

A large, 3D blue padlock is the central focus, set against a dark blue background filled with glowing binary code (0s and 1s) and hexadecimal characters (A-F, 0-9).

Odhalenie Cyber hrozieb

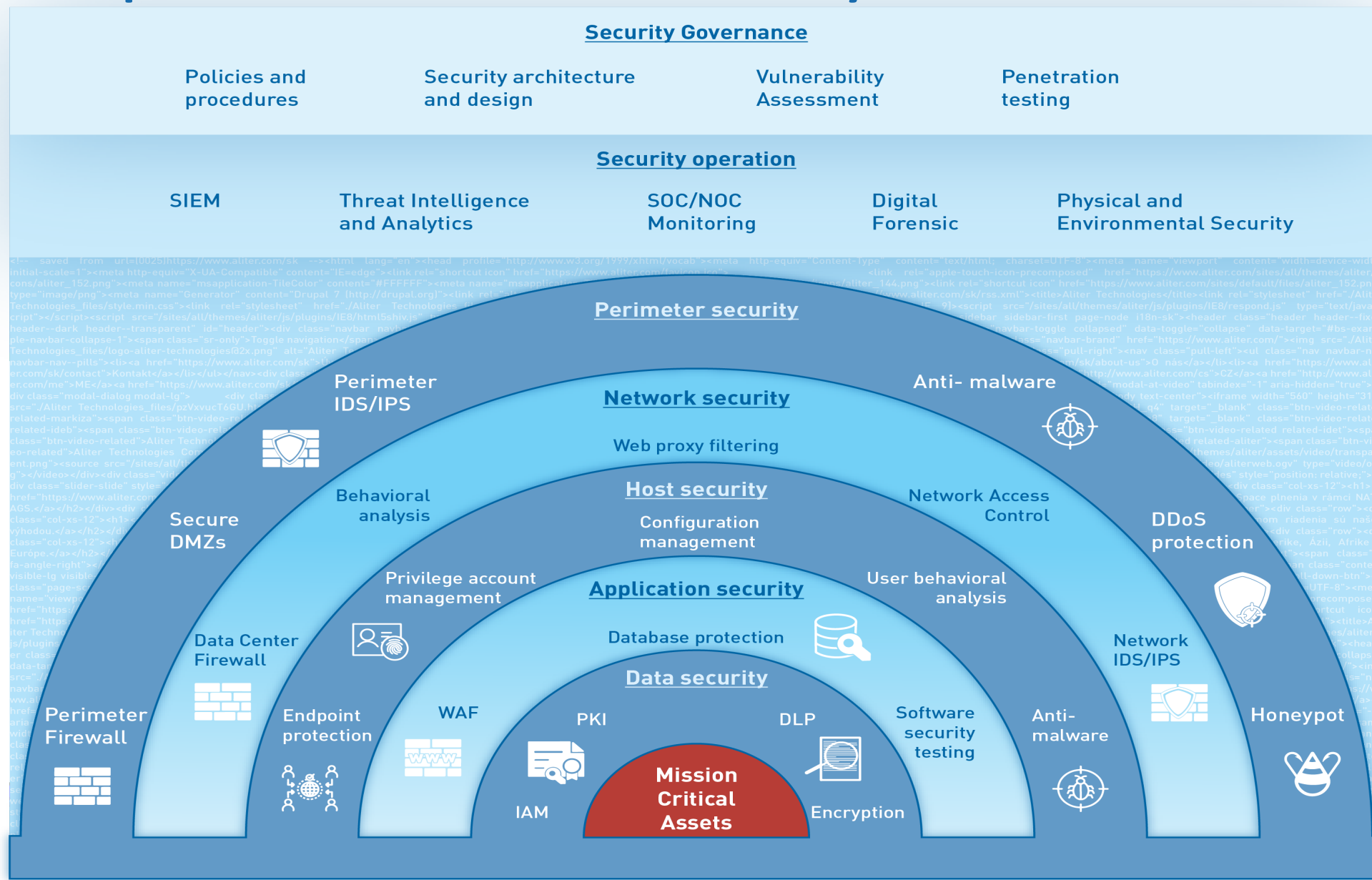
Aliter Technologies, a.s.

Filip Mikuš, Security Specialist

25.06.2019

Bratislava

Zabezpečenie infraštruktúry

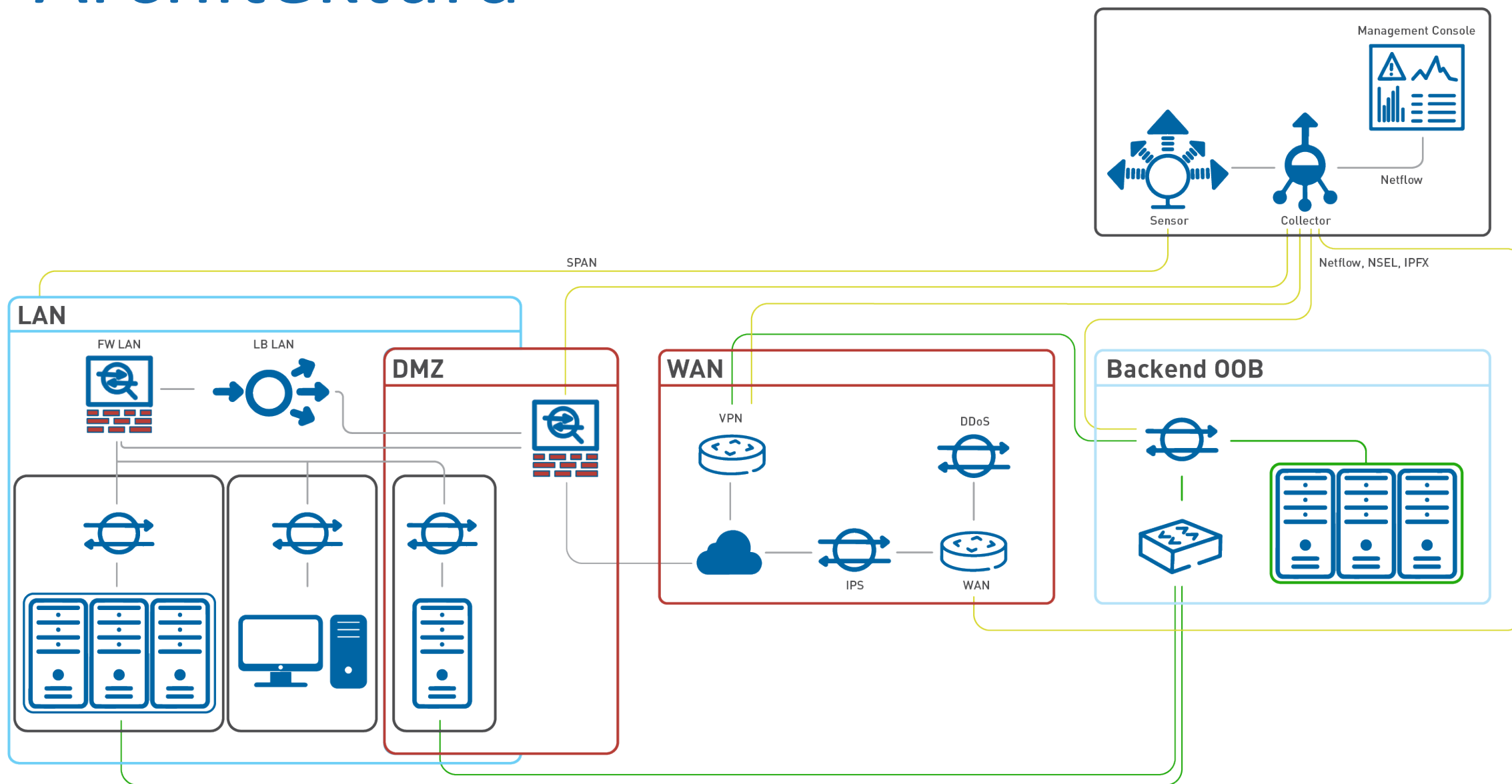


Požiadavky na úspešné odhalenie Cyber hrozieb

- potreba dobrej viditeľnosti siete
- odhalenie anomálií v správaní používateľov - úmyselné alebo náhodné
- detekcia hrozieb v reálnom čase

- reakcia na incidenty, rýchla a presná forenzná analýza
- súlad s predpismi (ISO27000, ZoKB, ...)
- uchovávanie záznamov o odhalených anomáliách

Architektúra



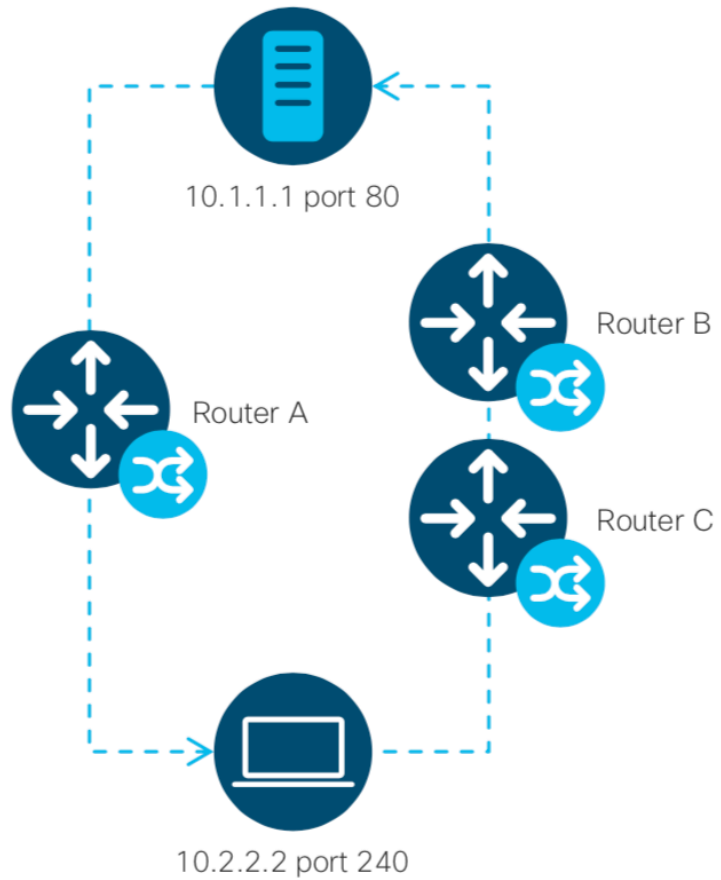
Stitching



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

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

Deduplikácia



Router A: 10.1.1.1:80 → 10.2.2.2:1024

Router B: 10.2.2.2:1024 → 10.1.1.1:80

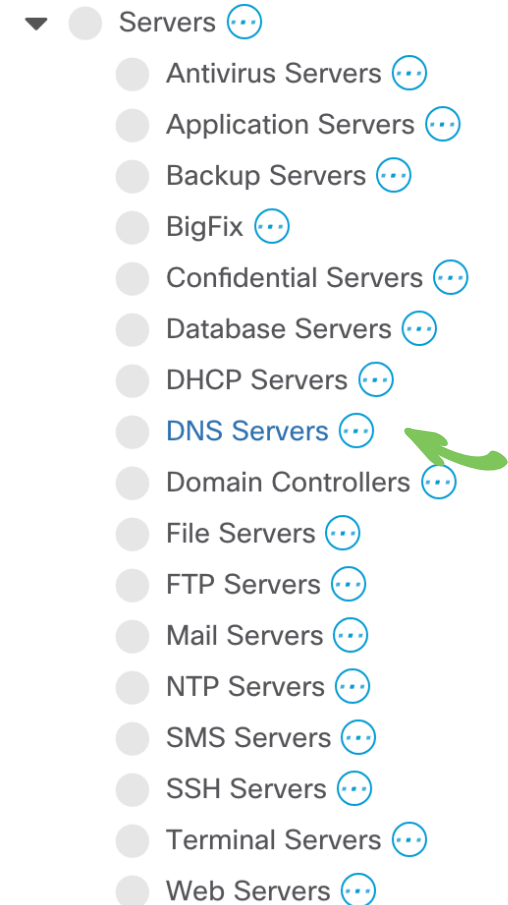
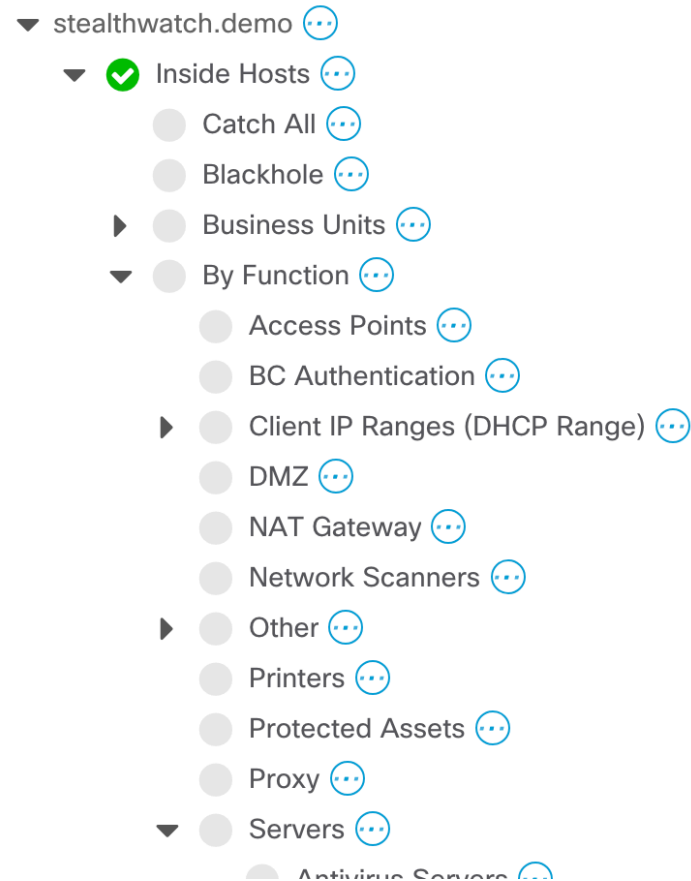
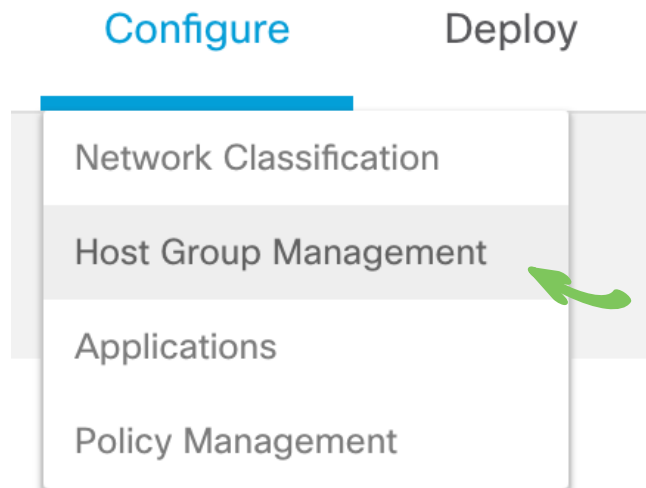
Router C: 10.2.2.2:1024 → 10.1.1.1:80

Duplikácia

Host Groups

- zníženie false-positive pri správnej klasifikácii zariadení
- schopnosť segmentovať sieť a používateľov do logických skupín
- automatizácia hostiteľských skupín
- poskytuje metódy na hlásenie akýchkoľvek anomálií nad danými skupinami

Definovanie vlastnej siete, aby sme ju mohli chrániť



Klasifikácia serverov podľa funkcionality



Dashboards

Moni

- Network Security
- Cognitive Threat Analytics
- Stealthwatch Cloud
- Host Classifier
- Visibility Assessment
- ETA Cryptographic Audit

Sort Classifiers By:

Suggested

Web Servers 86

DNS Servers 5

Exchange S... 5

NTP Servers 2

DHCP Servers 1

Mail Servers 0

Domain Con... 0

Host Classifier | DNS Servers

(last run 5 hours ago)

Suggested (5) Confirmed (0) Excluded (0)

Enabled ON

Auto Classification OFF

Confirm that these hosts belong to the DNS Servers host group, or exclude them from future suggestions for this search.

☒	IP ADDRESS	Host Name	Host Group(s)	Count ↓	Last Suggested
☐	10.201.0.16	--	Domain Controllers	4488	11/26/2018
☐	10.201.0.15	--	DHCP Servers, Domain Controllers	3467	11/26/2018
☐	10.10.30.16	--	End User Devices, DNS Servers, Domain Controllers, Desktops, New York	2537	11/26/2018
☐	10.10.30.15	--	DNS Servers, Domain Controllers, New York	2046	11/26/2018
☐	10.201.1.239	--	Catch All	1302	11/26/2018

Komunikácia na neznáme DNS servery



SEARCH TYPE

Top Hosts

TIME RANGE *

Last Hour

SEARCH NAME *

Top Hosts on 11/26/2018 at 7:51 PM

Subject

HOST IP ADDRESS

ex. 192.168.10.10 or !192.168.10.10

HOST GROUPS

Select

Outside Hosts

Connection

PORT / PROTOCOL

53/udp

APPLICATIONS

Select

DIRECTION

Total

Peer

HOST IP ADDRESS

ex. 192.168.10.10 or !192.168.10.10

HOST GROUPS

Select

Inside Hosts

Advanced Options

SUBJECT ORIENTATION

☐ Either ☐ Client ☒ Server

FLOW COLLECTOR NAME

Komunikácia na neznáme DNS servery

Top Hosts Search Results (51)

Edit Search

Last Hour (Time Range)

Save Search

Save Results

Start New Search

Subject:

Outside Hosts (Host Groups)

Server (Orientation)

100% Complete

Delete Search

Connection:

53/udp (Port / Protocol)

Total (Direction)

Peer:

Inside Hosts (Host Groups)

Manage Columns

Export

% OF BYTES	HOST IP ADDRESS	HOST NAME	HOST GROUPS	HOST ROLE	PACKETS	FLOWS	PEERS	HOST BYTES RA...
31.18%	64.14.29.84	--	United States	Server	1.23 M	4	2	99.56%
23.26%	64.14.29.82	--	United States	Server	881.39 K	3	2	99.64%
12.81%	8.26.206.253	--	United States	Server	480.64 K	2	2	99.92%

Definícia alarmu na neznáme DNS servery



NAME *

NO DNS to Outside except DNS servers

DESCRIPTION

NO DNS to Outside except DNS servers

STATUS

OFF

When any host within *Inside Hosts* except those within *DNS Servers* communicates with any host within *Outside Hosts*; through *53/UDP*, an alarm is raised.

FIND ⓘ

SUBJECT HOST GROUPS ⓘ

Inside Hosts × EXCEPT ! DNS Servers ×

⊗ AND

PEER HOST GROUPS ⓘ

Outside Hosts ×

⊗ AND

PEER PORT/PROTOCOLS

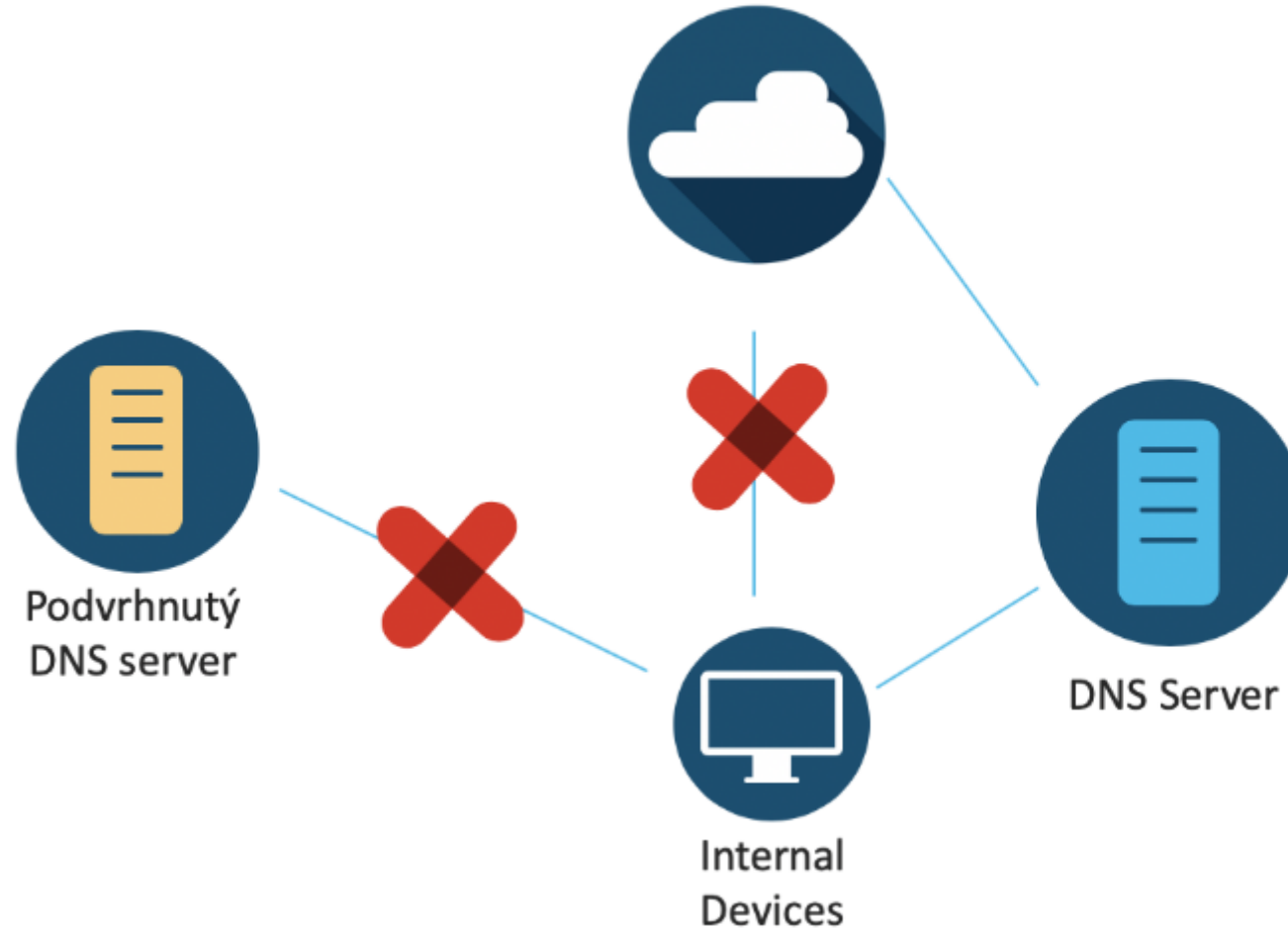
53/UDP ×

⊗

ACTIONS

🔔 Alarm when a single flow matches this event.

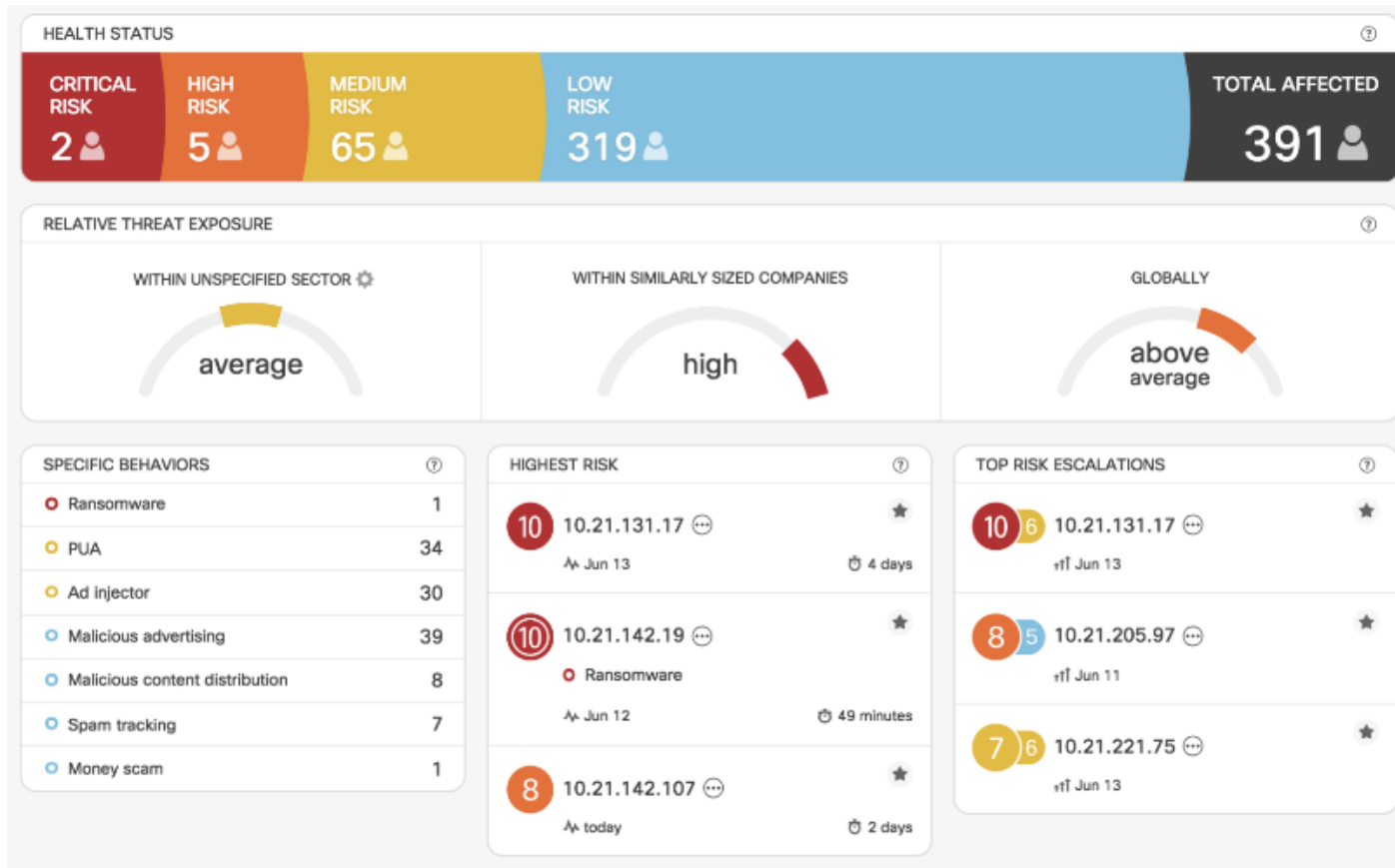
Korektná komunikácia na DNS servery



Cognitive Traffic Analytics

- CLOUD služba detekuje podozrivú komunikáciu v sieti
- reaguje na výskyt anomálií alebo neobvyklé správanie používateľov
- podozrivá komunikácia je odosielaná do cloud-u, na analýzu a vyhodnotenie (metadáta)
- schopnosť odhaliť škodlivý kód aj v zašifrovanej komunikácii - **Encrypted Traffic Analytics**

Encrypted Traffic Analytics



- takmer 90% všetkých tokov (Flows) je šifrovaných a môžu obsahovať skryté hrozby
- používanie zastaraného TLS 1.0 so známymi chybami
- približne **5000** udalostí bolo zredukovaných na **390** významných udalostí, vďaka strojovému učeniu

Ďakujeme

Viac informácií na: www.aliter.com