

Cisco Cross Domain Security Architecture

Cisco Knowledge Network session



Gyula Nagy
Senior Network Security Architect

12th Nov 2020



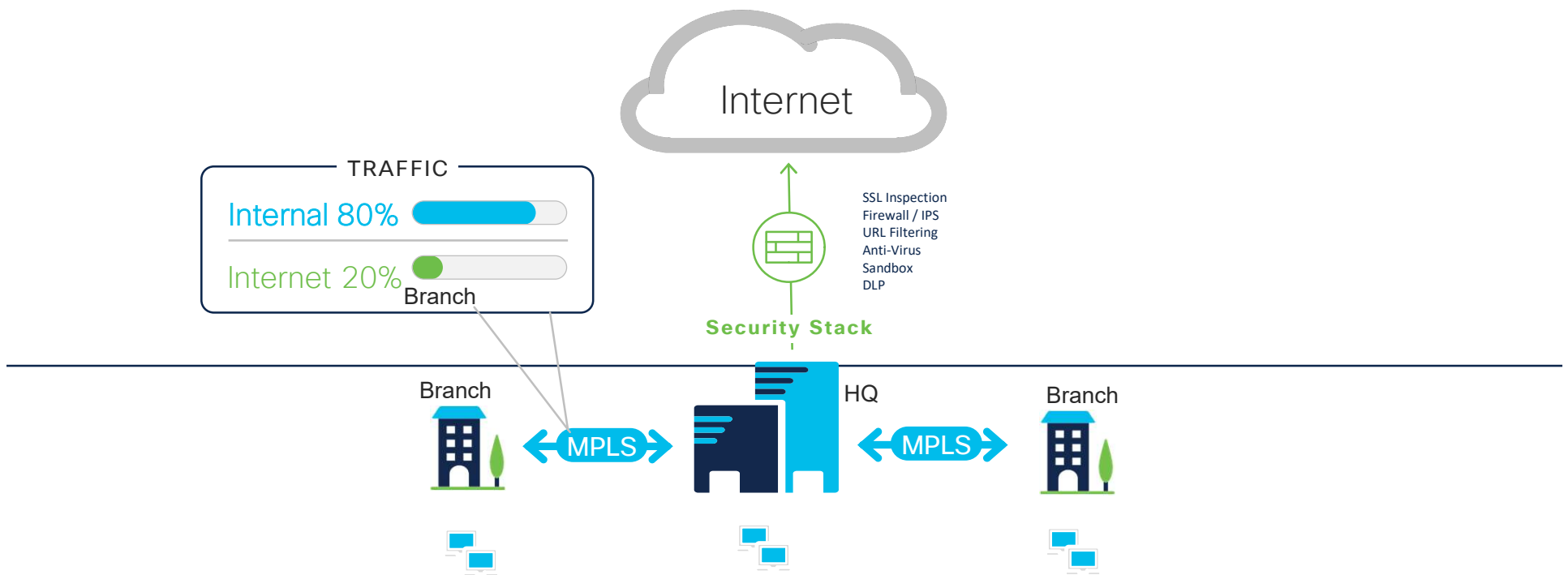
Pramod Nair, Gyorgy Acs
Technical Solution Architects

Agenda



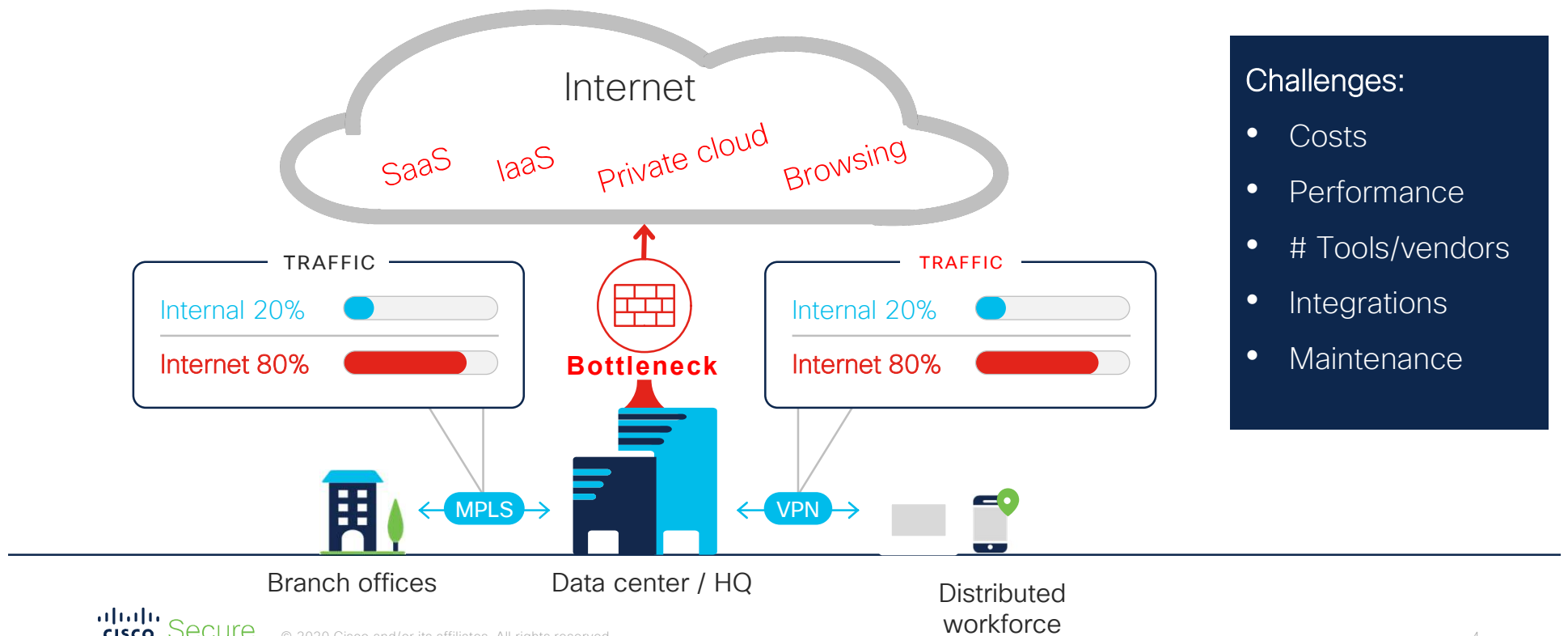
- ▶ Changing Traffic models & Key security requirements in SP IT infra
- ▶ Cisco Cross-Domain security Architecture
- ▶ Magyar Telekom Case study - Practical deployment of Cisco's Cross Domain security architecture

Traditional deployments & Traffic models



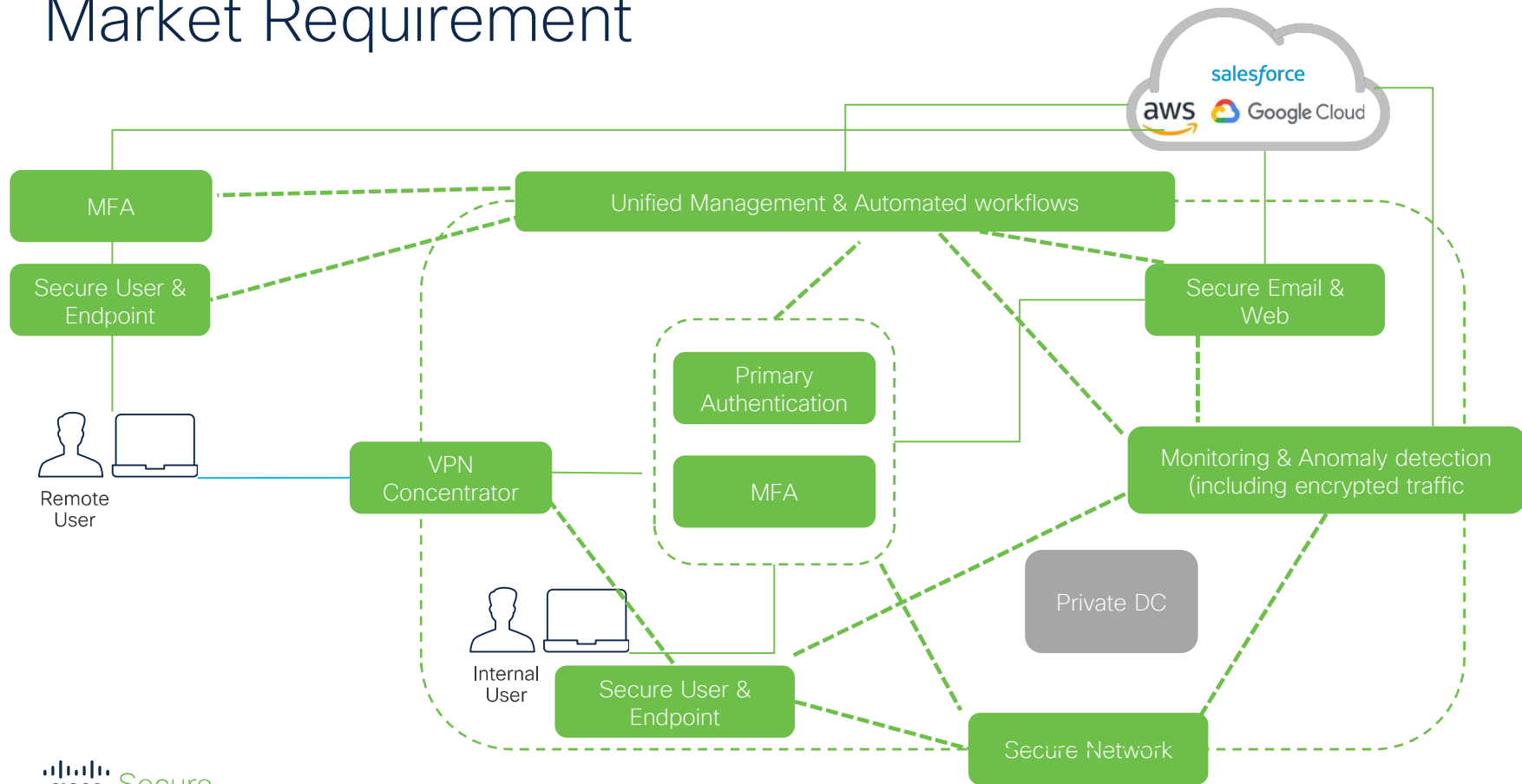
Inverted Traffic Model

Changes in Types of Traffic, Origins and Destinations



- Challenges:
- Costs
 - Performance
 - # Tools/vendors
 - Integrations
 - Maintenance

Market Requirement



True cross-domain security



Case study – Cross Domain security architecture deployment in Magyar Telekom

Case Study: Magyar Telekom



Hungarian service provider streamlines security with Cisco

Magyar Telekom, a leading European telecommunications provider serving five million customers, achieves business efficiencies and builds ambitious plans that include fiber and 5G enabled by Cisco's unified security platform.

[Watch video \(1:51\) \(English - Hungarian subtitles\)](#)

[Read case study](#)

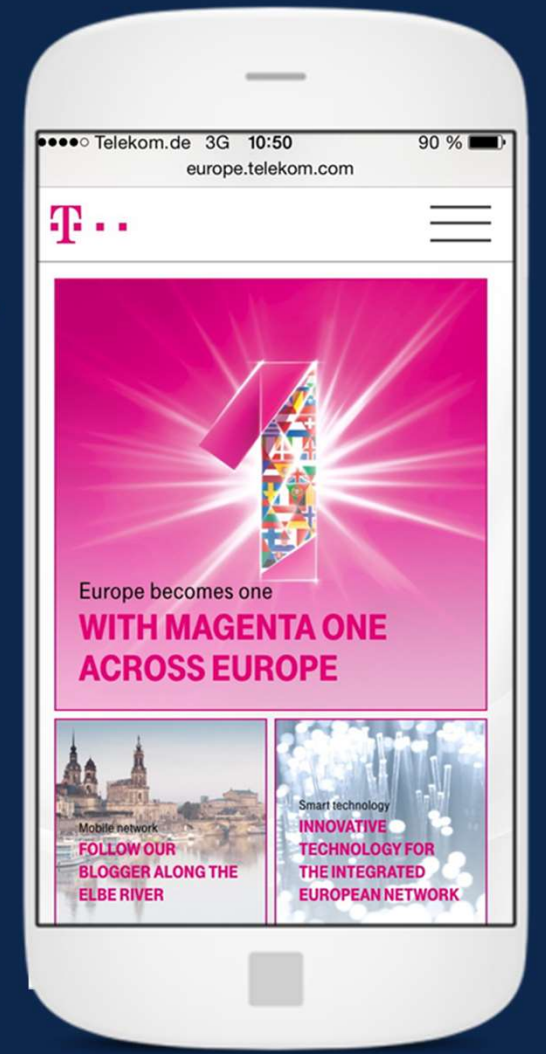


“The most important thing is that the Cisco security platform simplifies everything we do”

Source: <https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/magyar-telekom.html>

Introducing of Magyar Telekom

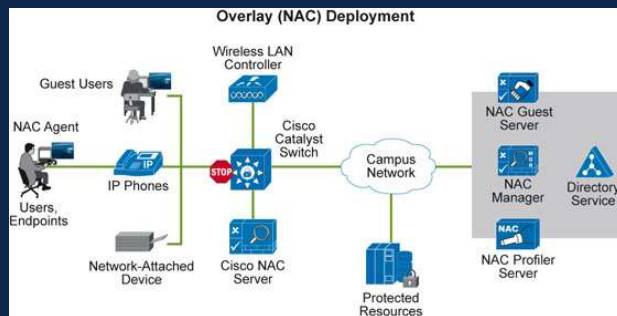
- Magyar Telekom is Hungary's leading telecommunications operator, providing the full range of telecommunication and info communication (ICT) services
- Fixed line, mobile (2G- 5G) and integrated services, as well as IT and system integration services, B2B, B2C
- Magyar Telekom Group has more than 8,300 employees including our subsidiary, Makedonski Telekom.
- Magyar Telekom's majority owner (59.21 %) is Deutsche Telekom



Evolution of Access Control

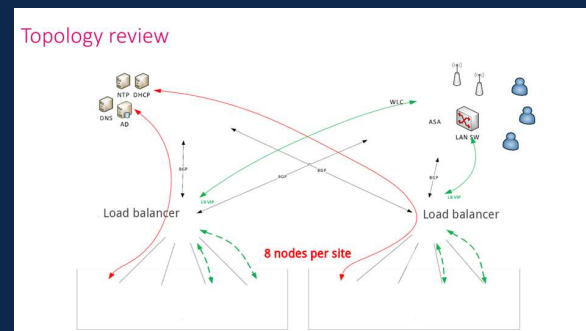
Past with NAC appliance:

- only for wired
- AD integration



Now with ISE:

- For wired, wireless, VPN
- Multi-forest support
- Info sharing with PxGrid
- IoT support
- We are waiting cloud connector
- Posture as the 1st level of enforcement (for example: WannaCry)



Posture Assessment Policy against RDP vulnerability (CVE-2019-0708)

- At that time there was no official rule for it
- Very flexible possibility to create own rule

Service Conditions List > [Remote_desktop_win_notrun](#)

Service Condition

* Name

Description

* Operating Systems

Compliance Module Any version

* Service Name

Service Operator

Registry Conditions List > [pc_WIN7_x86_KB4499175](#)

Registry Condition

* Name

Description

* Operating System

Compliance Module Any version

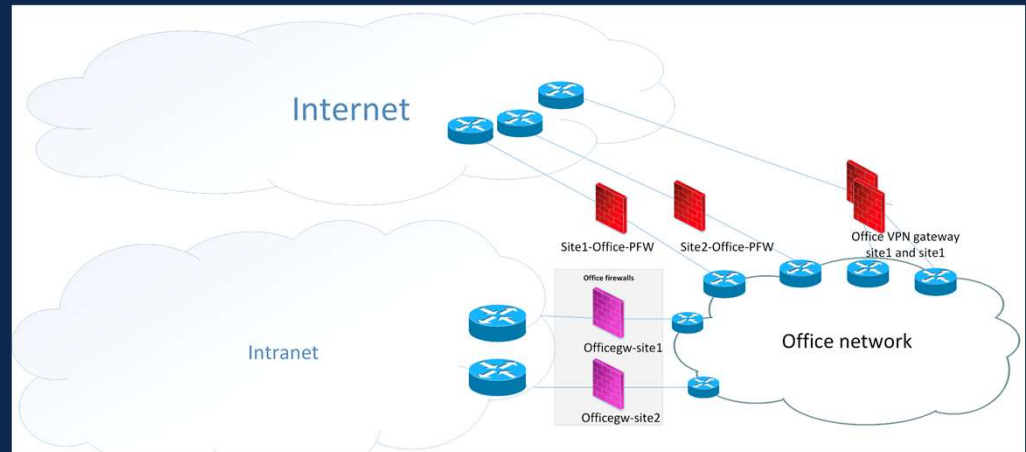
Registry Type

Registry Root Key * Sub Key (enter sub-key without leading backslash)

Value Operator

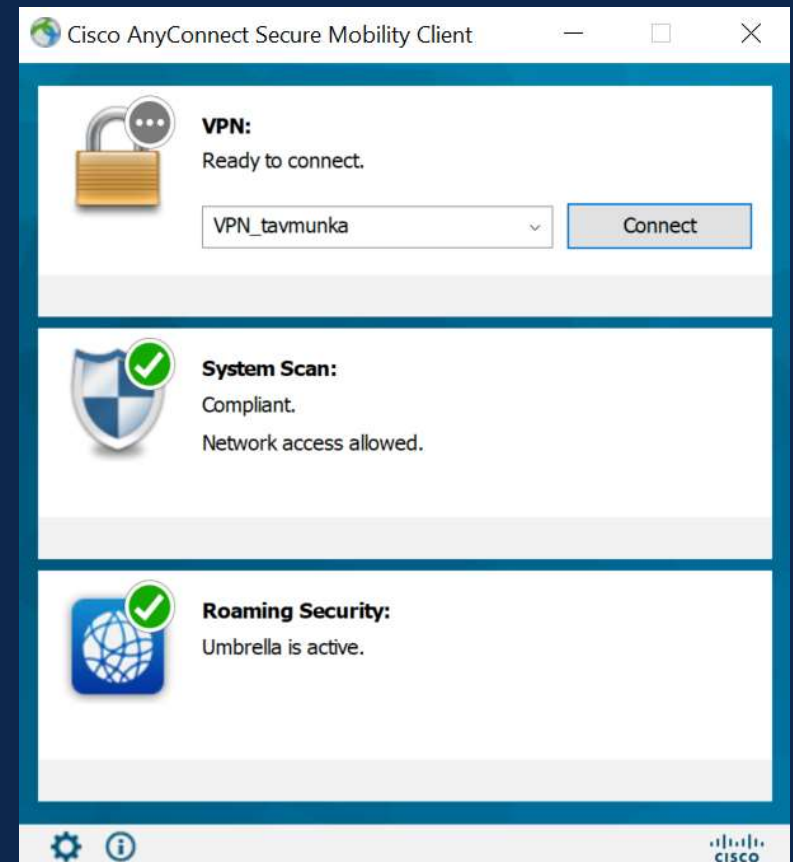
Firewall

- User information sharing with PxGrid
- Role Based Access Control (AD membership) -> easier rule set
- For both directions, in and out
- NG Firewall with NGIPS and AMP
- Threat Intelligence



Secure Remote Access

- VPN (~5000 concurrent AnyConnect user + ASA software) + Umbrella + Duo
- Same security level like in the HQ, for posture, for example
- Visibility with AnyConnect Network Visibility Module and ASA NetFlow
- Defense for Remote Workers by Umbrella Roaming Client
- Duo: More comfortable solution than just a simple SMS



Cisco Secure Endpoint / AMP Threat Grid Appliance

- More than 10k active endpoints
- Cloud based management
- Orbital queries against new vulnerabilities, like SMB, logged-in users and running apps
- Fine-tuned, special policy for servers
- On prem Threat Grid around 1,500 samples per day
- Integration with WSA, ESA, FTD and TheHive

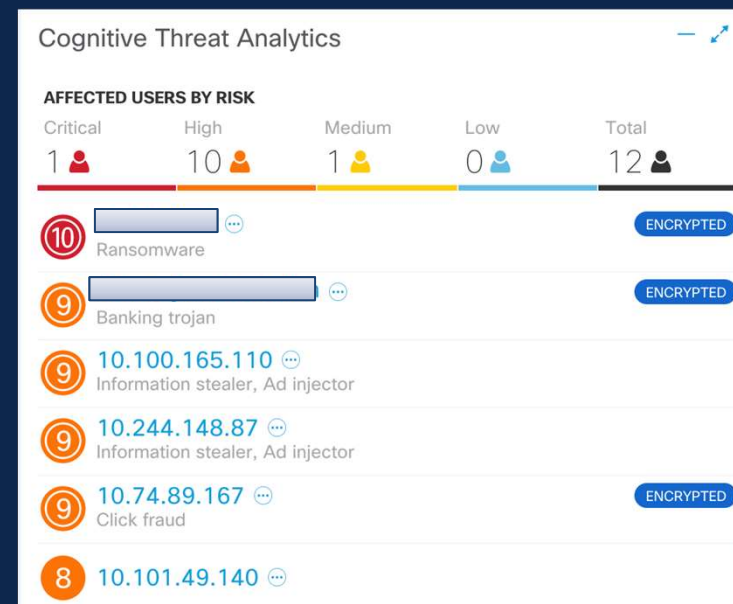
The screenshot displays the 'Query Catalog' interface. On the left, there is a navigation pane with a '< Back' button. The main content area is titled 'CVE-2020-1472 Monitoring 2.0.0'. Below the title, there are sections for 'CREATED' and 'ABOUT'. The 'CREATED' section indicates the query was created by Cisco on 2020-09-17 and updated on 2020-10-05. The 'ABOUT' section provides a detailed description of the query, stating it is applicable to Windows and checks for hosts vulnerable to CVE-2020-1472 by verifying if correct patches were applied. It also mentions that the query retrieves registry key data for 'FullSecureChannelProtection' and that a value of '1' indicates that DCs will deny vulnerable Netlogon secure channel connections unless the connection is allowed by the Cisco Vulnerability Assessment (CVA) engine.

On the right side of the interface, there is a notification box stating 'Catalog queries are designed to run independently.' Below this, there is a 'SQL' section with a '+ Add to query' button. The SQL query is as follows:

```
WITH b1 AS (SELECT 1 AS one, name FROM os_version), b2 AS (SELECT 1 AS one, GROUP_CONCAT(hotfix_id) AS kb_installed FROM patches), b3 AS ( SELECT 1 AS one, DATETIME(mtime, "unixepoch", "UTC") AS enforcement_mode_status_last_modified, CASE data WHEN "1" THEN "Enabled" ELSE "Disabled" END enforcement_mode_status FROM registry WHERE path LIKE "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\FullSecureChannelProtection" ) SELECT b1.name, b2.kb_installed, b3.enforcement_mode_status, b3.enforcement_mode_status_last_modified,
```

Monitoring & Anomaly detection

- Stealthwatch for anomaly detection
 - Host Group is crucial
 - Multi Domain capability
 - Integration with ID provider and user monitoring
 - Cognitive Intelligence
 - Flow rate: 15k FPS
- Encrypted Traffic Analytics, ETA:
 - Precise incident reporting
 - Using Catalyst 9k series as a Sensor
 - ETA support from Flow Sensor 7.1

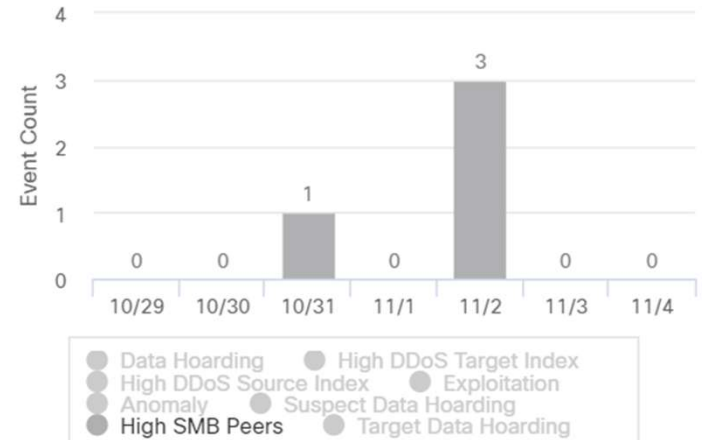


WannaCry Example for Stealthwatch

The screenshot shows the StealthWatch Management Console interface. On the left, a tree view displays 'Enterprise' and 'Host Groups'. A context menu is open over the 'Security' section, listing options like 'Concern Index', 'Target Index', 'File Sharing Index', 'Worm Tracker', 'Touched Hosts', 'Touched Hosts - High CI Hosts', 'Email Alerts', and 'Security Events'. The main panel shows a 'Host Group Dashboard' with a table of hosts and their CI% values. A table titled 'Targets of Attack - Today - 921 records summarized into ...' lists various host groups and their associated alerts.







Host Groups	Host	CI%	Alerts
Catch All	192.168.1.200	4...	
SZE-DC, PROD	10.20.158.7	4...	TCP Scan
Kelenfold	10.3.64.1	4...	
CCCATCH	10.12.84.32	4...	Port Scan
Taviro office	10.230.52.159	3...	Excess Clients, Ping Oversized Packet, Port Scan, TCP Scan
SHOPSKA, Nyiregyhaza	10.34.74.84	3...	Excess Clients, Excess Servers, Ping
Possible Victims - Today			
Touched Hos...			
Touched Host			
High CI Country			
High CI Host			

Alarms by Type



Cisco Secure Web and Email

- Web:
 - Part of AMP integration, common policy
 - Over 15 millions requests per day (Web)
 - 0.5% blocked (URL category, bad reputation, advanced malware)

 1.53 TB Total Data Used ↑ 2.46% Prior Day	 15.35 M Total Transactions ↑ 4.60% Prior Day	 13.58 M HTTPS Transactions ↑ 3.61% Prior Day	 11.59 k Transactions Blocked by Policy ↑ 119.91% Prior Day	 1 Transactions Blocked by Threat Engines No Data For Prior Day	 161 Malicious Verdicts by AMP ↑ 87.21% Prior Day
--	---	---	--	--	--

- Email:
 - SecureX integration in production
 - Microsoft 365 and on-premise Email servers are protected

Security Efficacy Order

- Cisco Advanced Malware Protection
- Cisco Identity Services Engine
- Cisco Stealthwatch Enterprise
- Cisco Next-Generation Intrusion Prevention System
- Cisco Umbrella

SecureX threat hunting with the help of analyzers

- Cisco SecureX platform for unified view of e2e security controls
- We can compare the results coming from SecureX threat hunting and TheHive analyzers
- We can save these IoCs into casebooks and we can share them with other analysts

The screenshot displays the Cisco Threat Response Investigate interface. At the top, there are navigation tabs for 'Threat Response', 'Investigate', 'Snapshots', 'Incidents', 'Intelligence', and 'Modules'. Below the navigation, there are buttons for 'New Investigation', 'Assign to Incident', and 'Snapshots ...'. A summary bar shows 5 Targets, 15 Observables, 77 Indicators, 5 Domains, 6 File Hashes, and 4 IP Addresses. A popup window titled '3 Networks • 2 Endpoints' is open, showing details for two endpoints:

- ALEXA-WIN10**
WINDOWS 10, SP 0.0
AMP GUID: f4496b86-14c4-413e-a2c3-c40042cdad7d
HOSTNAME: ALEXA-WIN10
IP ADDRESS: 192.168.249.111
MAC ADDRESS: 00:50:56:b8:86:5e
- IP ADDRESS**
192.168.249.166
IP ADDRESS: 64.100.2.10
ODNS IDENTITY: 285278818
ODNS IDENTITY LABEL: ciscothreatresponse.local

The background shows a network diagram with various nodes including Target Networks (350355562, 285278902), Domains (hr-wipro.com, mx-pool48.kron...), and Target Endpoints (Windows 10, SP 0.0). File hashes (SHA-256) are also visible, such as b017b9f and 8ec4b61.

SecureX integration with TheHive

- Analyzers: observables will be tagged by analyzers
- Responders: after / during investigation analysts can initiate an incident action

Analyzers (10)

Data Types (7) Analyzer

Select - Search for analyzer description Search Clear

EmlParser_1_2 Version: 1.2 Author: ninemith License: AGPL-V3
Parse Emi message
Applies to: file

Investigate_Categorization_1_0 Version: 1.0 Author: Cisco Umbrella Research @opendns License: AGPL-V3
Retrieve investigate categorization and security features for a domain.
Applies to: domain fqdn

Investigate_Sample_1_0 Version: 1.0 Author: Cisco Umbrella Research @opendns License: AGPL-V3
Retrieve sample data from investigate for a hash. (Sample data provided by ThreatGrid)
Applies to: hash

Msg_Parser_3_0 Version: 3.0 Author: CERT-BDF License: AGPL-V3
Parse Outlook MSG files and extract the main artifacts.
Applies to: file

ThreatGrid_1_0 Version: 1.0 Author: Cisco Security License: MIT
Threat Grid Sandbox
Applies to: file url hash

ThreatResponse_1_0 Version: 1.0 Author: Cisco Security License: MIT
Threat Response
Applies to: domain hostname fqdn hash ip url

TorProject_1_0 Version: 1.0 Author: Marc-André DOLL, STARC by EXAPROBE License: AGPL-V3
Query https://check.torproject.org/exit-addresses for TOR exit nodes IP addresses.
Applies to: ip

Umbrella_Report_1_0 Version: 1.0 Author: Kyle Parrish License: AGPL-V3
Query the Umbrella Reporting API for recent DNS queries and their status.
Applies to: domain

Responders (6)

Data Types (1) Responder

Select - Search for responder description Search Clear

AMPforEndpoints_IsolationStart_1_0 Version: 1.0 Author: Cisco Security License: MIT
Start host isolation for an AMP for Endpoints connector
Applies to: thehive:case_artifact

AMPforEndpoints_IsolationStop_1_0 Version: 1.0 Author: Cisco Security License: MIT
Stop host isolation for an AMP for Endpoints connector
Applies to: thehive:case_artifact

AMPforEndpoints_MoveGUID_1_0 Version: 1.0 Author: Cisco Security License: MIT
Move an AMP for Endpoints connector GUID to a different Group
Applies to: thehive:case_artifact

AMPforEndpoints_SCDAdd_1_0 Version: 1.0 Author: Cisco Security License: MIT
Add a SHA256 to an AMP for Endpoints Simple Custom Detection list
Applies to: thehive:case_artifact

AMPforEndpoints_SCDRemove_1_0 Version: 1.0 Author: Cisco Security License: MIT
Remove a SHA256 to an AMP for Endpoints Simple Custom Detection list
Applies to: thehive:case_artifact

Umbrella Blacklister_1_1 Version: 1.1 Author: Kyle Parrish License: AGPL-V3
Add domain to Umbrella blacklist via Enforcement API.
Applies to: thehive:case_artifact

file FW_NAV adóvisszatérítés [.]msg

None

MsgParser:Attachments="1" TG:Analysis="81"

domain internetbadguys[.]com

telekom phishing

Investigate:Content Categories="Computer Security" Investigate:Status="Blocked" Investigate:Security Categories="Malware, Phishing" Umbrella:Hits="False" TR:Talos Intelligence="Unknown" TR:Umbrella="Malicious"

What Cisco SecureX means in Practice?

- Feed information from different channels, like MISP
- The role of SecureX:
 - Quick threat hunting and response
 - Deeper integration with Cisco security systems, like Orbital
 - Automation and orchestration option
- The role of TheHive:
 - Long term incident handling and documentation
 - Playbooks for different incident types, case template

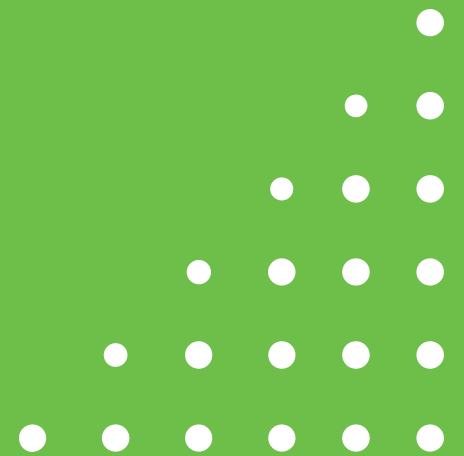
The screenshot shows a task list for a phishing e-mail incident. The header is "Phishing e-mail" with a subtitle "Phishing Telekom via spam e-mail". The list is titled "Tasks (8)" and contains the following items:

- [Dokumentáció készítése] Adatok rögzítése
- [Dokumentáció készítése] Bizonyíték rögzítése
- [Technical Response] Phishing URL Jelentése a Google safe browsing weboldalán
- [Technical Response] Phishin domain tiltása InvDDoS rendszerben vezetői Jóváhagyás után
- [Technical Response] Phishing domain tiltása az Umbrella rendszerben
- [Technical Response] Phishing domain tiltása a WSA rendszerben
- [Technical Response] IPS block
- [Communication] Válasz és Külső kommunikáció szervezése

Summary

- Cisco's Cross domain security architecture has got a strong backend integration allowing better threat mitigation
- The Cisco ecosystem involves interlocking security modules including 3rd party solutions and provides holistic approach in a multi-vendor environment
- SecureX key practical capabilities:
 - Quick threat hunting and response
 - Deeper integration with Cisco security systems, like Orbital
 - Enhanced Automation and orchestration option

Question?





Thank You!