

cisco *Engage*

On-line každých 14 dní

Cisco Tech Club Webináře



You make **possible**

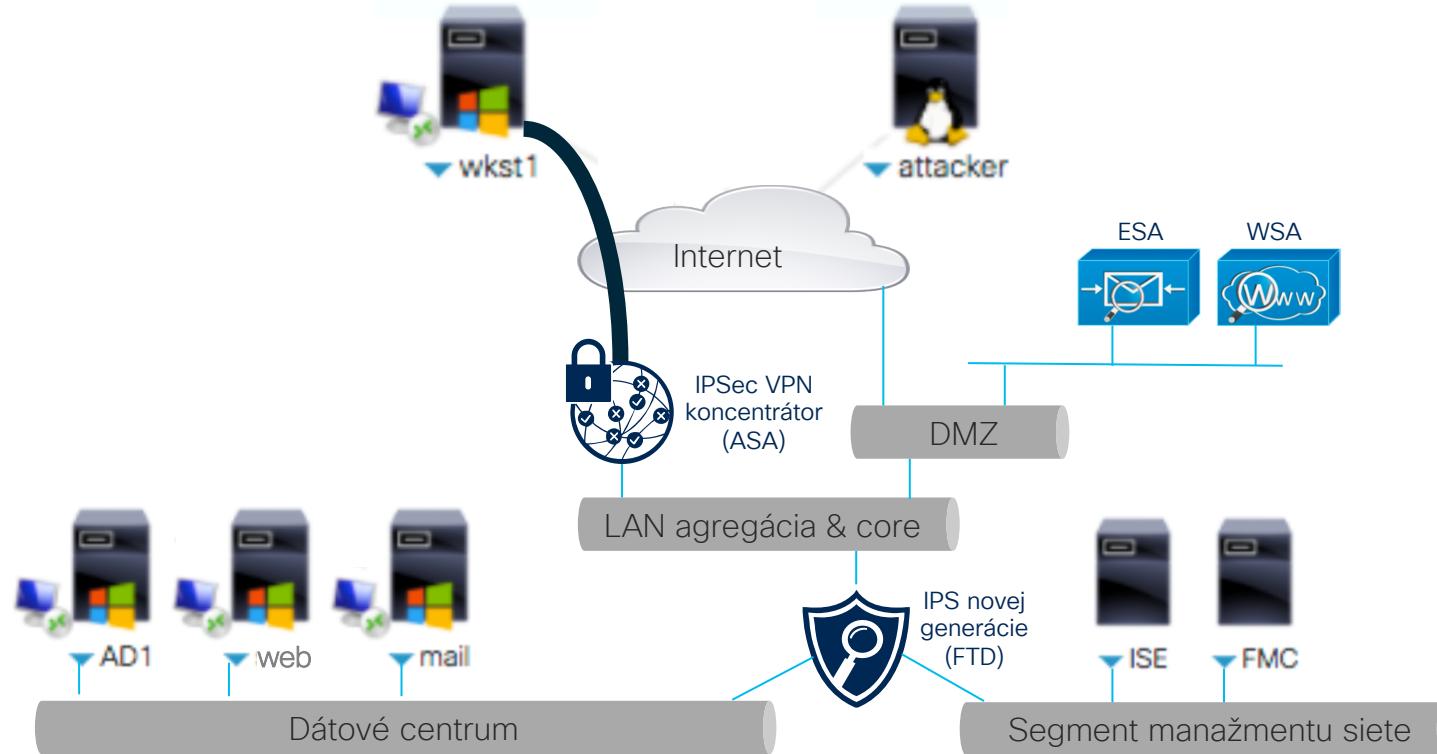
Aby Vás infikované koncové zariadenie nestálo hlavu

12.5.2020

Peter Mesjar
Technical Solutions Architect
pmesjar@cisco.com



Ako sa dostať k cenným dátam vnútri podnikovej siete?



Využime fakt, že väčšina pracuje z domu...



“Houston” nemáme problém ☺

Fáza pred útokom



198.18.133.36

Pár poznámok k phishing-u - Punycode

Viac informácií v Techclub seminári na tému Umbrella zo dňa 28.4.2020

Dear Apple iCloud user,

the following changes to your Apple ID were made today:

Credit card updated: ACTION REQUIRED!

Your credit card data may have been breached. In order to protect your security, please update your account and reset your password by visiting our Apple website at

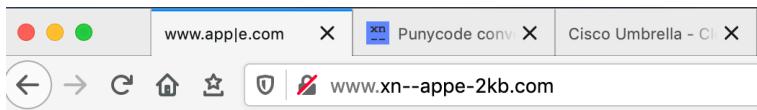
<https://appleid.apple.com>



Failure to do so might result in suspension of your account and you could be at risk of losing access to your iCloud services including music, photos and data backup.

Thank you for helping us keeping you secure.

Sincerely, Apple Support



This is [www.apple.com](https://appleid.apple.com) ;-)

It is neither [www.apple.com](https://appleid.apple.com) nor [www.apple.com](https://appleid.apple.com)

These are not the droids you're looking for, probably.

See [IDN homograph attack](#) and [Tenuis dental click](#)

Cisco ESA

Subject: [SUSPICIOUS] ACTION REQUIRED!

Dear Apple iCloud user,

the following change



Cisco Security

Credit card updated The requested web page may be dangerous

Your credit card data:

our Apple website a

Previewing http://www.apple.com

<https://secure-web.cisco.com>

Cisco Email and Web Security protects your organization's network from malicious software. Malware is designed to look like a legitimate email or website which accesses your computer, hides itself in your system, and damages files. Your email administrator has configured this prevention system to ensure against such damage.

qoR6KwyB0bzZvffA6

L8/https%3A%2F%

This is www.apple.com ;-)

Failure to do so might
and data backup.

Thank you for helping!
Sincerely, Apple Support

It is neither www.apple.com nor [www.apple.com](http://apple.com).

These are not the droids you're looking for, probably.

See [IDN homograph attack](#) and [Tenuis dental click](#).

Inspired by [Phishing with Unicode Domains POC](#) and [this arstechnica article](#).

Do you trust the rendered site?

No

Leave this site and report it as malicious

Yes

Leave protected area and visit this site directly



“Houston” máme problém!

Fáza počas útoku

File Edit View History Bookmarks Tools Help

Cisco Firepower Management X Identity Services Engine X New Tab https://ise.dcloud.cisco.com/admin/#home Search

ISE FMC SMA WSA ESA Corporate Portal Dev Portal Remediation Portal Quarantine/Unquarantine 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 1 Active Endpoints 1 Rejected Endpoints 0 Anomalous Behavior 0 Authenticated 0

AUTHENTICATIONS Identity Store Identity Group Network Device Failure Reason ad1: [100%]

ENDPOINTS Type Profile workstations: [100%]

BYOD ENDPOINTS Type Profile No data available.

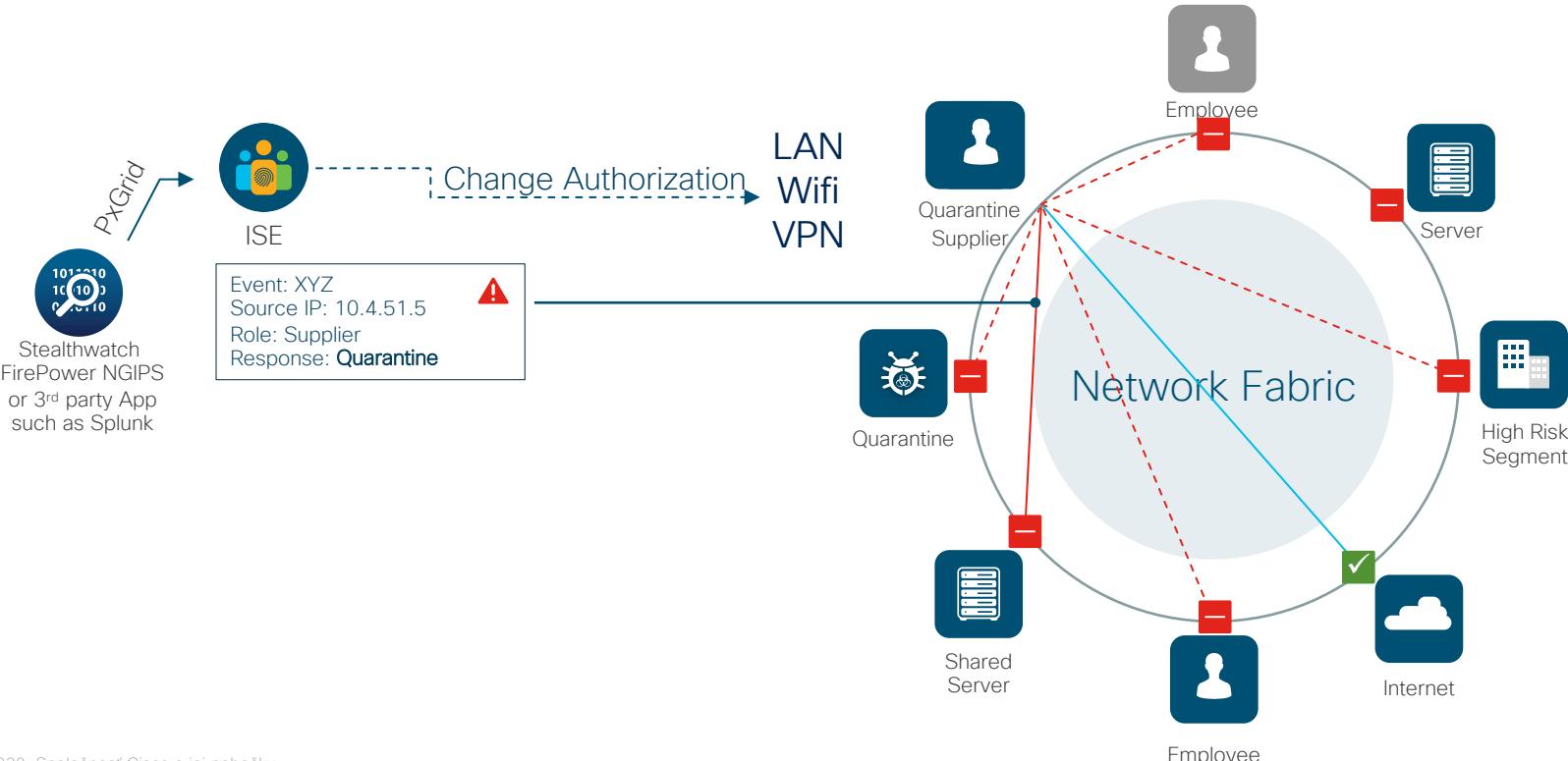
ALARMS Severity Name Occurred Last Occurred Name ISE Authentication Inacti 10270 14 mins ago

SYSTEM SUMMARY 1 node(s) All 24HR ise CPU Memory Authentication Latency

ISE Authentication Inacti 10270 14 mins ago 2:44 PM 4/29/19

Cisco Integrovaná Kybernetická Bezpečnosť

Detekcia -> Karanténa -> Riešenie bezpečnostného incidentu



Nezahadzujte svoj IPS

1) Endpoint protection softvér nič neukázal, je toto false positive?

[1:37618:1] "MALWARE-CNC Win.Trojan.Latentbot variant outbound connection"

[Impact: Vulnerable] From "Firepower" at Sat Oct 12 10:29:48 2019 UTC [Classification: A Network Trojan was Detected] [Priority: 1] {tcp} 172.16.7.13:50141 (unknown)->188.40.252.115:443 (germany)

2) TALOS reputácia pre IP 188.40.252.115 Unknown, Umbrella riziko benign/medium zaujímavý ale bol hostname:

IP ADDRESS	188.40.252.115
② FWD/REV DNS MATCH	Yes
HOSTNAME	supremogw64.nanosystems.it
② DOMAIN	your-server.de

3) V skutočnosti išlo o komunikáciu **neželanej aplikácie** pre vzdialený prístup stiahnutieľnej zadarmo



Who we are

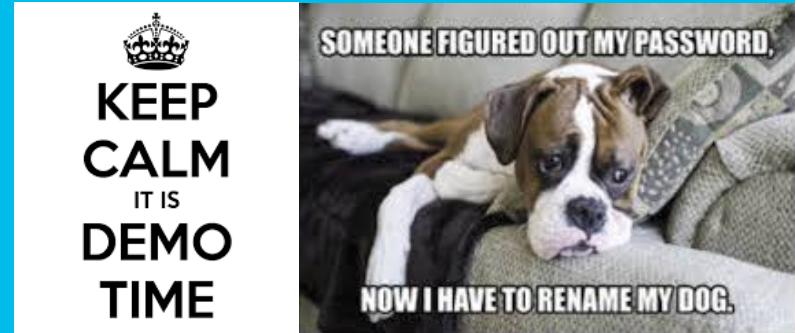
Products

Purchase

Contact

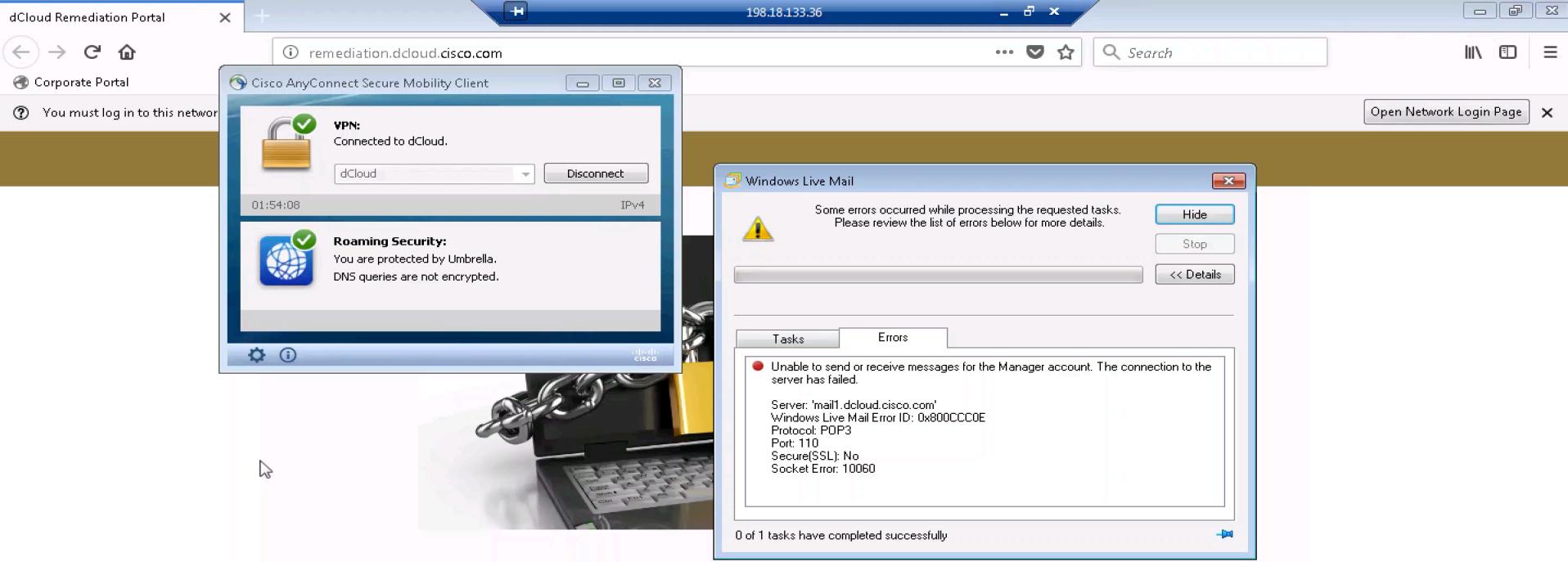
Login

Provide remote technical support without having to configure a firewall or router and without any installation.
Get connected in a few clicks to your customer's PC, ready to help him/her.



“Houston” máme po probléme?

Fáza po útoku



Welcome to Cisco dCloud Remediation Portal

Your system has been quarantined automatically via Cisco Rapid Threat Containment.
Please contact security operations at extension 5555 or 888-555-1234



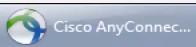
Cisco is Protecting You with [Rapid Threat Containment](#)



Stuff



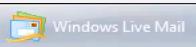
dCloud Remediat...



Cisco AnyConnec...



Inbox - Windows ...



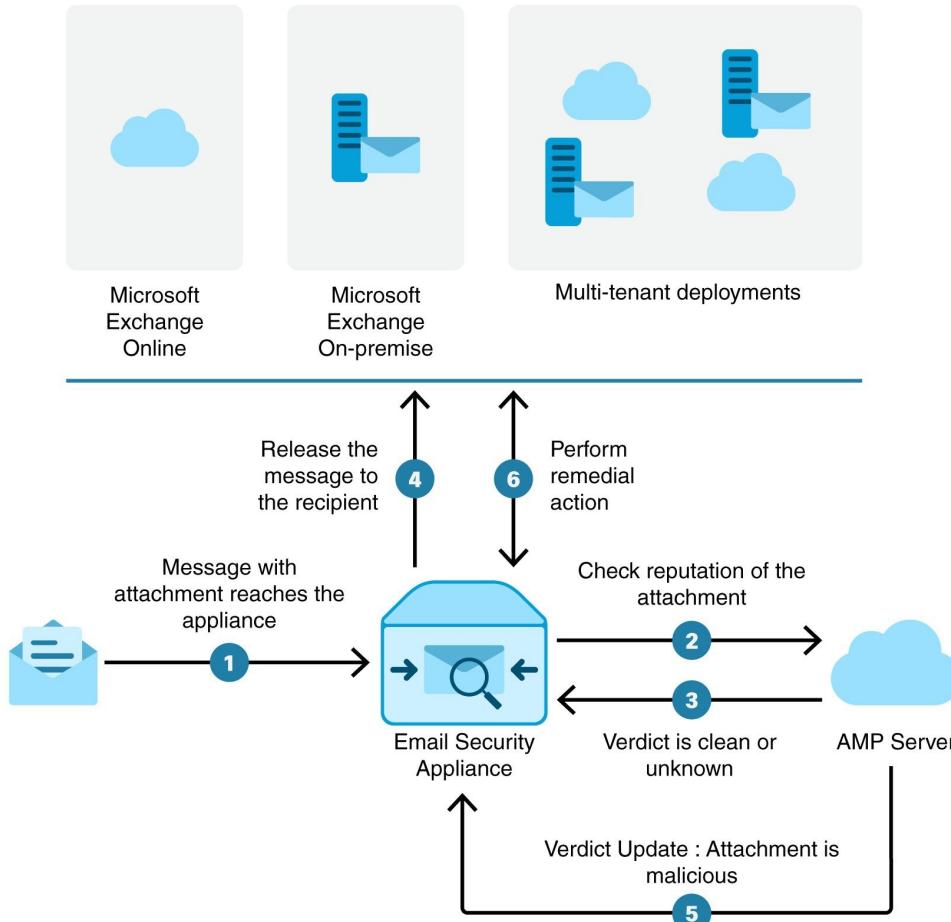
Windows Live Mail



3:01 PM

4/29/2019

Cisco ESA 13.0 – Mailbox Autoremediation



Cisco Threat Response - vyhľadanie IoC (Indication of Compromise)

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate

Clear

Reset

What can I search for?

8

Targets

1

Observable

0

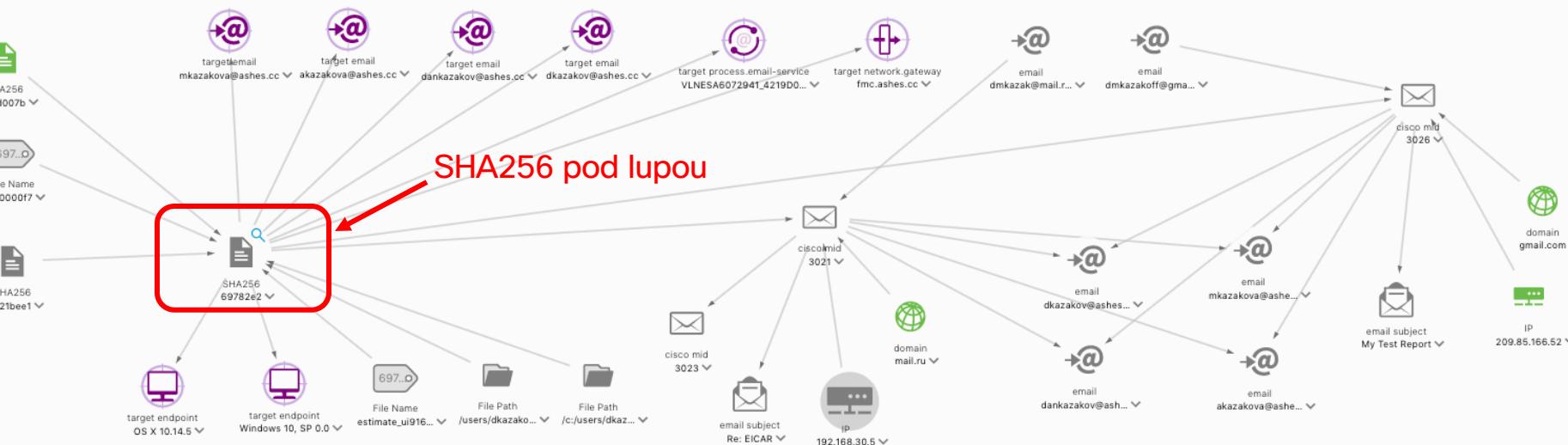
Indicators

0

Domains

1

File Hash

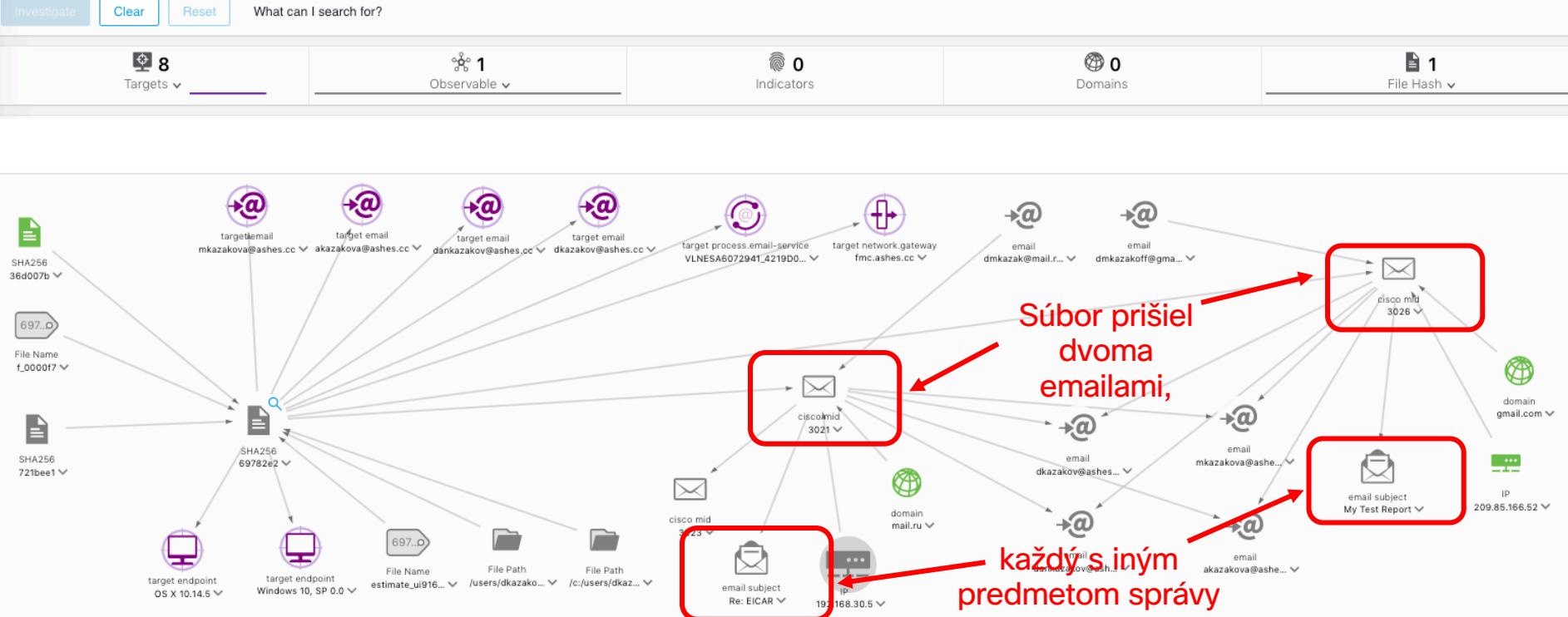


Cisco Threat Response - trasovanie IoC cez siet'

(1/3)

Investigation 1 of 1 enrichments complete

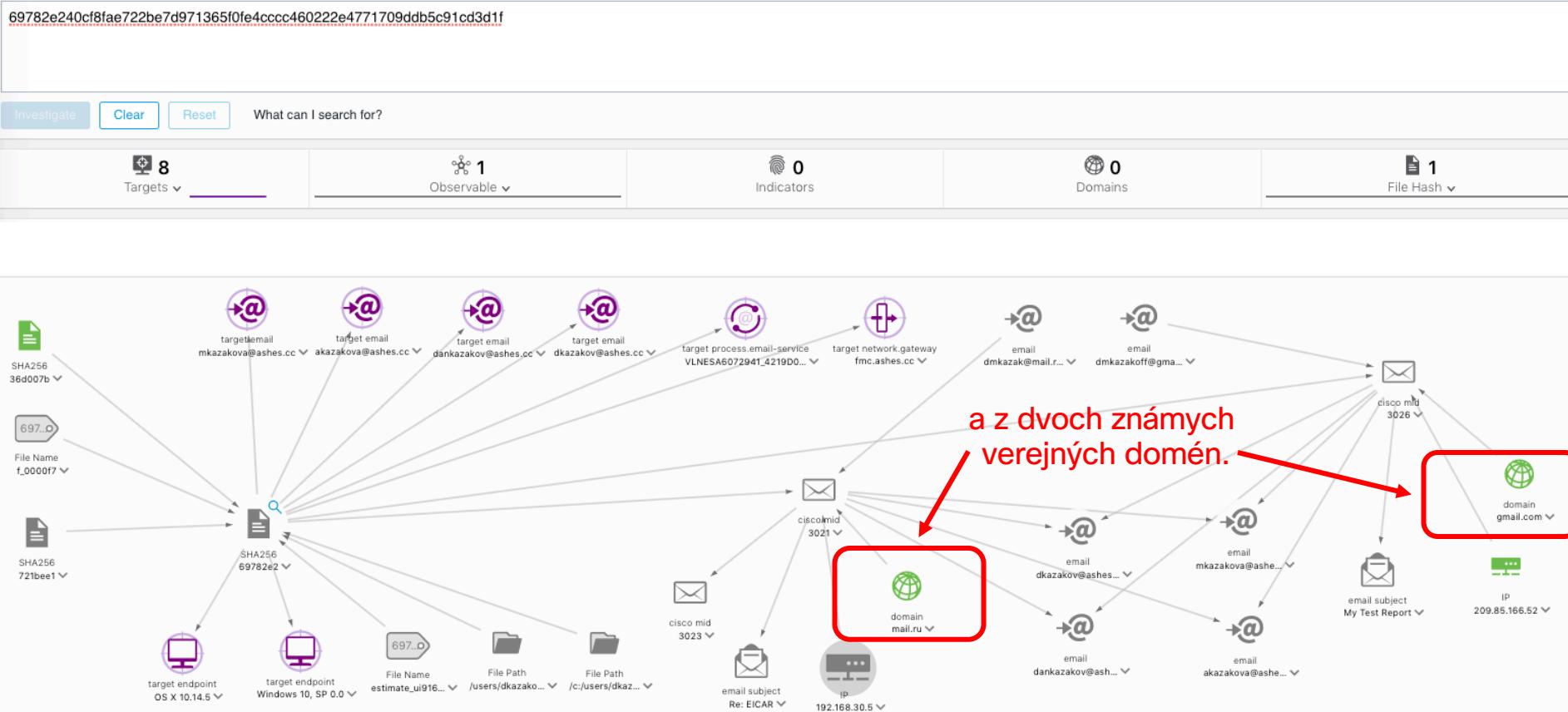
69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f



Cisco Threat Response - trasovanie IoC cez siet'

(2/3)

Investigation 1 of 1 enrichments complete



Cisco Threat Response - trasovanie IoC cez siet'

(3/3)

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate

Clear

Reset

What can I search for?

8

Targets

1

Observable

0

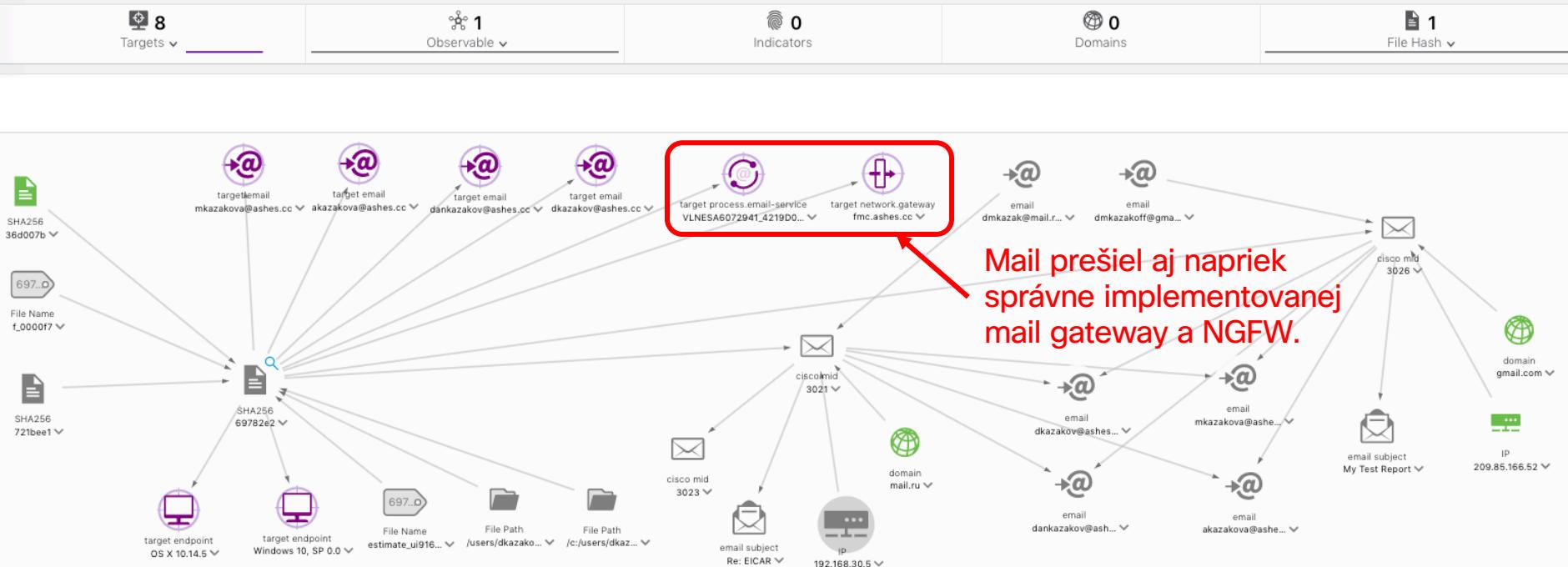
Indicators

0

Domains

1

File Hash



Cisco Threat Response - analýza cieľa

Investigation 1 of 1 enrichments complete

69782e240cf8fae722be7d971365f0fe4cccc460222e4771709ddb5c91cd3d1f

Investigate

Clear

Reset

What can I search for?

8

Targets

1

Observable

0

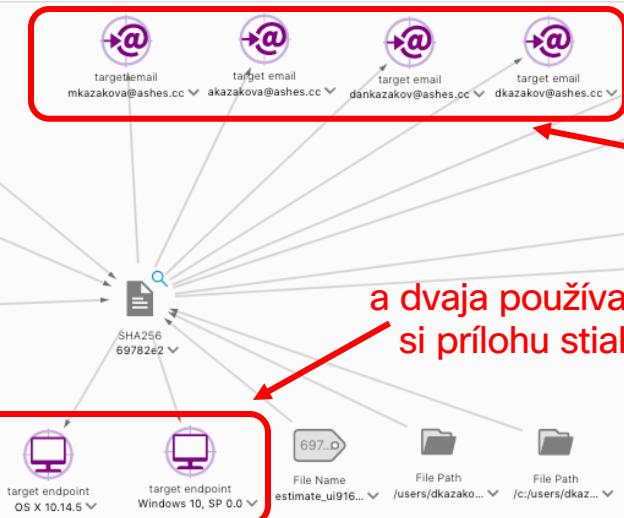
Indicators

0

Domains

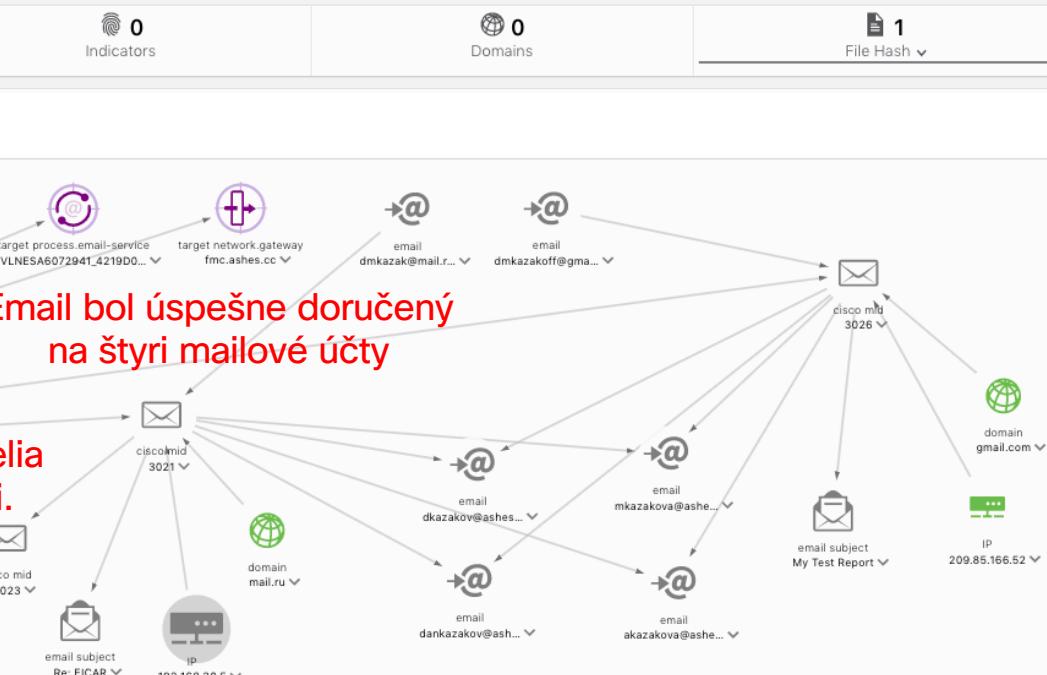
1

File Hash

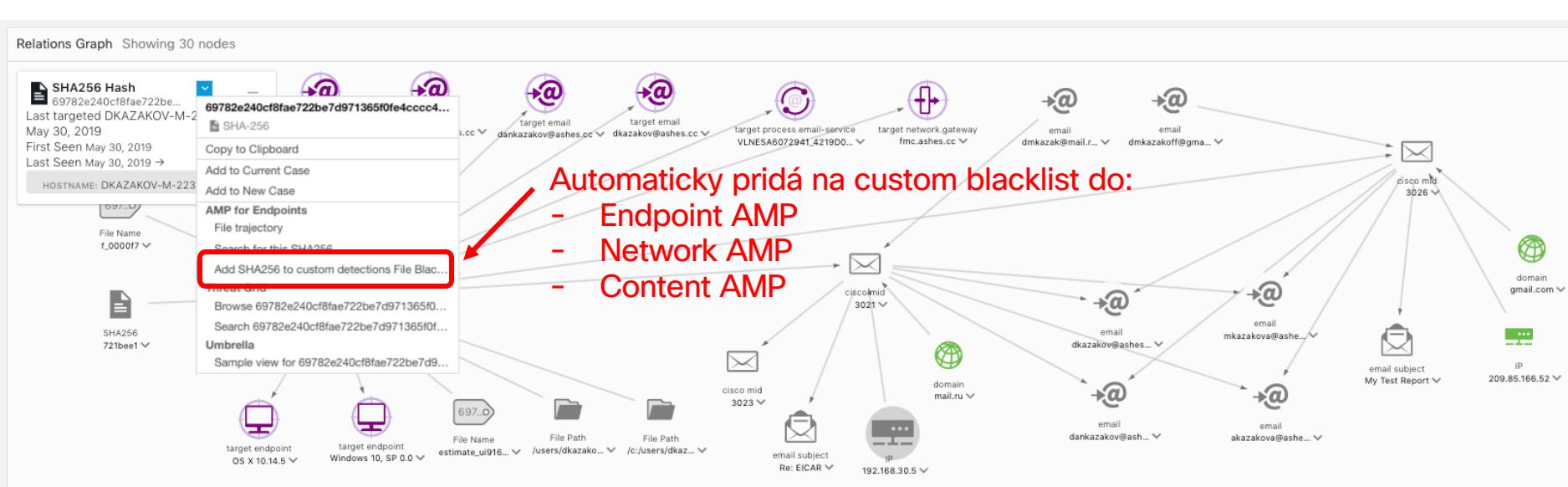


Email bol úspešne doručený
na štyri mailové účty

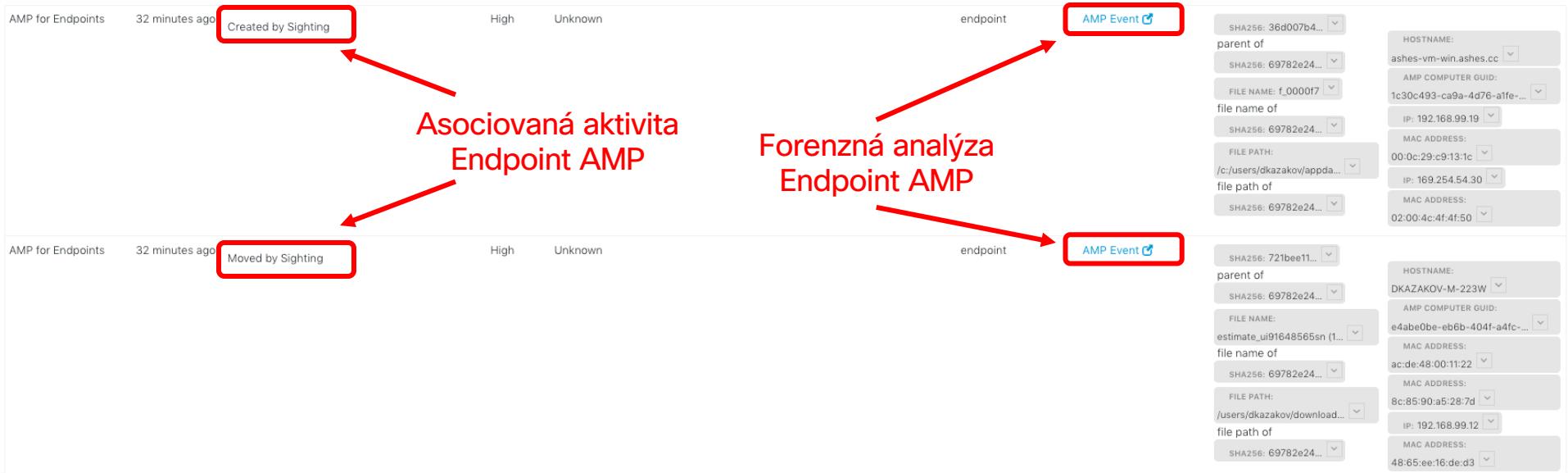
a dva používatelia
si prílohu stiahli.



Cisco Threat Response - bloknutie na pár klikov



Cisco Threat Response - sled udalostí v čase



Endpoint AMP engines

Attack Timeline

Proactive

Orbital search

Low Prevalence Applications

Sandboxing

Custom Blacklists
Vulnerability mapping

In Memory

Exploit Prevention

System Protection

On Disk

Reputation 1:1

Fuzzy Fingerprinting

Machine Learning

Tetra / ClamAV

Script Protection

DFC

Retrospection

Post Infection

Server Side IOC

Client Side IOC

MAP (offline anti-ransomware)

CTA

Device / File Trajectory

IP & Application Blocking

Integration (ISE, FTD ...)

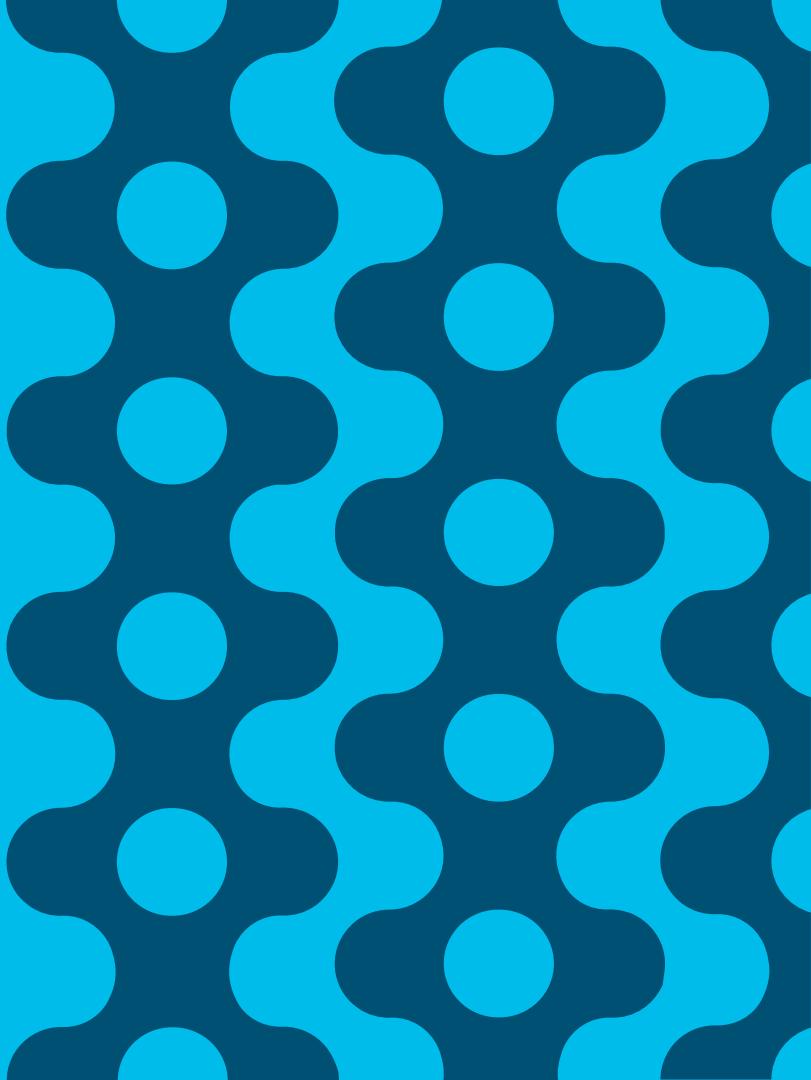
Host Isolation

shorter

Time To Detection

longer

Na záver



Proti útokom sa treba chrániť na viacerých vrstvách

CIEĽ

KOMPROMITÁCIA

PRIENIK

RECONNAIS
SANCE

WEAPONIZA
TION

DELIVERY

EXPLOITATI
ON

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVES

Vzájomná
integrácia a
Cisco Threat
Response



pre rýchle
riešenie
bezpečnostných
incidentov



Analýza správania
Stealthwatch



Segmentácia
na báze identity
ISE



zero trust for
workforce

TALOS
Threat
Intelligence



Threat Grid
globálny
sandbox

Umbrella
DNS
Security



Cisco Email
Security



Cisco Web
Security



Signatúry
NGIPS



Pokročilá
ochrana proti
malvéru
AMP



Aplikačná
ochrana so
segmentáciou
Tetration



Pokročilá
ochrana proti
malvéru
AMP

inštalovaná na
koncové
zariadenia a
servery



Umbrella
DNS Security



Cognitive Threat
Analytics
pre webovú
ochranu a
Stealthwatch



Threat
intelligence
pre NGIPS



Analýza správania
Stealthwatch

integráciou s
identitami **ISE**,
analytikou
šifrovanej
prevádzky bez
nutnosti
dešifrovania **ETA** a
dát zasielaných
koncovými
zariadeniami
Anyconnect

Ďakujeme

Cisco Tech Club Webináře

14.05.2020 Cisco HyperFlex – nie iba obyčajná hyperkonvergovaná platforma

19.05.2020 Kybernetická bezpečnosť v prostredí IoT sietí

21.05.2020 Dizajn a vlastnosti moderných Wi-Fi 6 sietí



You make **possible**