Napoli, 4 Dicembre 2015

Security Operations in una Telco, Esperienze e Riflessioni dal Campo

Seminario - Corso di Network Security
(Ing. Informatica, Laurea Magistrale)
Università degli Studi di Napoli Federico II

Fabio Zamparelli

Agenda

- **Who Am I? / Where Do I work?**
- **Protezione infrastrutture: DDoS Mitigation**
- **L’esperienza Expo 2015**
- **Infosharing & IOC**

Who Am I?

- A Geek and a Manager ☺
- Passionate about and Working in “Networking and Internet World” since 1996
- Graduated at “Federico II, Napoli - Computer Engineering & Systems department”
- A period of collaboration with “GRID/COMICS research Group” on “IP Network Security”
- Joined Telecom Italia in 2001 and entered the “IP Backbone NOC team”
- Since 2003 I’ve been working in Technical Security teams; my first role was Public Network Security Engineering Team Leader
- In 2008 I’ve been officially appointed, in organization charts, as the “SOC Manager”
- More or less 15 years experience in ICT Security “technical and management stuff”, with a strong understanding of “Critical Infrastructures Protection” and “Carrier Class Network Security”

Where Do I Work?

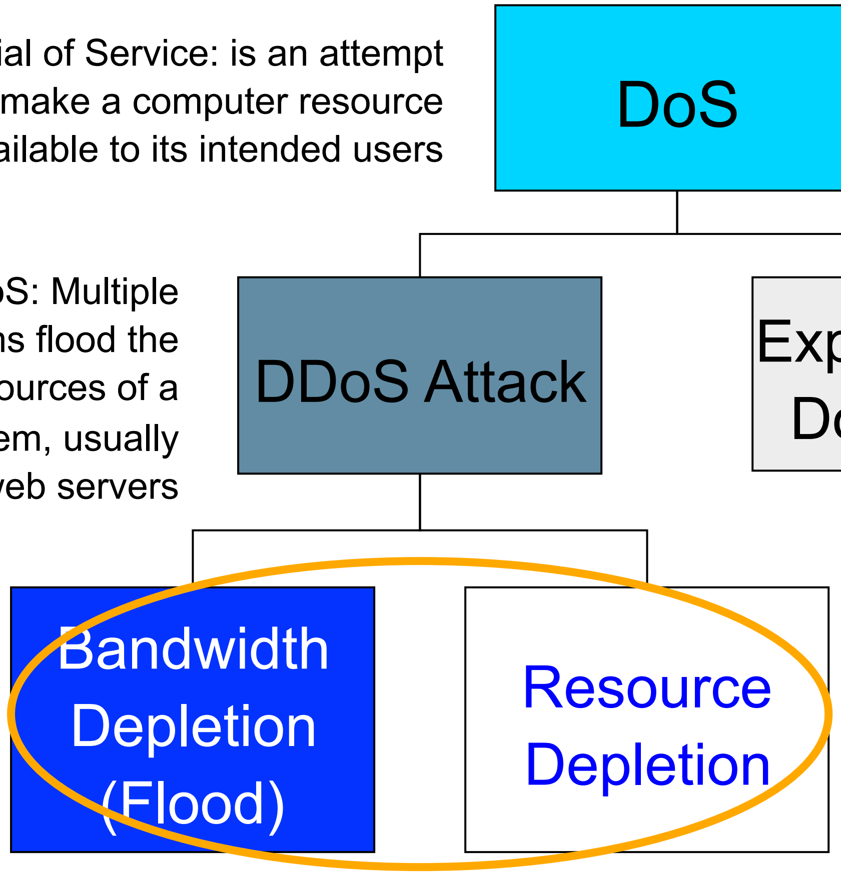
- In Telecom Italia's "ICT Infrastructures Corporate Security Operation Center"
  - A team of internal and external security specialists I'm proud to lead
  - In charge of
    - Public and Corporate Network Security
    - IT OSS&BSS applications, IT Infrastructures and Office Automation Security
  - Dealing with:
    - H24 Security Monitoring and Incident Handling
    - OSINT and Hunting
    - Collaborations with other SOCs & CERTs
  - Only Logical Security, not Physical
  - Different from the dedicated MSS SOC

Agenda

- Who Am I? / Where Do I work?
- **Protezione infrastrutture: DDoS Mitigation**
- L’esperienza Expo 2015
- Infosharing & IOC

What are we going to talk about?

1) What a DDoS is



DoS

Denial of Service: is an attempt to make a computer resource unavailable to its intended users

DDoS Attack

Distributed DoS: Multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers

Exploit-based DoS Attack

Exploit errors in the operating system/ application, causing resource starvation and/ or thrashing and/or crash and/or unauthorized access and riconfiguration.

Bandwidth Depletion (Flood)

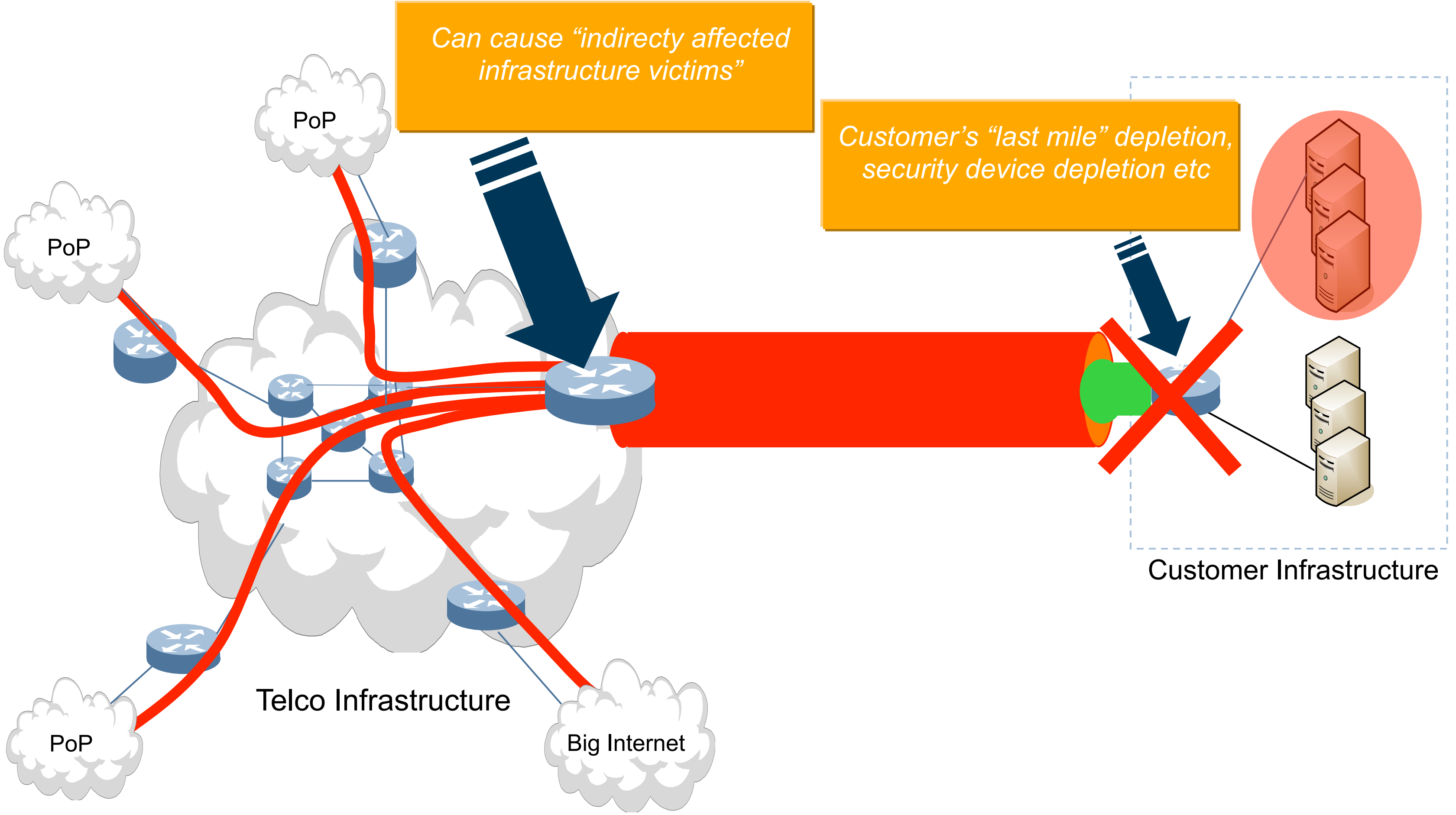
Flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system

Resource Depletion

Tie up the resources (CPU/Mem/ Time) of a victim host or other devices (ie: Firewall).

What are we going to talk about?

2) DDoS: last mile bandwith & resources depletion



Can cause "indirecty affected infrastructure victims"

Customer's "last mile" depletion, security device depletion etc

What are we going to talk about?

3) DDoS: Trends 1/2

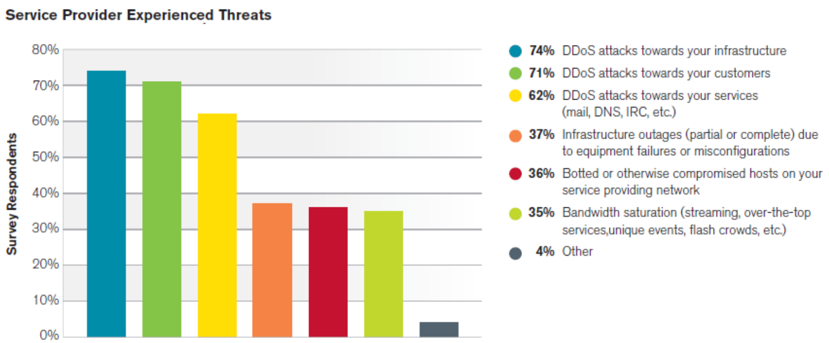
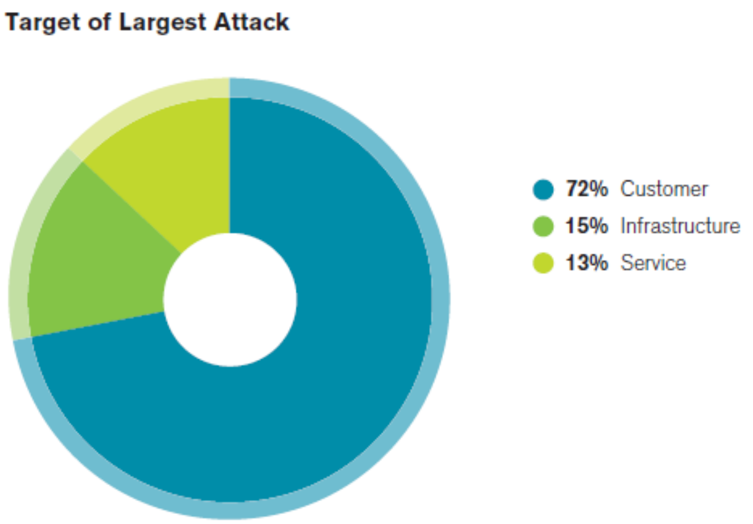


Figure 9 *Source: Arbor Networks, Inc.*

DDoS Attacks are indicated to be the most significant operational threat (with a significant influence on Infrastructure Outages)

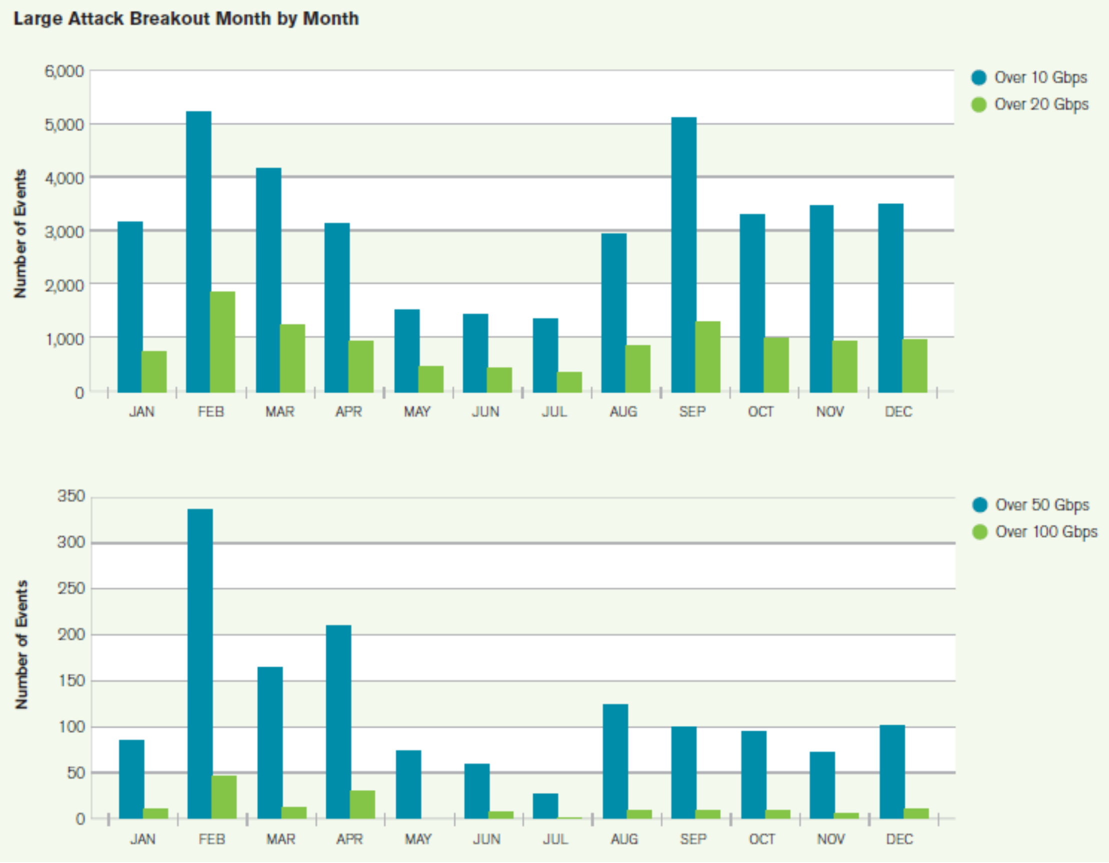


72% percent of respondents reported that the highest-bandwidth DDoS attacks they experienced during this survey period was directed at their end customers, 15% indicated that their own network infrastructure was the target of the highest-bandwidth attack they experienced, while 13% reported that their own ancillary support services such as DNS and Web portals were targeted;

Source: Arbor Networks' "Worldwide Infrastructure Security Report - 2014".

What are we going to talk about?

3) DDoS: Trends 2/2



Average Number of DDoS Attacks per Month

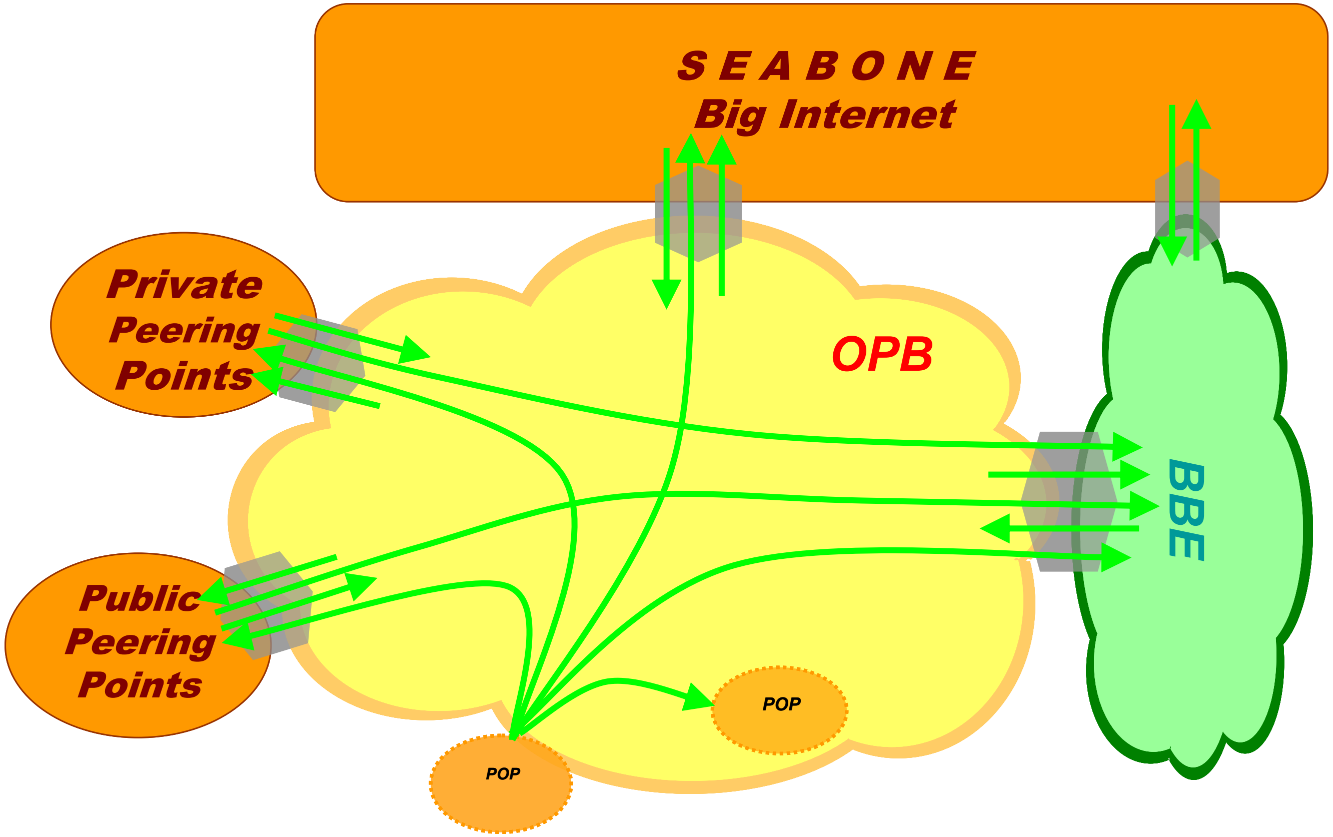
The number of attacks is increasing year by year and the volume is growing up.

Fonte: Survey Arbor Network

Source: Arbor Networks' "Worldwide Infrastructure Security Report - 2014".

When are we going to talk about the real field experience?

1) T.I. IP Public Network’s Anomaly Detection Platform 1/2

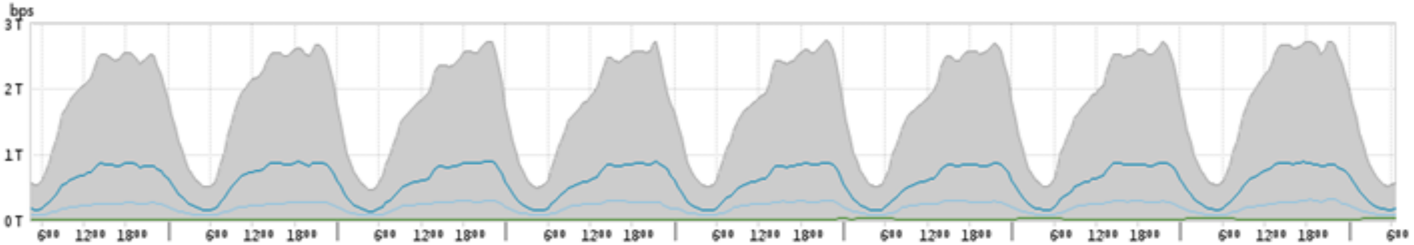


- Detection built on Aggregated & Statistically Monitored Traffic
  - Through Sampled NETFLOW/CFLOW from Giga-Routers & Tera-Routers
  - Configured on Perimeter/Border Routers’ interfaces
  - Reaching Specific Statistical Aggregations to detect Critical Infrastructure events and anomalies

When are we going to talk about the real field experience?

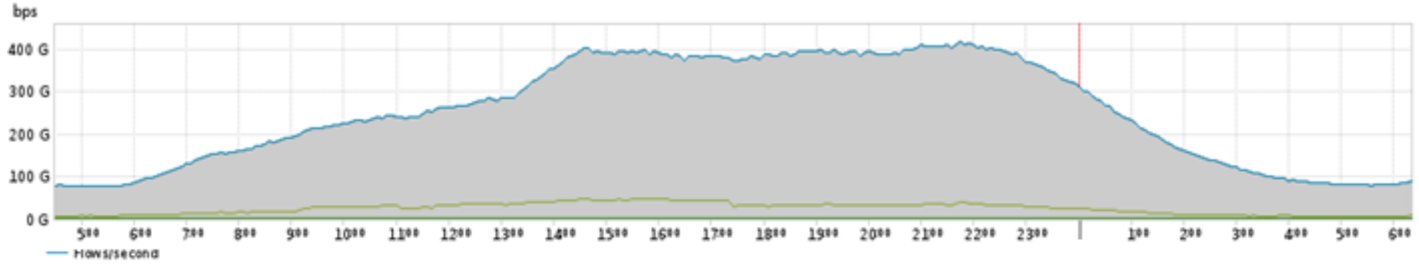
1) T.I. IP Public Network's Anomaly Detection Platform 2/2

Some Figures….

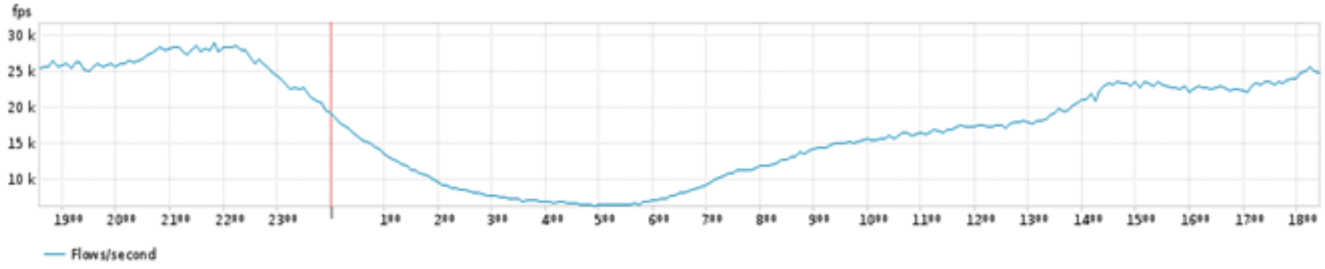


Up to 2,5 Terabit per second of traffic sampled collected and statistically analyzed

Up to 400 Gigabit per second of traffic sampled and statistically analyzed from a single "Top Tera Router"



Up to 30k Flow per Second collected and statistically analyzed from a single "Top Tera Router"



When are we going to talk about the real field experience?

2) Where does it become to be a critical infrastructure events?

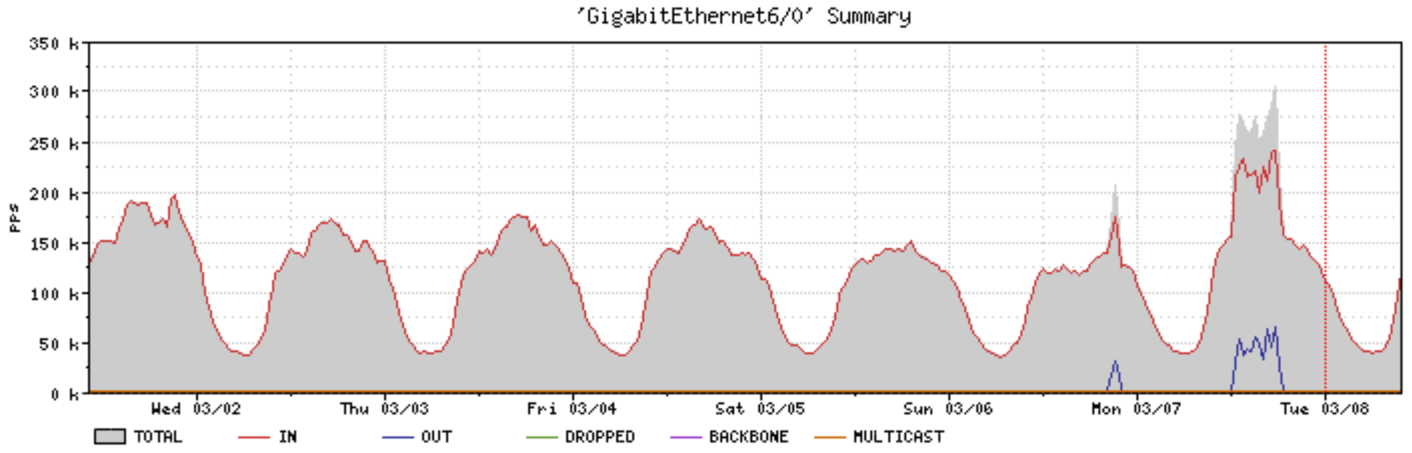
- Some “Numbers” of actually managed DDoS Attacks “towards us” during the last few weeks
  - Up to 124 Gbps targeting a single IP
  - Up to 24 Mpps targeting a single IP
  - “Sustained Attack” lasting for more then 12 hours; “Average Under Attack Condition” for certain web portal lasting for some days and, in some cases, weeks
- What problem these attacks can bring to a Telco operator?
  - When is it considered a “Customer Issue”?
  - When does it become a “localized degradation of Quality”
  - At which point are we going to consider it a Critical Infrastructure event?

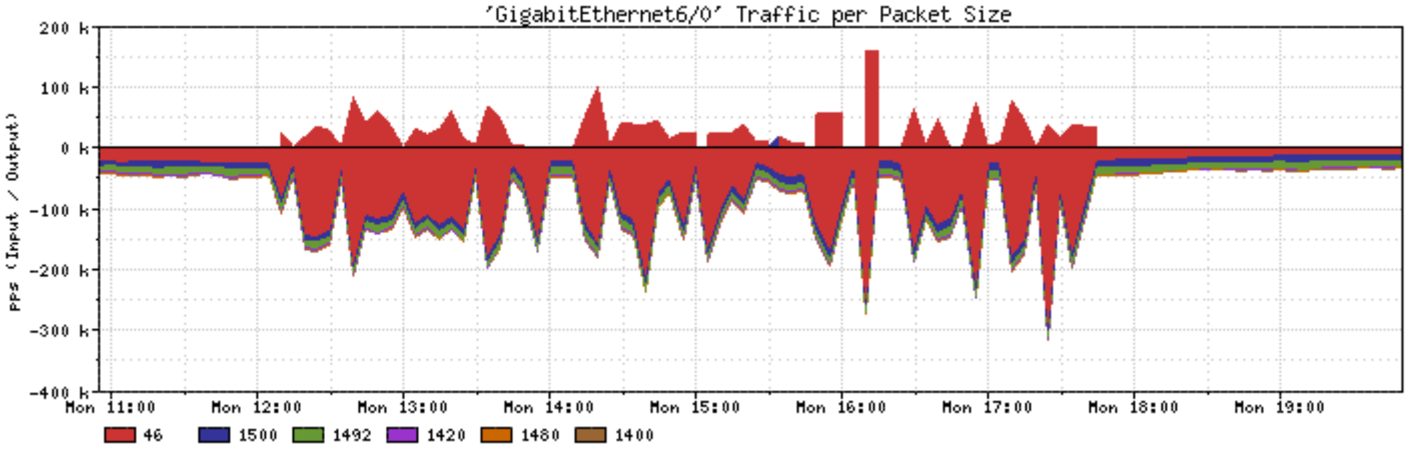
What info/detection tools do we need “during the Battle”?

- Ability to Configure/Profile what net-prefixes you want to monitor and to aggregate data for
- Clear and Real-Time updated Anomaly Detection within Gps pipes of data
- War-Time Reaction Strategy and Decisions, mainly built by identifying:
  - “What KIND of Attack it is”
  - “Where the attack is entering FROM”
  - “Where it is going TO”
    - Which router is announcing the targeted prefix?
    - What is the links bandwidth though which the indirectly victimized router is connected TO the backbone?

Some “Real World” case studies from the “battle field”

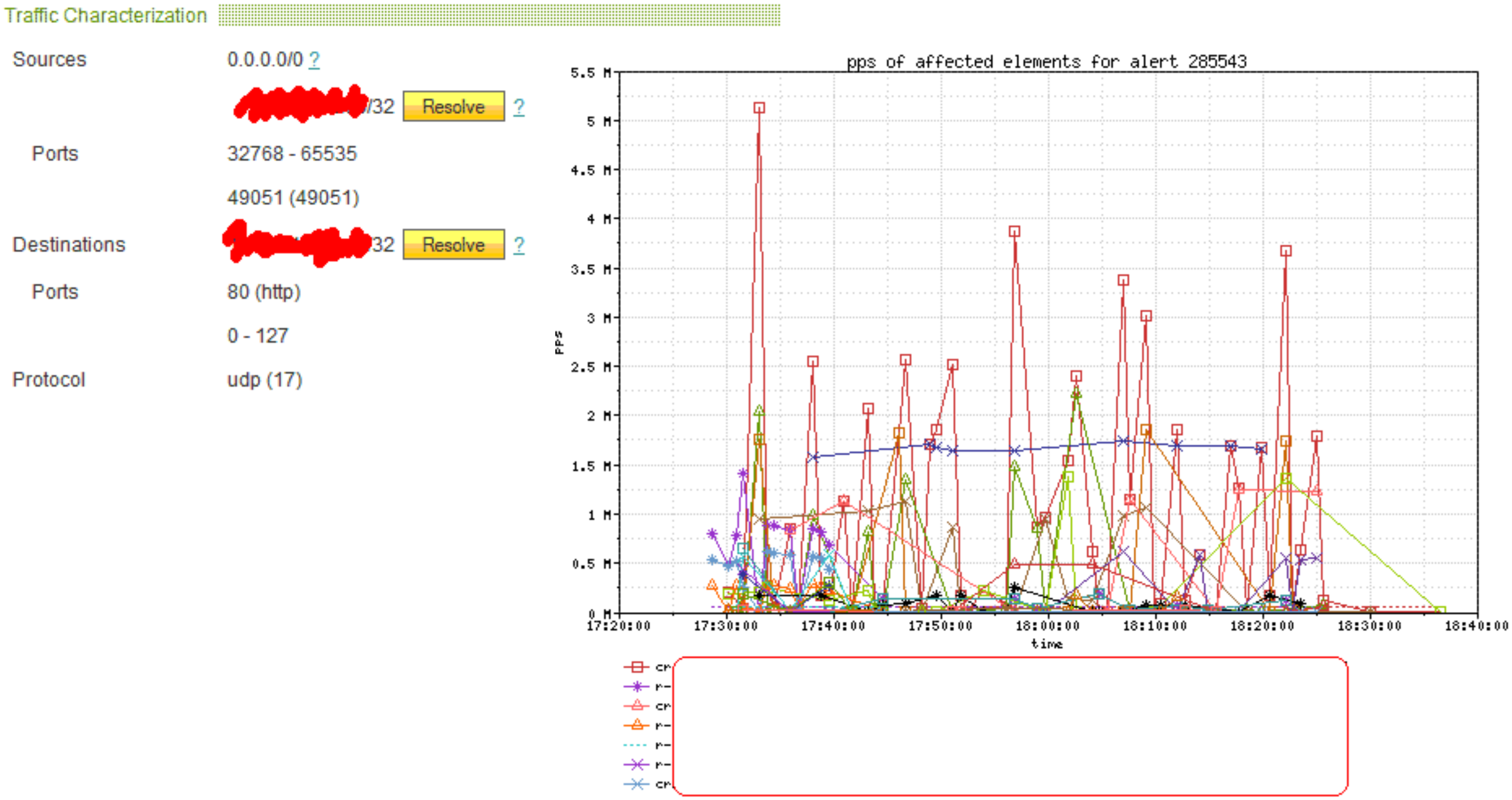
1) First Case Study 1/2





Some “Real World” case studies from the “battle field”

1) First Case Study 2/2



Traffic Characterization

Sources	0.0.0.0/0 ?
	[redacted]/32 Resolve ?
Ports	32768 - 65535
	49051 (49051)
Destinations	[redacted]32 Resolve ?
Ports	80 (http)
	0 - 127
Protocol	udp (17)

[redacted]

Agenda

- Who Am I? / Where Do I work?
- Protezione infrastrutture: DDoS Mitigation
- **L’esperienza Expo 2015**
- Infosharing & IOC

Expo 2015: SOC's Setup & Operations

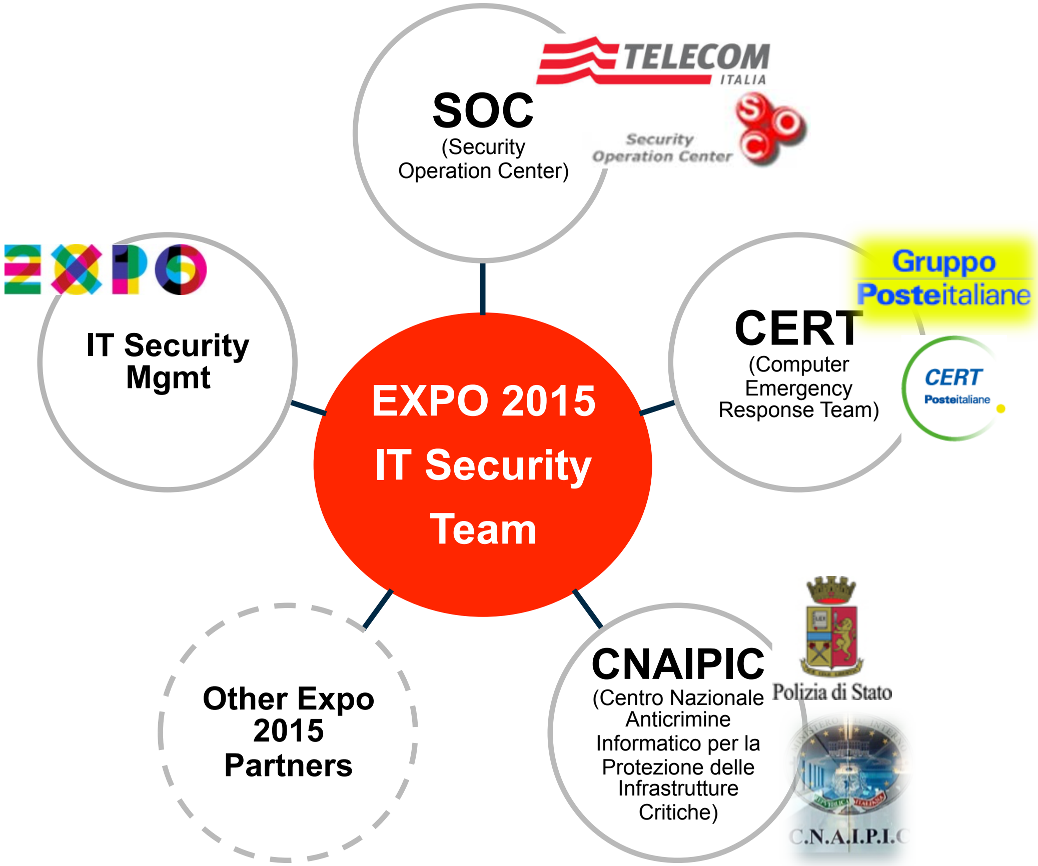
Organizational and Technological Setup

- Activation of **SECURITY** countermeasures and **CORE SECURITY PLATFORMS** throughout EXPO2015 IT infrastructures
- Integration of Data **SOURCES** (105 total data sources) on the SOC **Security Information and Event Management (SIEM)** platform
- Defining **INCIDENT HANDLING** and escalation **PROCEDURES**, communication interfaces, templates and reporting flows

Operations

- **OPEN SOURCE INTELLIGENCE** monitoring and analysis **(OSINT)**
- **REAL-TIME** and continuous **SIEM MONITORING**
- **RESPONSE** to possible **INCIDENTS**, cooperating with **CERT**, **CNAIPIC** and **EXPO2015** teams

Expo 2015: Private2Public Cyber Security Cooperation Model


SOC
(Security Operation Center)
TELECOM ITALIA
Security Operation Center
IT Security Mgmt
EXPO 2015 IT Security Team
CERT
(Computer Emergency Response Team)
Gruppo Posteitaliane
CERT Posteitaliane
Other Expo 2015 Partners
CNAIPIC
(Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche)
Polizia di Stato
C.N.A.I.P.I.C

- Telecom Italia **Security Operation Center** (SOC) was the core **IT security monitoring** and alert management Function within Telecom Italia Group. It offers not only the latest technological solutions, but also a **high level of expertise and skills**.
- Within the Expo2015 cooperation model, SOC provided **H24/7 IT security monitoring** and **incident management services.** SOC represented, along with Poste Italiane CERT, the IT security **operational unit** of Expo2015, **supervised by CNAIPIC**.
- The cooperation model also **involved** the Expo2015 **IT SECURITY REPRESENTATIVES** and provided interaction with other Expo2015 **IT PARTNERS**.

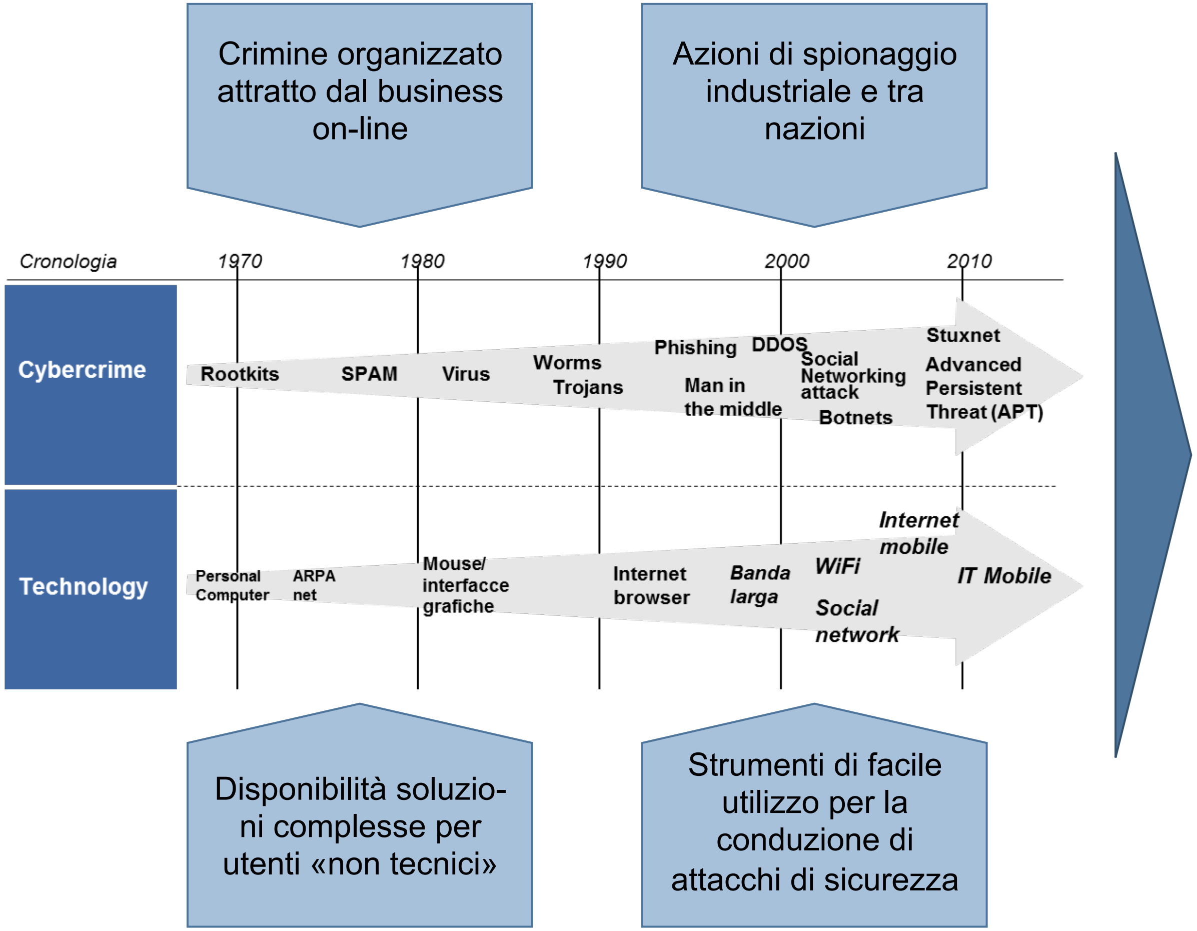
Expo2015: Risultati

- After a **challenging, intense start,** given the **complexity of the communication flows** between the various stakeholders, **cooperation mechanisms were quickly strengthened by augmented collaboration** and teamwork, thus maximizing results
- **Synergy between the diverse stakeholders** enabled reduction of incident response to a minimum and limited their criticality
- Correlati e gestiti – sul perimetro di rete, applicazioni e sui **454 server** dedicati alla gestione di EXPO - circa **800 eventi al secondo** con un **picco giornaliero di 500 milioni di eventi**.
- Le contromisure di **prevenzione attacchi DDOS** (Denial of service) si sono rivelate particolarmente efficaci, rendendo i sistemi esposti ad Internet disponibili nei momenti più critici: solo il 5% degli incidenti hanno riguardato i tentativi di negazione del servizio.
- Dei **circa 200 incidenti** gestiti il **20% è stato classificato come "Rilevante"**, il restante è rimasto a valori "Business As Usual" e **nessun** incidente è arrivato a classificazione di **"Emergenza" o "Crisi"**.
- **Nei primi due mesi** è stato affrontato e risolto **più del 50% degli incidenti** abbattuti del 90% nei momenti di picco più "critici" per la manifestazione.

Agenda

- Who Am I? / Where Do I work?
- Protezione infrastrutture: DDoS Mitigation
- L’esperienza Expo 2015
- **Infosharing & IOC**

Comunicazione con altri per fronteggiare la complessità



Crimine organizzato attratto dal business on-line

Azioni di spionaggio industriale e tra nazioni

Cronologia *1970* *1980* *1990* *2000* *2010*

Cybercrime

Rootkits **SPAM** **Virus** **Worms** **Trojans** **Phishing** **Man in the middle** **DDOS** **Social Networking attack** **Botnets** **Stuxnet** **Advanced Persistent Threat (APT)**

Technology

Personal Computer **ARPA net** **Mouse/ interfacce grafiche** **Internet browser** ***Banda larga*** ***WiFi*** ***Social network*** ***Internet mobile*** ***IT Mobile***

Disponibilità soluzio-ni complesse per utenti «non tecnici»

Strumenti di facile utilizzo per la conduzione di attacchi di sicurezza

1

COLLABORAZIONE

I nuovi attacchi si sviluppano in contesti non completamente controllabili dal singolo

2

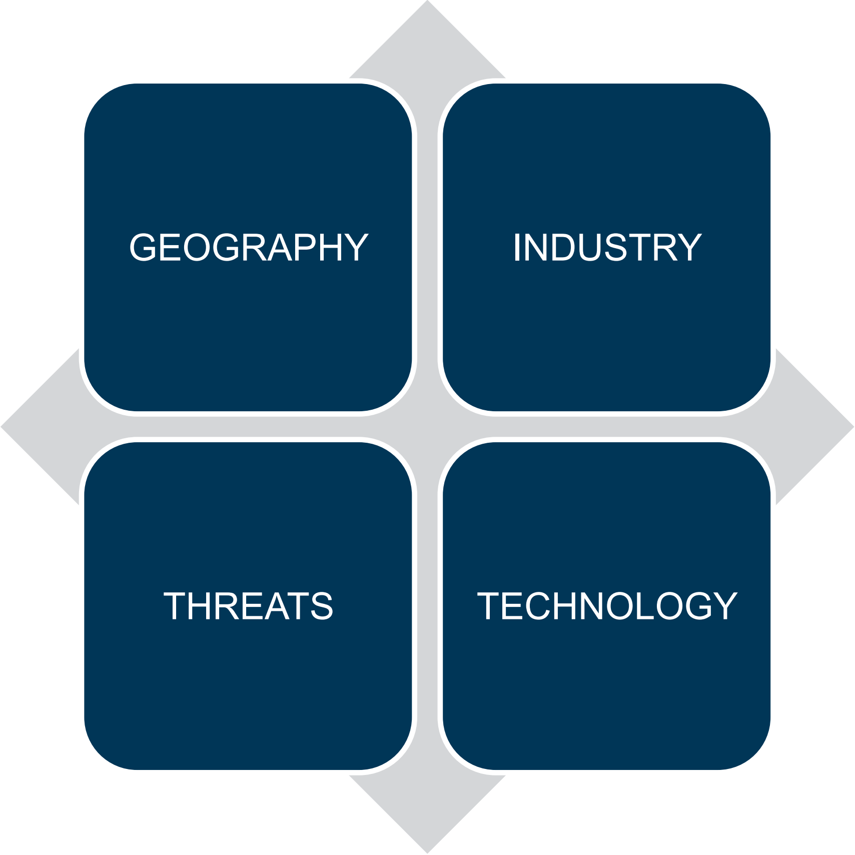
INFO-SHARING

Fondamentale conoscere le caratteristiche e la provenienza di una minaccia in diffusione

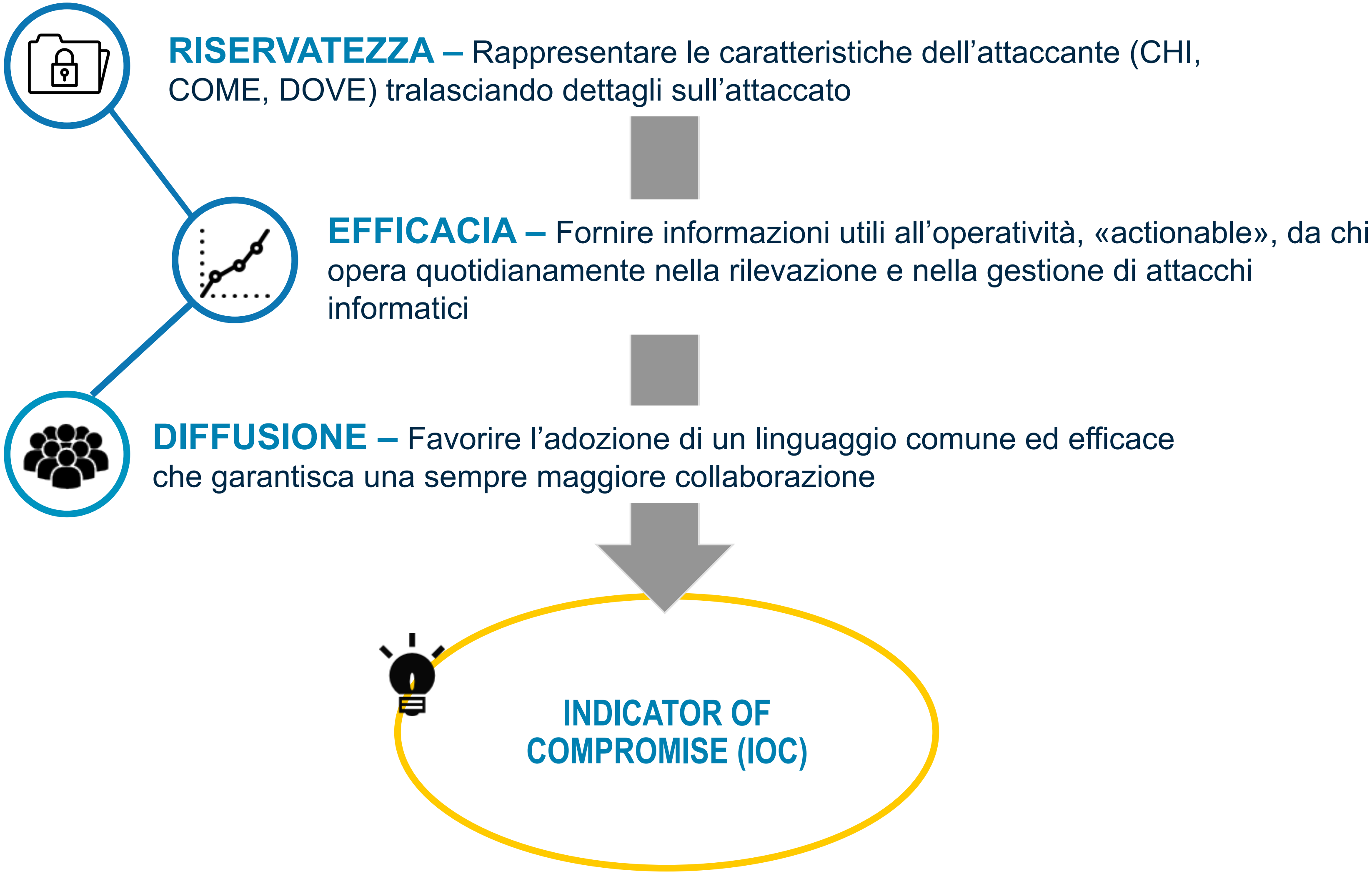
Community come elemento abilitante all'infosharing

Rappresentano gruppi TRUSTED di persone provenienti da contesti operativi simili ed animati dal medesimo interesse di capire come fornire un contributo per individuare e gestire nuove minacce

CARATTERIZZAZIONE DELLE COMMUNITY



Linguaggio comune per facilitare scambio di informazioni



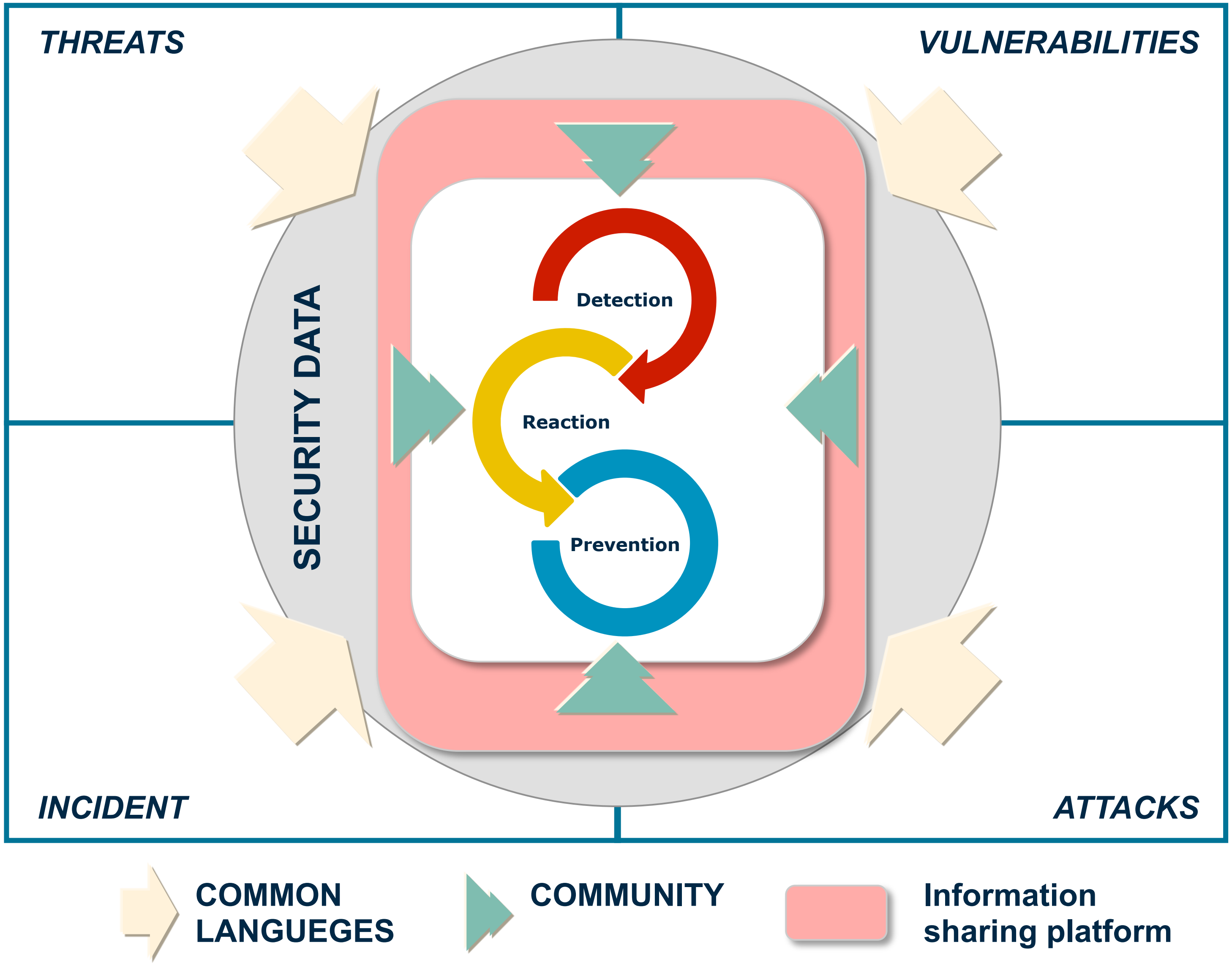
RISERVATEZZA – Rappresentare le caratteristiche dell’attaccante (CHI, COME, DOVE) tralasciando dettagli sull’attaccato

EFFICACIA – Fornire informazioni utili all’operatività, «actionable», da chi opera quotidianamente nella rilevazione e nella gestione di attacchi informatici

DIFFUSIONE – Favorire l’adozione di un linguaggio comune ed efficace che garantisca una sempre maggiore collaborazione

INDICATOR OF COMPROMISE (IOC)

Modello di fruizione delle informazioni



E ora… sbizzarritevi con lo spazio Q&A e…

Grazie