



Cyber Security for SDN

Moshe Markovitz Gen. Res.
C.E.O Celare

Agenda



- **Introduction of BATM – CELARE**
- **SDN – How to attack ? What can we do to defend?**
- **Celare solutions**
- **Summery**



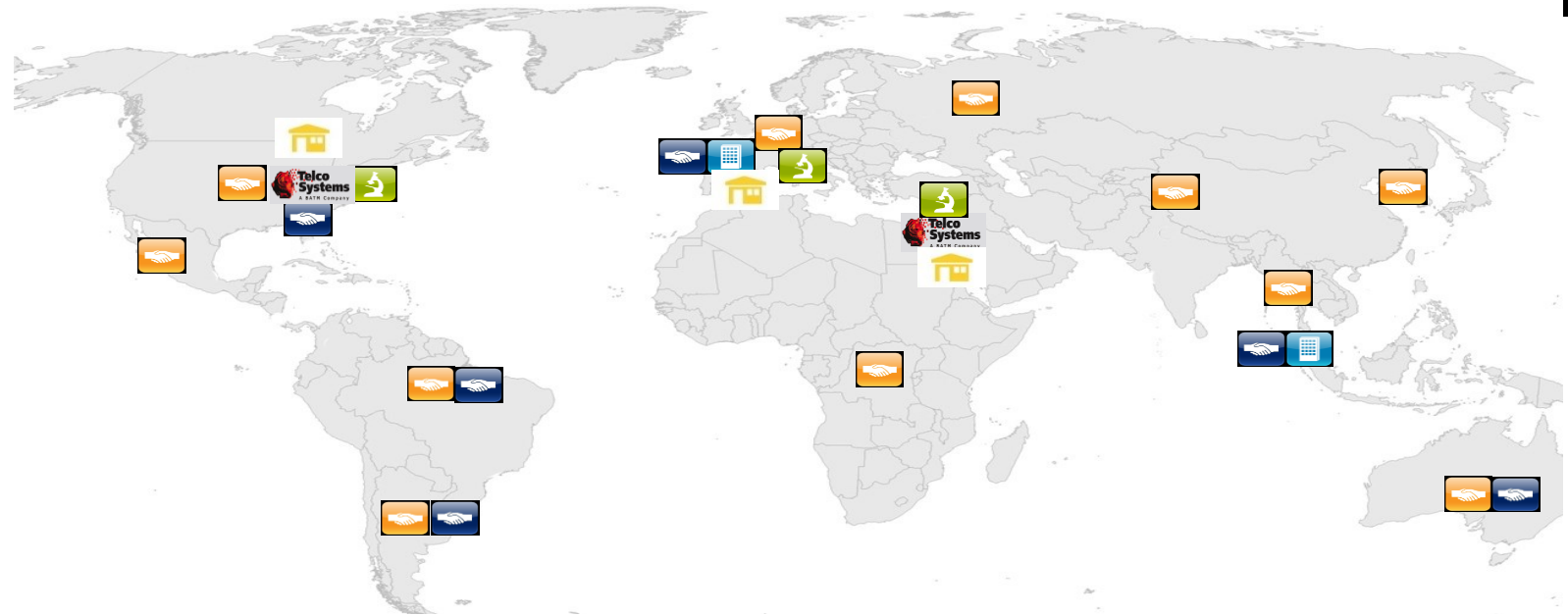
BATM – Celare introduction of BATM – Celare

About CELARE



- ***CELARE Cyber Systems*** is subsidiary of the ***BATM Advanced Communications group*** - London Stock Exchange (LSE:BVC)
- ***Market focus*** - provides comprehensive Cyber Security solutions for Utilities, Defense, Governments, Homeland security and critical infrastructures organizations.
- ***Cyber security solutions:***
 - ***T-Metro-XG*** - Network security platform for Encryption and Cyber defense.
 - ***NETWIZ*** - Network visibility solution that provides organizations an overall understanding what is happening on the network enabling most effective management of even the most hidden network threats.

CELARE Cyber Systems is the Cyber Arm of BATM Advanced Communications group



- Leading provider of real-time technologies for:
 - Networking & Cyber market
 - Diagnostics and ECO market
- Established in 1992
- 700 engineers and scientists
- +300,000 systems deployed
- Headquarters: Israel
- International offices:
 - North America: Boston, US
 - Europe: Bulgaria; France; Germany; Hungary; Italy; Moldova; Romania; UK
 - RoW: Argentina; Australia; Russia; Singapore
- Listed on London Stock Exchange (LSE: BVC)

- BATM Established 1992
- CELARE Cyber Systems Established at 2012
- BATM www.batm.com Advanced Communications group - London Stock Exchange (LSE:BVC)
- CELARE is subsidiary of the BATM

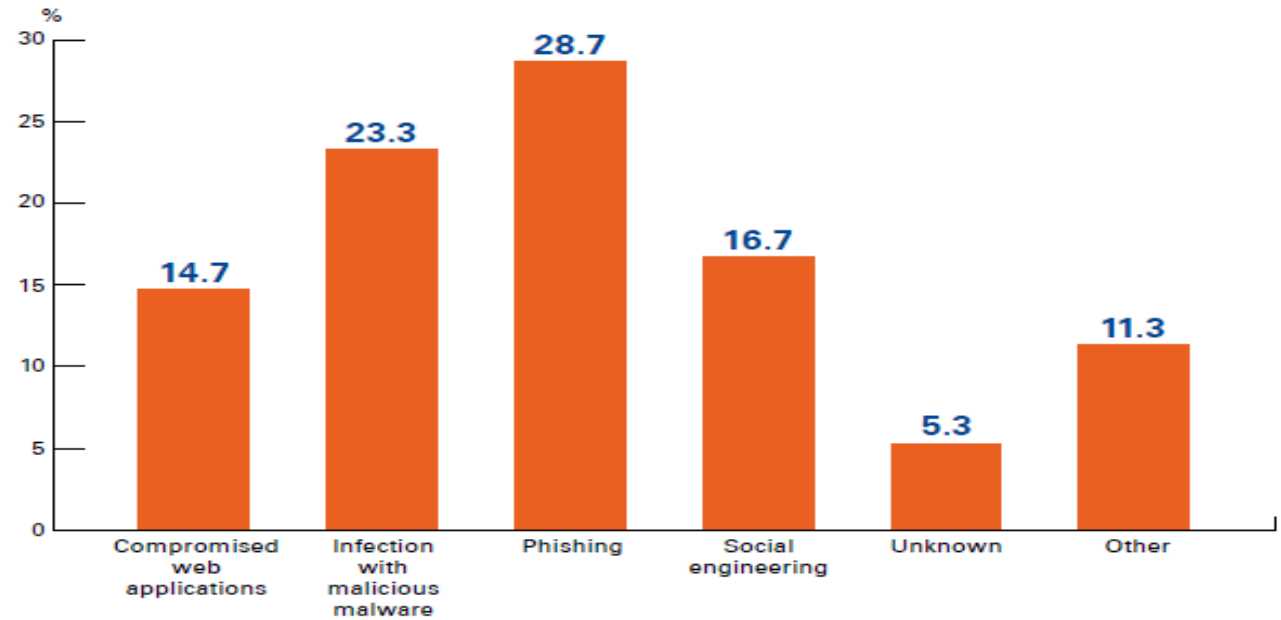
BATM Global Coverage



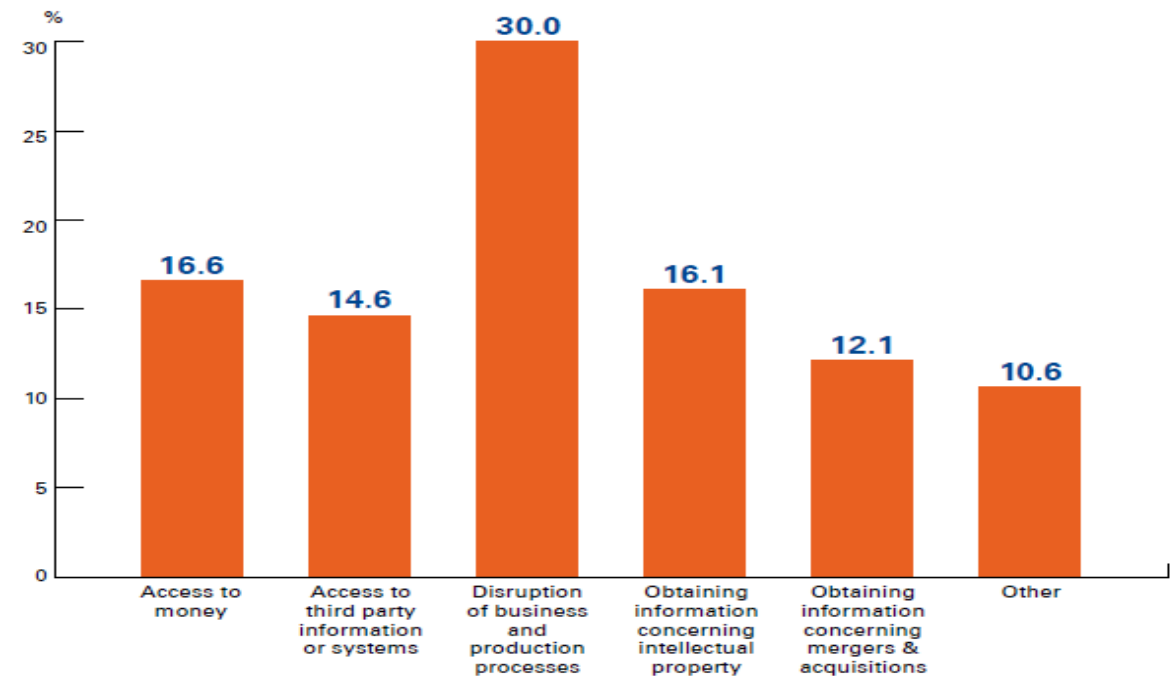


SDN – How to attack ? What can we do to defend?

Methods of Attack

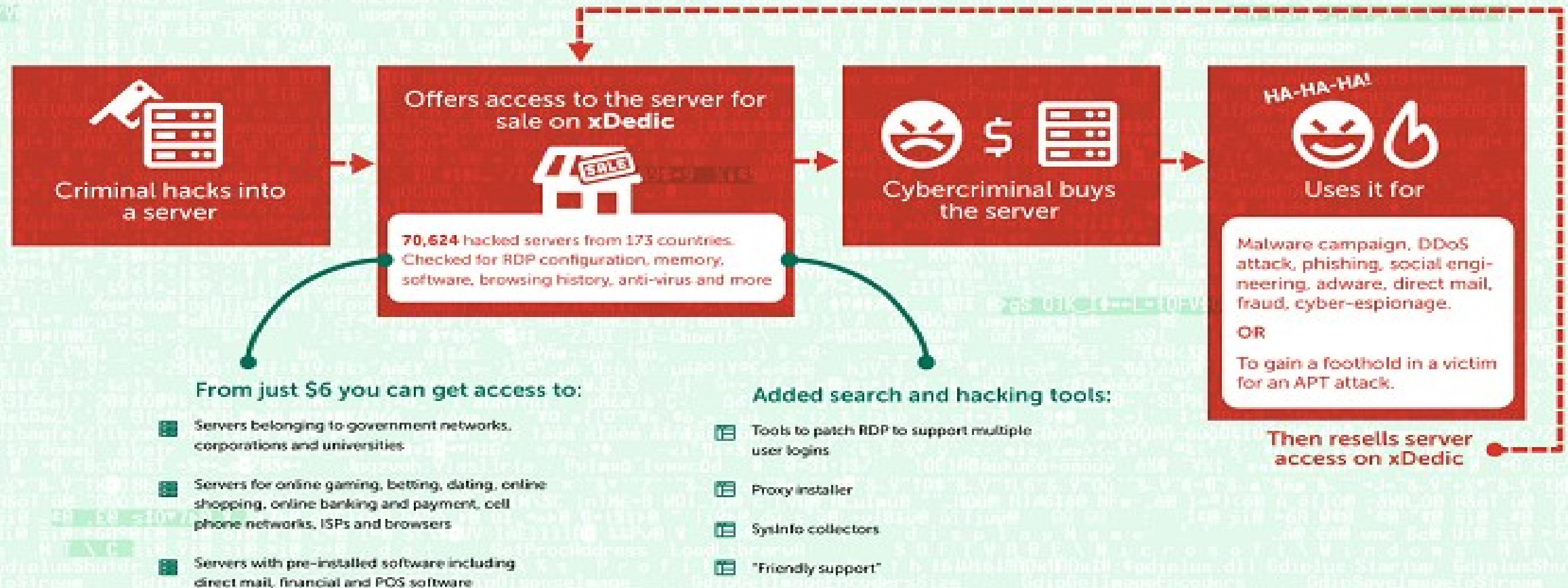


Purpose of Attack



How to buy and sell hacked servers all over the world

Kaspersky Lab has uncovered xDedic, a global marketplace for compromised Remote Desktop Protocol (RDP) servers, run by Russian-speakers.

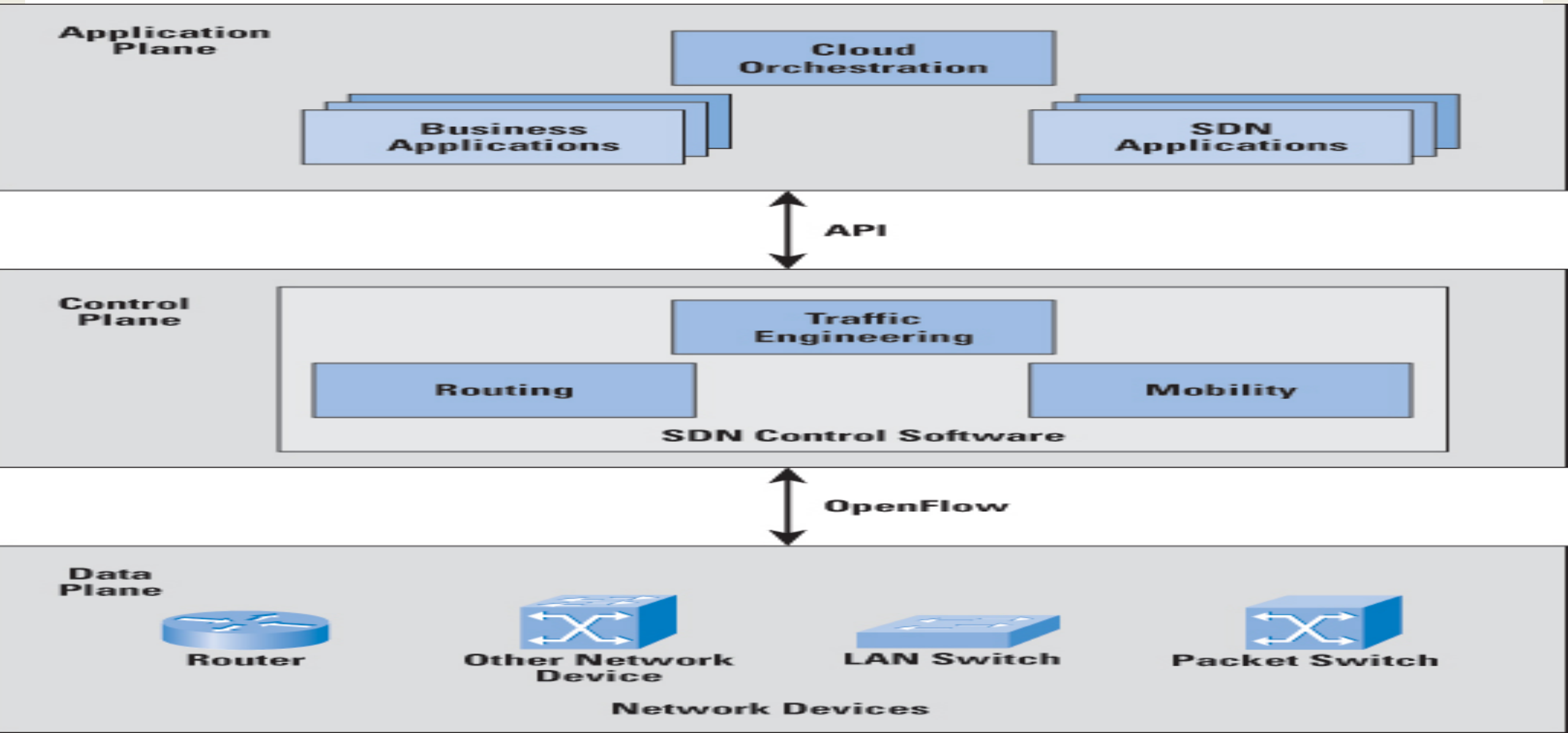


© 2016 AO Kaspersky Lab. All Rights Reserved.

GREAT

KASPERSKY

Software-Defined Networks structure



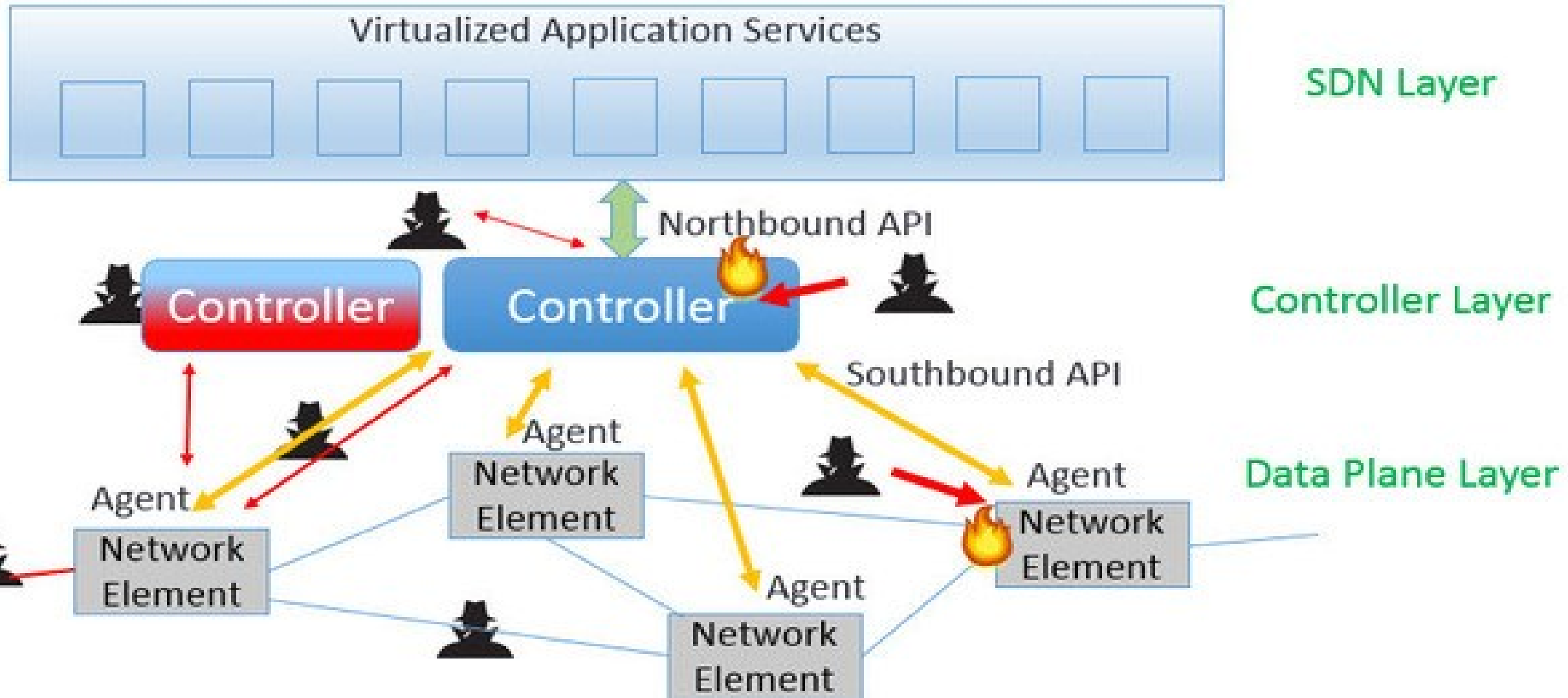
SDN ARCHITECTURE - ATTACK VECTORS



- ❑ **Most SDN architecture models have three layers:**
 - lower layer of SDN-capable network devices
 - middle layer of SDN controller(s),
 - higher layer that includes the applications and services that request or configure.
- ❑ **We can anticipate several attack vectors on SDN systems. The more common SDN security concerns include attacks at the various SDN architecture layers.**

Customer requirements – To protect all SDN Layers from Cyber attacks

SDN Security Attack Vectors





Operationalizing the Network with SDN



- ❑ An attacker would like :
 - ❑ **see what flows are in use and what traffic is being permitted across the network.**
 - ❑ eavesdrop on **southbound communication** between the network element and the controller.
 - ❑ This information could be useful for a replay attack or simply for reconnaissance purposes.
- ❑ SDN systems are deployed within data:
 - ❑ **Data Center Interconnect (DCI)** protocols such as Network Virtualization using Generic Routing Encapsulation (NVGRE), Stateless Transport Tunneling (STT), Virtual Extensible **LAN (VXLAN)**, Cisco Overlay Transport Virtualization (OTV), **Layer 2 Multi-Path (L2MP)**, TRILL-based protocols (Cisco FabricPath, Juniper QFabric, **Brocade VCS Fabric**), **Shortest Path Bridging (SPB)**, among others.
- ❑ **These protocols may lack authentication and any form of encryption to secure the packet contents. These new protocols could possess**
- ❑ **Standardization are the best news for Hackers**

Attacks at Controller Layer con.



- ❑ SDN controller runs on a general purpose operating system(Linux operating system) then the vulnerabilities of that OS become vulnerabilities for the controller.
- ❑ Often times the controllers are deployed into production using the default passwords and no security settings configured. .
- ❑ Attacker can created his own controller and got network elements to believe flows from the “rogue” controller.
- ❑ to those flows from the perspective of the production controller. In this case, the attacker would have complete control of the network

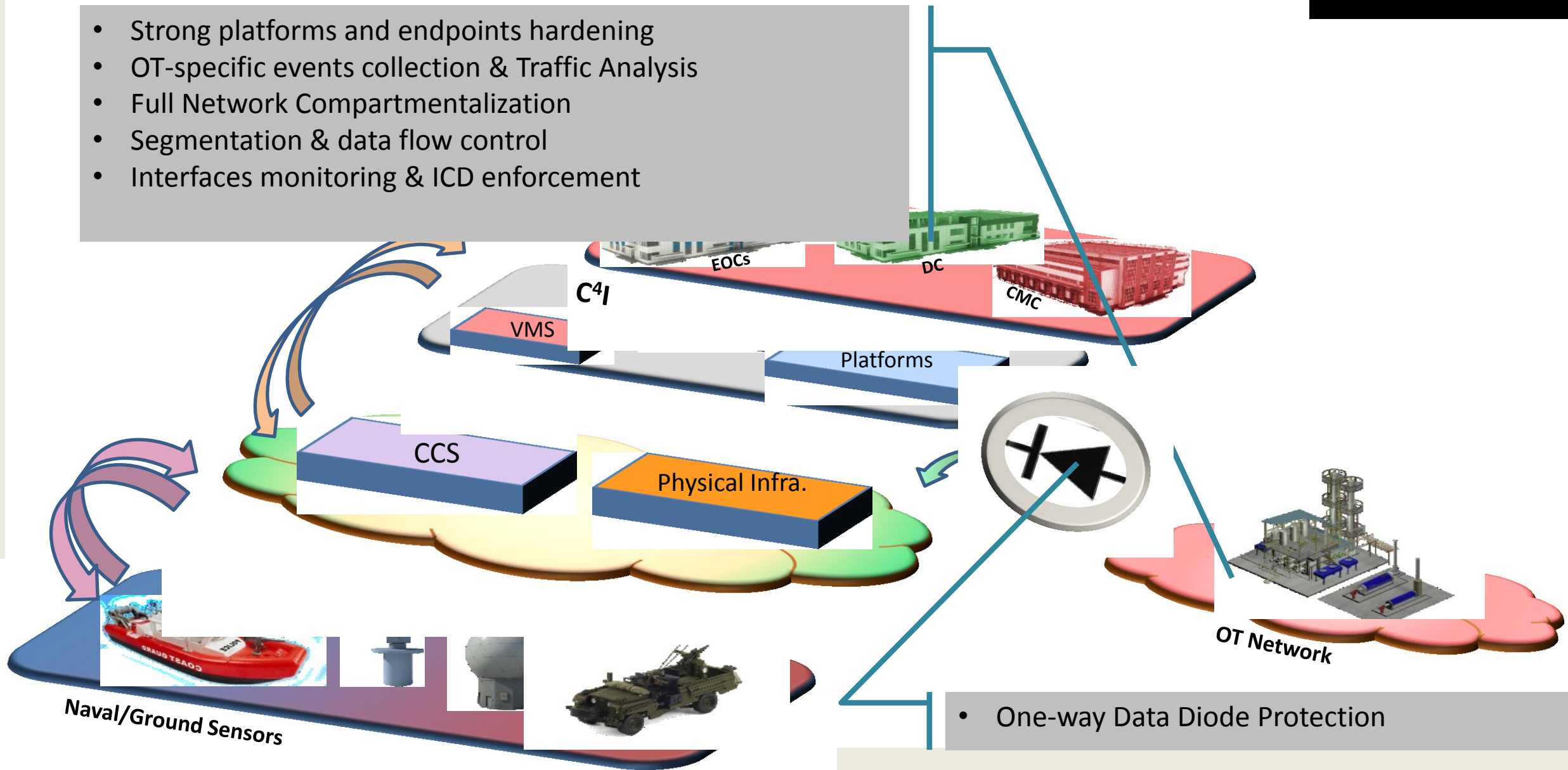


Actions for Governments

- Cyber protection is a National effort :
 - What to protect from ?
 - Risk assessment survey – analysis of the situation
 - What are the Gaps ? Critical security gaps in current situation
 - What are the external internal threats
 - Critical asset over view situation
 - Creating a master plan for 5 years
 - Developing an operational concept for Cyber protection
 - Technical design systems solution
 - Forming special units educating and training
 - Allocating resources

Cyber Security Implementation

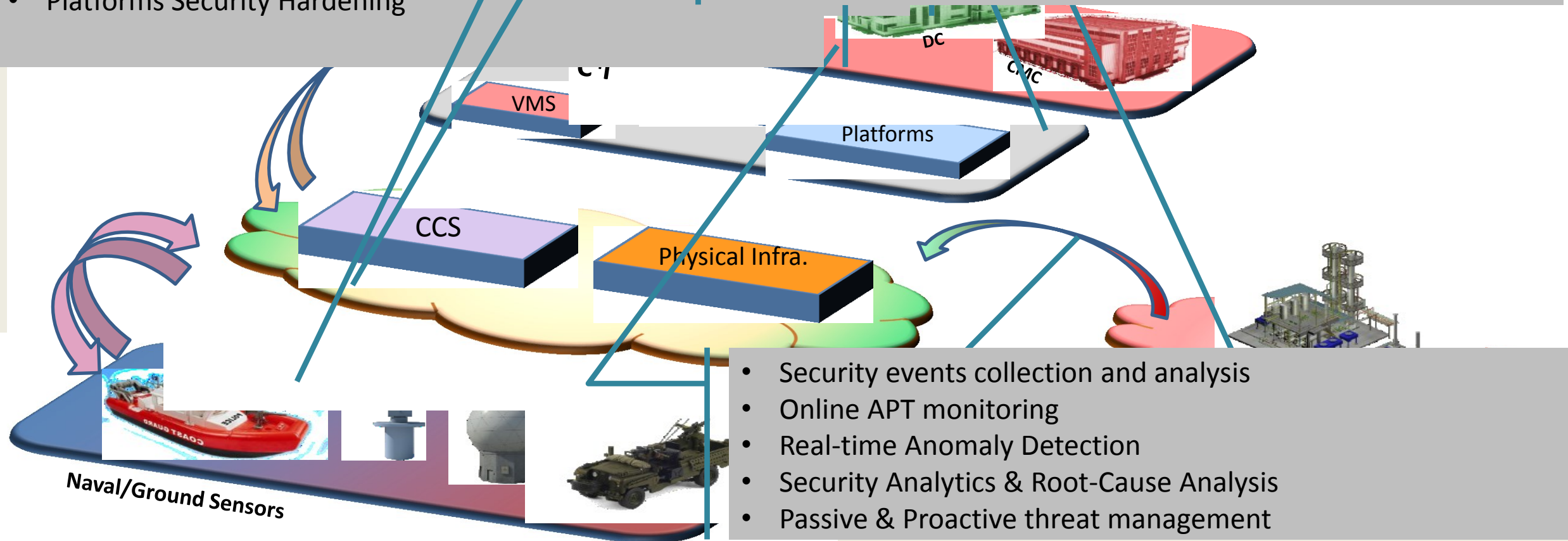
- Strong platforms and endpoints hardening
- OT-specific events collection & Traffic Analysis
- Full Network Compartmentalization
- Segmentation & data flow control
- Interfaces monitoring & ICD enforcement



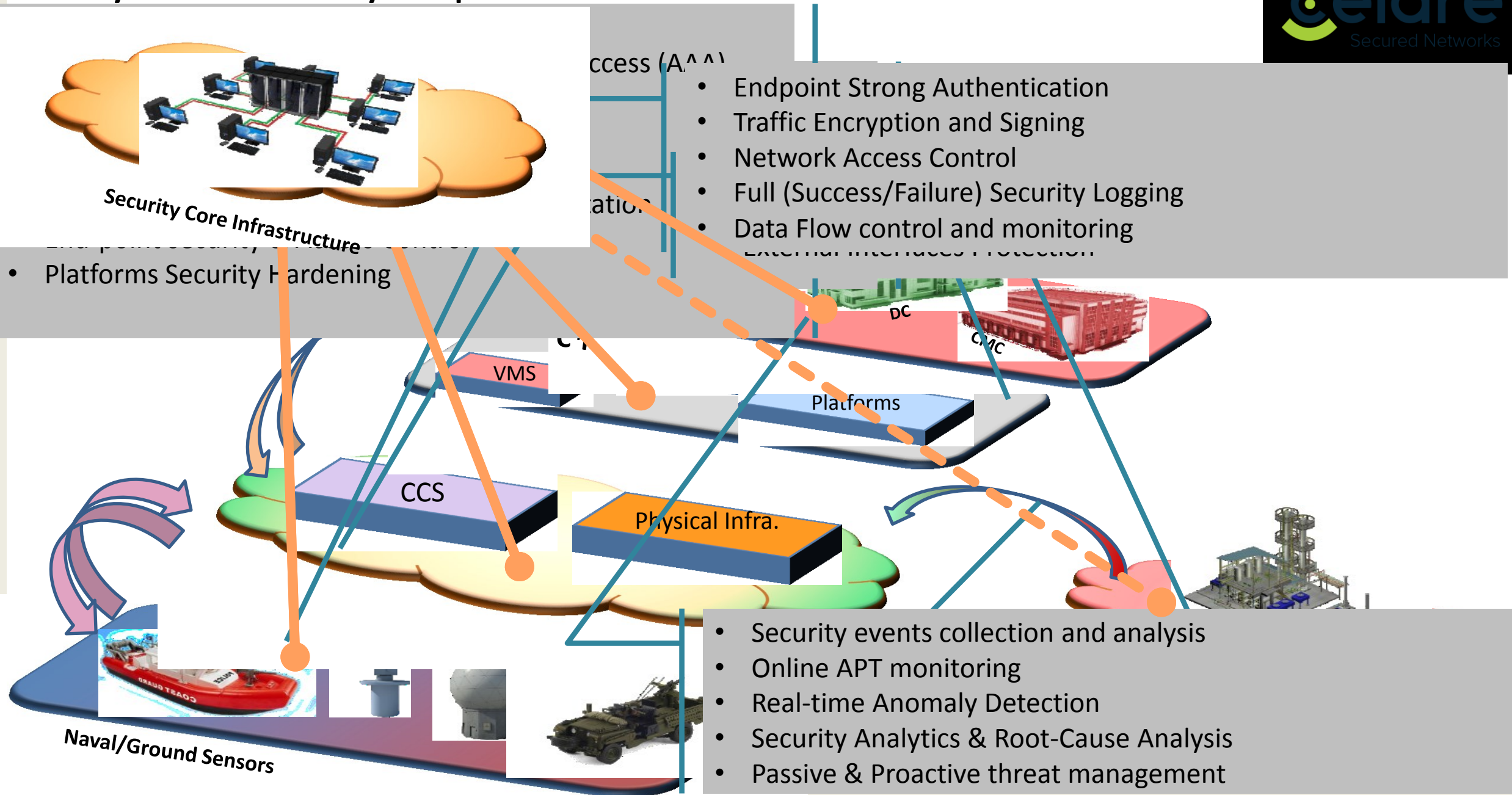
Cyber Security Implementation

- Network Segmentation
- Centralized Authentication, Authorization & Access (AAA) Management
- Centralized Security Policy Management
- Distributed, redundant Security Repository
- Virtualization and Storage Security Implementation
- Endpoint security & Access Control
- Platforms Security Hardening

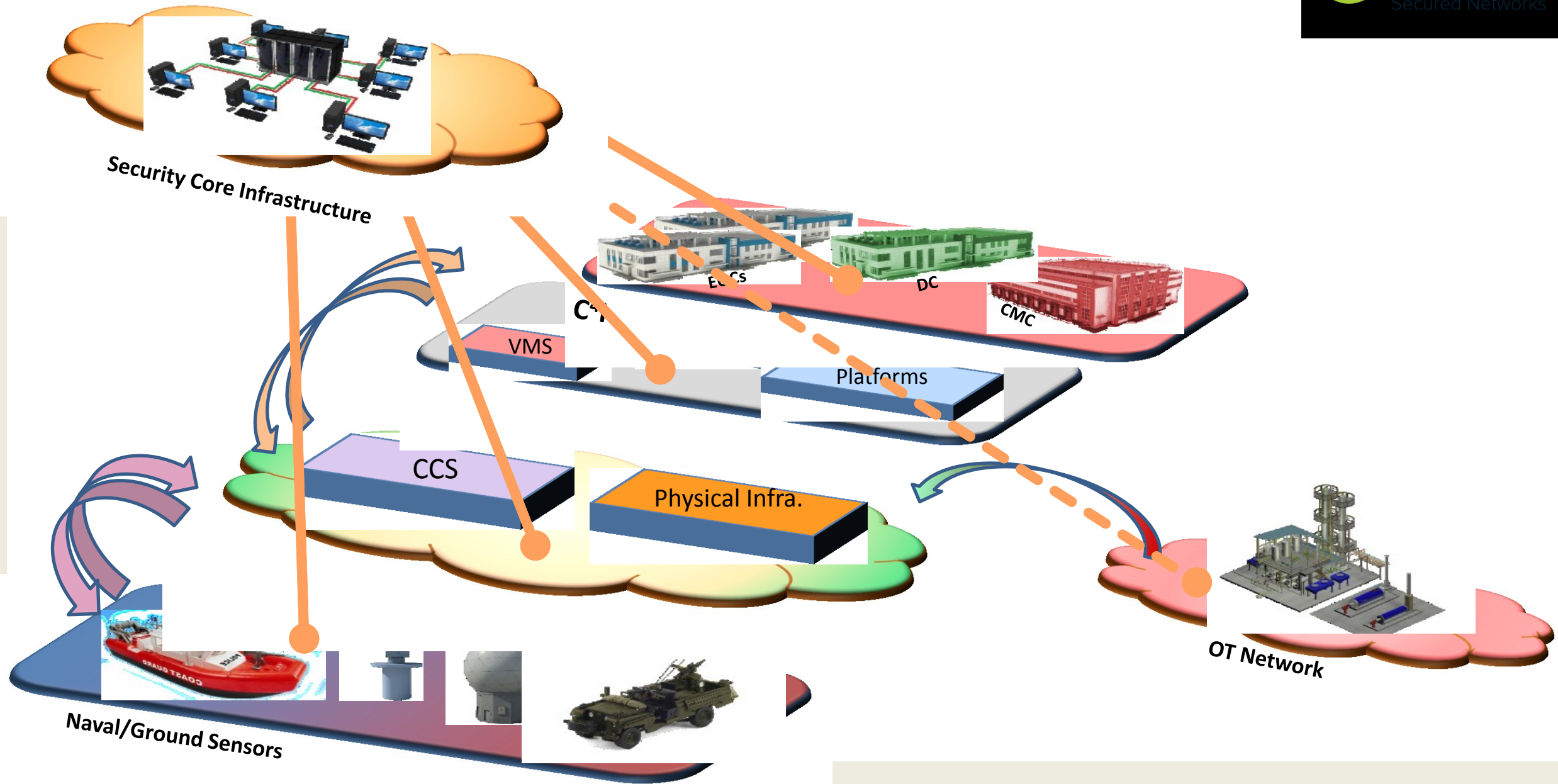
- Endpoint Strong Authentication
- Traffic Encryption and Signing
- Network Access Control
- Full (Success/Failure) Security Logging
- Data Flow control and monitoring



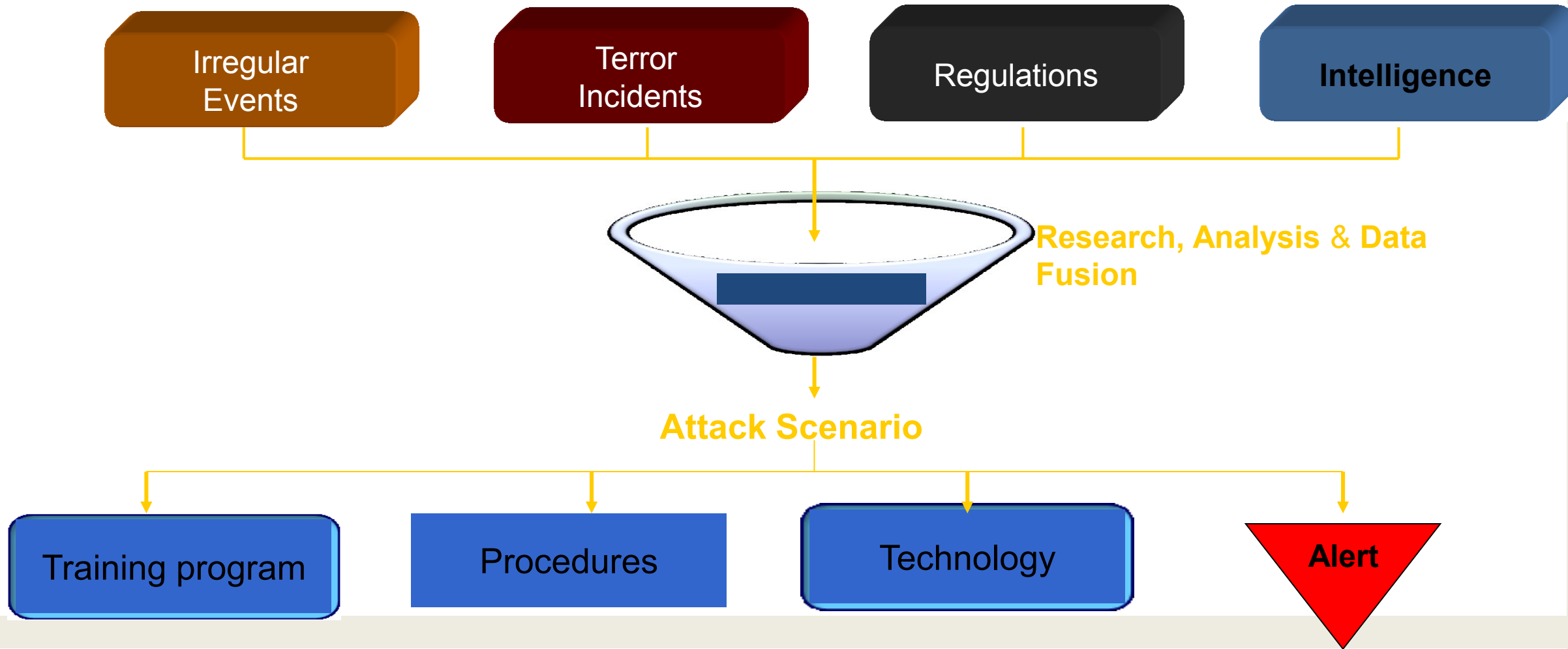
Cyber Security Implementation



Cyber Security Implementation



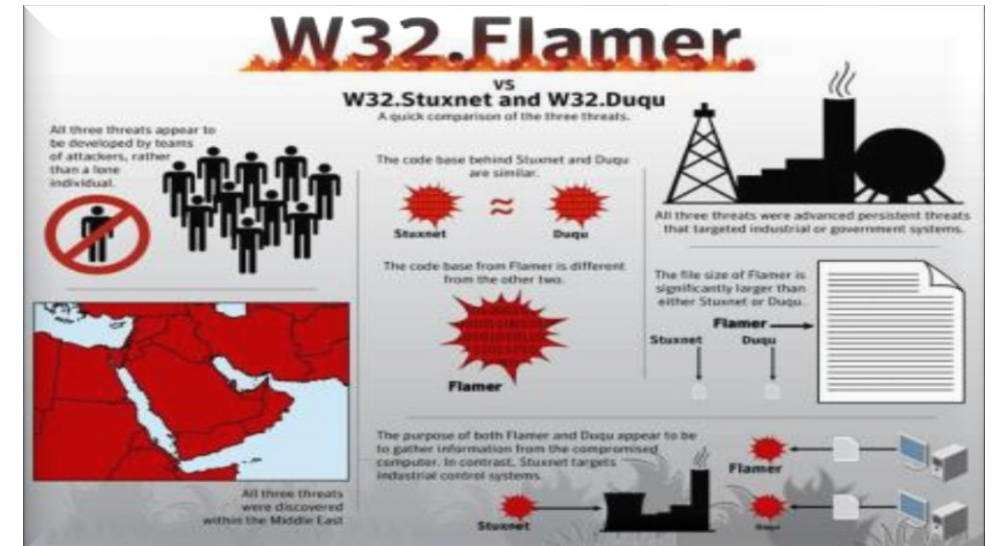
The OLS Model (Operational Learning System)



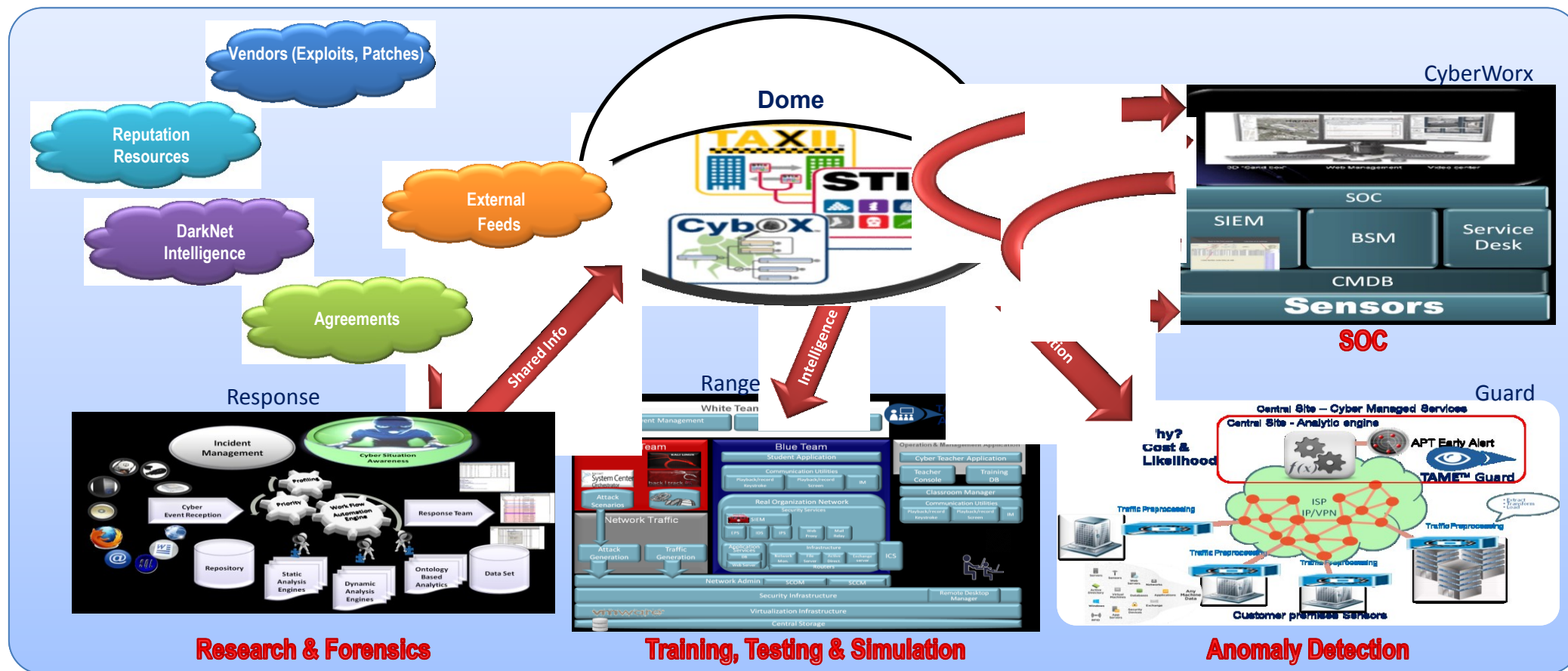
ADVANCED CYBER SECURITY

GROWING CYBER-ATTACK THREATS ON OIL & GAS INFRASTRUCTURE

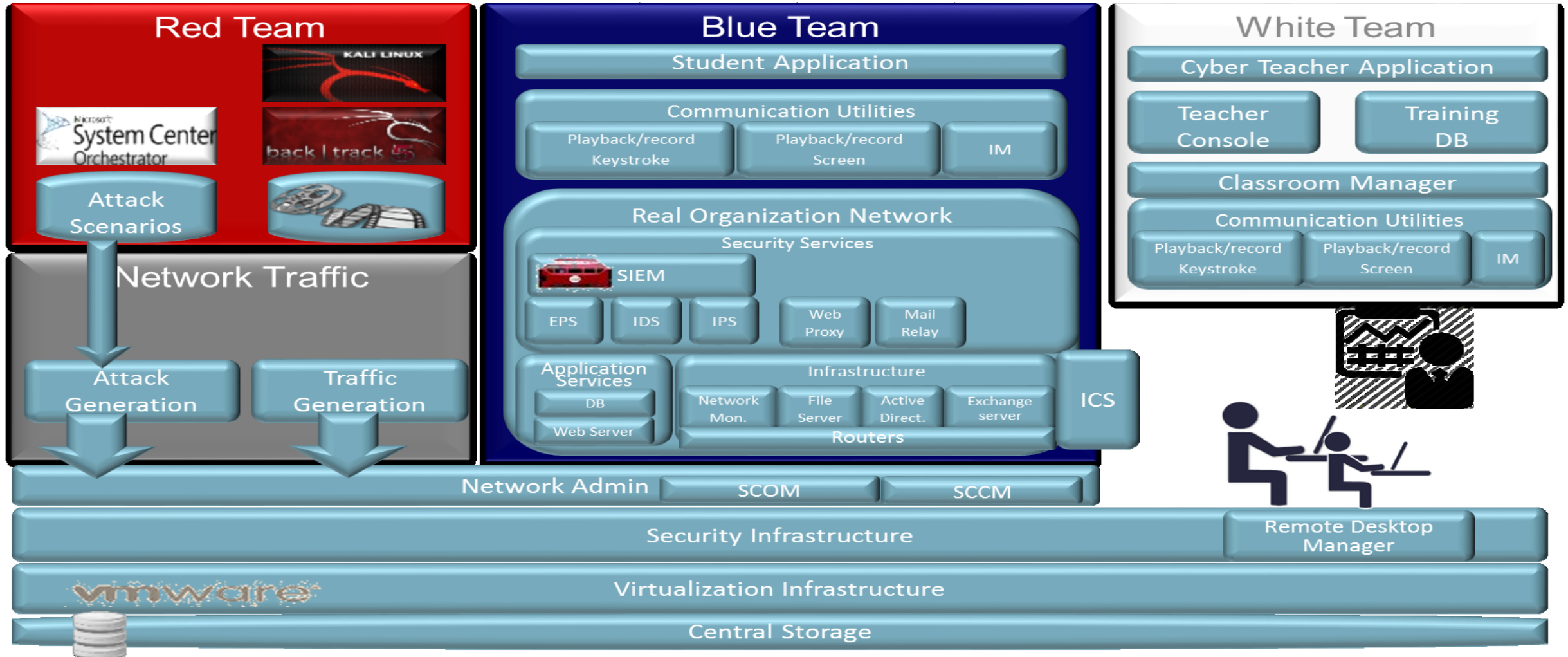
- Comprehensive cyber security suite for NRP
- Full OT/SCADA cyber protection
- External/internal interface protection
- Integrated cyber-security and C&C
- Cyber-security training facility



COMPREHENSIVE CYBER SECURITY SUITE

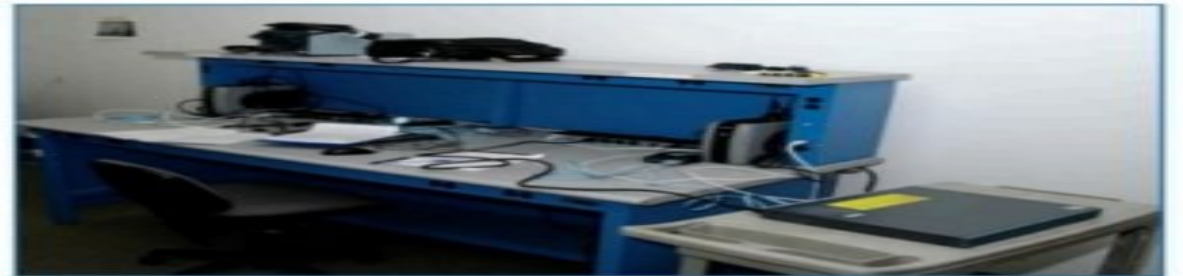


Comprehensive Cyber Training Facility



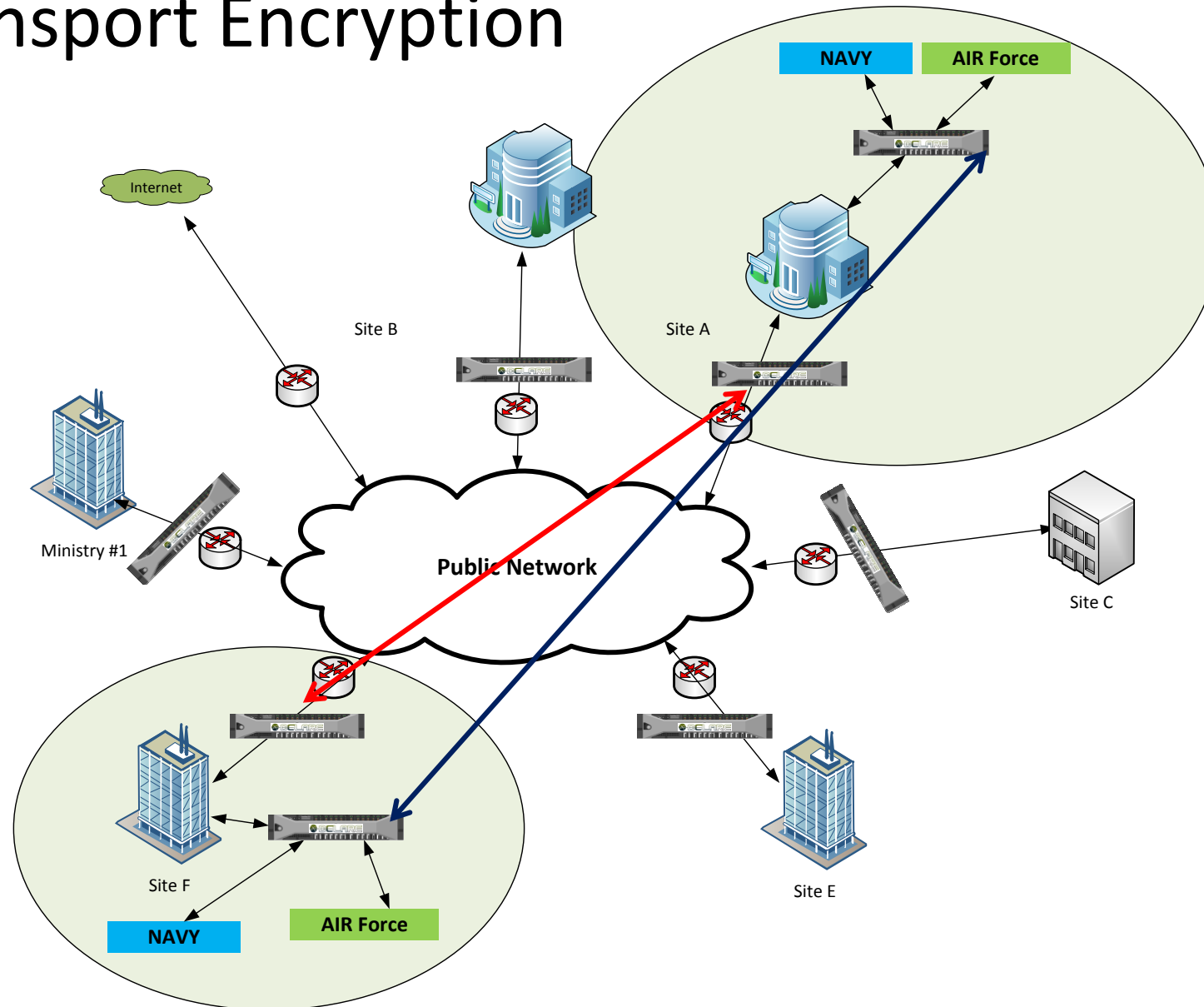
Intel Inside-Malware Inside

- **Cyber crime Photos of an NSA “upgrade” factory show Cisco router getting implant**
- Servers, routers get “beacons” implanted at secret locations by NSA’s TAO team
- by [Sean Gallagher](#) - May 14 2014, 10:30pm JDT

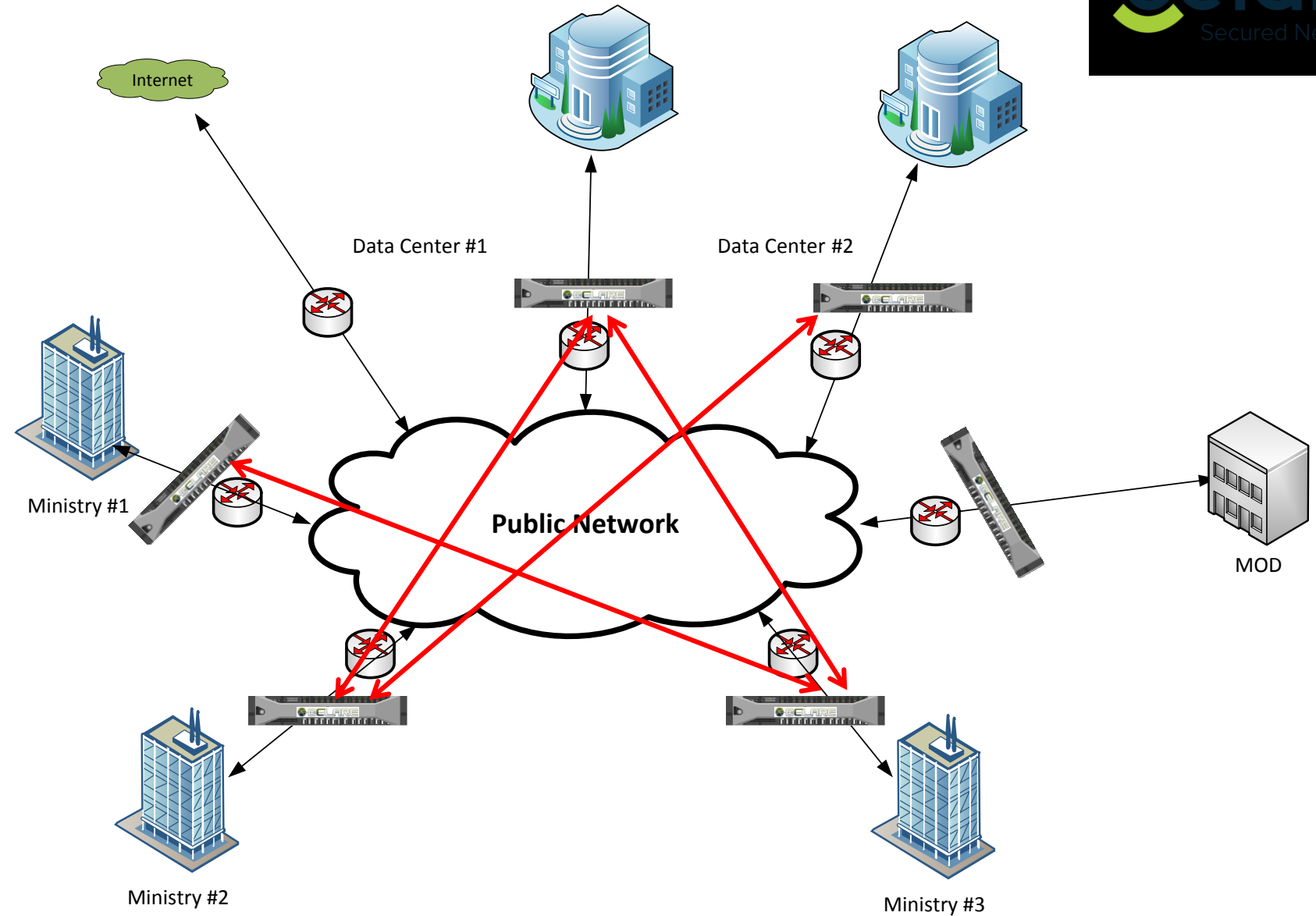


(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Access & Transport Encryption



Transport Encryption



Proposed Collaboration model



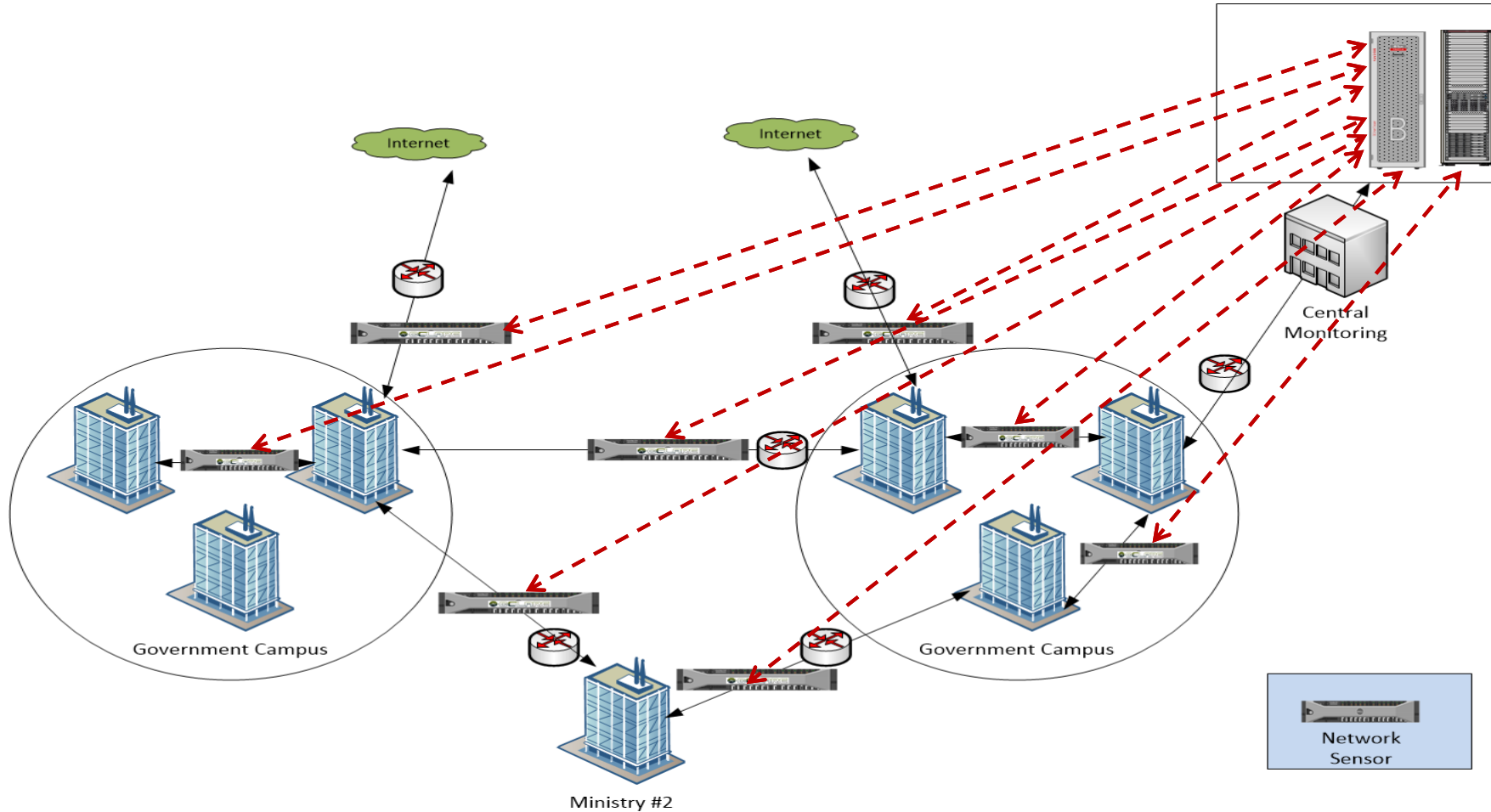
- CELARE will provide T-Metro-XG platform which was originally developed for the IMOD.
- The platform supports both Network Encryption in HW and Network visibility for Cyber defense.
- Celare will provide network SW infrastructure and all support for development.
- **Stage 1:** VTU will develop encryption capabilities (HW based) on the T-Metro-XG
- **Stage 2:** Adding network visibility capabilities
- Local production capability options

Proposed Collaboration model

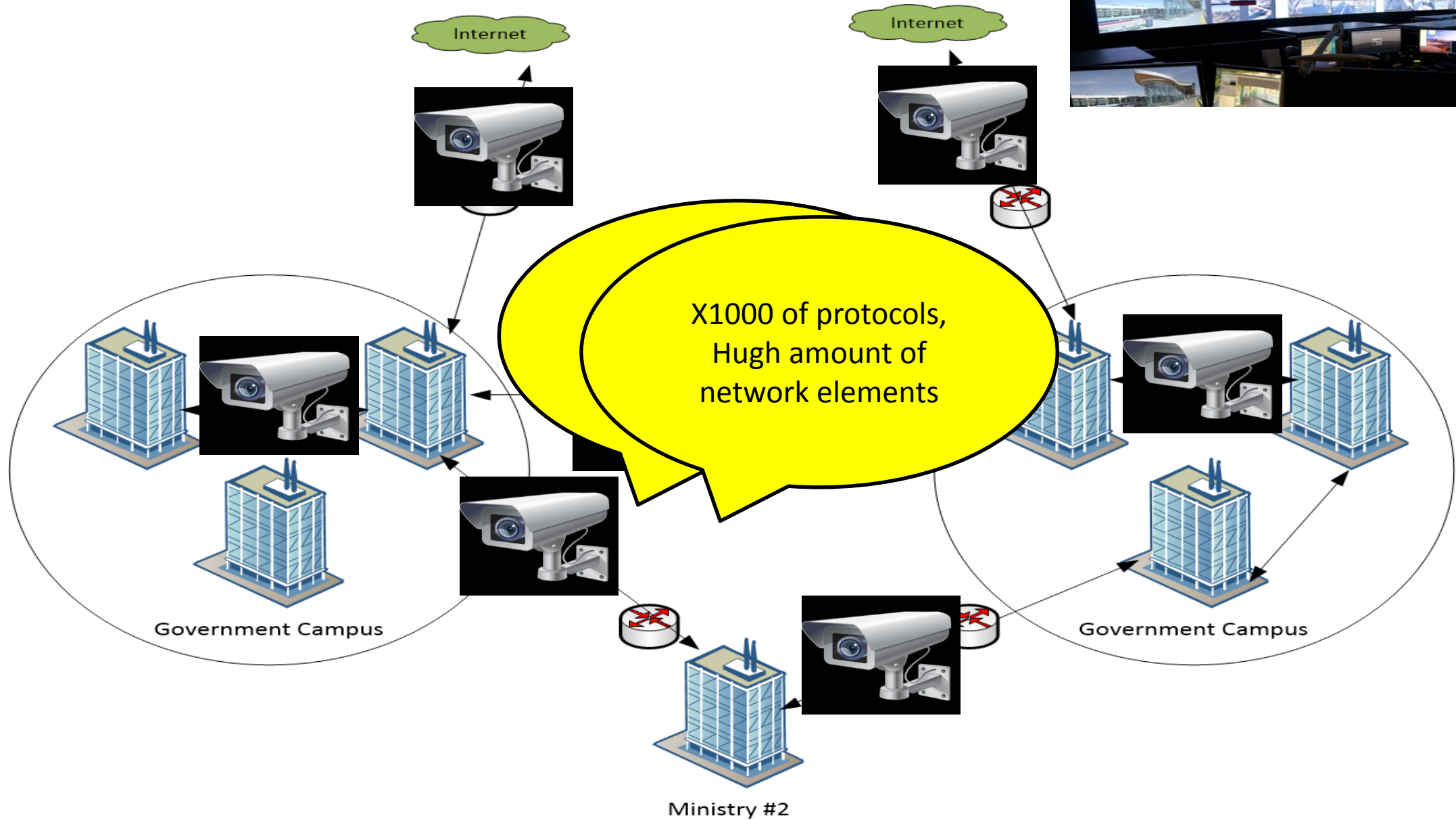


- Czech product with full control on:
 - Logistic chain
 - » Preventing logistic chain attacks
 - Production
 - » No HW threats
 - Proprietary and secure encryption.
 - » Secure transport for classified information
- Can work and interoperable with any commercial networks equipment
- Flexibility to use leased network infrastructure from local operators

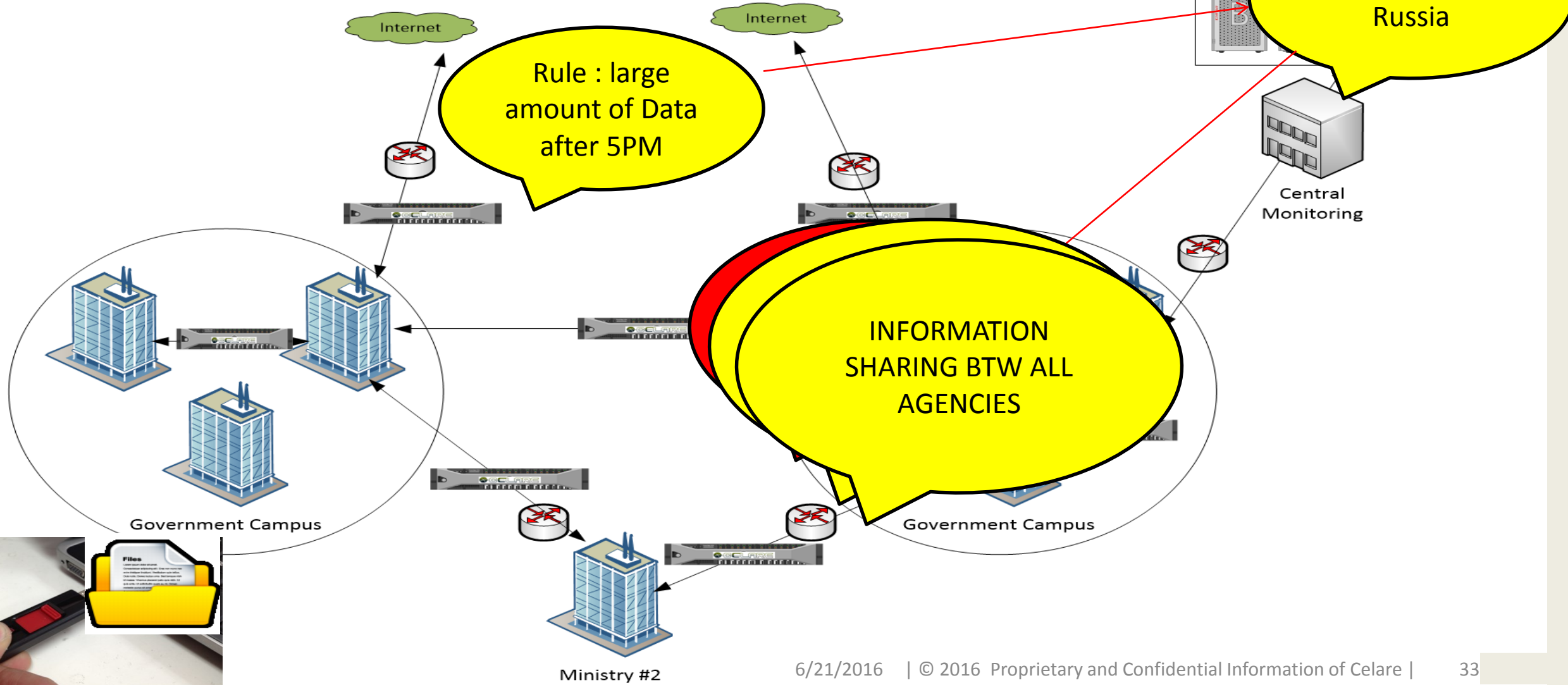
How to Monitor Multi Campus Segmented Network



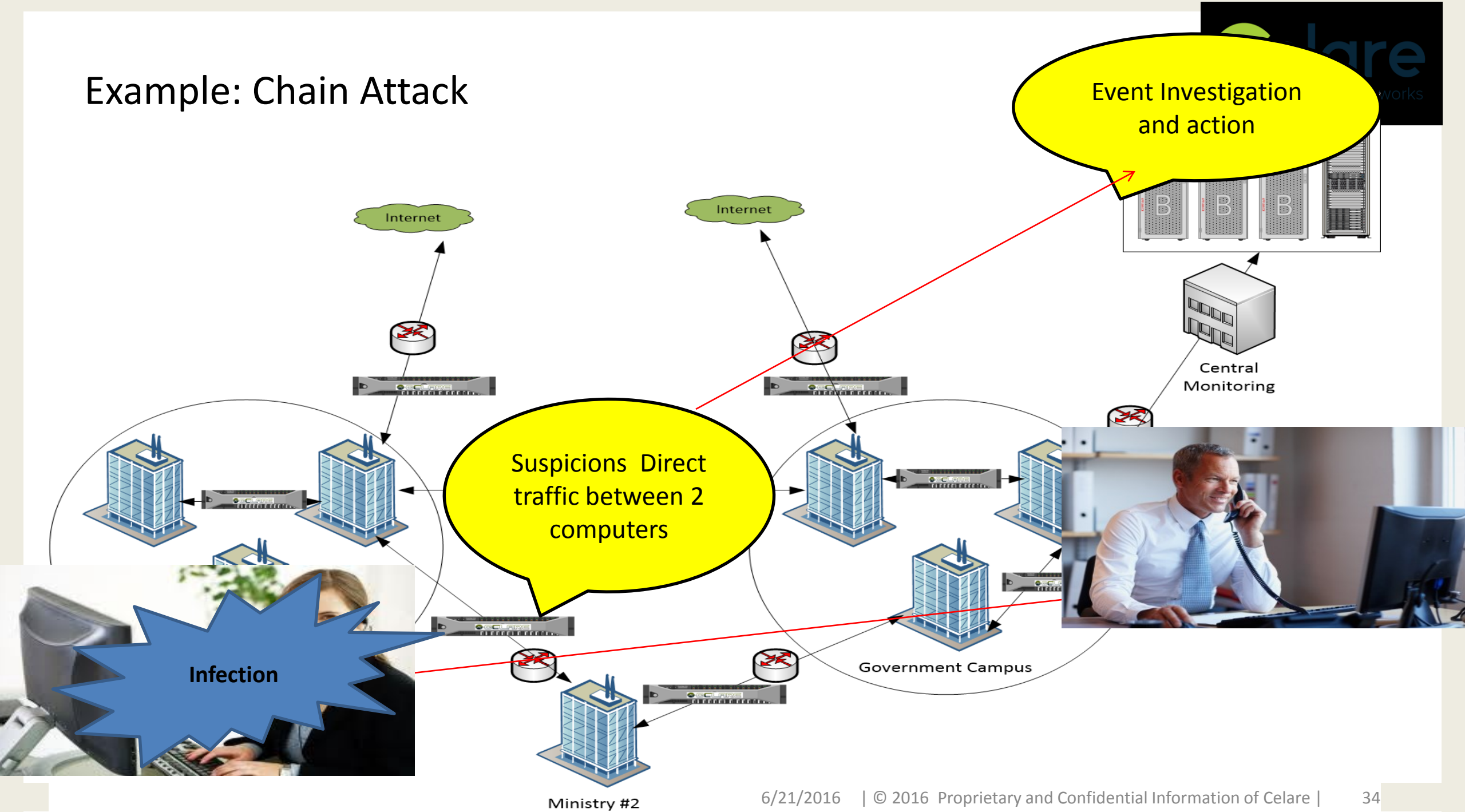
Network Visibility



Example: Incident Management



Example: Chain Attack





NetWiz Cyber defense Solution

The Challenges



- Insider threats !
- Attacks via Global International links
- Assumption: Even heavily secured networks have vulnerabilities and probably are already infected (HUMINT , lack of procedures, targeted attack).
- Networks become huge and complex
- New threats are not detected by conventional security technologies (FW, DLP...)
- How to identify new & unknown threats (APT's) ?

Solution Requirements

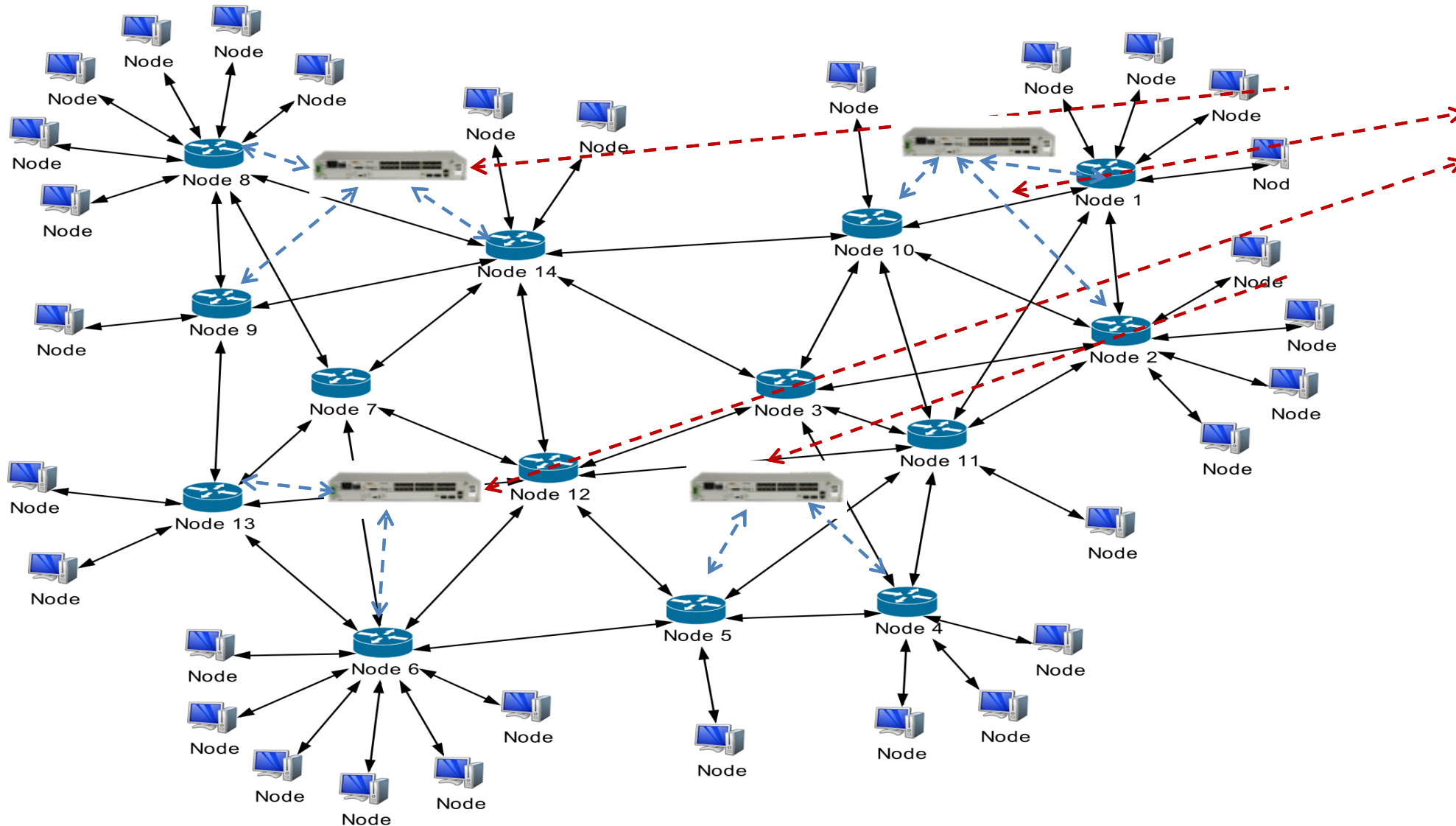


- Building the infrastructure for large scale network based cyber network system
- Big Data reservoir
- Full cycle threat Detection:
Collection, Recording, Analytics, Reporting, Detection
- Unknown Threats detection based on network anomalies algorithms
- Behavioral forensic tools to better understand happening in the network
- Tracking Suspicious user behavior and content

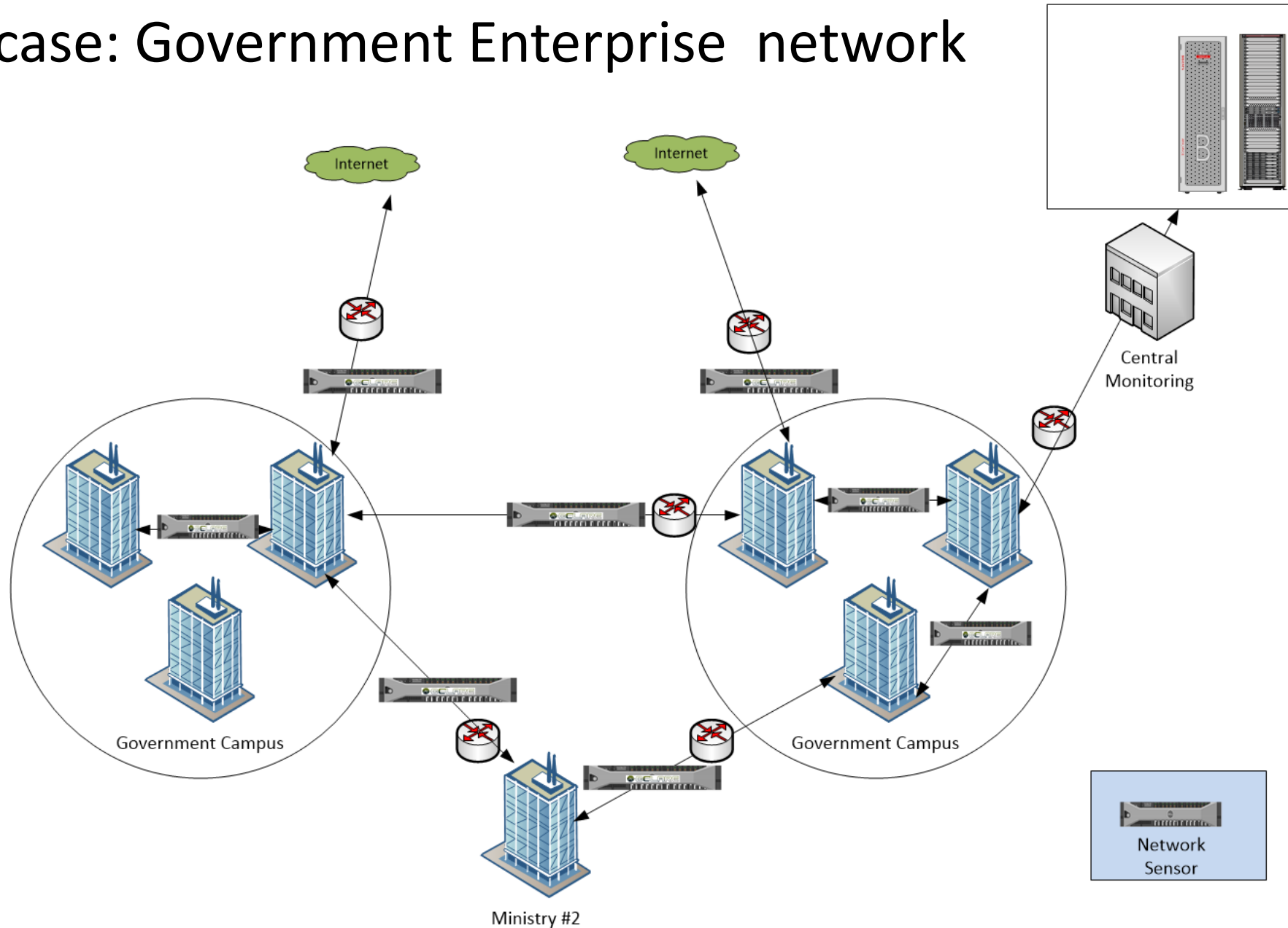
what is



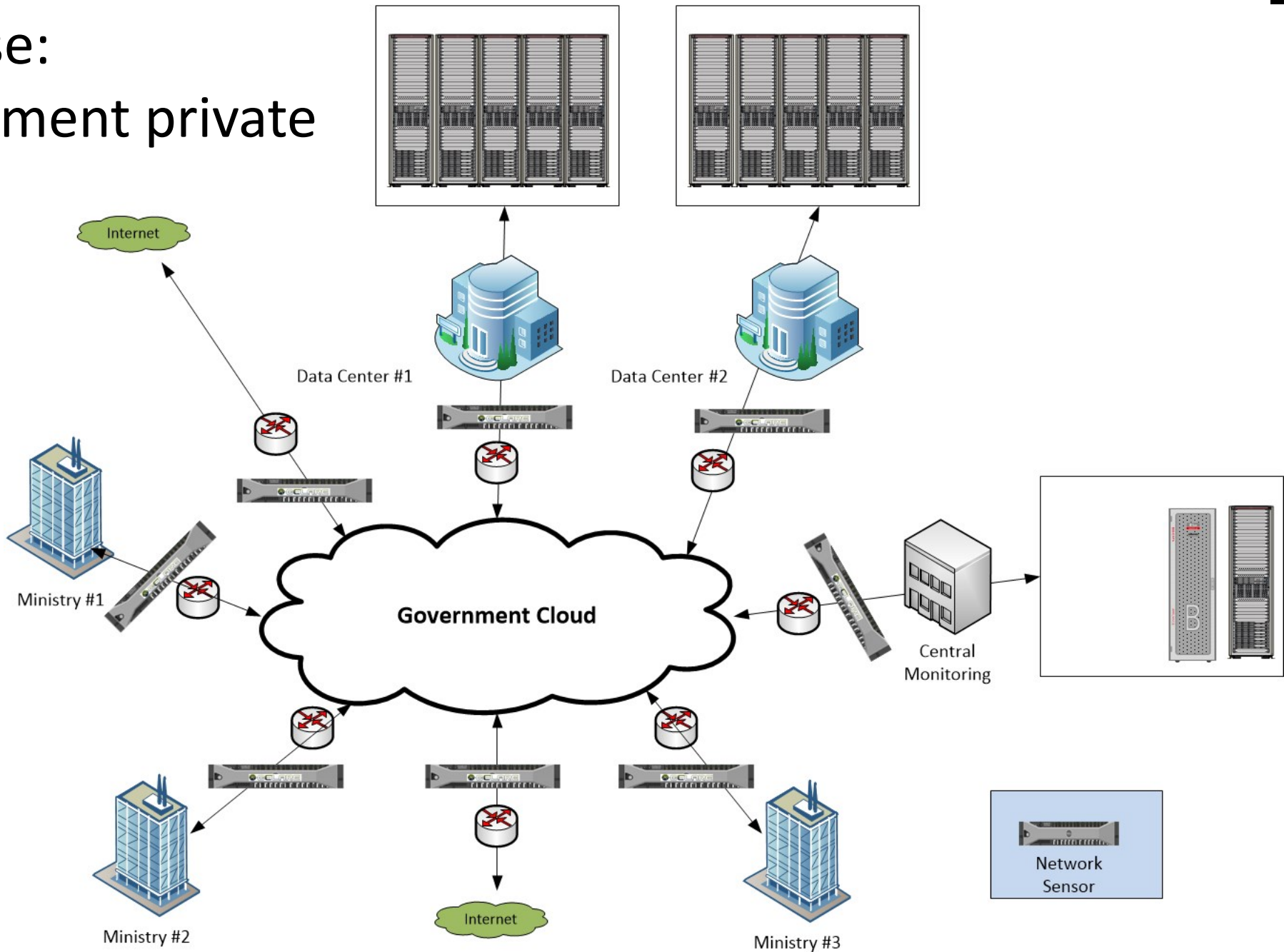
Use Case : Large Enterprise



Use case: Government Enterprise network



Use case:
Government private
cloud



NetWiz™ Performs Internal and External Monitoring and establish 24/7 incident monitoring



- Monitoring the Links within the Campuses and Internet Gateways.
 - Monitoring VPN connection between sites
 - **Non Intrusive** network connection using smart sensors
 - Creating **global view** of Network Traffic
 - Protocol classification
 - Metadata extraction
- Sending all relevant sessions information to central monitoring
 - Big Data Analysis indexing
 - **Rule based engine to detect**
 - ☐ Threats and malwares
 - ☐ Network anomalies
 - ☐ Network policy Abuse
 - ☐ Correlating suspicions events (One site, Several sites)
 - API to other detection systems
 - Reporting to central government **SIEM**

NetWiz™ Solution Overview



■ Collection:

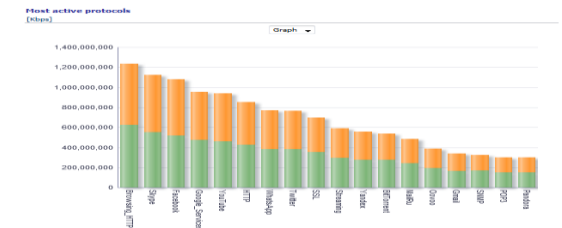
- Large deployment of Integrated Switch/Probes located at the network edge
- Full session reconstruction
- Metadata and content extraction

■ Aggregation:

- Oracle Big Data appliance – distributed file system
- Recording & indexing
- Real-time and batch analytics – filtering, aggregation & correlation
- Network Situational Awareness
- Investigation, Information discovery & analytics

■ Detection:

- User data reconstruction and analysis
- Network anomaly, Prediction
- Detectors searching threats on collected data



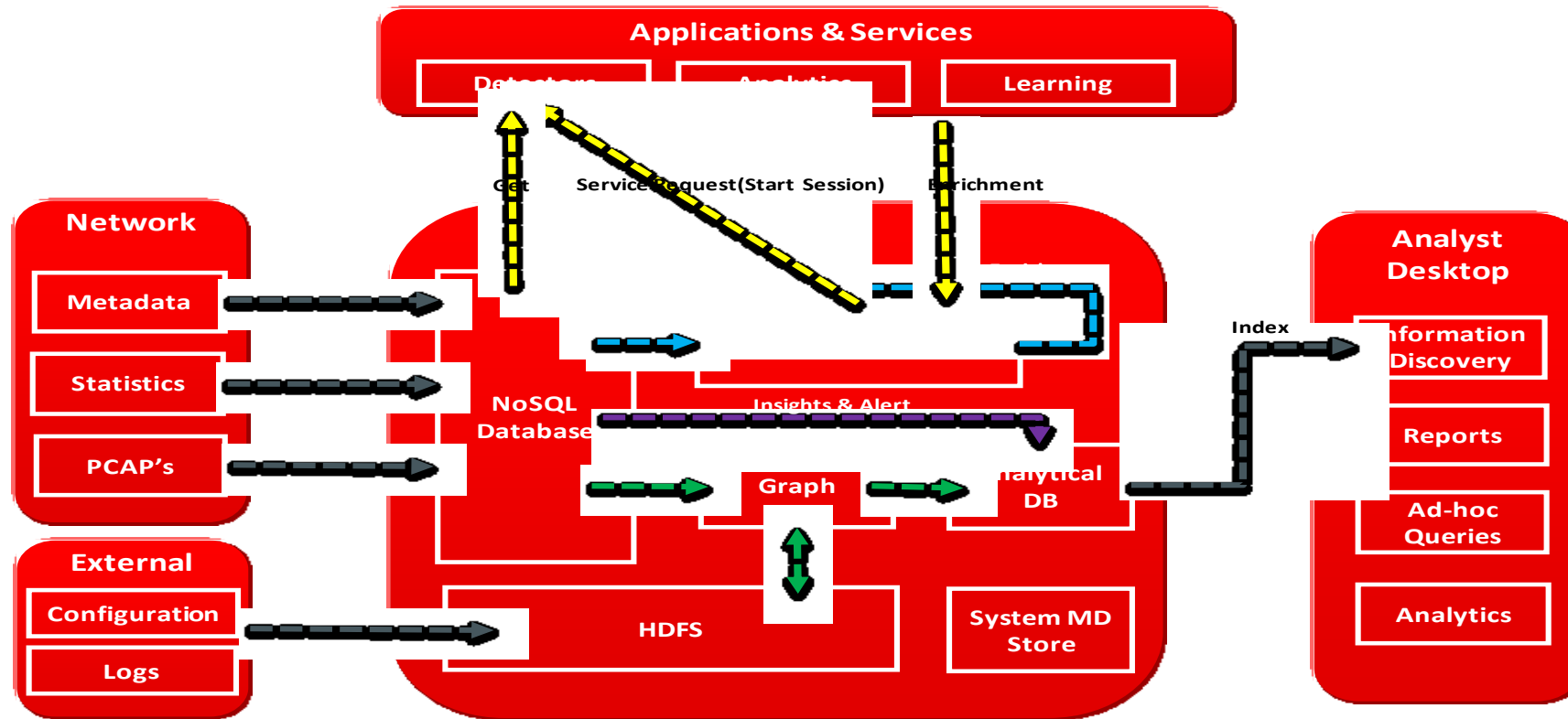
Over 2000 Recognized protocols and applications by signature/behavior



NETWIZ™ Cyber Solution Overview



Conceptual Architecture



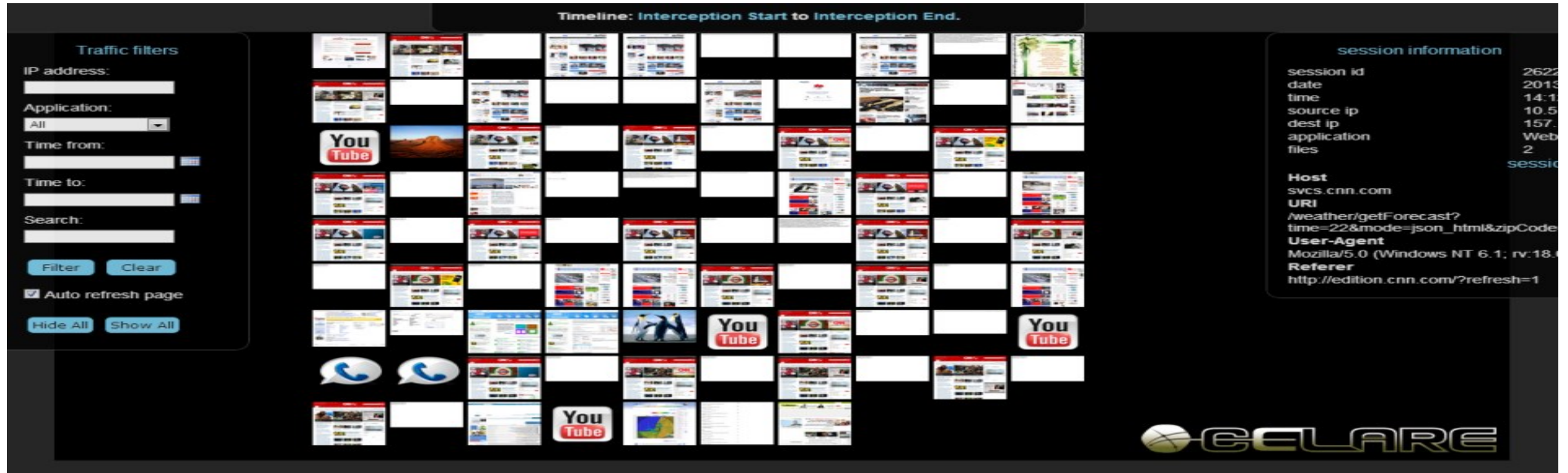
NetWiz™ Big Data Analytics - Enables effective investigation and forensic of network incidents



- **NoSQL Database:**
 - Central DB for all Data (Input\Output)
 - Scalable data capacity & throughput
- **OEP Stream processor:**
 - Enables easy definition of complex Network Rule set and can be activate immediately
 - Monitor streams in real-time
 - Filtering - New stream filtered for specific criteria
 - Pattern Matching - Notification of detected event patterns, e.g. events A, B and C occurred within 15 minute window
- **Graph DP & Visualization**
 - Advanced property graph stored on the DB
 - Building the actual network dynamically

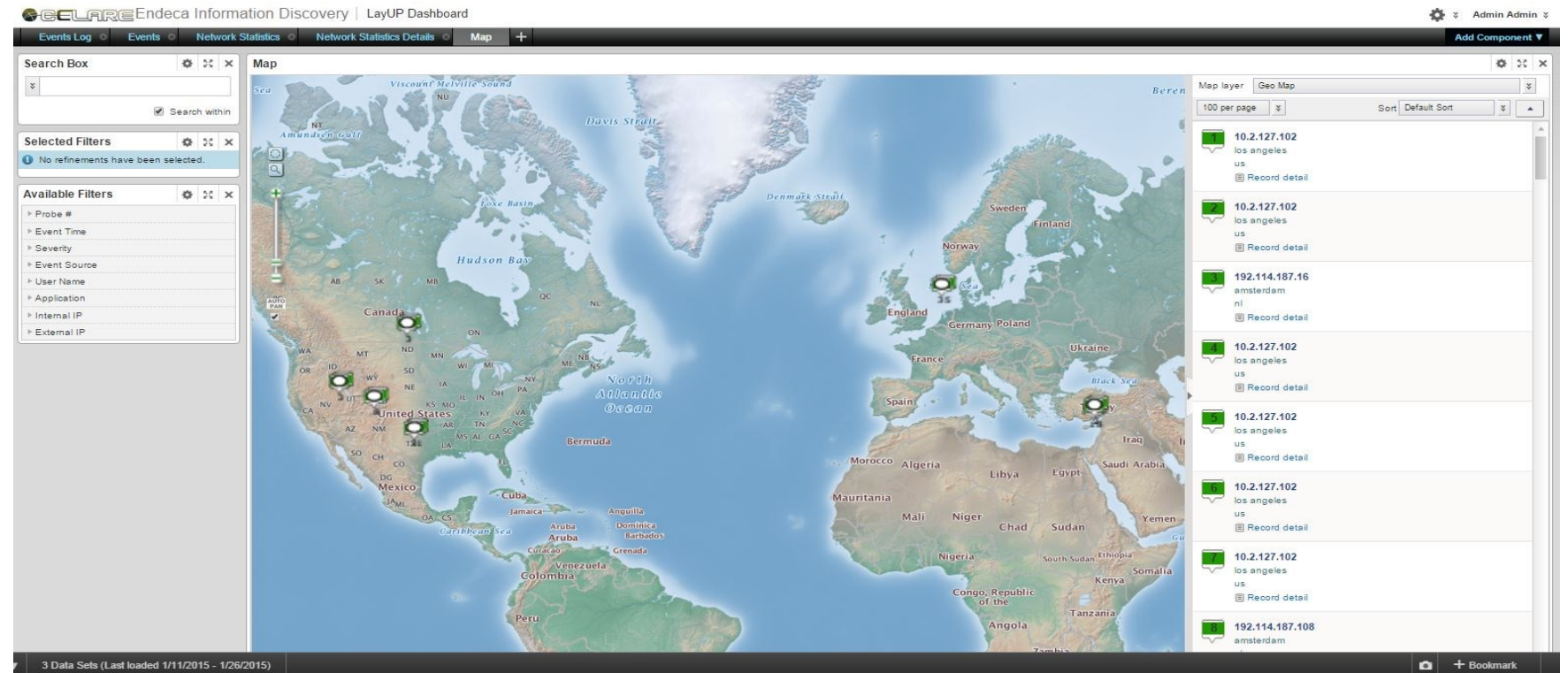


TLV Interception Visualization tool (User Behavior)



Visualization & Information Discovery

- Solution designed to be Event driven
- Supports GEO/Maps
- Advanced graphs and filters
- Network Situational Awareness
- Facet search



Information Discovery Event Dashboard



- Solution designed to be Event driven
- Supports GEO/Maps
- Advanced graphs and filters
- Network Situational Awareness

CELARE Endeca Information Discovery | LayUP Dashboard Cyber LayUP

Events Log Events Network Statistics Network Statistics Details Map

Search Box

☒ Search within

Selected Filters
No refinements have been selected.

Available Filters

- Probe #
- Event Time
- Severity
- Event Message
- Event Source
- Rule ID
- User Name
- Application
- MAC Address
- VLAN
- Internal IP
- External IP
- TCP/UDP
- Internal Port
- External Port

Summary
68 Total Events 52 Severity 1 0 Severity 2 16 Severity 3 1/6/15 Start Period 1/6/15 End Period

Events
0 records selected

		Seve...	Event ID	Event Time (Y...	Event Message	Internal IP	External IP	
☐	☐	3	358369467	1/6/15 5:10:50 PM	Alert: Communication with wrong or fake DC - 192.114.187.5	71.6.135.131	192.114.187.5	
☐	☐	1	1312019874	1/6/15 5:04:49 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.198	
☐	☐	1	420833934	1/6/15 5:04:49 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.198	
☐	☐	1	341233336	1/6/15 5:02:02 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.197	
☐	☐	1	1725211093	1/6/15 5:02:02 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.197	
☐	☐	1	1627922673	1/6/15 4:56:12 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.193	
☐	☐	1	438132589	1/6/15 4:56:12 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.193	
☐	☐	1	62310433	1/6/15 4:50:45 PM	DNS protocol exception: packet has extra payload (non dns)	192.114.187.32	80.179.52.100	
☐	☐	1	352773803	1/6/15 4:50:45 PM	DNS protocol exception: packet has extra payload (non dns)	192.114.187.32	80.179.52.100	
☐	☐	3	1985379601	1/6/15 4:29:33 PM	Alert: Communication with wrong or fake DC - 192.114.187.126	85.25.43.94	192.114.187.126	
☐	☐	1	1732291634	1/6/15 4:16:56 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.180	
☐	☐	1	280928892	1/6/15 4:16:56 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.180	
☐	☐	1	1999241527	1/6/15 4:13:33 PM	DNS protocol exception: a successful query response without answers/auth RRs	192.114.187.16	80.179.52.100	
☐	☐	1	769964678	1/6/15 4:13:33 PM	DNS protocol exception: a successful query response without answers/auth RRs	192.114.187.16	80.179.52.100	
☐	☐	1	1834496683	1/6/15 4:02:14 PM	DNS protocol exception: packet has extra payload (non dns)	192.114.187.32	80.179.52.100	
☐	☐	1	443909700	1/6/15 4:02:14 PM	DNS protocol exception: packet has extra payload (non dns)	10.5.1.246	80.179.52.100	
☐	☐	1	653104905	1/6/15 4:02:14 PM	DNS protocol exception: packet has extra payload (non dns)	192.114.187.32	80.179.52.100	
☐	☐	3	1956807491	1/6/15 3:55:47 PM	Alert: Communication with wrong or fake DC - 192.114.187.110	198.20.70.114	192.114.187.110	
☐	☐	1	1624474083	1/6/15 3:48:43 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.183	
☐	☐	1	2085667220	1/6/15 3:48:43 PM	DNS protocol exception: invalid question type:4096	58.97.74.88	192.116.252.183	

Page 1 of 4 1-20 of 68 | 20 per page

Sessions
0 records selected

	Pro...	Application	User Name	TCP/UDP	Rx Bv...	Tx Bytes	Internal ...	External ...	Rx Pa...	Tx Pa...	MAC Address	PCAP File	
☐							53	53					
☐							60609	53					
☐	2	HTTP	0	TCP	933	0	50737	2710	7	0	2C:6B:55:55:45:00	/S/383242650/44205508	

3 Data Sets (Last loaded 1/5/2015 - 1/6/2015) + Bookmark

Information Discovery Events Dashboard



CELARE Endeca Information Discovery | LayUP Dashboard Cyber LayUP

Events Log Events Network Statistics Network Statistics Details Map

Search Box

☒ Search within

Selected Filters

No refinements have been selected.

Available Filters

- Probe #
- Start Period
- End Period
- Application
- Internal IP
- External IP

Summary

26,344,521 Record Count 1/18/15 Start Period 2/1/15 End Period

Current Day

No data to display. Please broaden your selections.

Sort: Start Period Hour

Page 1 of 1 1-0 of 0 | 50 per pag

Value axis: TotalBytes (sum) Category axis: Start Period Hour

Application

923 Amazon_Cloud Browsing_HTTP Cloudfront DNS DoubleClick Dropbox ESP Facebook FTP_Data Github Gmail Google_Services GRE **HTTP** IMAP LDAP MailRu MS_Live OTHERS RDP SMB SMTP Soundcloud SSH **SSL** TeamViewer Waze YouTube Yting

Explore Application by: AllBytes (sum)

Internal IP

10.2.127.21 10.2.127.25 10.2.128.58 10.2.136.37 10.5.1.11 10.5.1.180 10.5.1.20 10.5.1.23 10.5.1.244 10.5.1.245 10.5.1.30 10.5.1.36 10.5.1.40 10.5.1.49 10.5.1.50 192.114.187.109 192.114.187.16 192.114.187.22 192.114.187.3 192.114.187.32 192.114.187.43 192.114.187.44 192.114.187.54 192.114.187.77 193.105.201.11 **212.199.108.62** 212.199.143.70 213.57.225.174 217.72.181.19 81.218.101.178

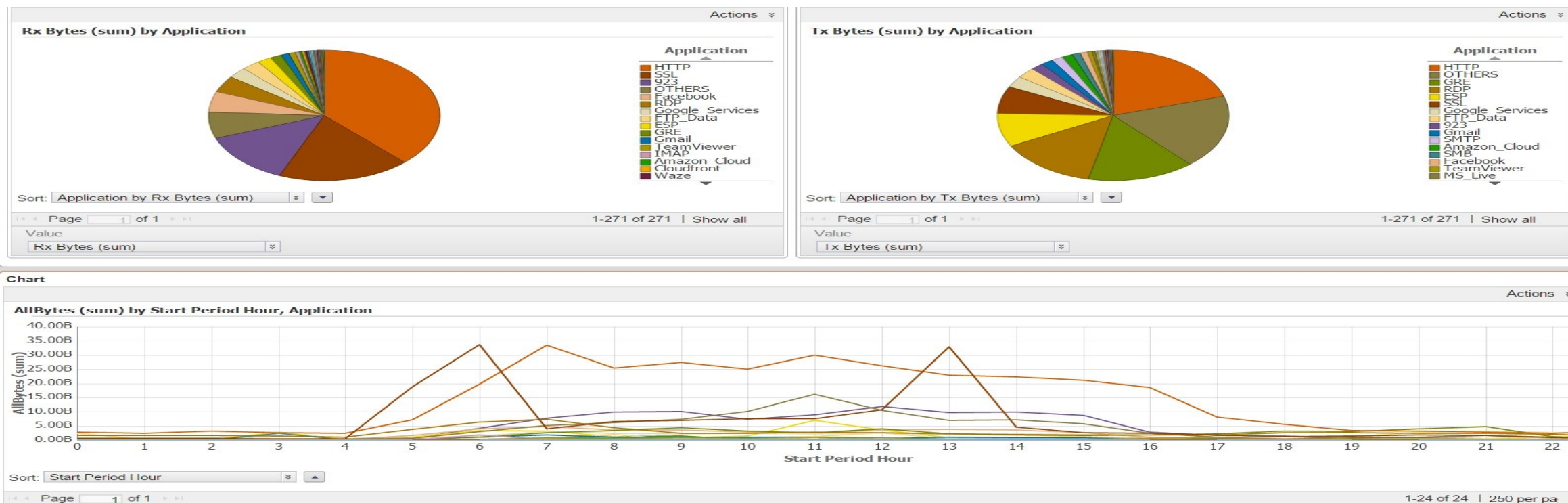
Explore Internal IP by: AllBytes (sum)

External IP

10.5.1.9 116.211.5.59 173.244.221.213 192.114.187.2 192.114.187.22 192.114.187.3 192.114.187.43 212.199.108.62 212.199.202.19 212.199.202.60 212.199.205.206 212.199.205.209 212.199.205.211 212.91.166.213 **23.221.153.30** 31.13.90.6 62.219.14.172 80.244.172.10 80.244.172.12 80.244.172.14 81.218.219.1 82.102.137.153 82.102.137.163 82.102.137.164 82.102.181.14 82.166.109.234 82.80.142.204 82.80.169.222 89.138.212.150 96.39.0.10

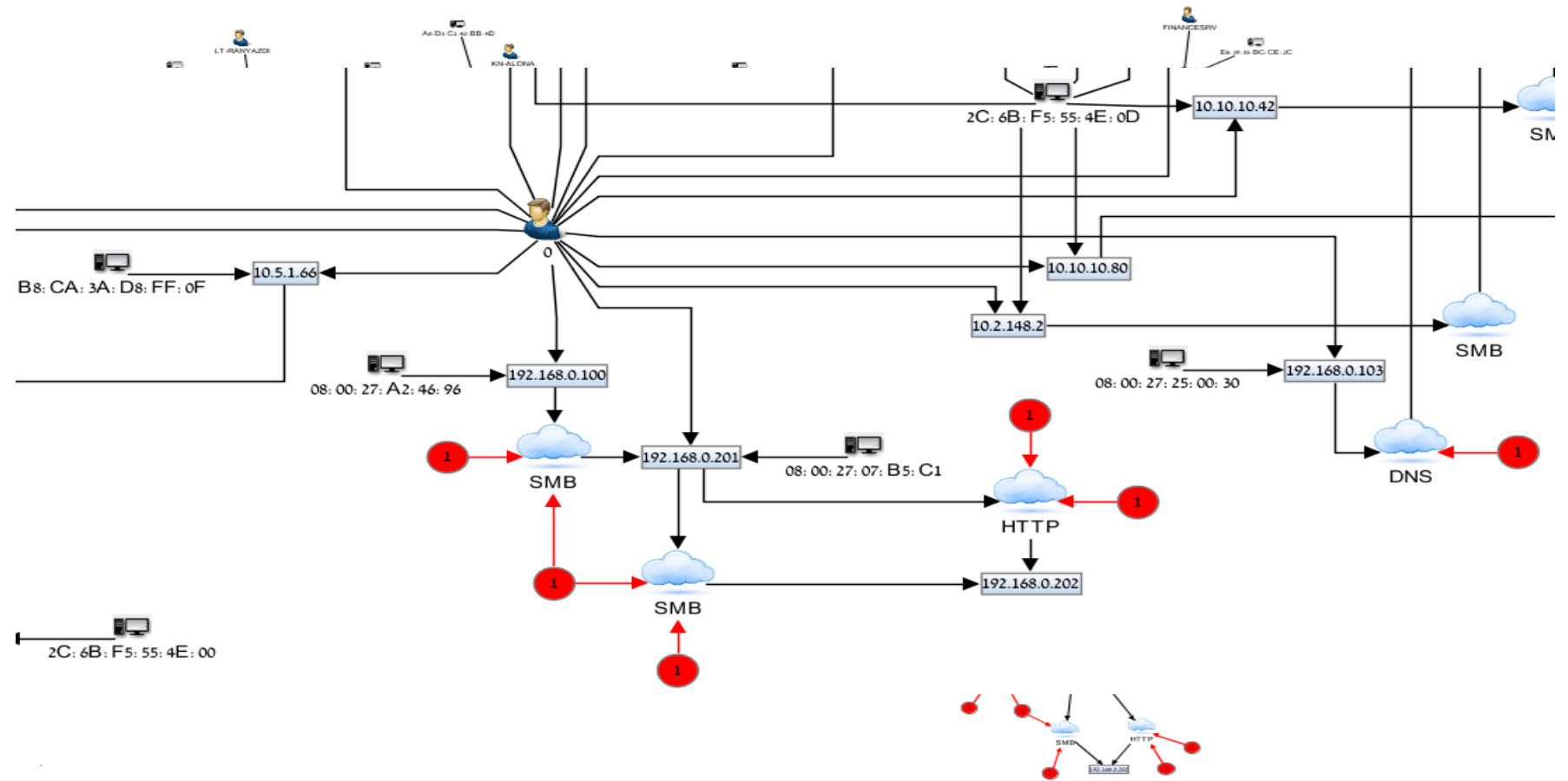
Explore External IP by: AllBytes (sum)

Information Discovery Events Dashboard



Graph DB Visualization

Internal Network Visualization

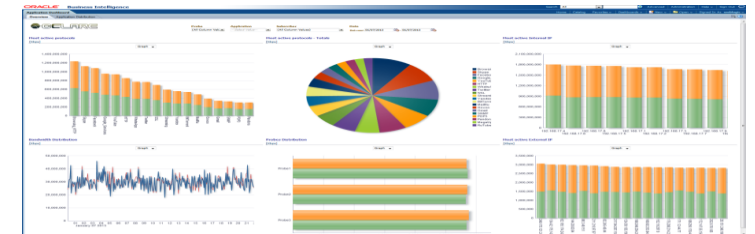


- Intuitive visualization
- Visual filters
- Advanced search: nodes & links
- Zoom for details
- Multiple views

Solution Benefits



- Monitoring multiple links with speeds up to 40Gbps
- Agnostic to physical link (SDH, PTN, Ethernet) and Transport protocol (IP, MPLS)
- Distributed & Low cost
- Open architecture and scalable
- Low cost Switch/probes enable flexible deployment over the network
- Integrated with Any Big Data & tools
- Based on standard analytics tools and products (e.g. Oracle Endeca, OEP, Open Source)
- Open API for external systems and 3rd party applications and Algorithms





Thank You