Aby vás infikované koncové zariadenie nestálo hlavu

Peter Mesjar
Consulting Systems Engineer
25.6.2019

Mám sa obávať novoobjavenej kybernetickej hrozby?

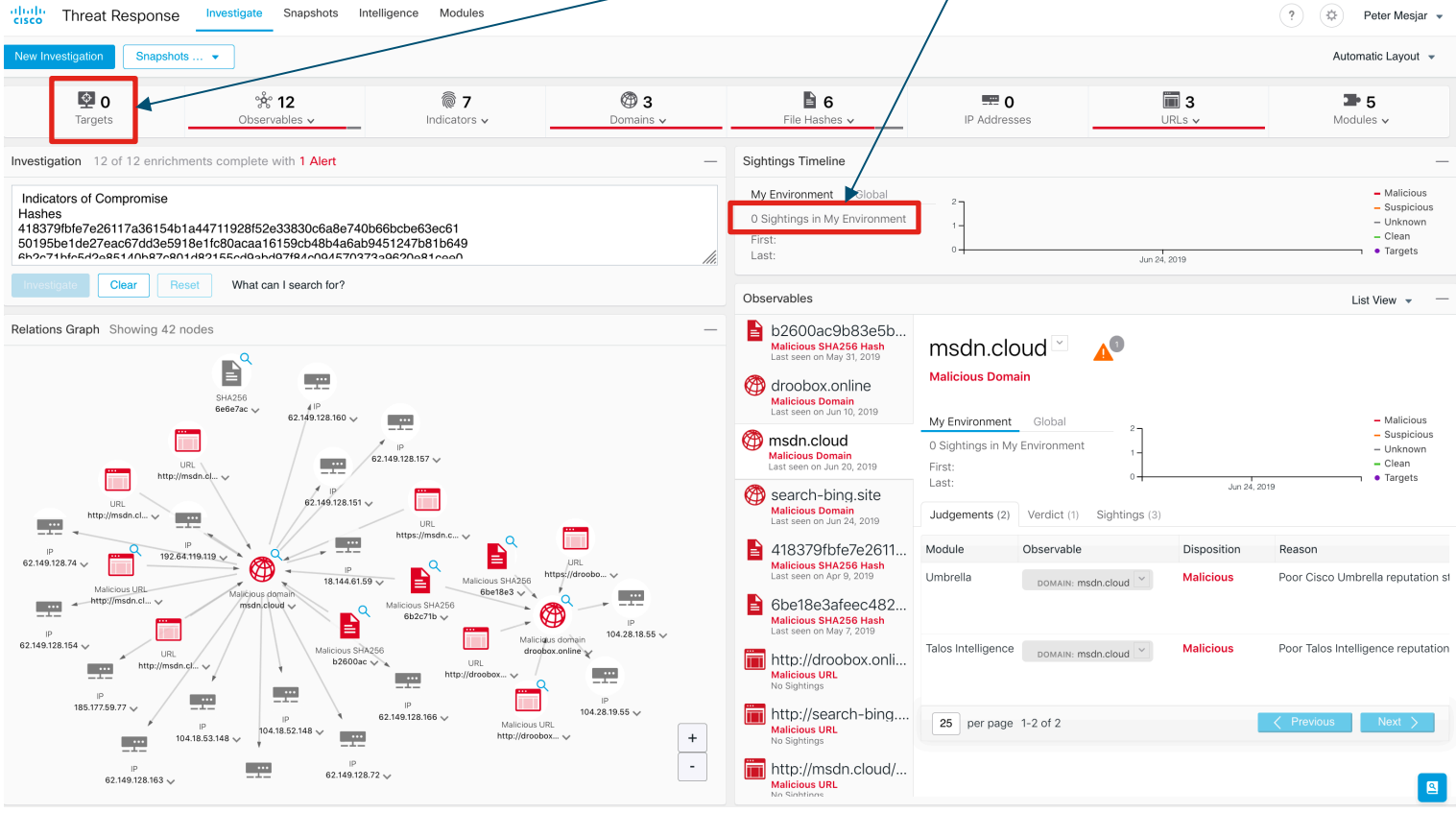
"Otázka za milión" v kybernetickej bezpečnosti

https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

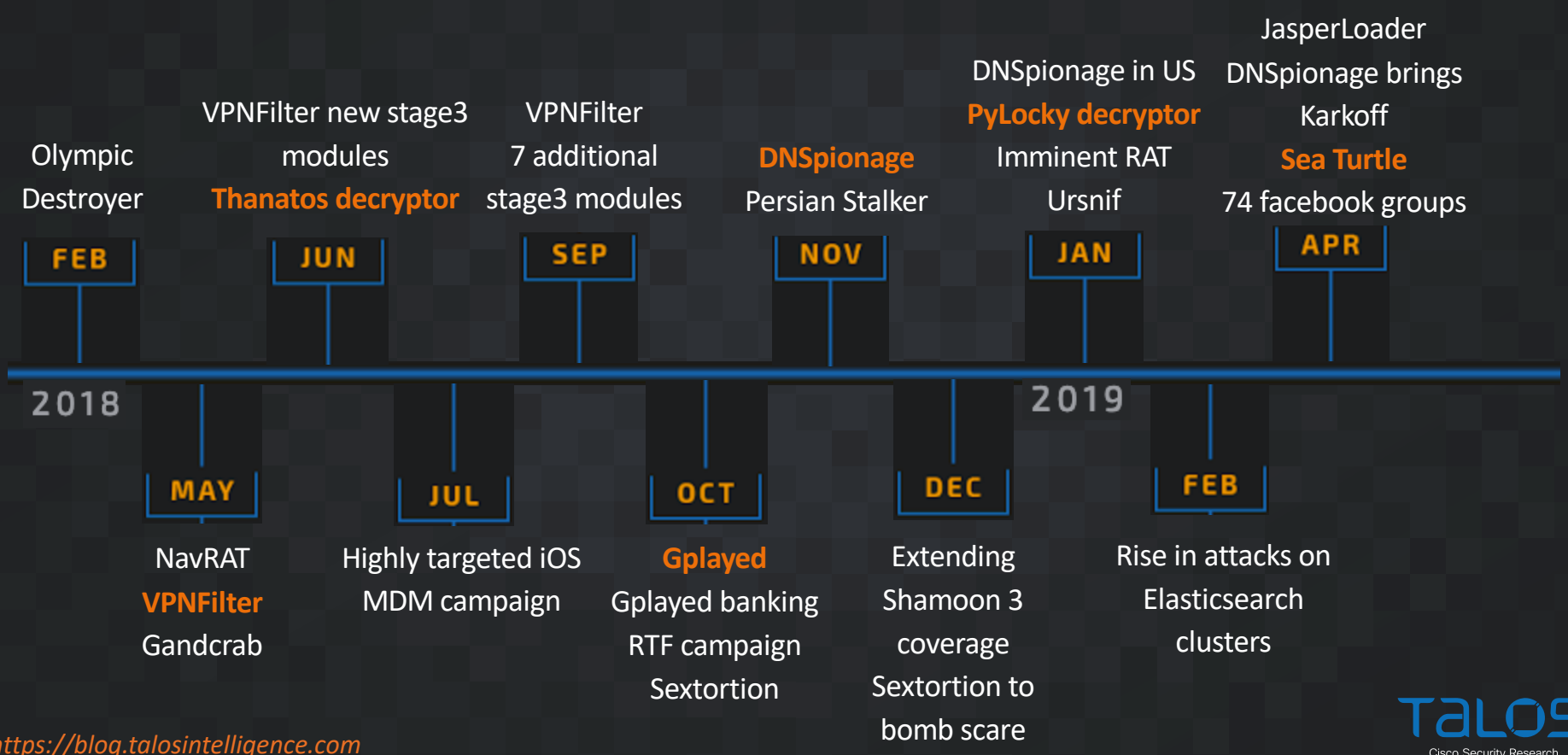
TUESDAY, JUNE 4, 2019

It's alive: Threat actors cobble together open-source pieces into monstrous Frankenstein campaign

Našťastie nemusím☺



What did TALOS find after Nyetya/Not Pyetya attack

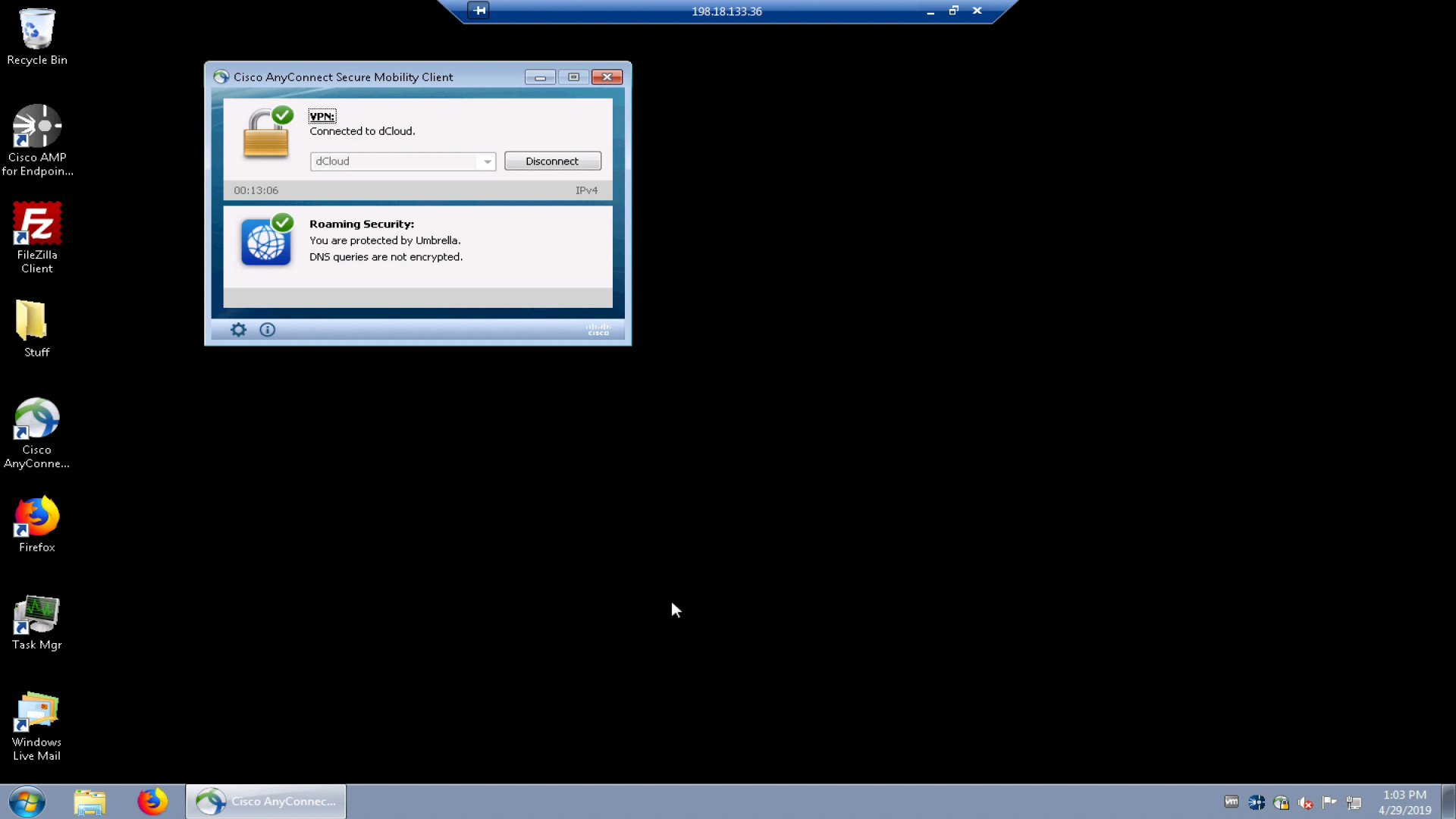


https://blog.talosintelligence.com

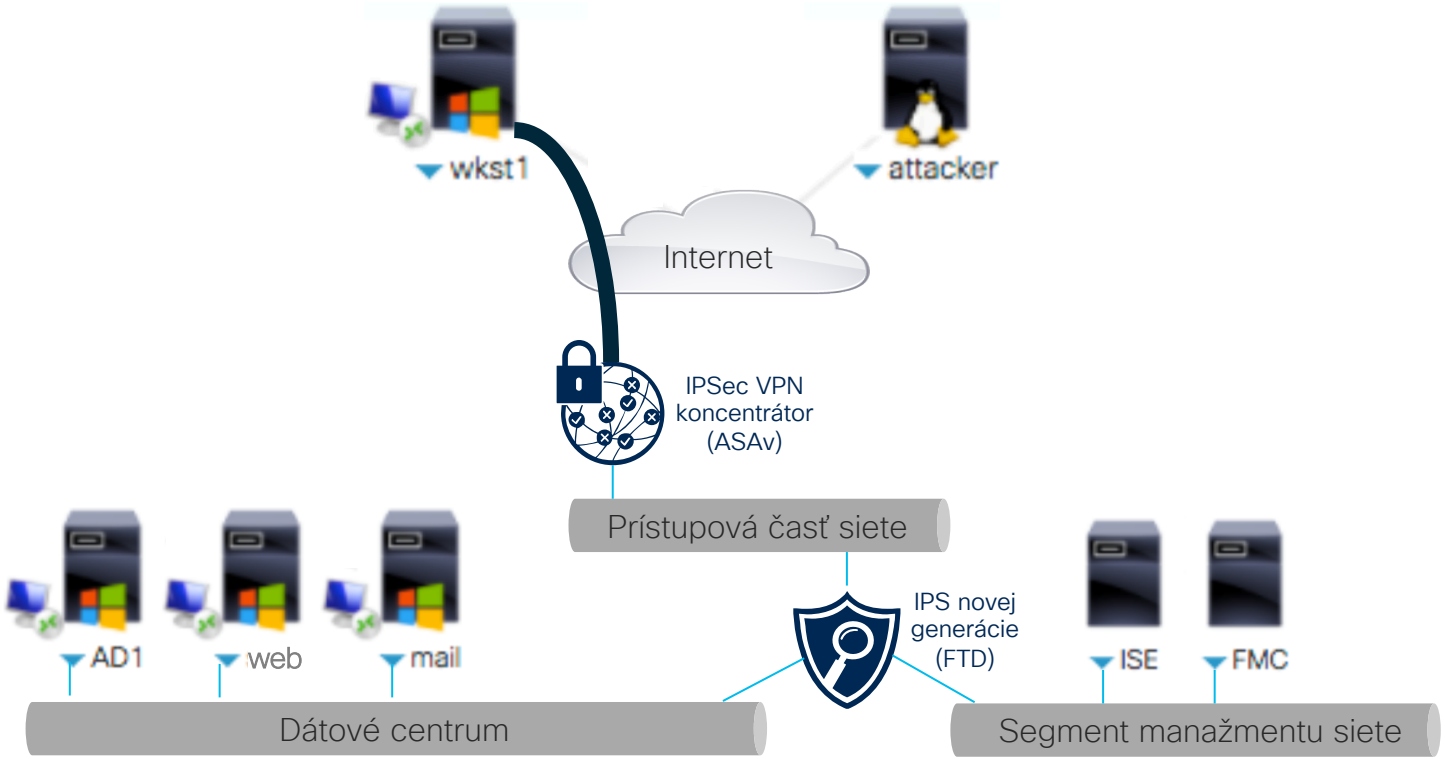
TALOS
Cisco Security Research

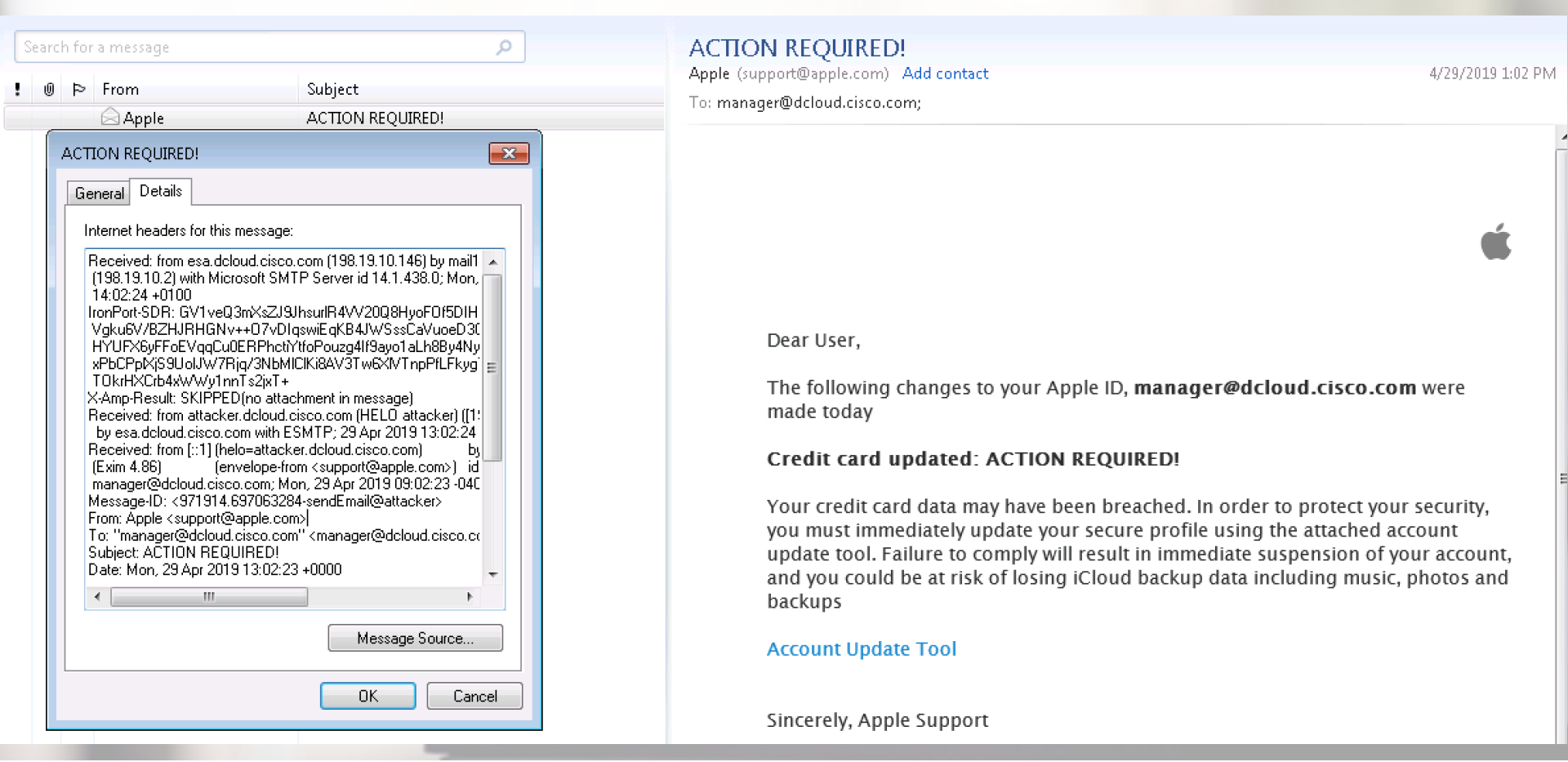
“Houston” nemáme problém☺

Fáza pred útokom


198.18.133.36
Recycle Bin
Cisco AMP for Endpoin...
FileZilla Client
Stuff
Cisco AnyConne...
Firefox
Task Mgr
Windows Live Mail
Cisco AnyConnect Secure Mobility Client
VPN:
Connected to dCloud.
dCloud
Disconnect
00:13:06
IPv4
Roaming Security:
You are protected by Umbrella.
DNS queries are not encrypted.
Cisco AnyConnec...
1:03 PM
4/29/2019

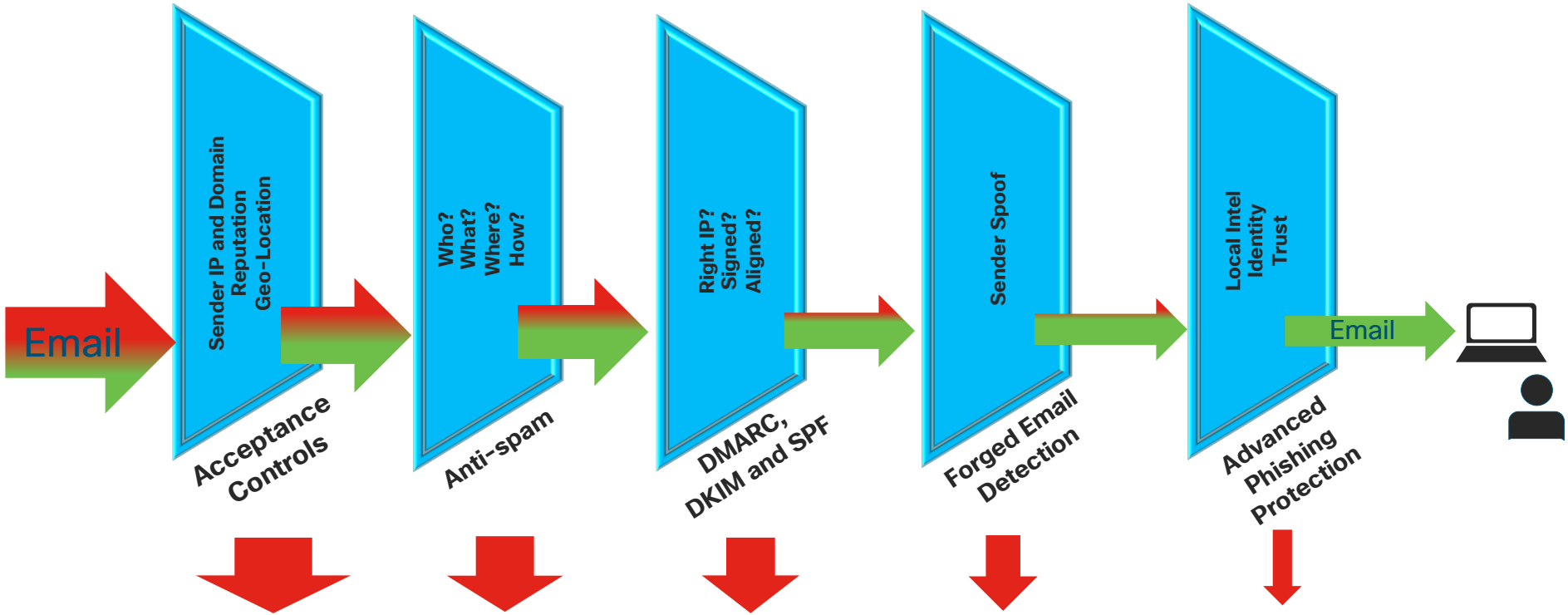
Typická počítačová sieť dnes





Email je stále číslo 1 pre počiatočné kompromitácie koncových zariadení!

Securing Inbound Email: Layers of Defense



“Houston” máme problém!

Fáza počas útoku

File Edit View History Bookmarks Tools Help

Cisco Firepower Management | Identity Services Engine | New Tab

https://ise.dcloud.cisco.com/admin/#home

Search

ISE FMC SMA WSA ESA Corporate Portal Dev Portal Remediation Portal Quarantine/Unquaran... vCenter

Identity Services Engine

Home | Context Visibility | Operations | Policy | Administration | Work Centers

Summary | Endpoints | Guests | Vulnerability | Threat | +

Click here to do visibility setup Do not show this again.

METRICS

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated
1	1	0	0	

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

ad1: [100%]

ENDPOINTS

Type | Profile

workstations: [100%]

BYOD ENDPOINTS

Type | Profile

No data available.

ALARMS

Severity	Name	Occu...	Last Occurred
	Name		
	ISE Authentication Inacti	10270	14 mins ago

SYSTEM SUMMARY

1 node(s) All 24HR

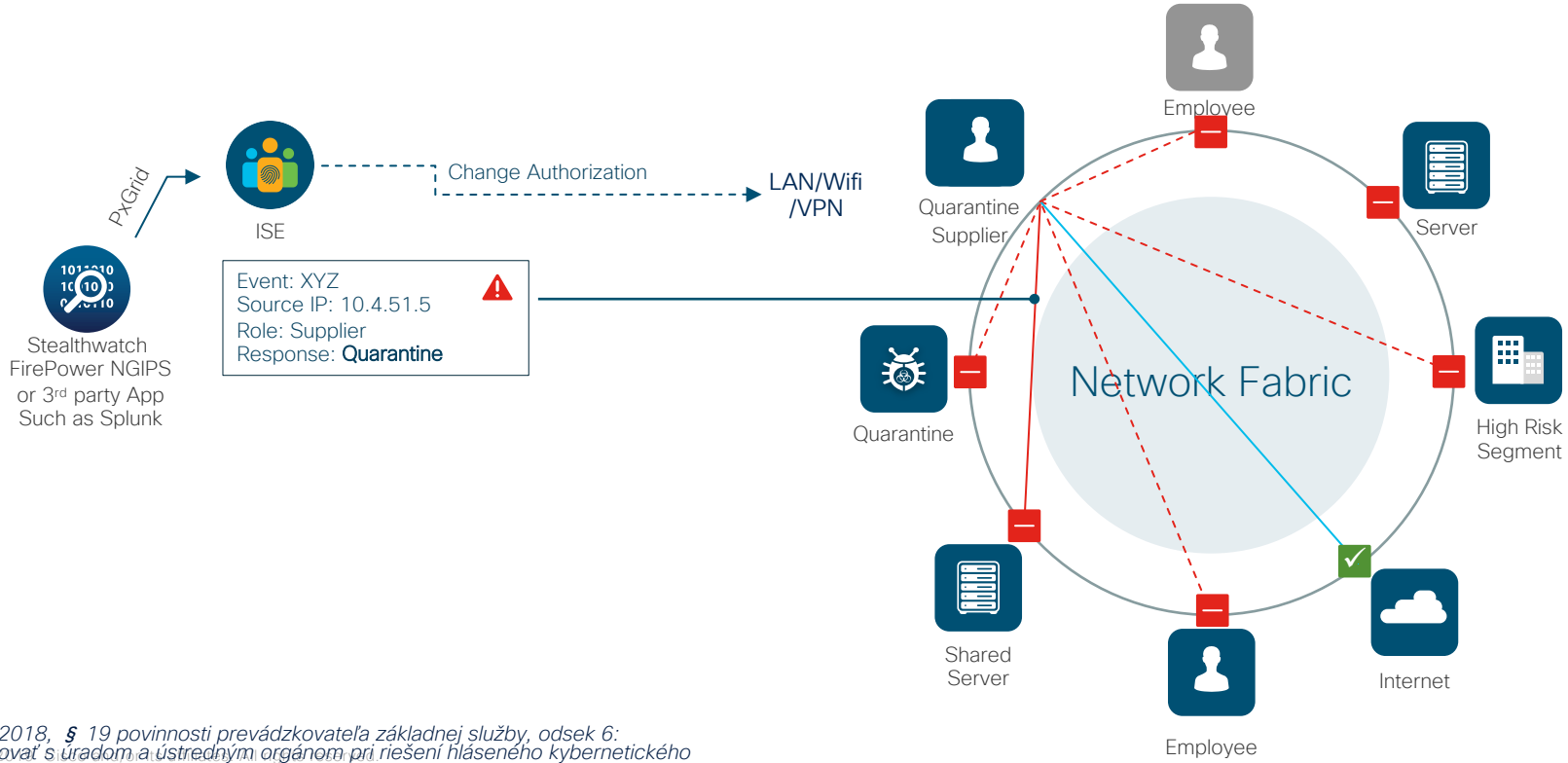
ise

CPU | Memory | Authentication Latency

2:44 PM
4/29/2019

Cisco Integrovaná Kybernetická Bezpečnosť

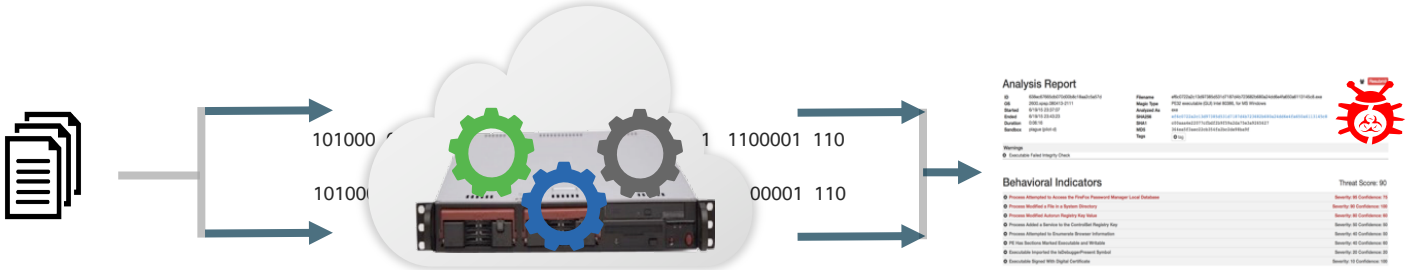
Detekcia -> Karanténa -> Riešenie bezpečnostného incidentu



zákon č. 69/2018, § 19 povinnosti prevádzkovateľa základnej služby, odsek 6:
c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

Cisco Threat Grid = Sandbox + Threat Intelligence

Malware Analysis / Threat Intelligence



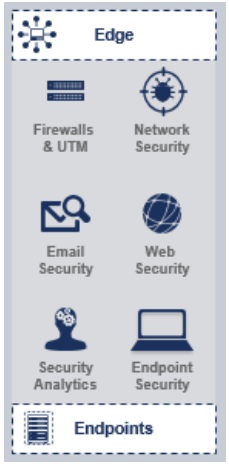
An automated engine observes, deconstructs, and analyzes using multiple techniques

Malware Analysis
- Automated Analysis
  - Static
  - Dynamic
- Global Correlation

Threat Intelligence
- Threat Score
- Behavior Indicators
- Observables
- Analysis Reports

Provides a single solution delivered multiple ways: through the cloud, as an on-premises solution, or integrated into security technologies such as AMP (Advanced Malware Protection).

Threat Grid Integrations



Supported Integrations & Partners

IBM Security
LogRhythm
The Security Intelligence Company
Phantom
TRAPX SECURITY
DFLABS
splunk>
wirex
CYBERSPONSE
opentext
exabeam
GUIDANCE SOFTWARE
RSA
DEMISTO
SECURITY
swimlane
MALFORMITYLABS
SYNCURITY
tripwire
BLUVECTOR
SIEMPLIFY

Select Recipe Integrations

BlueCoat
chrome
McAfee
Bro
ArcSight
Palantir

Select Threat Feed Integrations

THREATQUOTIENT
CENTRIPETAL NETWORKS
ANOMALI
THREATCONNECT
eclectic iq

“Houston” máme po probléme?

Fáza po útoku

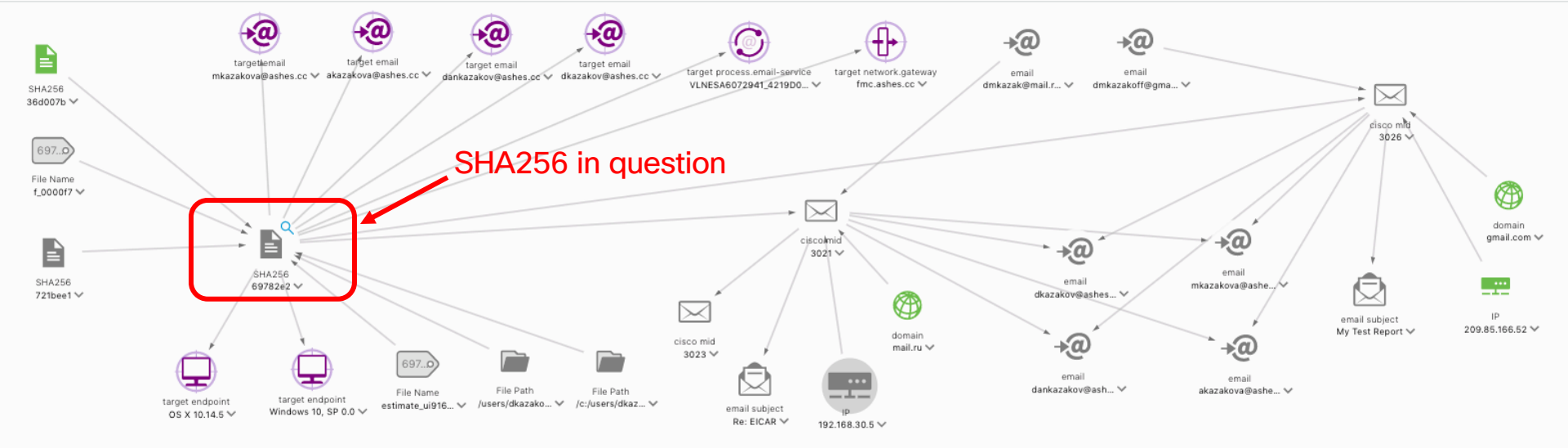
Cisco Threat Response – vyhľadanie IoC (Indication of Compromise)

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate | Clear | Reset | What can I search for?

8	1	0	0	1
Targets	Observable	Indicators	Domains	File Hash



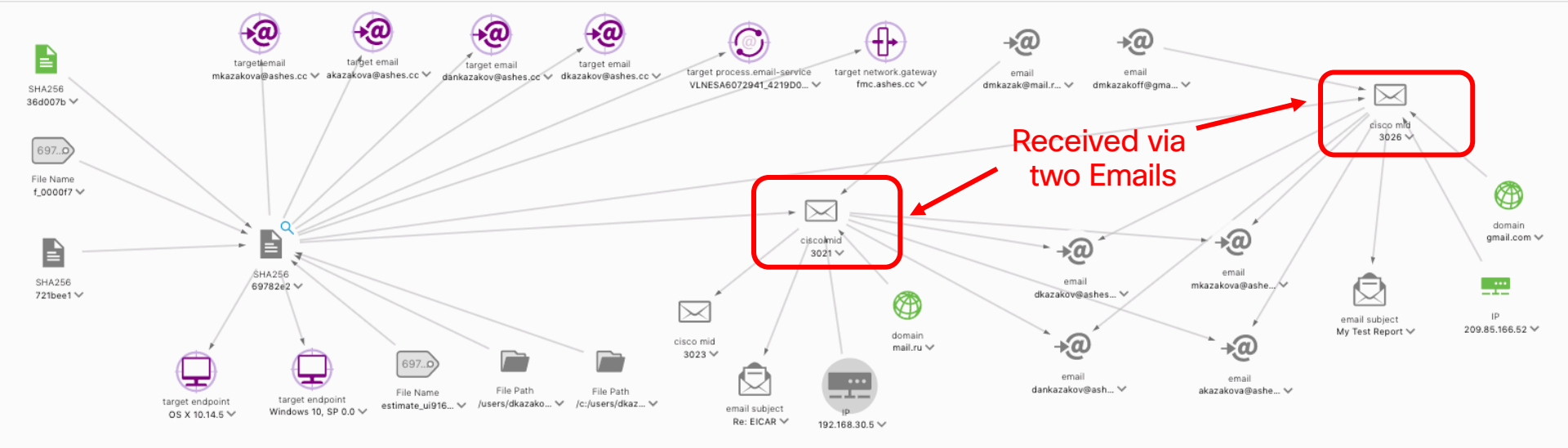
Cisco Threat Response – trasovanie IoC cez sieť

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate | Clear | Reset | What can I search for?

8	1	0	0	1
Targets	Observable	Indicators	Domains	File Hash



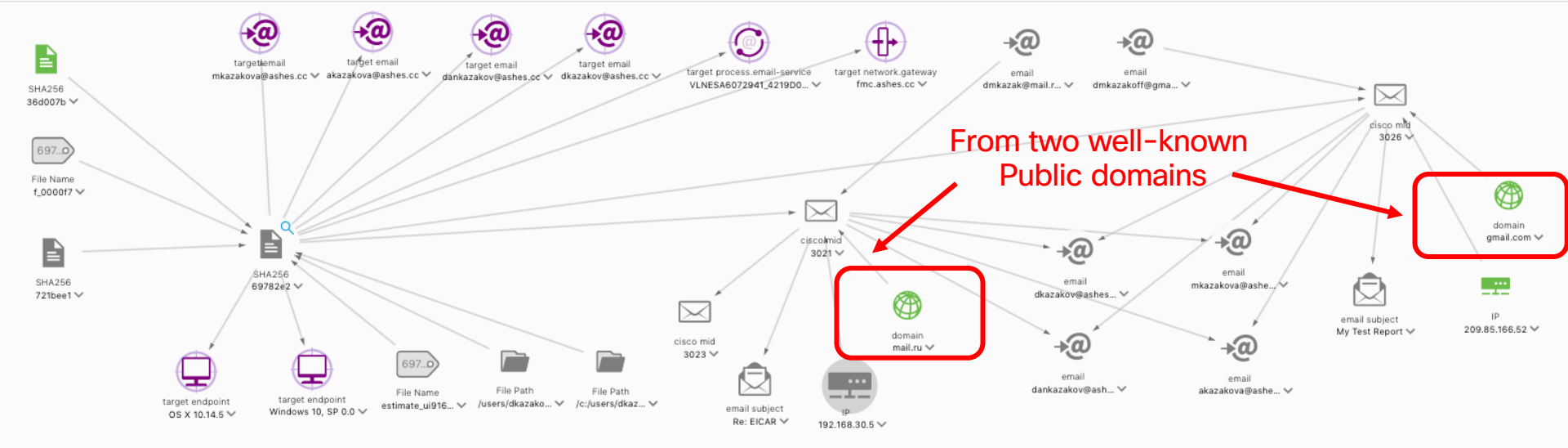
Cisco Threat Response – trasovanie IoC cez sieť

Investigation 1 of 1 enrichments complete

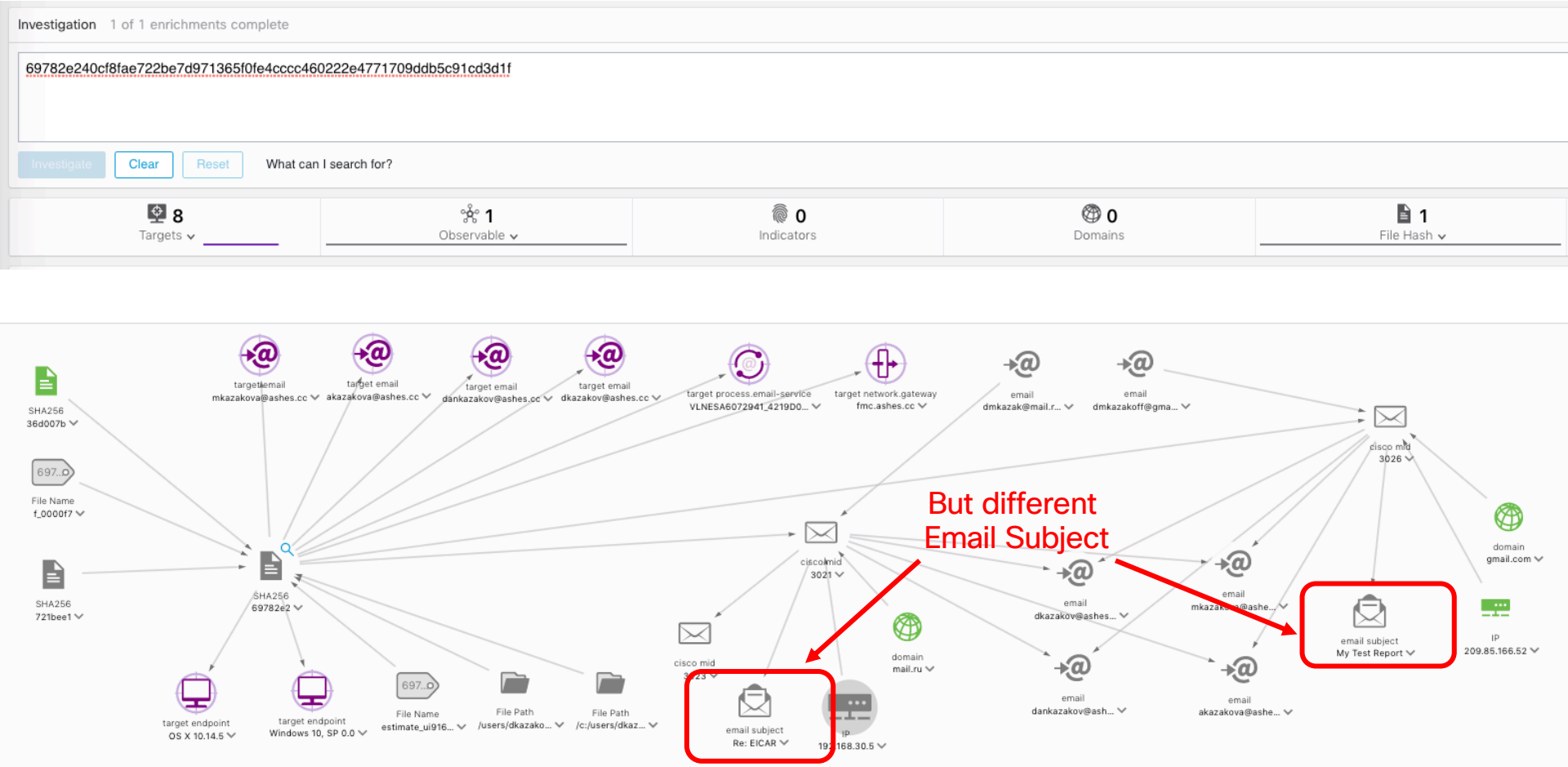
69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate | Clear | Reset | What can I search for?

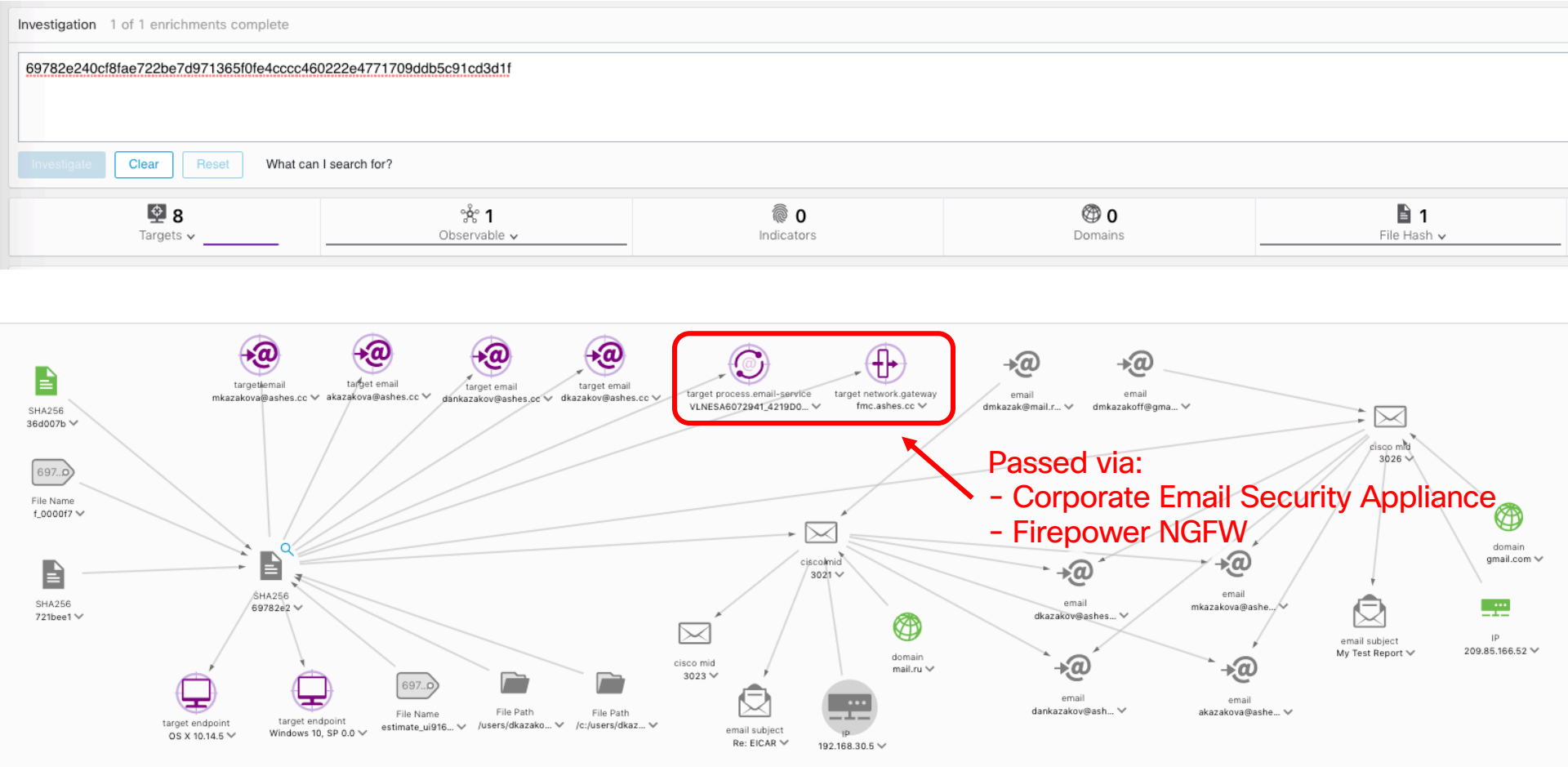
8	1	0	0	1
Targets	Observable	Indicators	Domains	File Hash



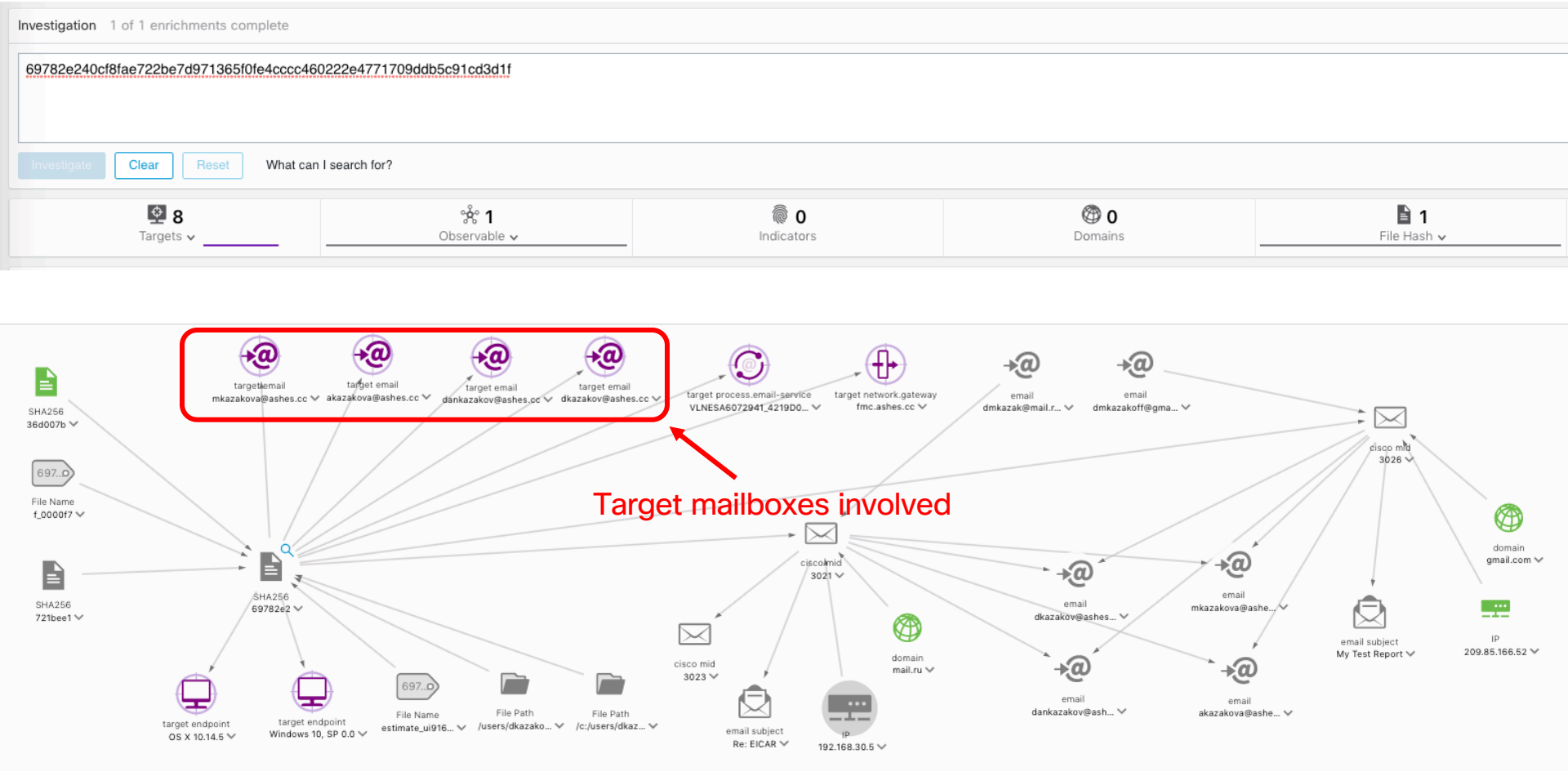
Cisco Threat Response – trasovanie IoC cez sieť



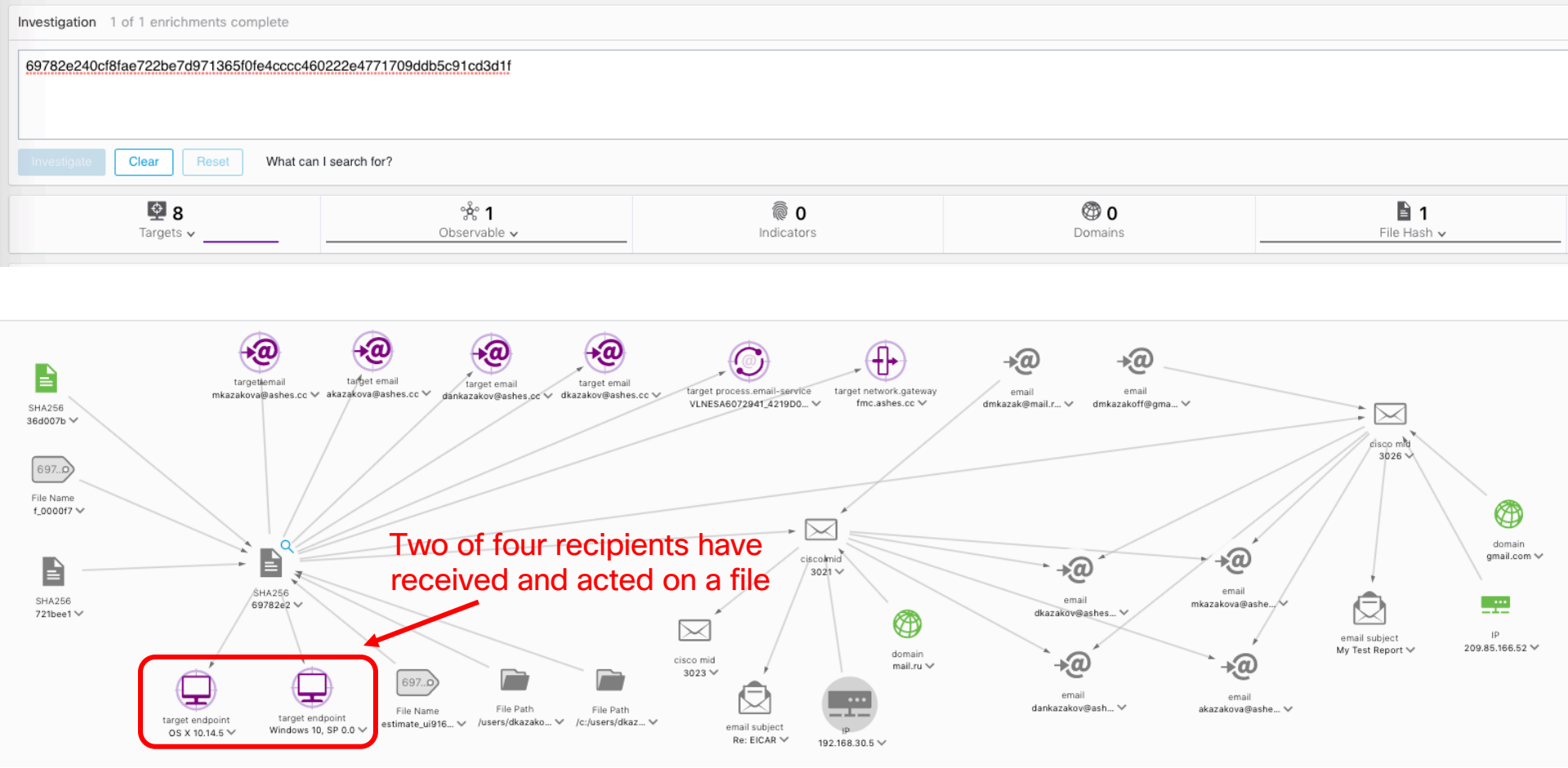
Cisco Threat Response – trasovanie IoC cez sieť



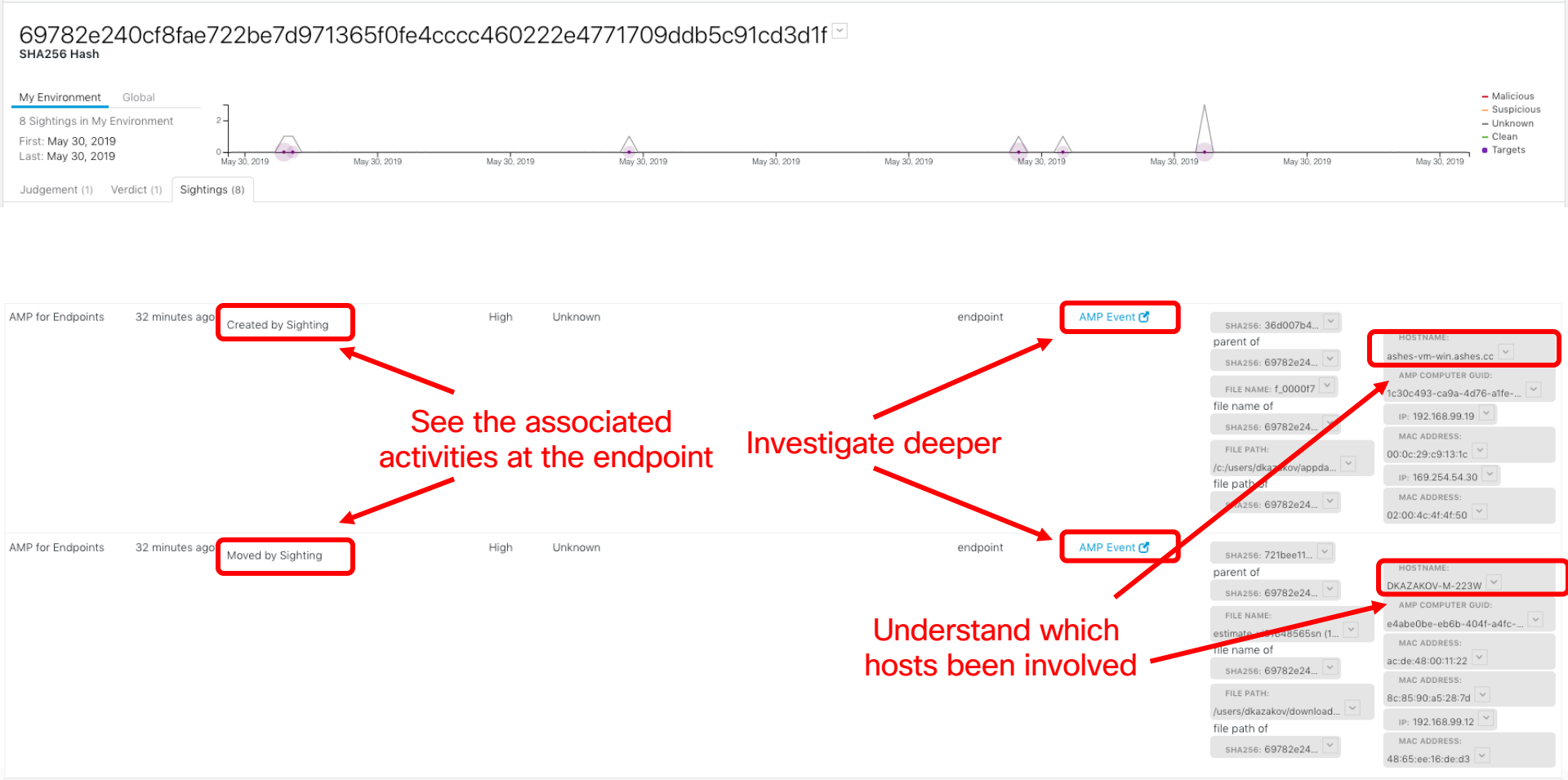
Cisco Threat Response – analýza cieľa



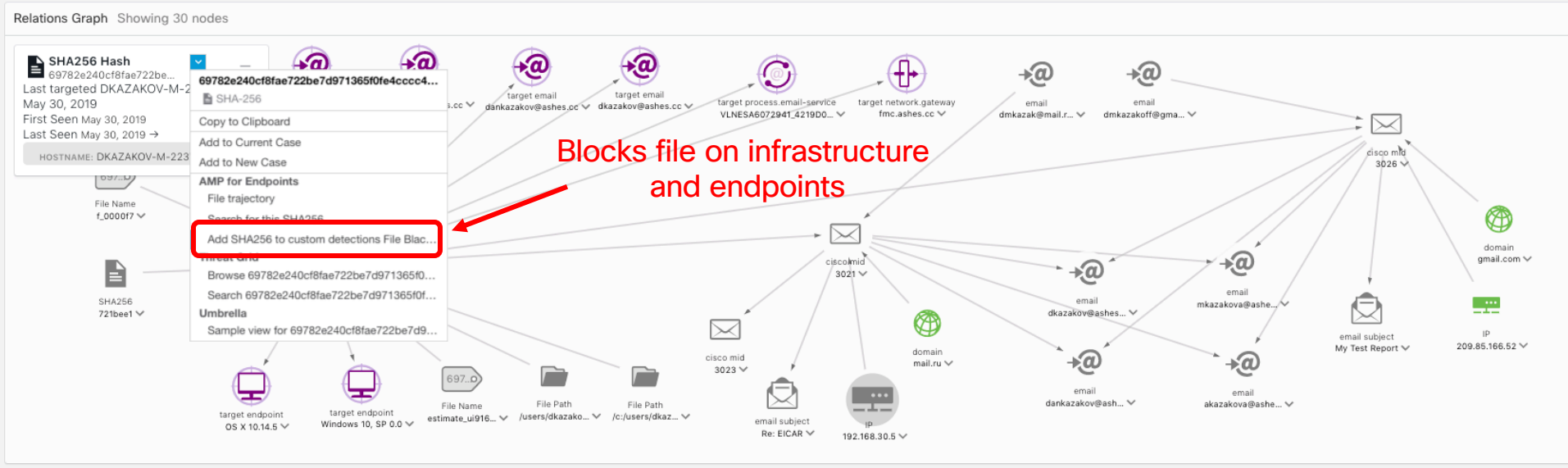
Cisco Threat Response – analýza cieľa



Cisco Threat Response – sled udalostí v čase



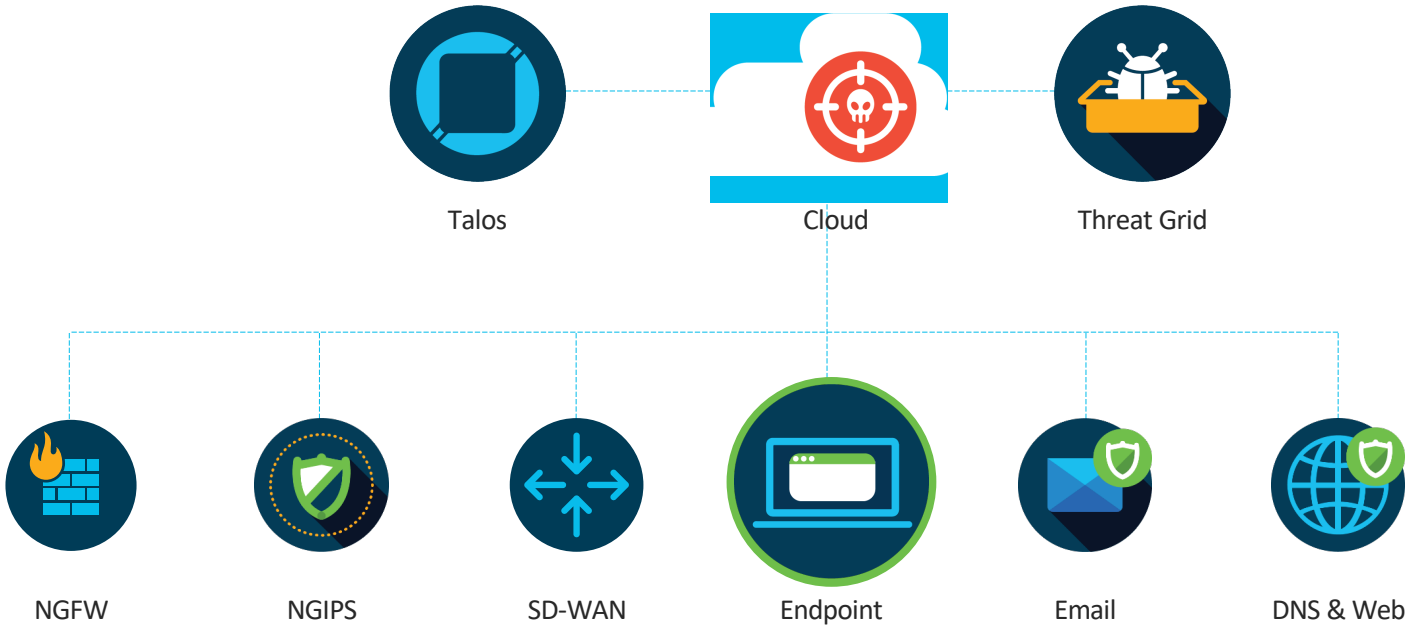
Cisco Threat Response – bloknutie na pár klikov



Na záver...

Cisco Integrated Threat Defense

Share intelligence across network, cloud, web, email, and endpoints to see once & block everywhere.



TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity