Italian Cyber Security Report 2014:
Consapevolezza organizzazione e difesa nel settore pubblico

Roberto Baldoni
baldoni@dis.uniroma1.it, @robertobaldoni

CIS SAPIENZA

RESEARCH CENTER FOR CYBER INTELLIGENCE AND INFORMATION SECURITY

Ramsonware
Denial of service
Cyber espionage
Wiping
Cyber2Physical
Dox(x)ing

Ramsonware

Denial of

Cyber es

Wiping

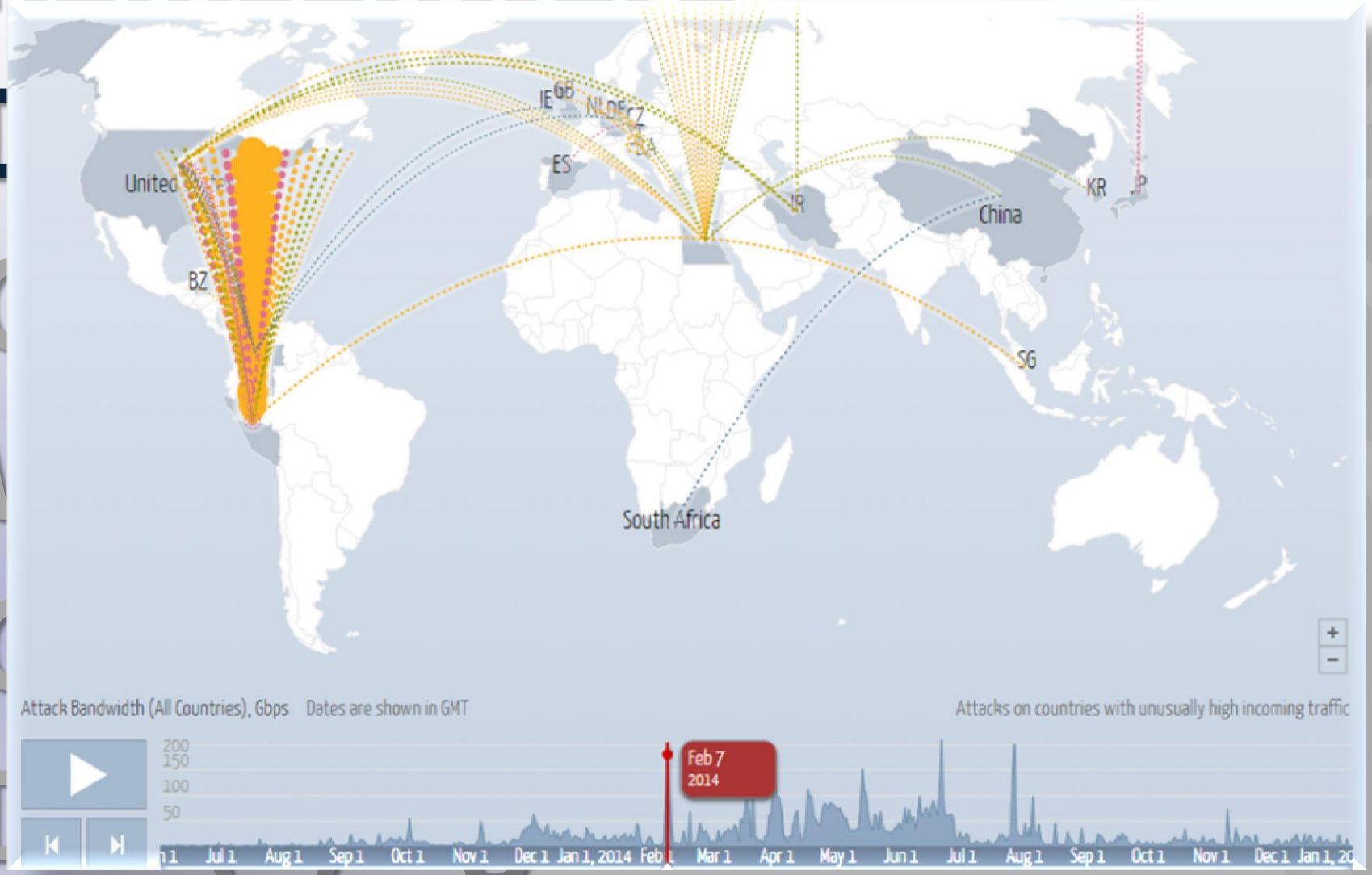
Cyber2Ph

Dox(x)ing

Perché i comuni italiani hanno subito un attacco informatico

Un malware in grado di criptare tutti i file del computer ha colpito le amministrazioni locali. Gli hacker chiedono un riscatto in bitcoin in cambio della liberazione dei dati

Ramsonware


United
BZ
IE
GB
ES
IR
China
KR
JP
SG
South Africa
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Attacks on countries with unusually high incoming traffic
200
150
100
50
Feb 7
2014
Jul 1
Aug 1
Sep 1
Oct 1
Nov 1
Dec 1
Jan 1, 2014
Feb 1
Mar 1
Apr 1
May 1
Jun 1
Jul 1
Aug 1
Sep 1
Oct 1
Nov 1
Dec 1
Jan 1, 20

Ramsonware

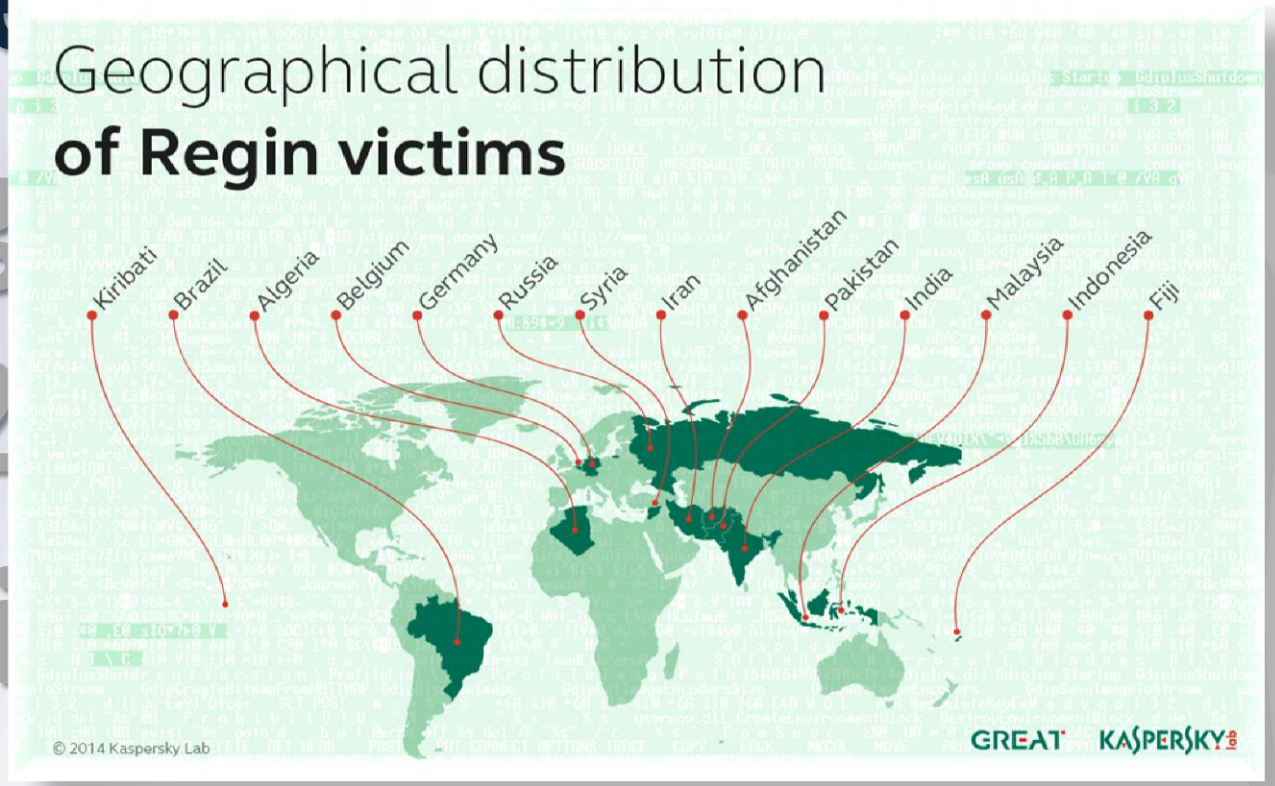
Denial of service

Cyber espionage

Wiping

Cyber2

Dox(x)i



Ramsonwa

Denial of s

Cyber espio

Wiping

Cyber2Physical

Dox(x)ing

```
rule unknown_wiper_error_strings{

meta: unique custom error debug strings discovered in the wiper malware

strings:

$IP1 = "203.131.222.102" fullword nocase

$IP2 = "217.96.33.164" fullword nocase

$IP3 = "88.53.215.64" fullword nocase

$MZ = "MZ"

condition:

$MZ at 0 and all of them

}
```

Ramsor

Denial c

Cyber e

Wiping

MILITARY

FOR THE SECOND TIME EVER, A CYBERATTACK CAUSES PHYSICAL DAMAGE

IT'S THE DAWN OF A NEW KIND OF WAR

By Kelsey D. Atherton Posted 12 hours ago

35 Shares

ThyssenKrupp

Cyber2Physical

Dox(x)ing

Ramsonware

Denial of service

Cyber espionage

Wiping

Cyber2Physical

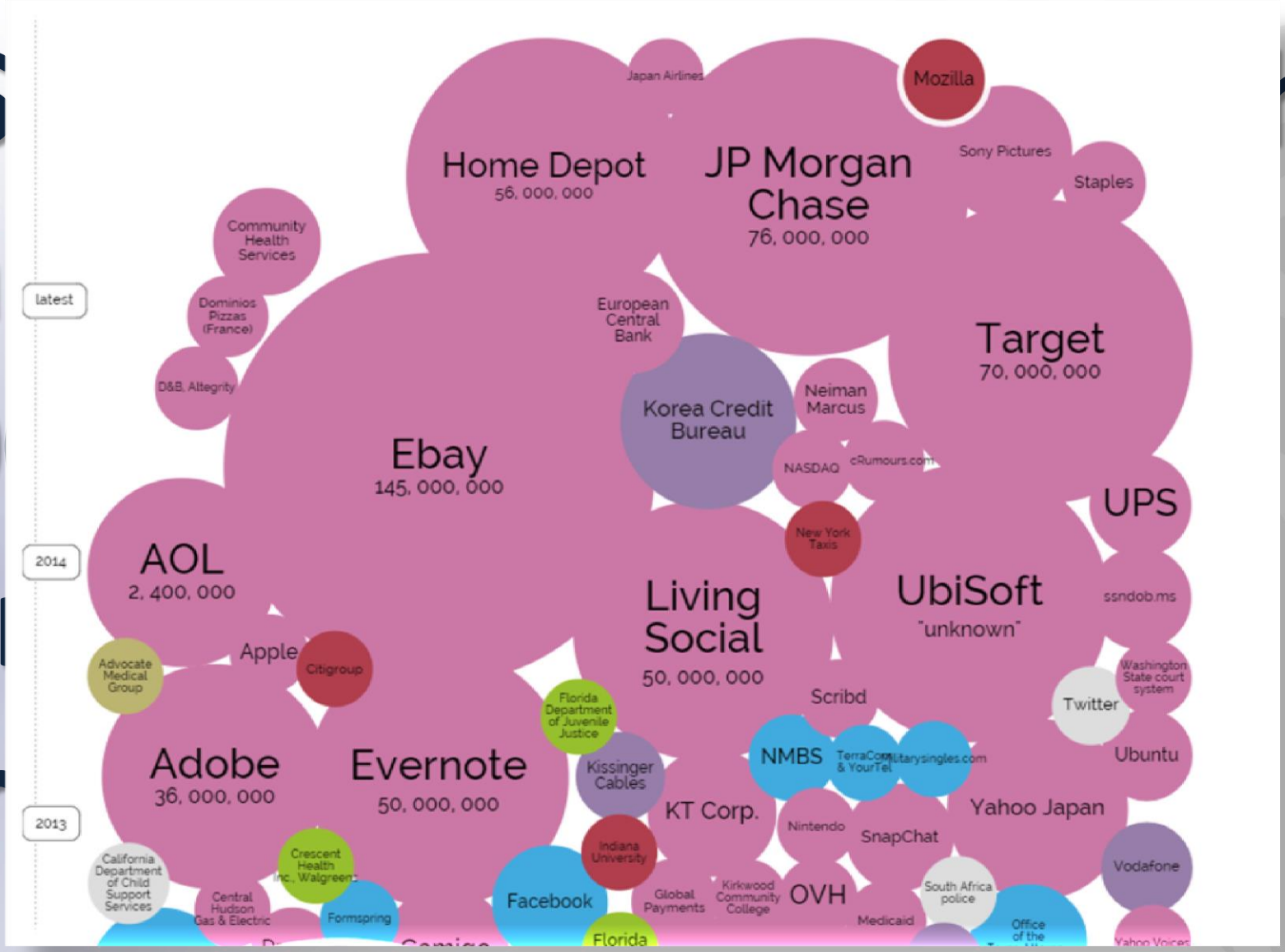
Dox(x)ing

Hacker stanno sviluppando una “big-data mentality”

Dal dox(x)ing al furto d’identità

US Agencies data breach passati da 27.000 nel 2009 a 46.000 nel 2013 con boom di attacchi a strutture ospedaliere

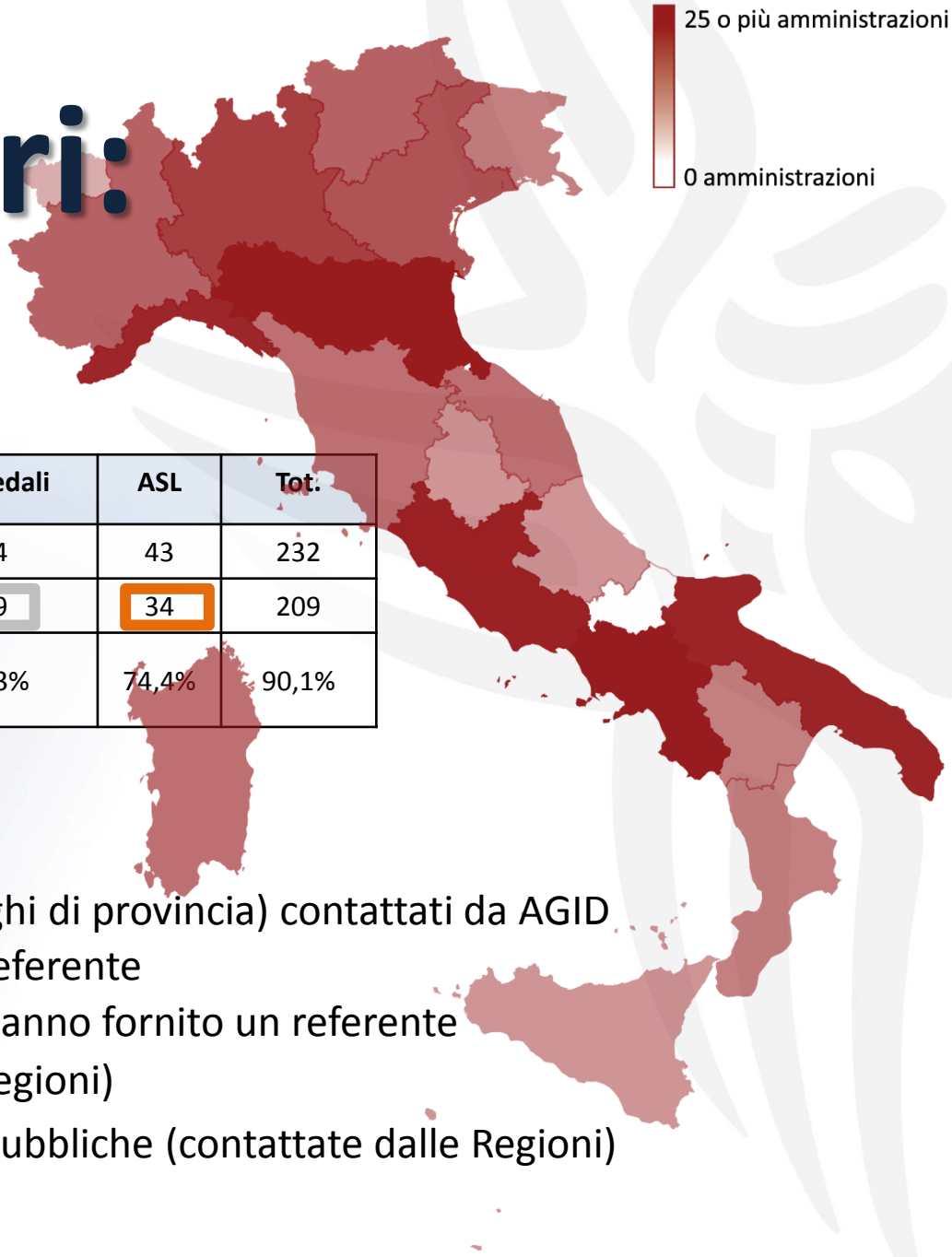
US
pa
20
co
str



Consapevolezza del valore strategico ed economico dell'informazione

Questionari:

61 domande



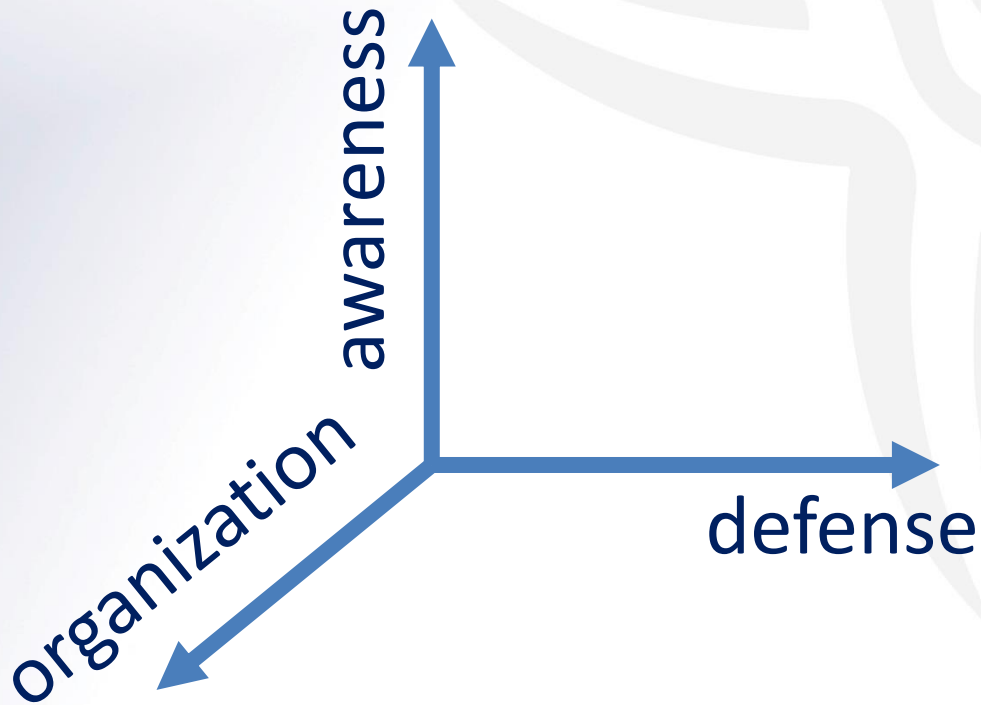
	PAC	Comuni	Regioni	Ospedali	ASL	Tot.
Inviati	42	83	30	34	43	232
Ricevuti	42	79	25	29	34	209
Percentuale ricezione	100%	95,2%	83,3%	85,3%	74,4%	90,1%

- 117 sono stati i comuni (capoluoghi di provincia) contattati da AGID
- 19 Regioni hanno fornito un un referente
- Tutte le PAC contattate da AGID hanno fornito un referente
- 25% delle ASL (contattate dalle Regioni)
- 4,5% delle Aziende Ospedaliere pubbliche (contattate dalle Regioni)

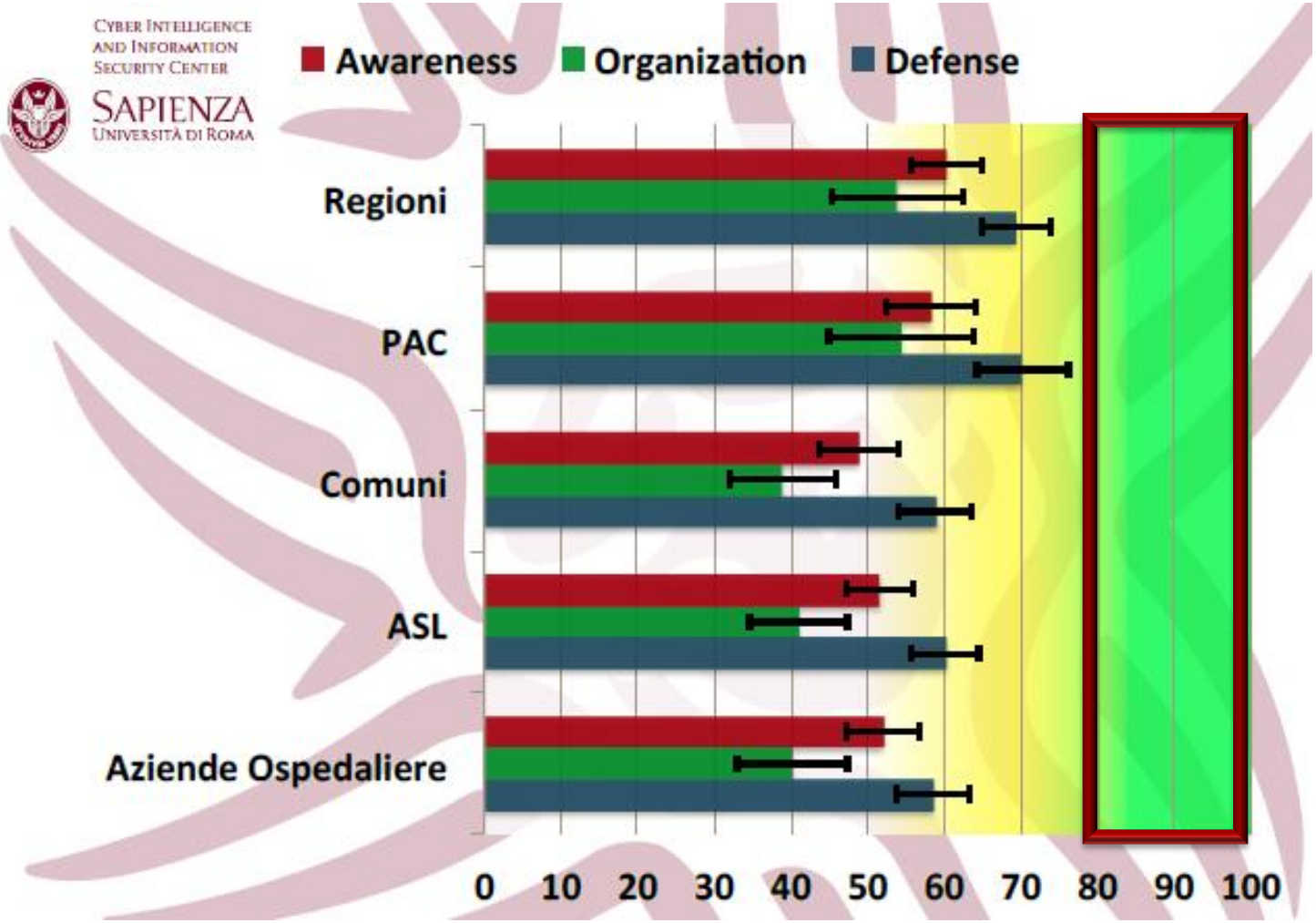
Analisi dei dati
Casi di Studio

Raccomandazioni

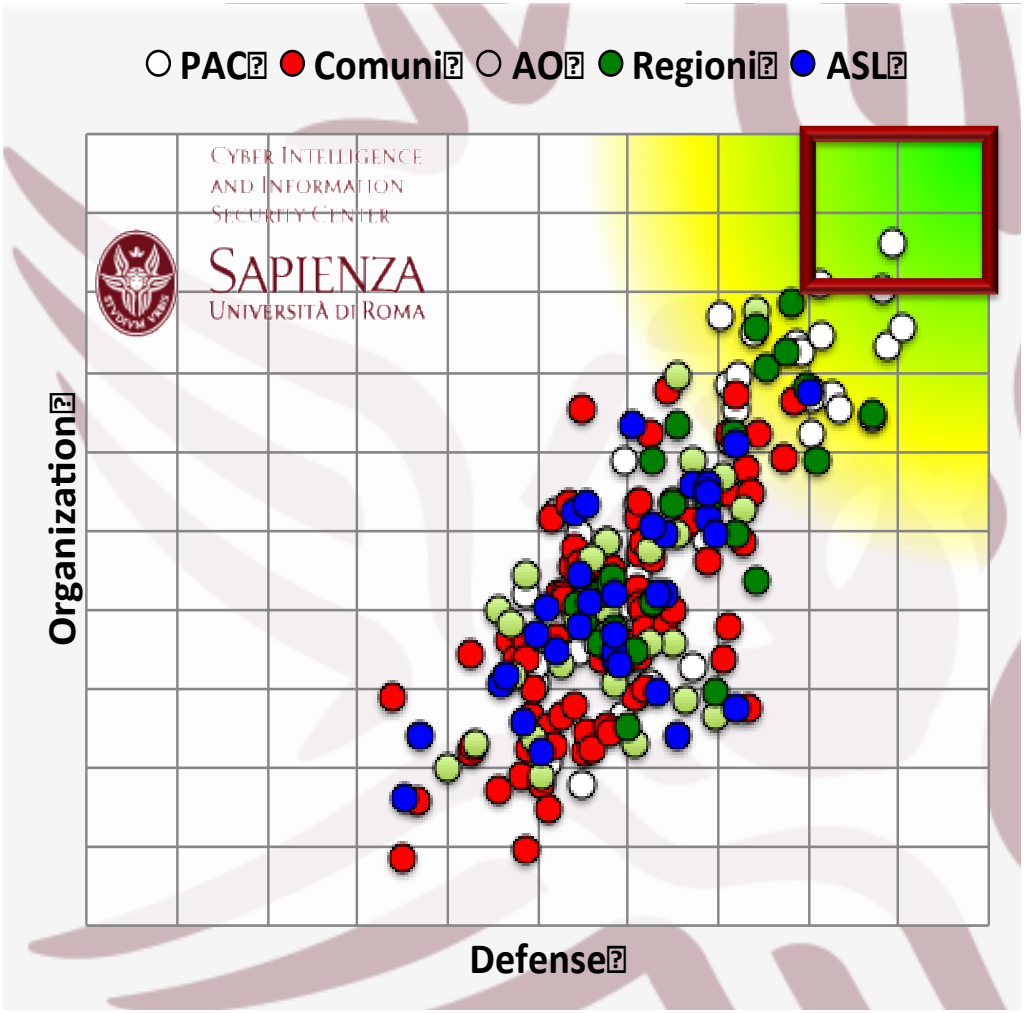
Key Performance Indicators

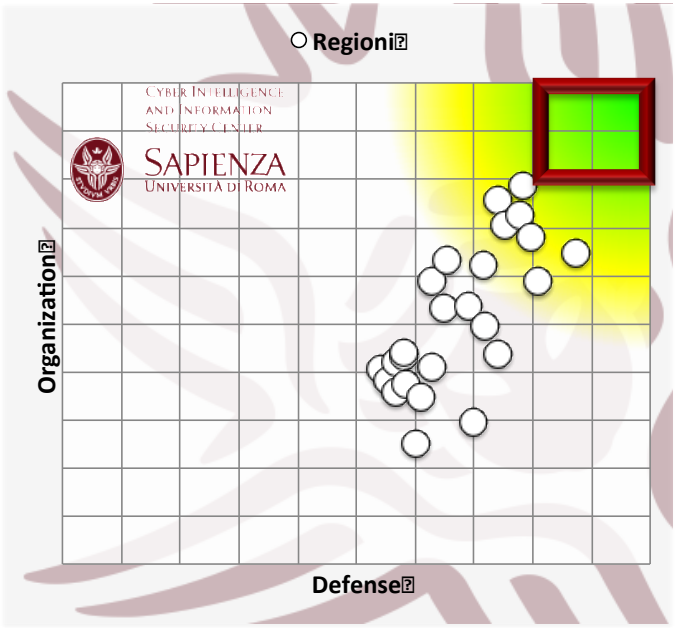


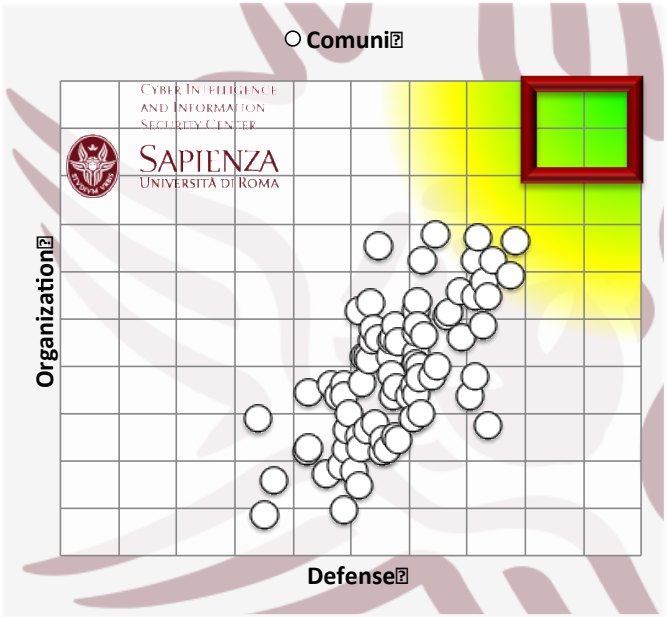
Risultati medi

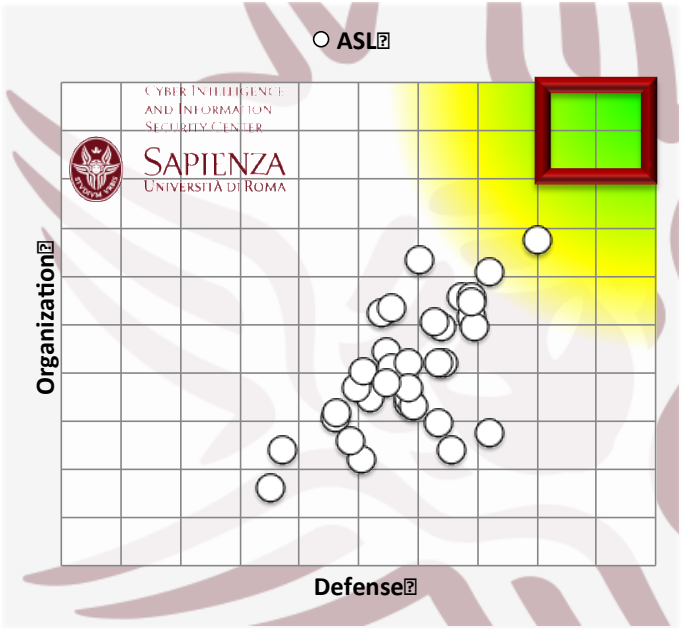


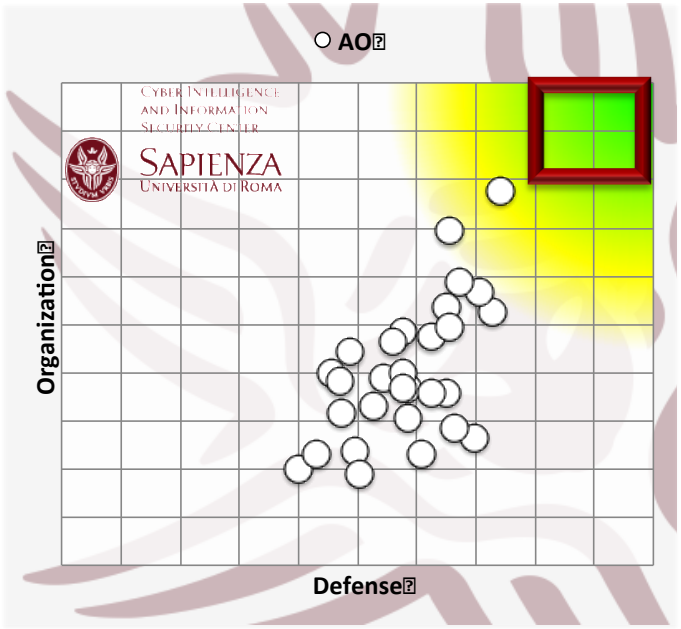
Organization vs Defense



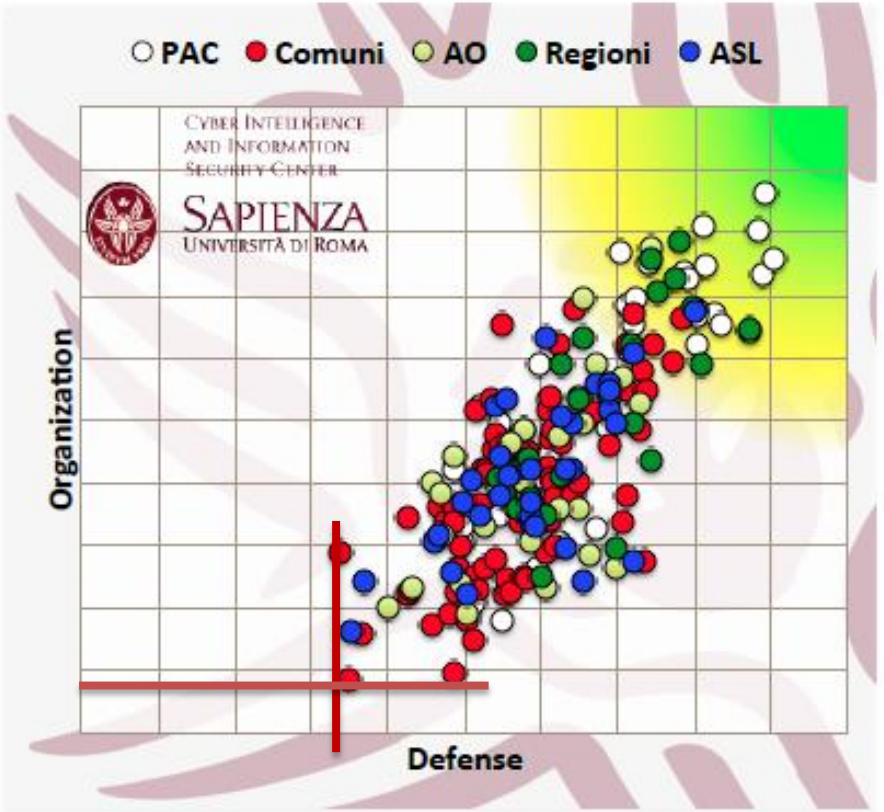

Regioni
Cyber Intelligence and Information Security Center
Sapienza
Università di Roma
Organization
Defense


Comuni
Cyber Intelligence and Information Security Center
Sapienza
Università di Roma
Organization
Defense


ASL
Cyber Intelligence and Information Security Center
Sapienza
Università di Roma
Organization
Defense

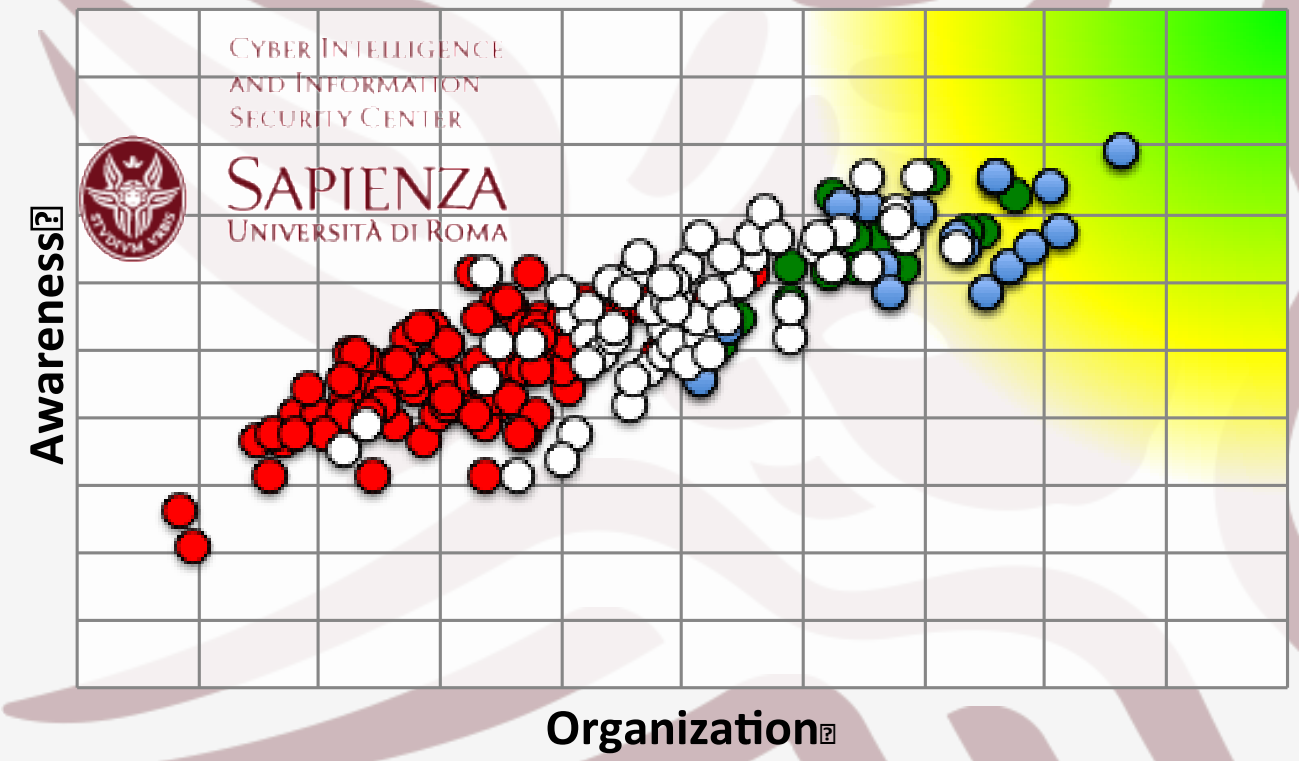

AO
Cyber Intelligence and Information Security Center
Sapienza
Università di Roma
Organization
Defense

tecnologia vs fattore umano



Analisi statistica dei dati

- No Risk Assessment, No Piano di Risposta, No ISMS
- Risk Assessment e Piano di Risposta
- Risk Assessment, Piano di Risposta, ISMS
- Altri



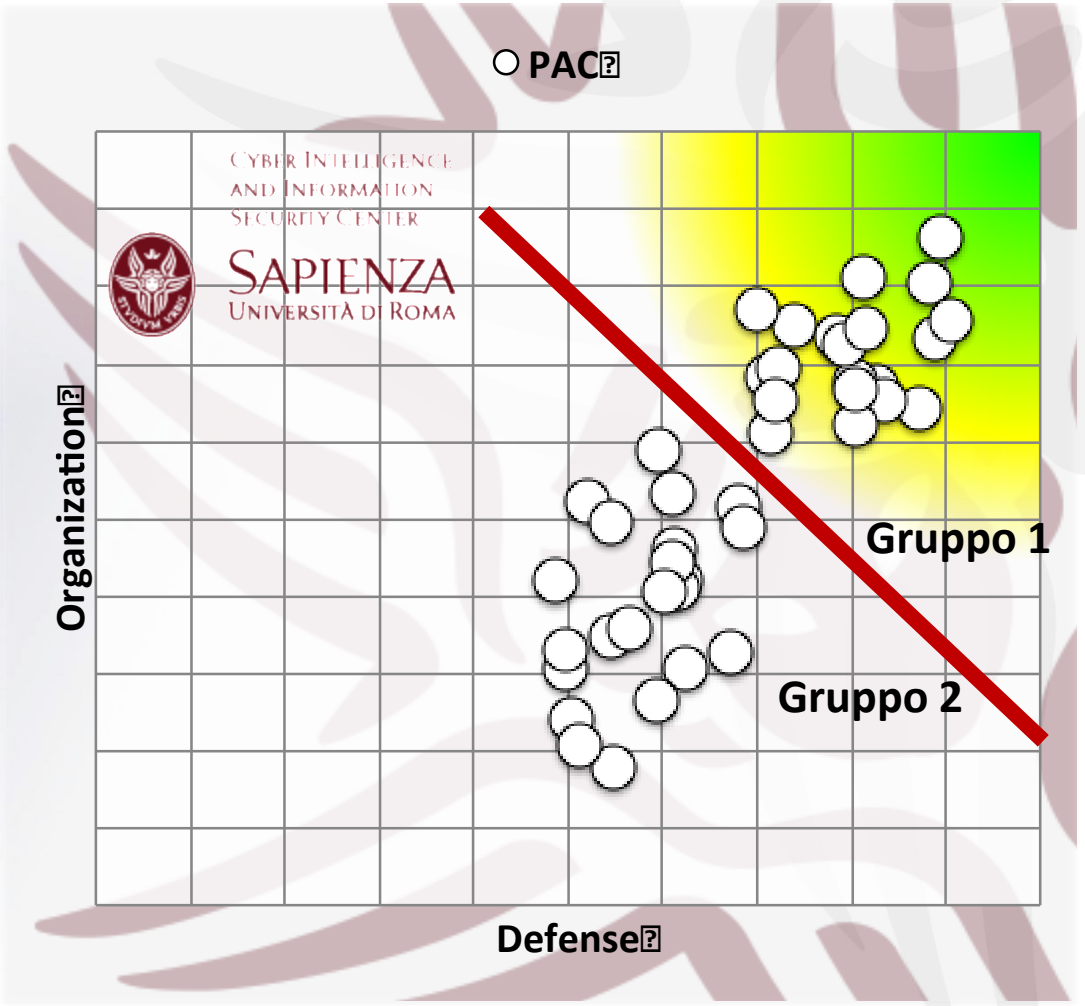
Pratiche Scorrette

- *No risk assessment*
- *No Piano di risposta ad un attacco*
- *No ISMS (Sistema di Gestione della sicurezza delle Informazioni)*
- *No Penetration Testing*
- *No gruppo per la gestione degli incidenti*
- *No verifiche periodiche org. e funz. Sicurezza ICT*
- *No Piano della Sicurezza ICT*
- *No parere di Agid su piani DR e BC*

Valuta la tua amministrazione

A breve disponibile sul sito web CIS il questionario on-line (segui @CIS_Sapienza per info)
www.cis.uniroma1.it

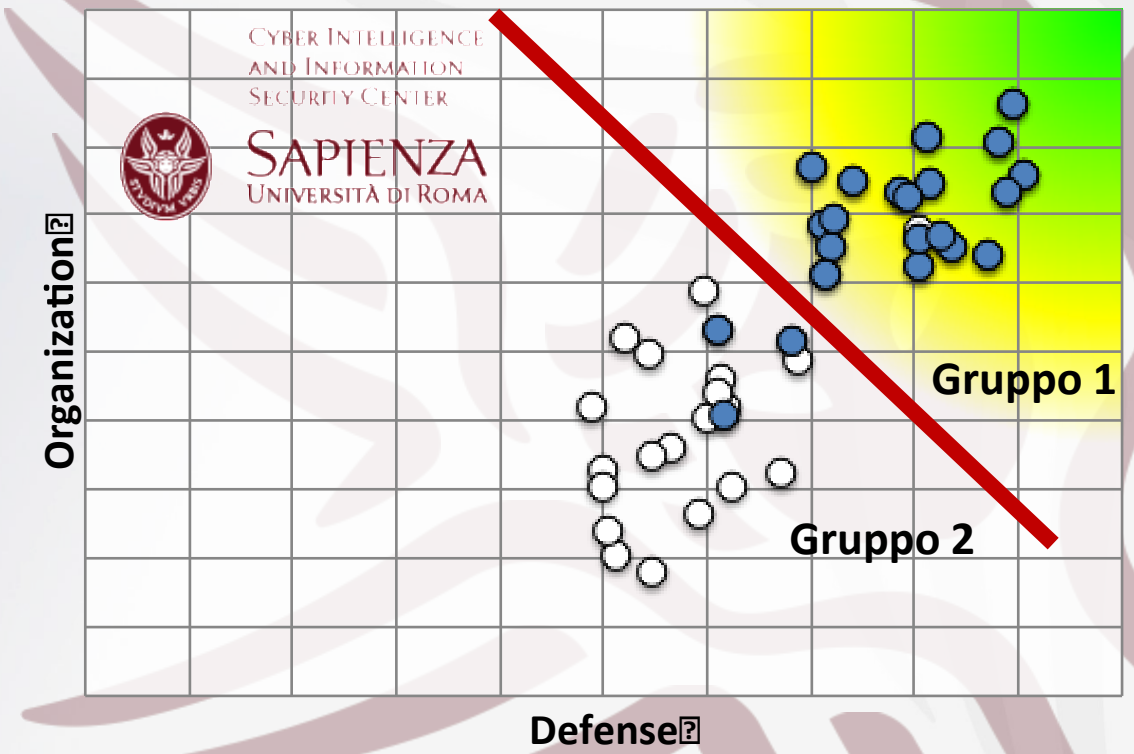
Pubbliche Amm. Centrali



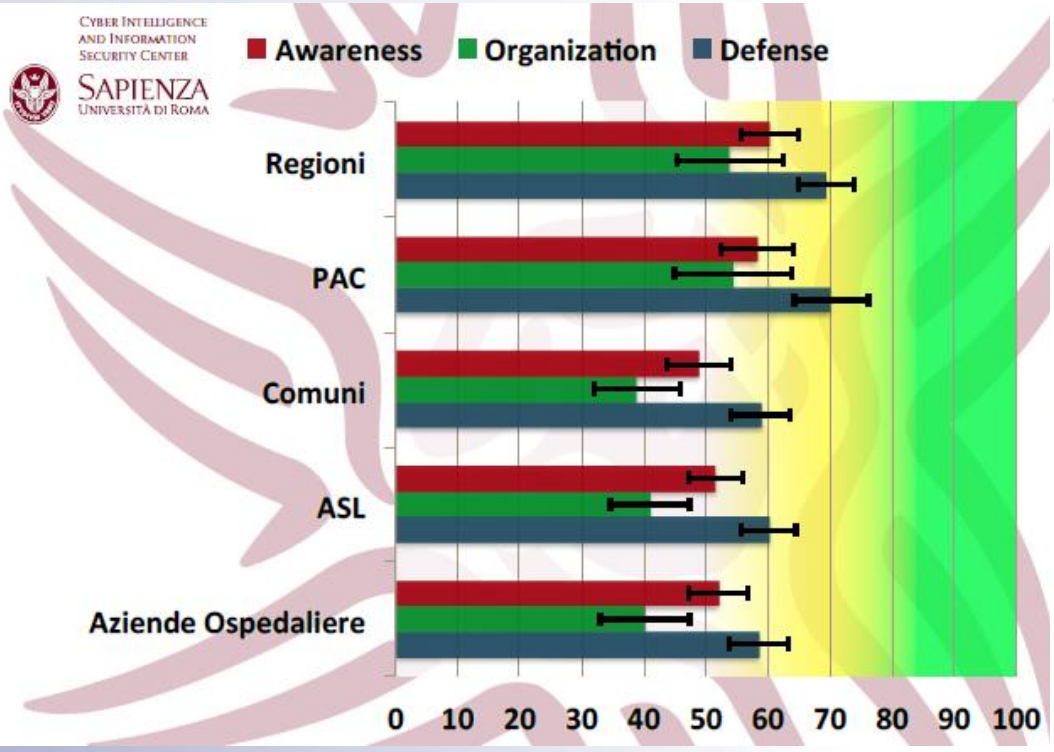
I due cluster nelle PAC

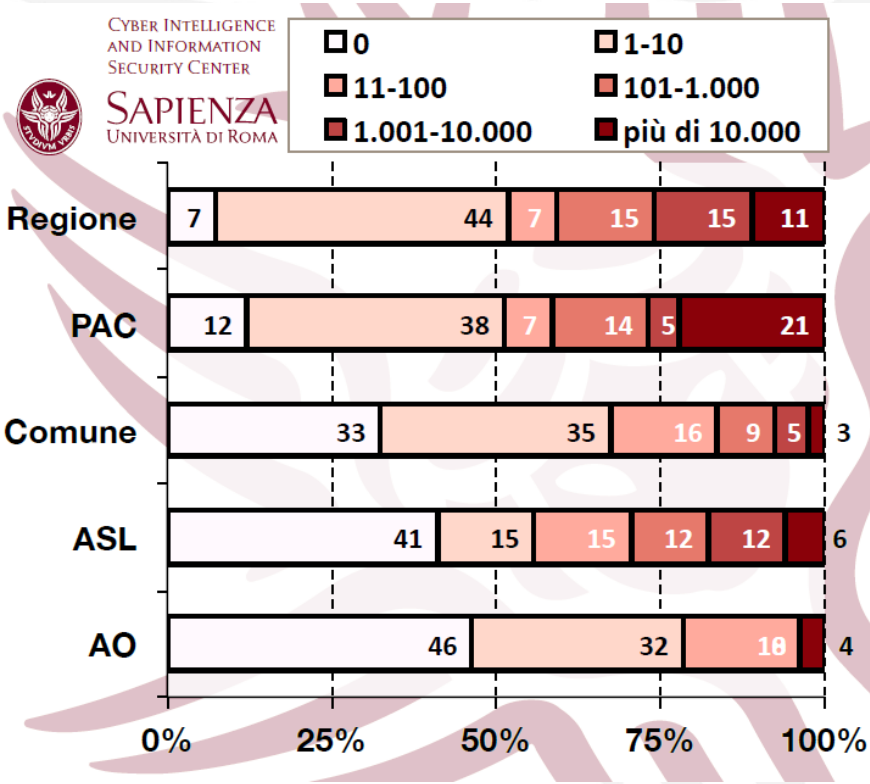
- PAC

- Risk Assessment, Vulnerability Assessment and Mitigation e Penetration testing



Attacchi alle PA





Razionalizzazione del patrimonio IT e sicurezza

Migliaia centri di spesa acquistano IT in Italia

Ridurre la superficie d'attacco

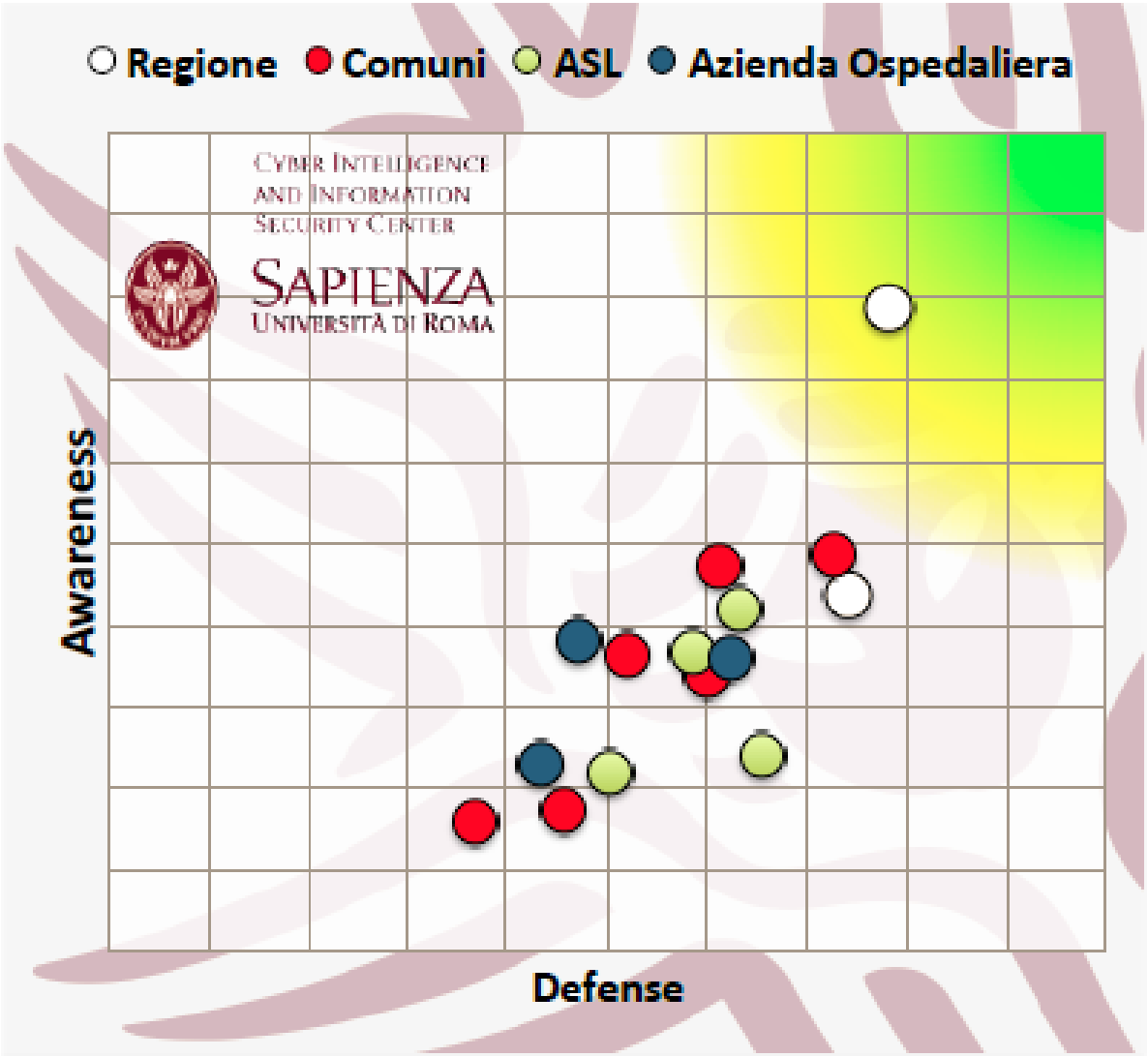
Migliaia
spesa ac
in Italia

Circa 430 CED per 214 amministrazioni

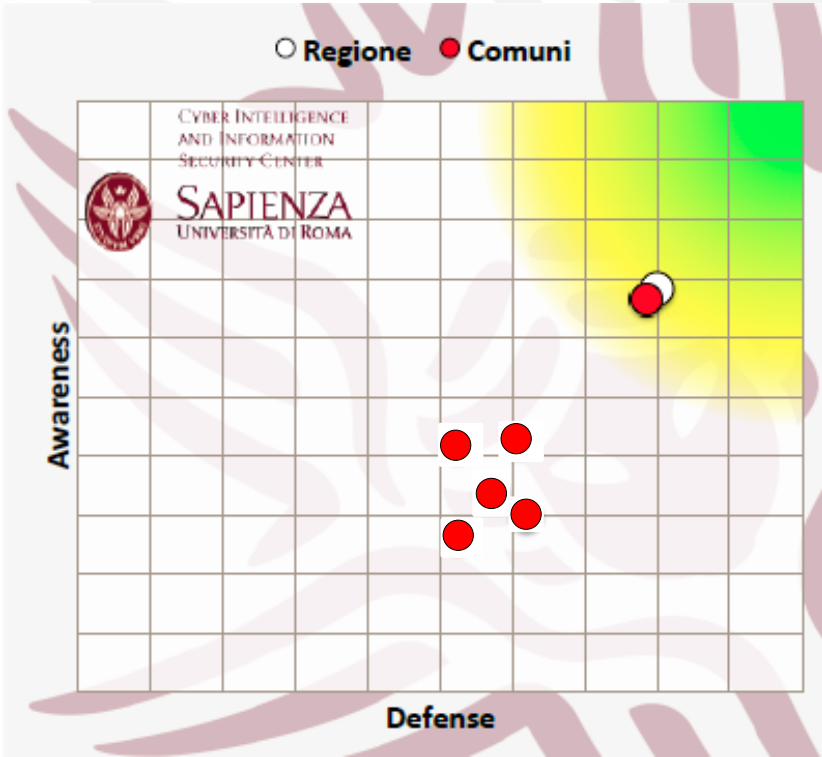
Domanda n.11: Selezionare il numero di Centri di Elaborazione Dati (CED o data center) della PA di riferimento

Ridurre la superficie d'attacco

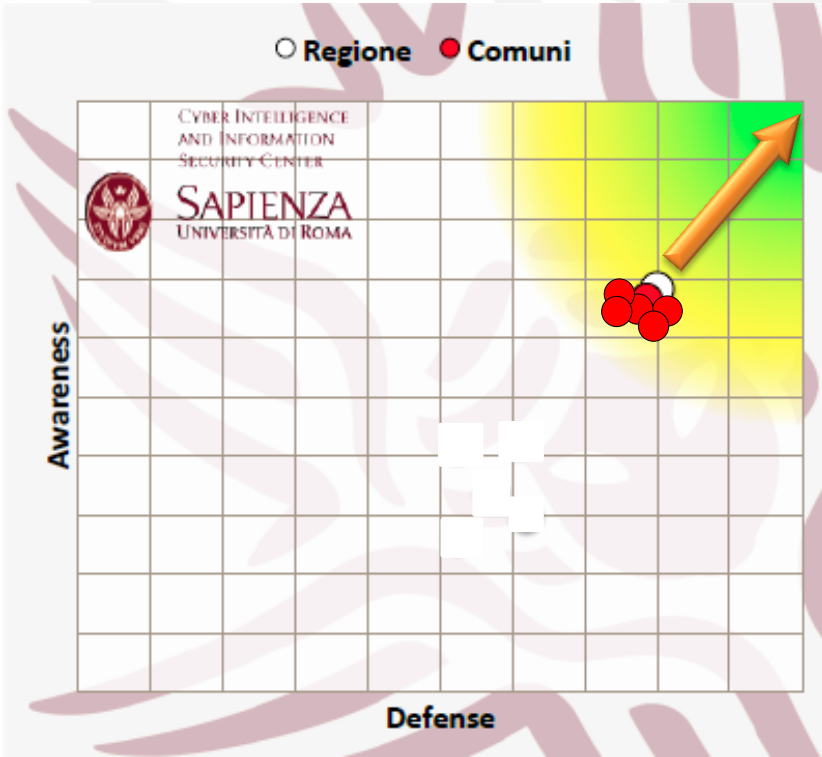
Regioni


Regione
Comuni
ASL
Azienda Ospedaliera
Cyber Intelligence and Information Security Center
Sapienza
Università di Roma
Awareness
Defense

Aggregazione delle amministrazioni su base geografica o di business



Aggregazione delle amministrazioni su base geografica o di business



Infrastruttura IT come asset strategico nazionale

Datacenter pochi e protetti

Riduzione della spesa

Senza lilli non si lalla

Investimenti!

Cloud “made in Italy” e volano economico per piccole e medie imprese

Una infrastruttura IT con buchi di sicurezza, renderà il sistema Italia meno attraente a qualsiasi tipo di investimento

Capacità cyber avanzate e prosperità economica sono un binomio inscindibile in una nazione sviluppata

Visione Strategica della Agenda Digitale per il sistema paese

Cambiamolo questo paese!