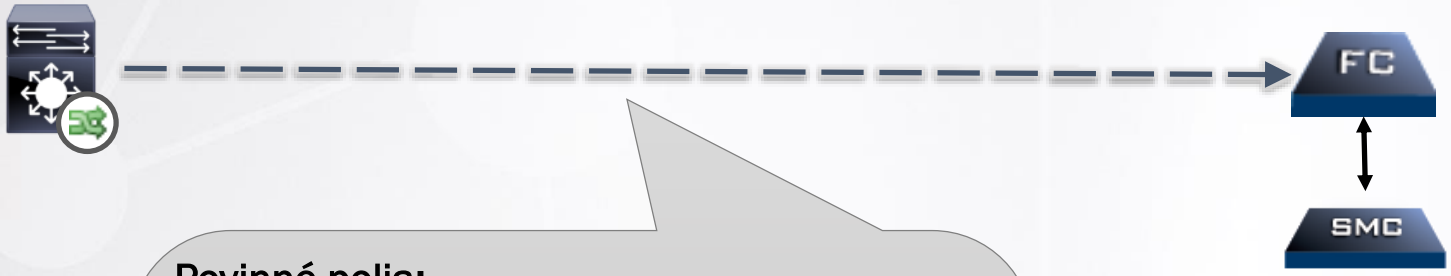
Atď.

- Host môže existovať vo viacerých Host Groups
- Host nemôže byť súčasne Inside a Outside

SOITRON

Základné flow dáta

Stealthwatch vyžaduje určité polia na vytvorenie záznamu do databázy:



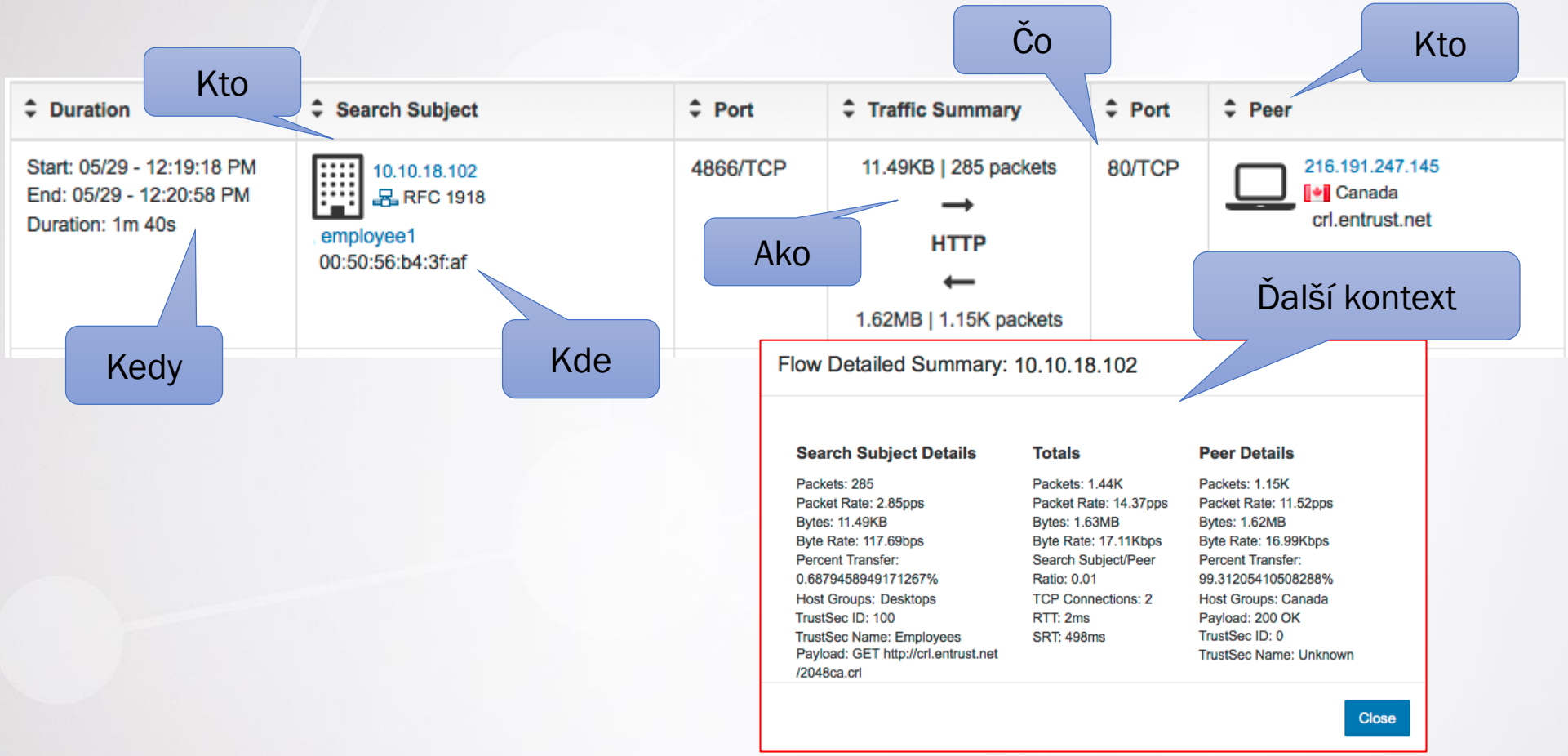
Povinné polia:
Source IP Address

- Source Port
- Destination IP Address
- Destination Port
- IP Protocol
- Byte count
- Packet count
- Start time (first switched)
- End time (last switched)
- Input Interface (*recommended*)

Ďalšie polia sú meta údaje, ktoré umožnia rozšírenú analytiku

SOITRON

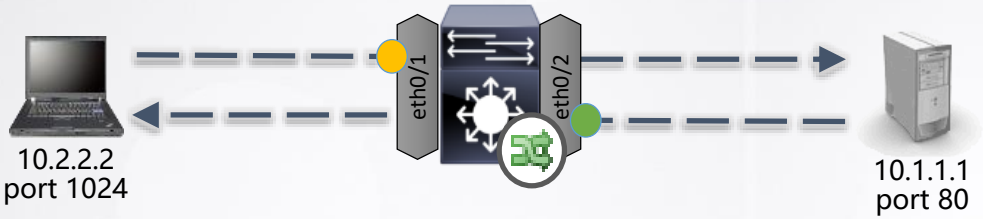
Základný flow záznam



SOITRON

Spracovanie telemetrie: deduplikácia flow dát

Jednosmerné flow records



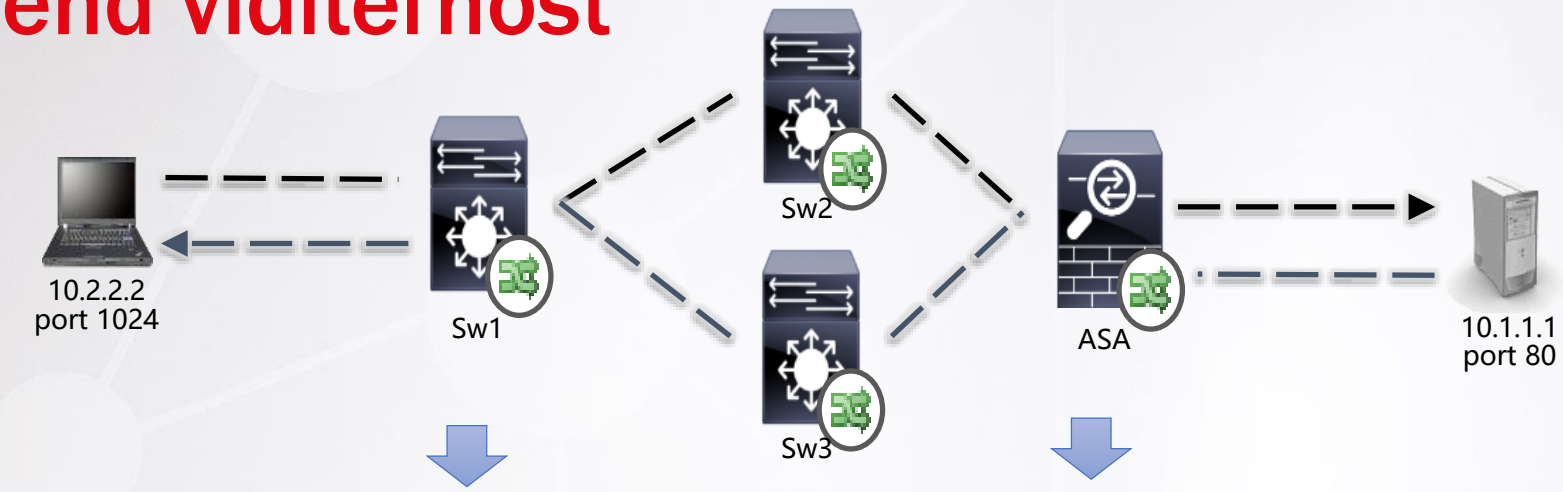
Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100

Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Client SGT	Server SGT	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	100	1010	eth0/1 eth0/2

Obojsmerné flow records:
- Conversation flow record
- Umožňuje jednoduchú vizualizáciu a analýzu

SOITRON

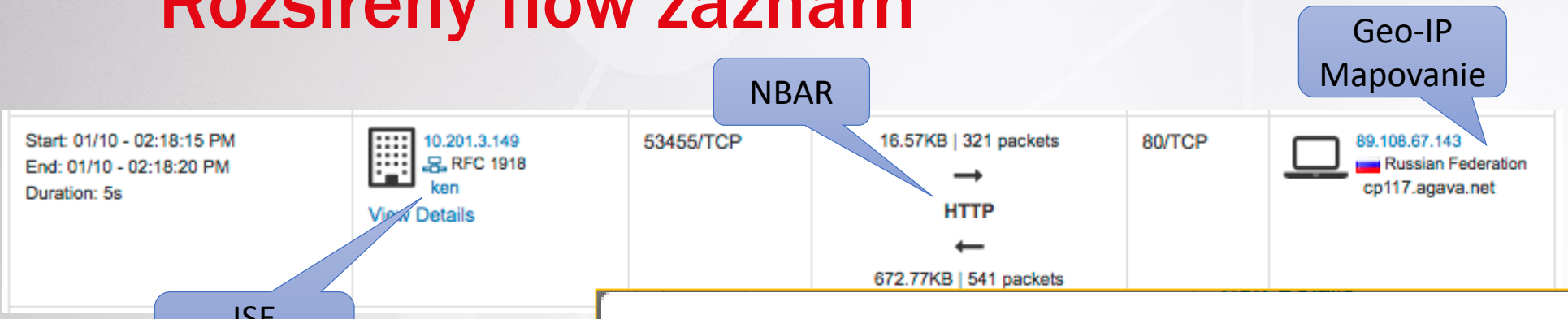
End to end viditeľnosť



Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	App	Client SGT	Server SGT	Exporter, Interface, Direction, Action
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	HTTP	100	1010	Sw1, eth0, in Sw1, eth1, out Sw2, eth0, in Sw2, eth1, out ASA, eth1, in **ASA**, eth0, out, Permitted ASA eth0, in, Permitted ASA, eth1, out Sw3, eth1, in Sw3, eth0, out Sw1, eth1, in Sw1, eth0, out

SOITRON

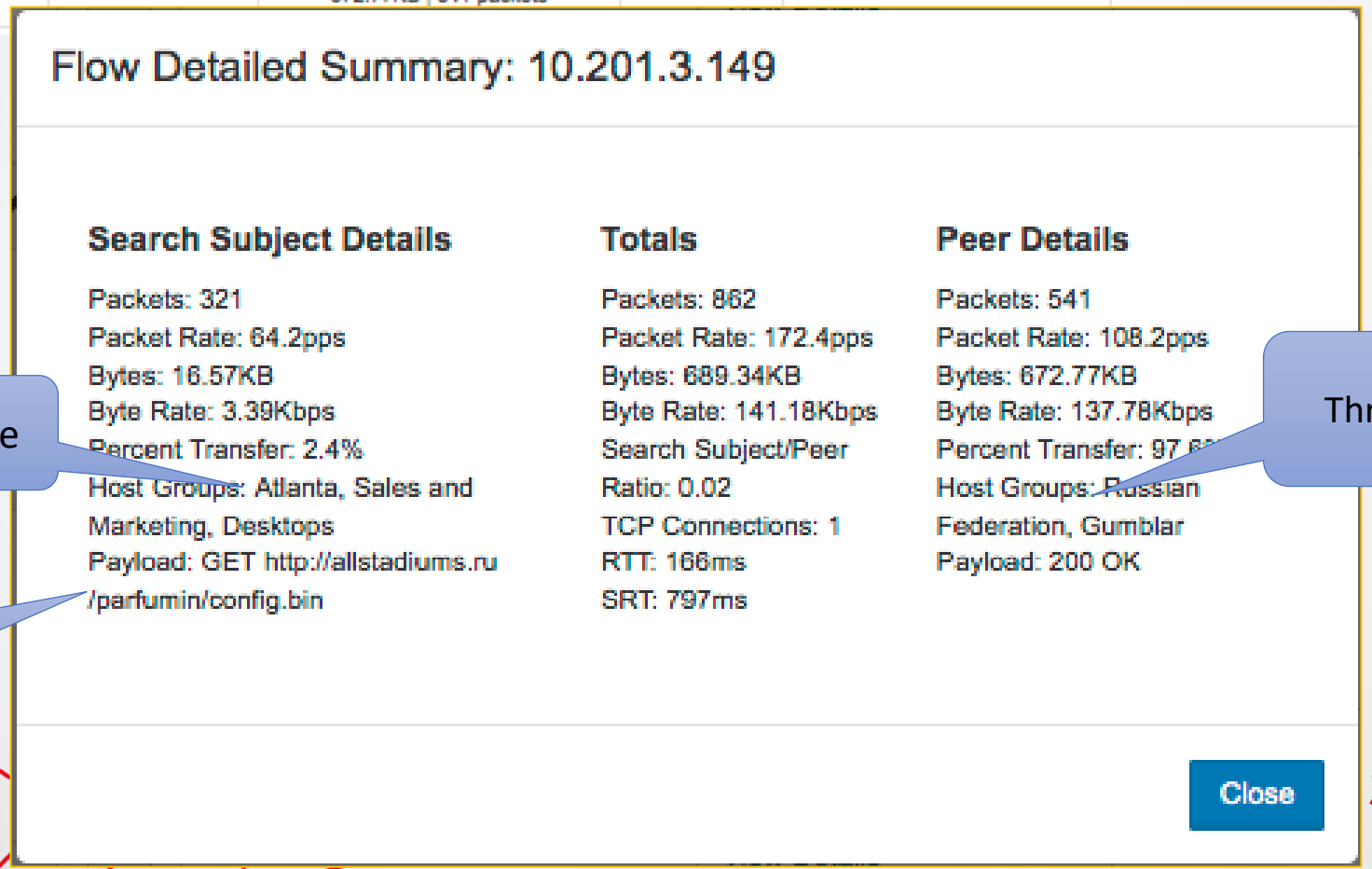
Rozšírený flow záznam



NBAR

Geo-IP Mapovanie

ISE Telemetria



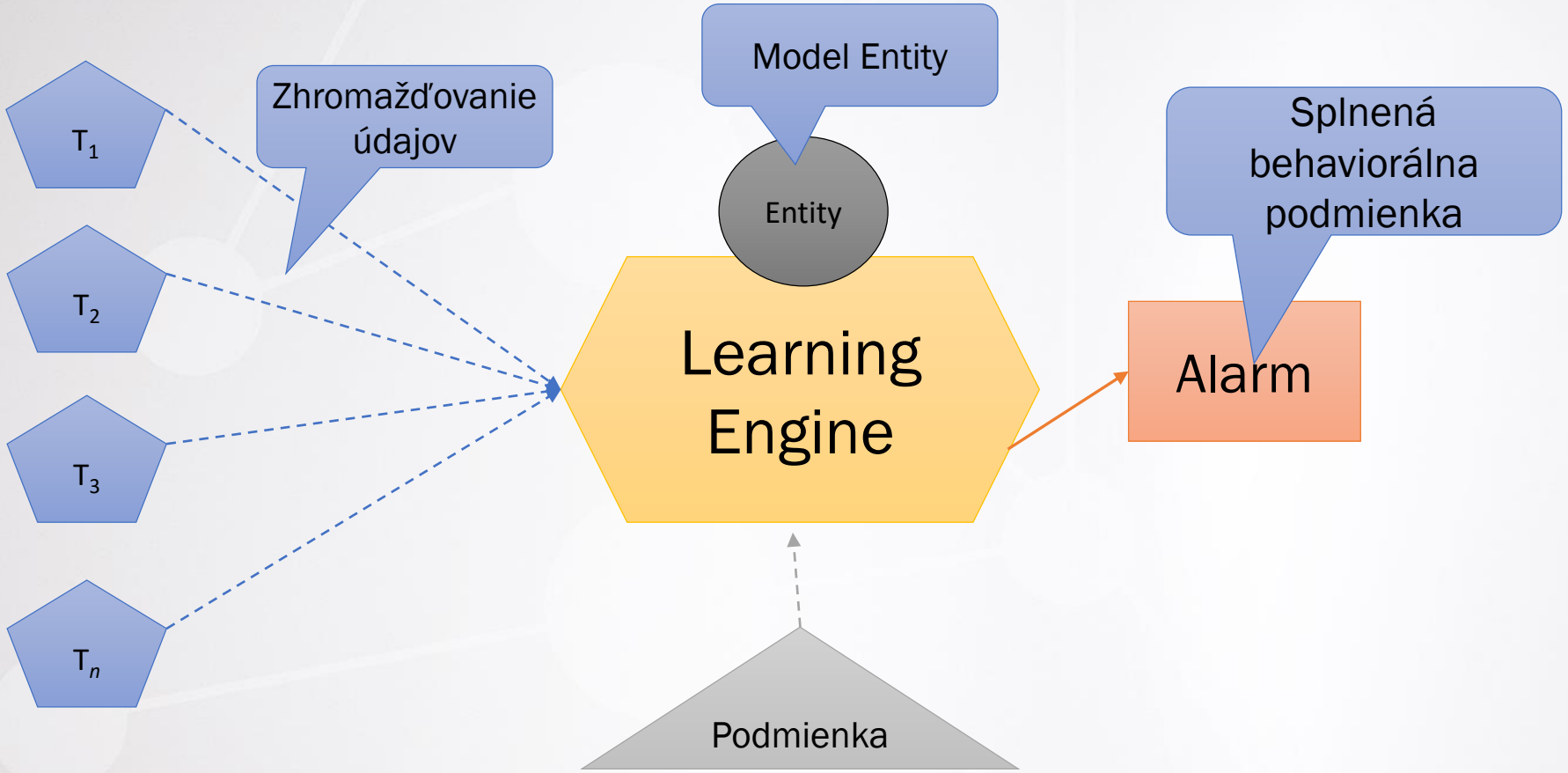
Aplikované situačné povedomie

Threat Intelligence

Flow Sensor

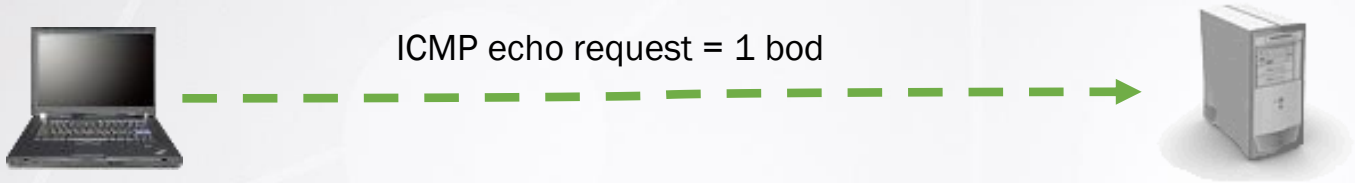
SOITRON

Learning Engine



SOITRON

Jednoduchý príklad Security Eventu: ICMP_ECHO_REQUEST



Pondelok	Utorok	Streda	Štvrtok
ICMP Points: • Dnes: 10 • 30-dňový model: 10	ICMP Points: • Dnes: 20 • 30-dňový model: 15	ICMP Points: • Dnes: 15 • 30-dňový model: 15	ICMP Points: • Dnes: 1000 • 30-dňový model: 15

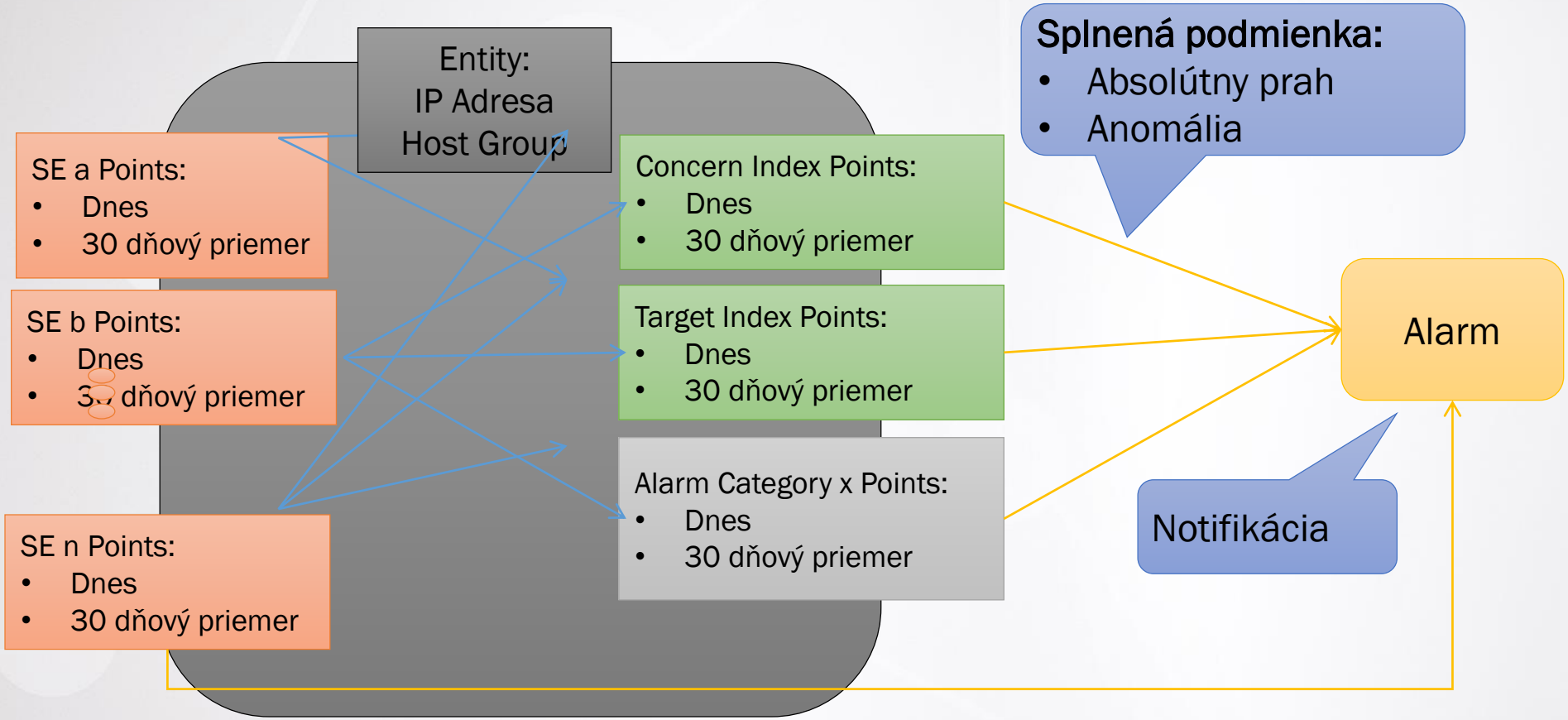
Splnená podmienka na algoritmus anomálie

Poznámka 1: Anomália vyžaduje 7 dní dát

Poznámka 2: Model je trochu zložitejší ako normálna krivka.

SOITRON

Stealthwatch „On-Box” generovanie alarmov



Stanovenie priorít alarmov

Priorita A: Závažnosť Critical

- Dobre vyladené, nízky počet
- Nízky počet false positive
- Okamžite využiteľné

Priorita B: Závažnosti Major

- Zaujímavé, vyladené, monitorované, dokumentované
- Zdroj informácii, skôr než akcie

Priority C: Severity Minor

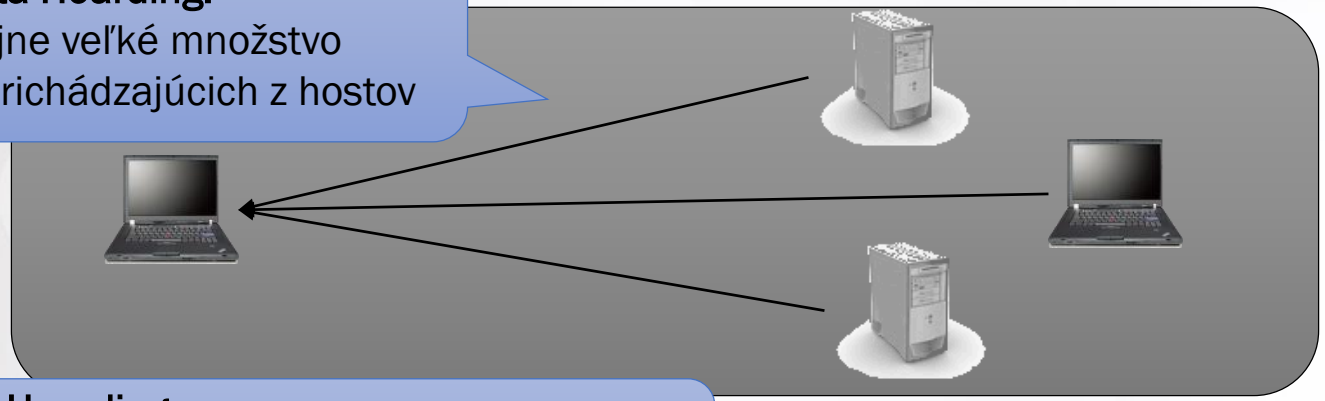
- Môže a nemusí byť zaujímavý
- Užitočné pre všeobecnú koreláciu

http://b2bcontact.com/cisco-stealthwatch/tiered_alarms

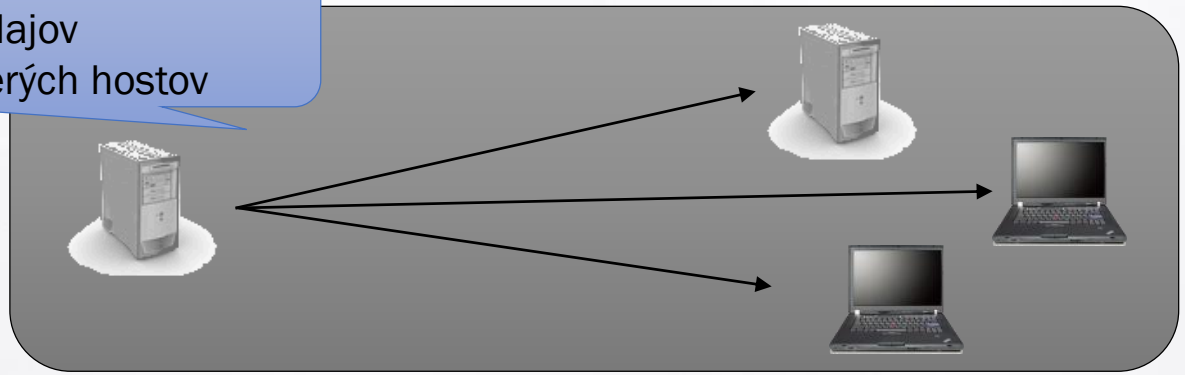
SOITRON

Príklad algoritmu: Data Hoarding

Suspect Data Hoarding:
- Nezvyčajne veľké množstvo údajov prichádzajúcich z hostov



Target Data Hoarding:
- Nezvyčajne veľké množstvo údajov odchádzajúce z hostu do viacerých hostov



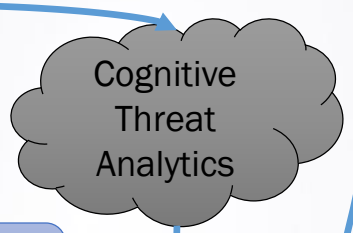
SOITRON

Umiestnenie enginov

Cognitive:
- Proxy log Tabuľky
- Bi-flows pre:
  - From Inside to Outside (default)
  - DNS from inside to anywhere
  - Z nakonfigurovaných skupín na vonkajšie a iné nakonfigurované skupiny
  - **Stealthwatch Host Classifier:**
- Všetky bi-flows

Zdroje Telemetrie

Flow Collector:
- Vytvára "General Ledger"
- Politika a behaviorálna analýza
- Štatistické learning algoritmy, zisťovanie anomálií



Detekcie zobrazené vo widgete

Host Groups zverejnené

Management a reporting

SOITRON

Príklad triedenia incidentov pre Stealthwatch toky

CONFIRMED INCIDENTS

anomaly detection + global feature cache + IOCs

10 - 3

- ad injector
- anonymization software
- banking trojan
- click fraud
- cryptocurrency miner
- exfiltration
- exploit kit
- information stealer
- malicious advertising
- malicious content distribution
- malware distribution
- maney scam
- PUA
- ransomware
- scareware
- spam botnet
- spam tracking
- trojan

DETECTED INCIDENTS

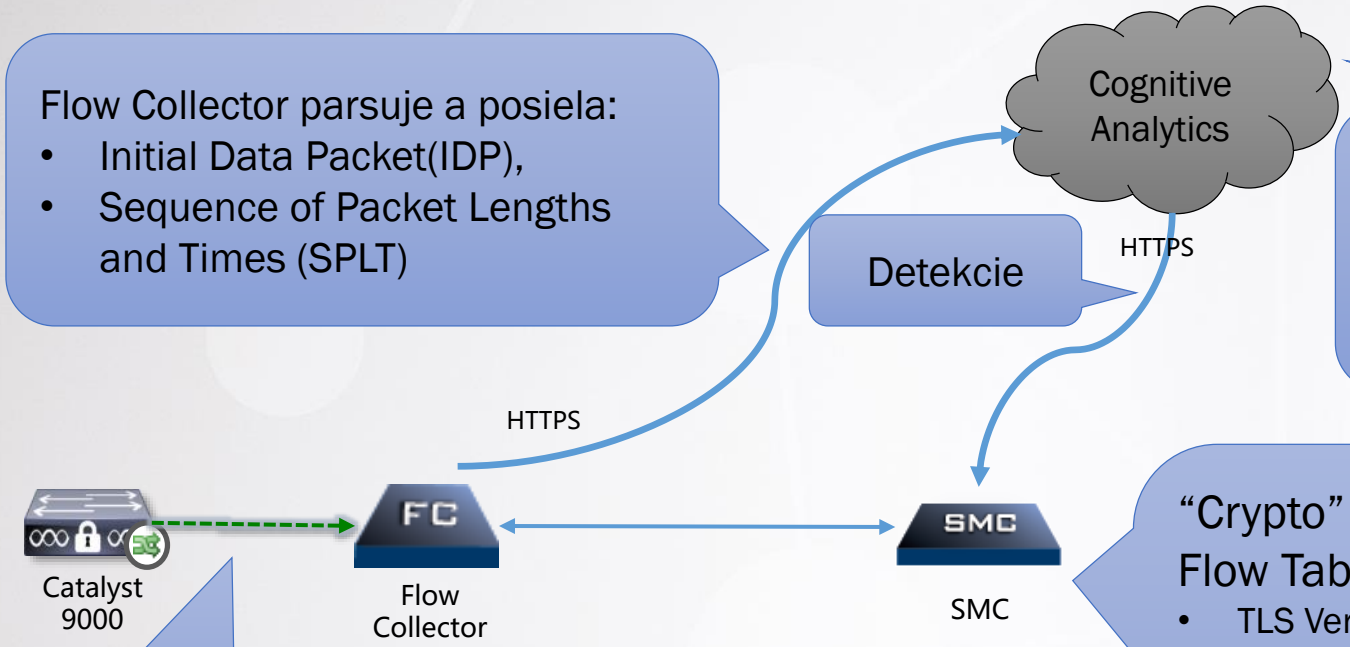
risk

- 10 cryptowall
- 9 ramnit
- 8 sality
- 8 botnet
- 8 c&c
- 8 - 6 SMB service discovery
- 7 DNS sinkhole
- 7 suspicious file download
- 7 ICMP burst
- 6 unexpected DNS usage
- 6 SSH cracking
- 5 torrent
- 5 excessive communication
- 5 vulnerability scanning tool
- 5 phishing
- 4 TOR

SOITRON

Encrypted Traffic Analytics

Flow Collector parsuje a posiela:
- Initial Data Packet(IDP),
- Sequence of Packet Lengths and Times (SPLT)



Features/IOCs sú extrahované z:
- Stealthwatch Flow
- Stealthwatch Flow + ETA
- Stealtwhatch Flow + PayloadEX

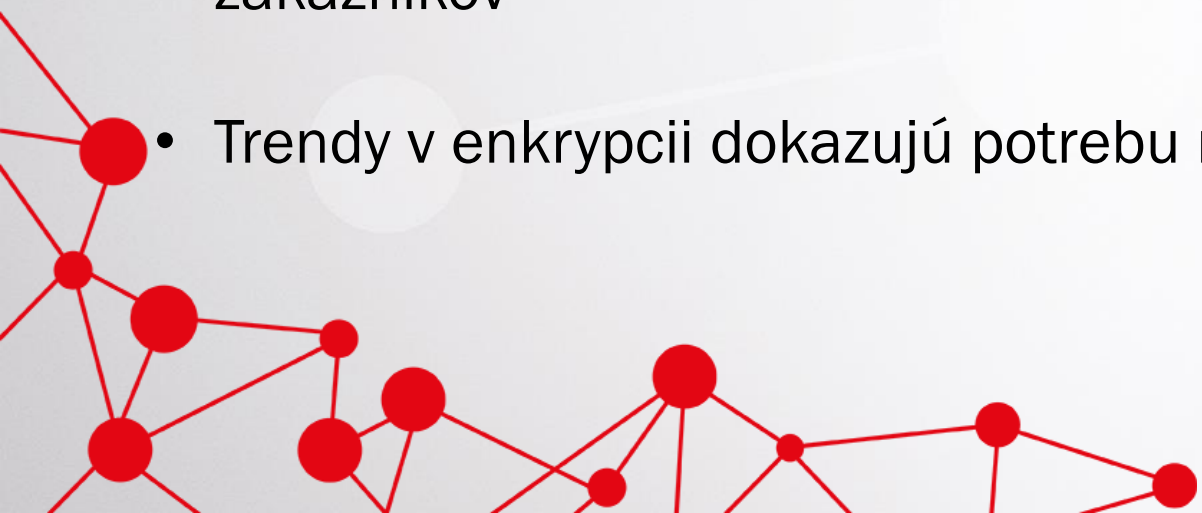
Nové polia odoslané v NetFlow

“Crypto” Informácie zobrazené v Flow Tabuľke:
- TLS Version
- TLS Extension
- Selected Cipher Suite
- Key Exchange Algorithm
- Encrypted Algorithm & Key Length
- Authentication
- MAC Algorithm

SOITRON

Pár myšlienok na záver

- Lokálna behaviorálna analytika dnes už nestačí
- Stealthwatch ponúka “best of both worlds”:
  - On premise nesupervizovaný behaviorálny system Stealthwatch Enterprise
  - Cloud supervizovaný detekčný mechanizmus Cognitive(Netflow aj Proxy logy)
- Cisco Stealthwatch a Cisco Stealthwatch Cloud kombinácia: ideálne pre hybridných zákazníkov
- Trendy v enkrypcii dokazujú potrebu riešenia ako ETA



SOITRON

SOITRON