CISCO Connect

Ukraine cybersecurity learnings

Cyber Resilience lessons

Volodymyr Ilibman
Security Account Executive - Ukraine

02.12.25

CISCO Connect

Ukraine cybersecurity learnings

Cyber Resilience lessons

Volodymyr Ilibman
Security Account Executive - Ukraine

02.12.25

Agenda

1. Cyber Resilience in Totalförsvar
2. Major attacks retrospective
3. Security trends in Ukraine
4. Case studies of IT shifts under pressure
5. Cisco’s role and ongoing engagement

Cyber Resilience

The ability to protect the integrity of every aspect of the business to withstand unpredictable cyber threats or changes…

…and then emerge stronger

Major cyber attacks against Ukraine

February 2014

Russia has seized the Crimean peninsula and started a proxy war in Donbas region

May 2014

Attack against Central election comission

December 2015

Russia launches cyber attack, Black Energy 2, disrupting power

December 2016

Industroyer attack disrupts power again

2017 NotPetya

Supply Chain attack – costliest global attack in history

Jan 2022

Pre-Invasion Cyber Offensives

February 2022

Russia invades Ukraine. Viasat satellite hack

March 2022

Industroyer2 attempts to disrupt power

December 2023

Attack against National telecom operator JSC Kyivstar

December 2024

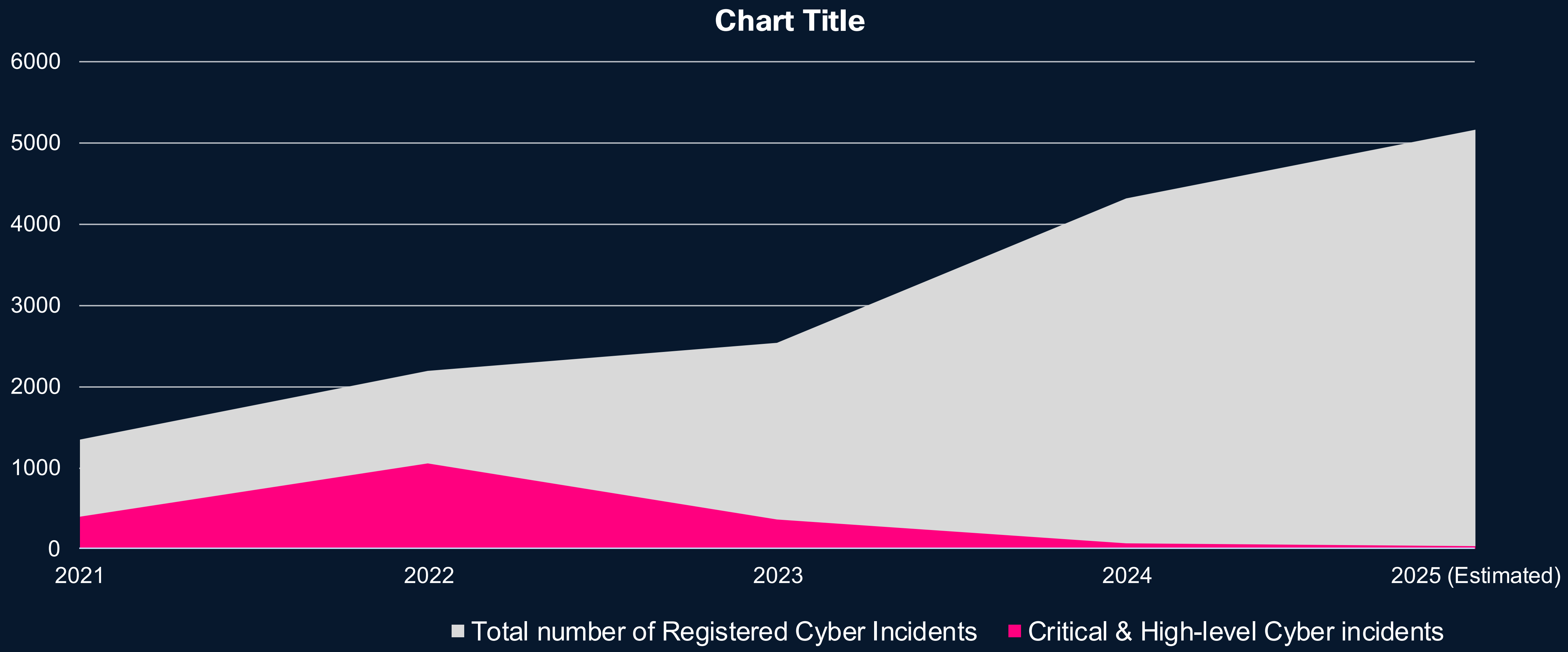
Attack on the Ministry of Justice’s national registries

March 2025

Ukrainian Railway hack

Cyber Incidents in 2021-2025

The increase in cyber incidents and the decrease in significant incidents amount



Analytical Materials of the SSSCIP & CERT.GOV.UA https://cip.gov.ua/en/statics/analitichni-materiali-derzhspeczv-yazku

The 5 trends in Security Risks, based on Ukraine experience

1. There is shift from *Computer network attack* (**CNA**) - disrupt, deny, degrade, or destroy to *Computer network exploitation* (**CNE**) – like espionage
2. Cyber attacks use advanced techniques and legitimate tools & services to bypass classical security controls
3. Cyber attacks against critical infrastructure often correlate with physical and information attacks, geopolitical targets
4. Military attacks and resulting blackouts threatens on-prem infrastructure availability
5. People remain primary social-engineering targets for attackers

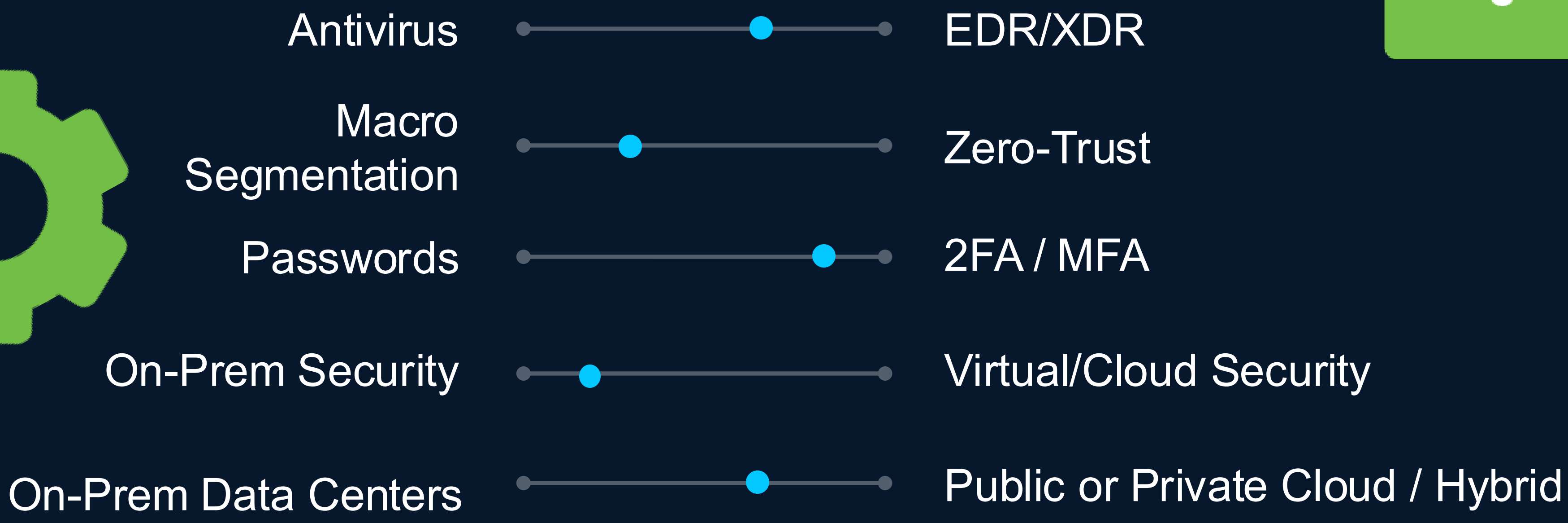
Cyber/IT shifts

Disaster makes security resilience harder

Before war

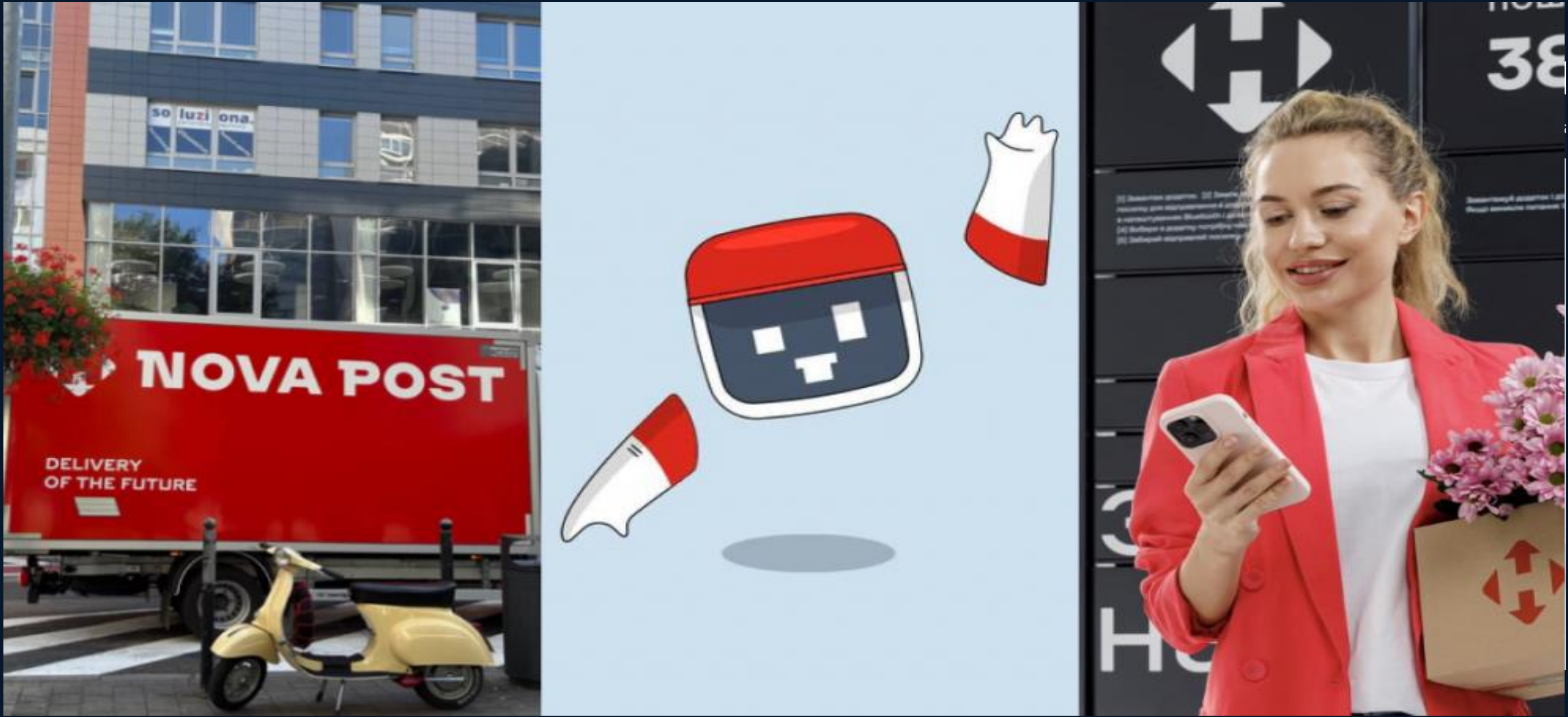
Now

People awareness changed !



Before war	Now
Antivirus	EDR/XDR
Macro Segmentation	Zero-Trust
Passwords	2FA / MFA
On-Prem Security	Virtual/Cloud Security
On-Prem Data Centers	Public or Private Cloud / Hybrid

They all use the cloud now !



Nova Poshta is the largest postal operator in Ukraine.

Nova Post Embraces a Universal Approach to Zero Trust with Cisco Secure Access

Customer Highlight Cisco Public

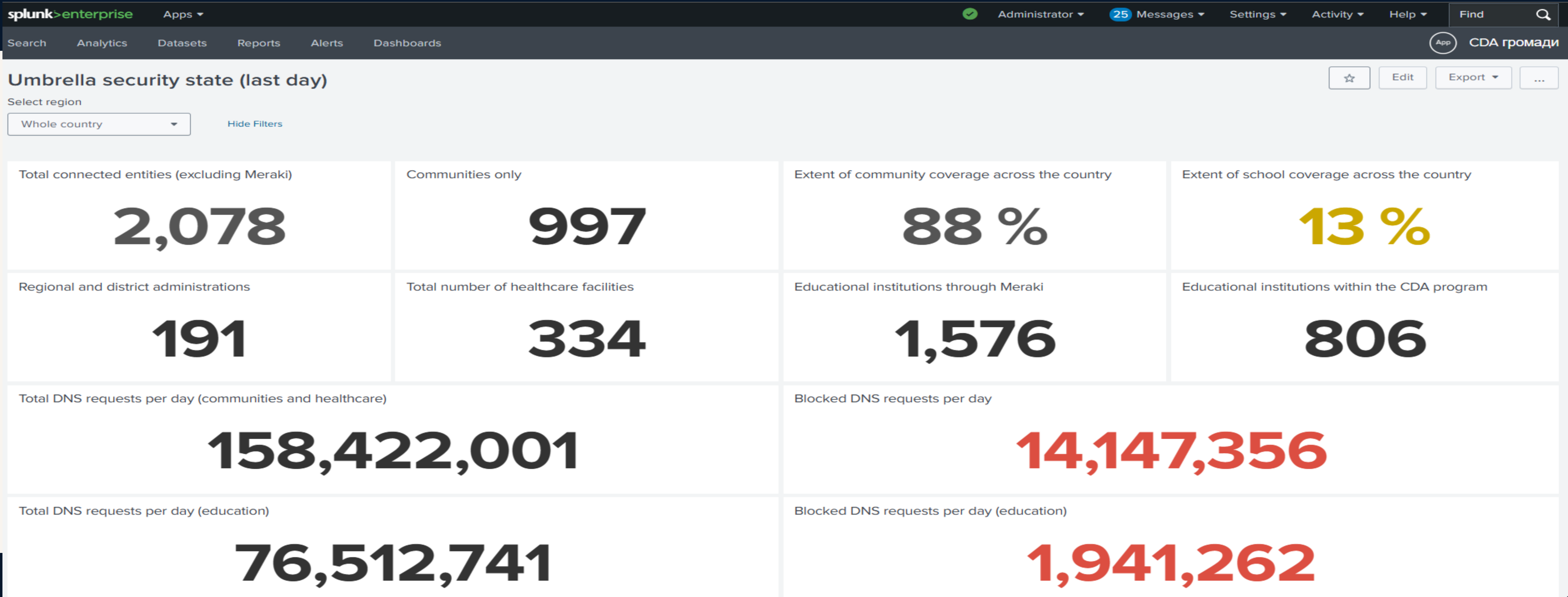
Nova Post Embraces a Universal Approach to Zero Trust with Cisco Secure Access

Industry:	Location:	Organization:	Solution:
Logistics and	Kyiv, Ukraine	30,000 employees, 13,837 branches	Cisco Secure Access

What is Cisco doing to help with Ukrainian Cyber Defence?

Now Cisco provided Umbrella to 2000+ customers all around Ukraine

We are covering 997 local communities, 1500+ schools, 300+ healthcare facilities



Umbrella security state (last day)

Select region: Whole country

Total connected entities (excluding Meraki): 2,078

Communities only: 997

Extent of community coverage across the country: 88 %

Extent of school coverage across the country: 13 %

Regional and district administrations: 191

Total number of healthcare facilities: 334

Educational institutions through Meraki: 1,576

Educational institutions within the CDA program: 806

Total DNS requests per day (communities and healthcare): 158,422,001

Blocked DNS requests per day: 14,147,356

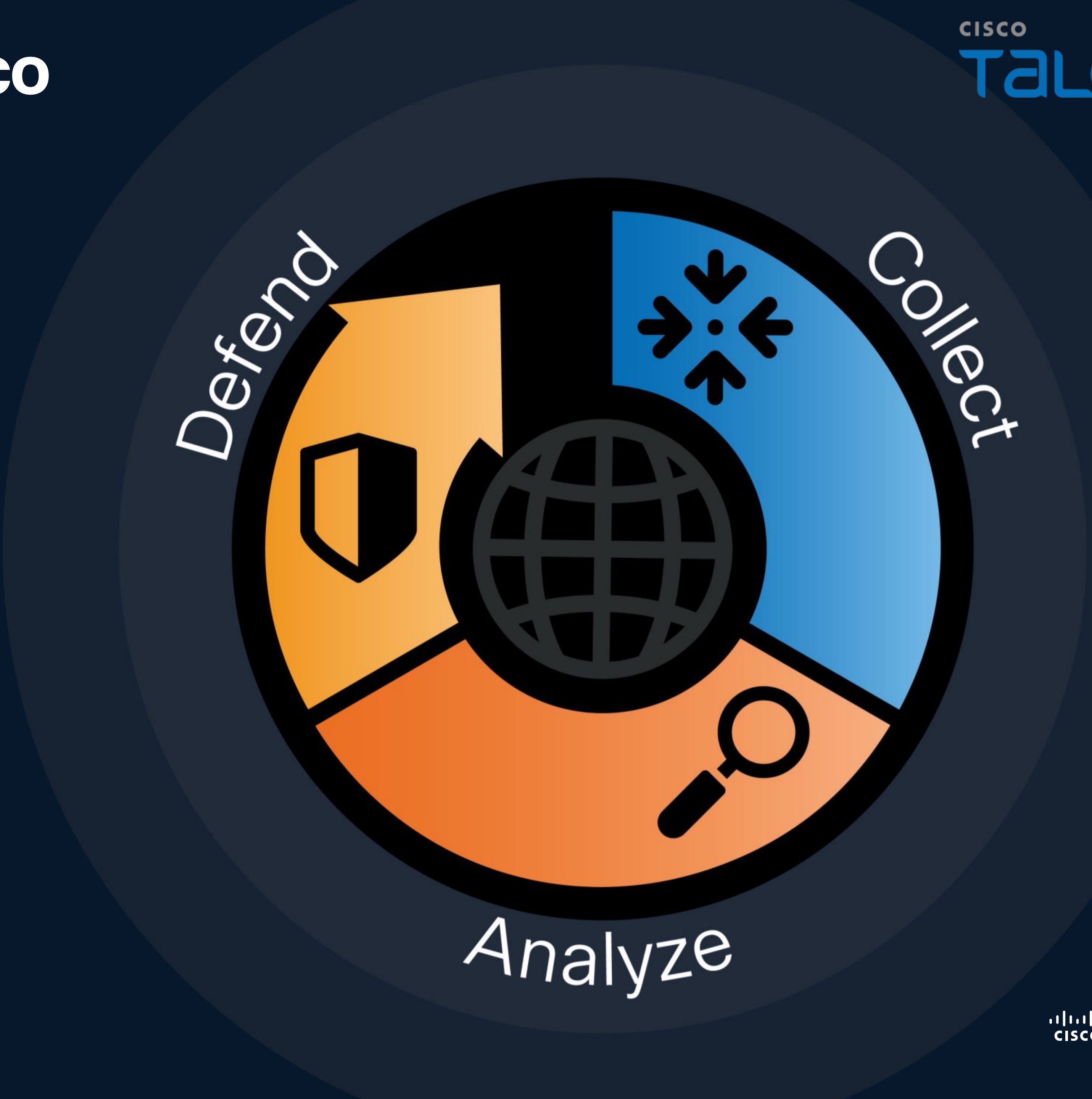
Total DNS requests per day (education): 76,512,741

Blocked DNS requests per day (education): 1,941,262

Talos powers the Cisco portfolio with comprehensive intelligence

886 billion daily events =
one mission

Every customer environment,
every event, every single day,
all around the world



Current Ukraine Talos Support

30+

Critical infrastructure & government partners

45K

Endpoints

650+

Cisco employees monitoring open-source

45

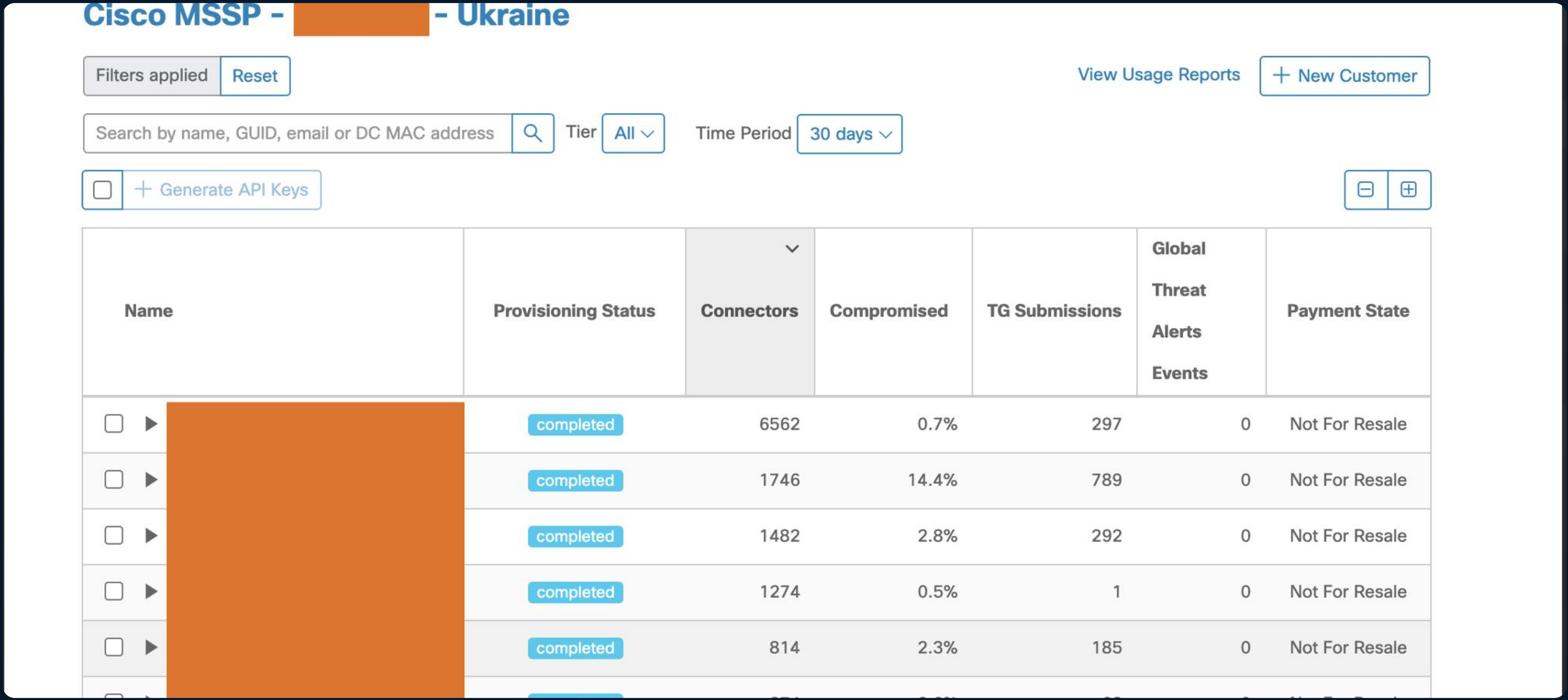
Talos threat hunters

Cisco Secure Endpoint

Cisco Umbrella

Cisco Talos Threat Hunting

Stats for monitored Cisco Secure Endpoints in Ukraine



Cisco MSSP - [redacted] - Ukraine

Filters applied | Reset

View Usage Reports

+ New Customer

Search by name, GUID, email or DC MAC address

Tier: All

Time Period: 30 days

□ + Generate API Keys

Name	Provisioning Status	Connectors	Compromised	TG Submissions	Global Threat Alerts Events	Payment State
□ ▶ [redacted]	completed	6562	0.7%	297	0	Not For Resale
□ ▶ [redacted]	completed	1746	14.4%	789	0	Not For Resale
□ ▶ [redacted]	completed	1482	2.8%	292	0	Not For Resale
□ ▶ [redacted]	completed	1274	0.5%	1	0	Not For Resale
□ ▶ [redacted]	completed	814	2.3%	185	0	Not For Resale

The first rule about the cloud: Everything can change quickly ☺

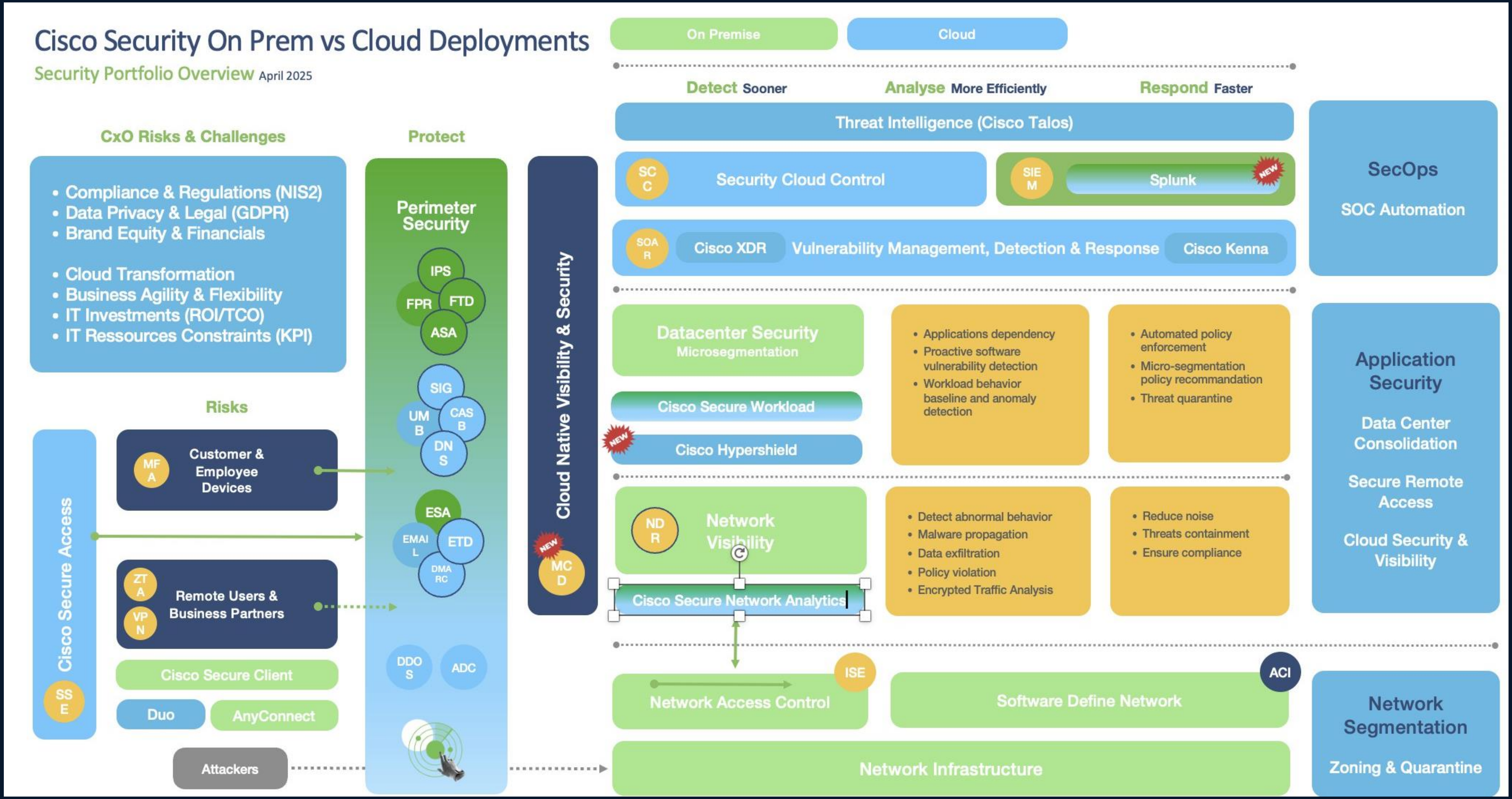
Compliance risks

Finance reasons

Performance Risks

On-premise, Hybrid or Multi-Cloud

Cisco Approach to On-Prem vs Cloud Deployment



Cisco Security On Prem vs Cloud Deployments

Security Portfolio Overview April 2025

On Premise

Cloud

Detect Sooner **Analyse** More Efficiently **Respond** Faster

CxO Risks & Challenges

- Compliance & Regulations (NIS2)
- Data Privacy & Legal (GDPR)
- Brand Equity & Financials

- Cloud Transformation
- Business Agility & Flexibility
- IT Investments (ROI/TCO)
- IT Ressources Constraints (KPI)

Risks

Customer & Employee Devices

Remote Users & Business Partners

Cisco Secure Client

Duo

AnyConnect

Attackers

Cisco Secure Access

Protect

Perimeter Security

Cloud Native Visibility & Security

Threat Intelligence (Cisco Talos)

Security Cloud Control

Splunk

Cisco XDR

Vulnerability Management, Detection & Response

Cisco Kenna

SecOps

SOC Automation

Datacenter Security

Microsegmentation

Cisco Secure Workload

Cisco Hypershield

- Applications dependency
- Proactive software vulnerability detection
- Workload behavior baseline and anomaly detection

- Automated policy enforcement
- Micro-segmentation policy recommandation
- Threat quarantine

Application Security

Data Center Consolidation

Secure Remote Access

Cloud Security & Visibility

Network Visibility

Cisco Secure Network Analytics

- Detect abnormal behavior
- Malware propagation
- Data exfiltration
- Policy violation
- Encrypted Traffic Analysis

- Reduce noise
- Threats containment
- Ensure compliance

Network Access Control

Software Define Network

Network Infrastructure

Network Segmentation

Zoning & Quarantine

Sep 24, 2025

Cisco Announced Cisco Sovereign Critical Infrastructure for Europe

Comprehensive, customizable offering

On-premises deployment

Air-gap licensing

Certifications

Ukraine cybersecurity learnings

There Are No Borders and No Exceptions in Cyber Operations !

1. Adopt a Zero-Trust approach for IT and OT, assuming possible compromise by default.

2. Add Tabletop exercises, Capture the Flag (CTF), and cyber hygiene training to uncover risks, identify resilience gaps, and raise awareness among executives, staff, and users.

3. Establish Information exchange and Proactive threat hunting to identify and respond to hidden threats.

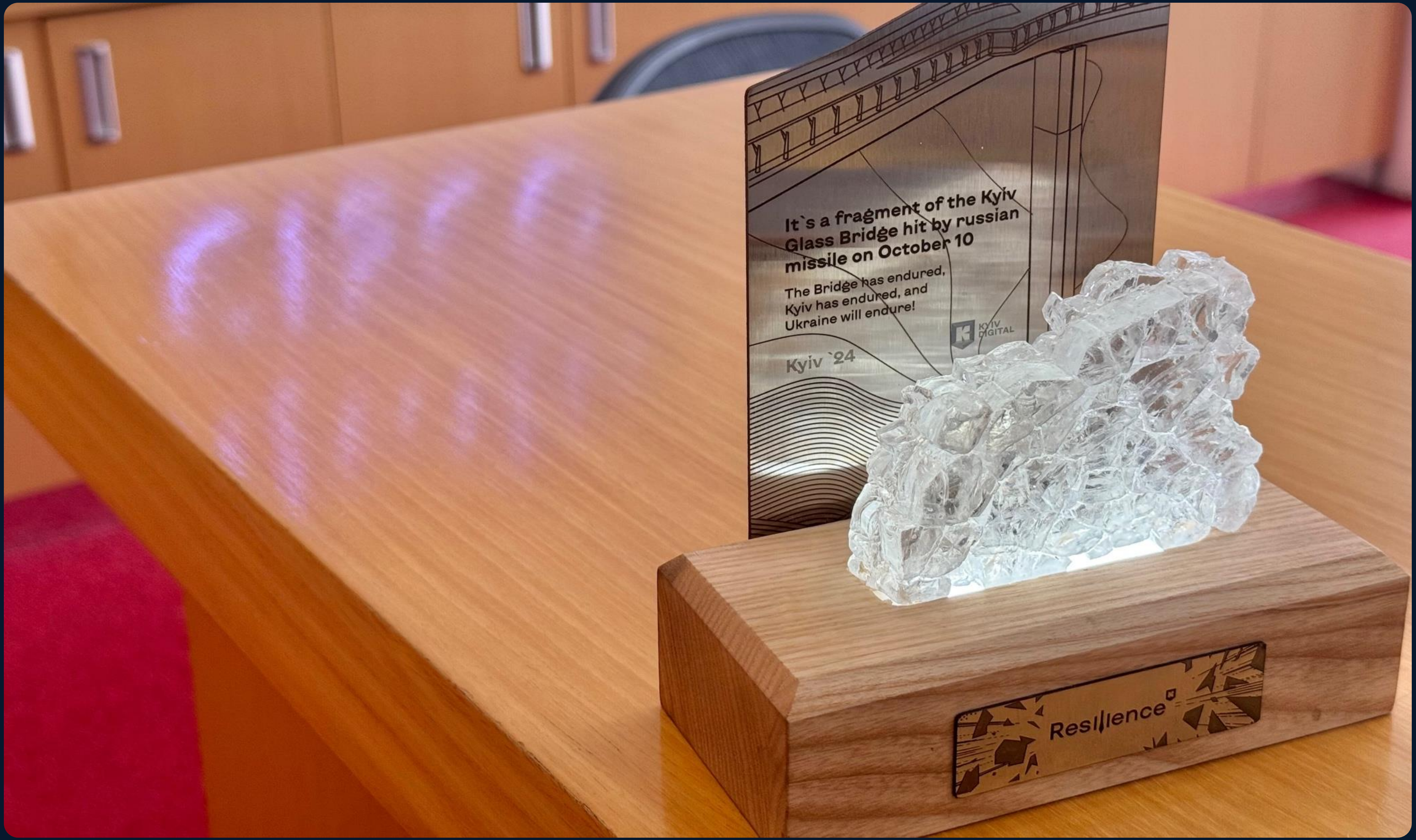
4. Make your IT and Security architecture cloud-ready and flexible to adapt to change*.

5. Approach resilience holistically including human, physical and supply-chain risks.

* https://www.cisco.com/c/en_au/solutions/hybrid-cloud/2022-trends-report-cte.html

… one more story – “Klitschko” Glass Bridge

(Cyber) Resilience in Kyiv


It`s a fragment of the Kyiv Glass Bridge hit by russian missile on October 10
The Bridge has endured, Kyiv has endured, and Ukraine will endure!
KYIV DIGITAL
Kyiv `24
Resilience

Look at the bigger picture !

CISCO
It`s a fragment of the Kyiv Glass Bridge hit by russian missile on October 10
The Bridge has endured, Kyiv has endured, and Ukraine will endure!
Kyiv '24
Resilience

Låt ljusen lysa !

Thank you and be Safe and Secure !