CiberSeguridad

Telefónica
2013

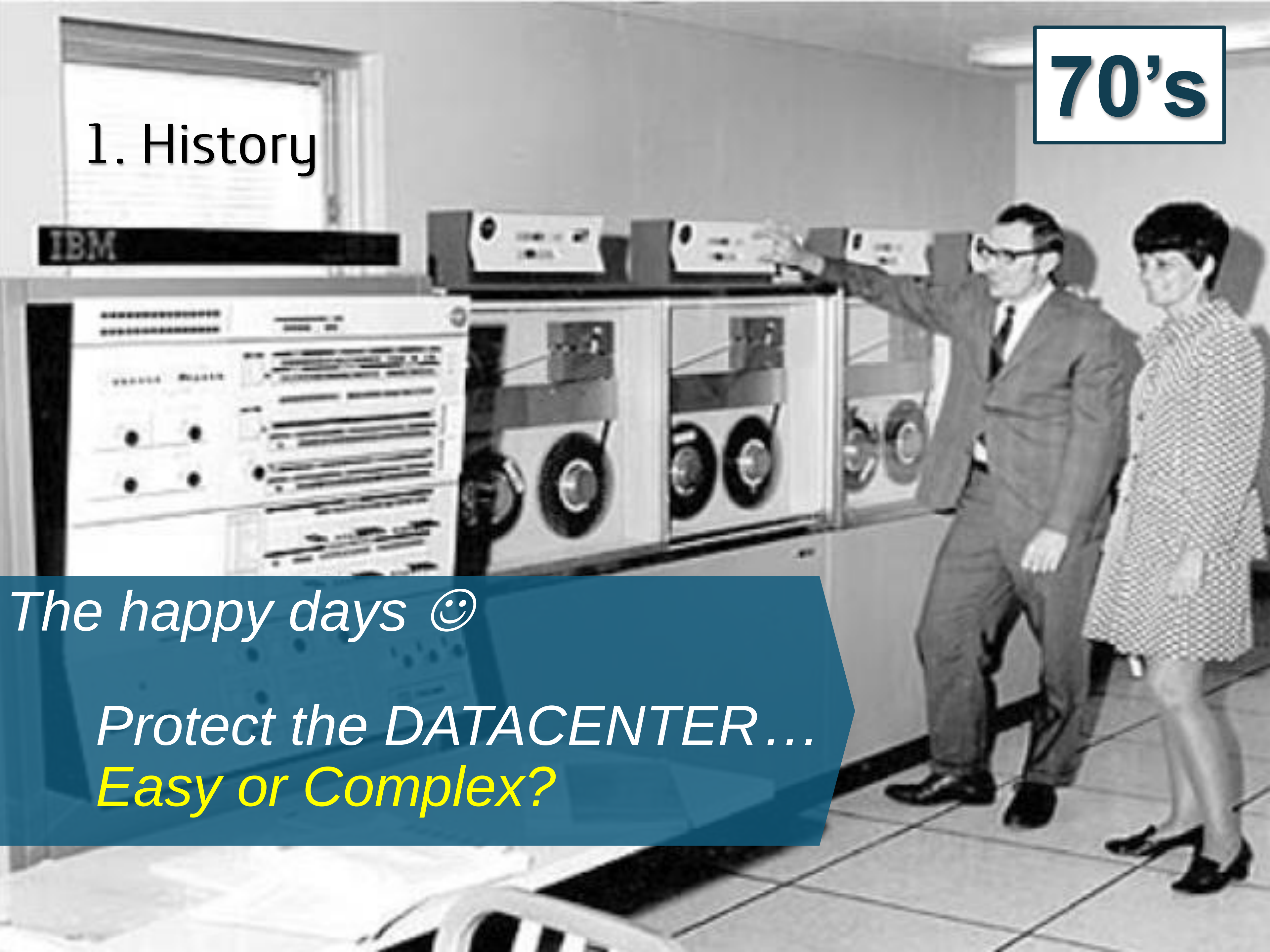
Index

1. History
2. New Challenges
3. CBS: Threat Prevention
4. CBS: Continuous Pentesting

Telefónica

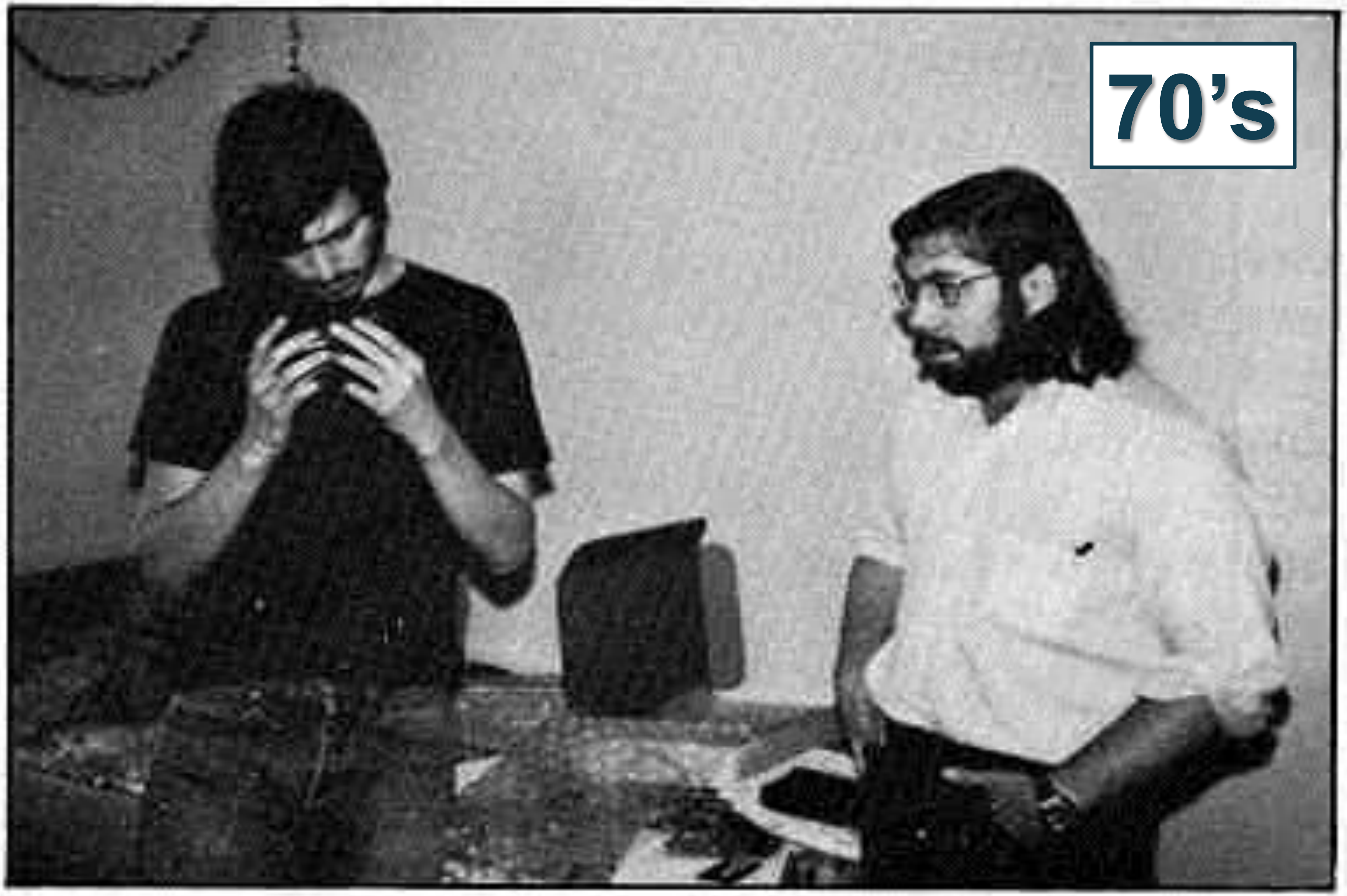
1. History

70’s



The happy days ☺

Protect the DATACENTER…
Easy or Complex?



70's

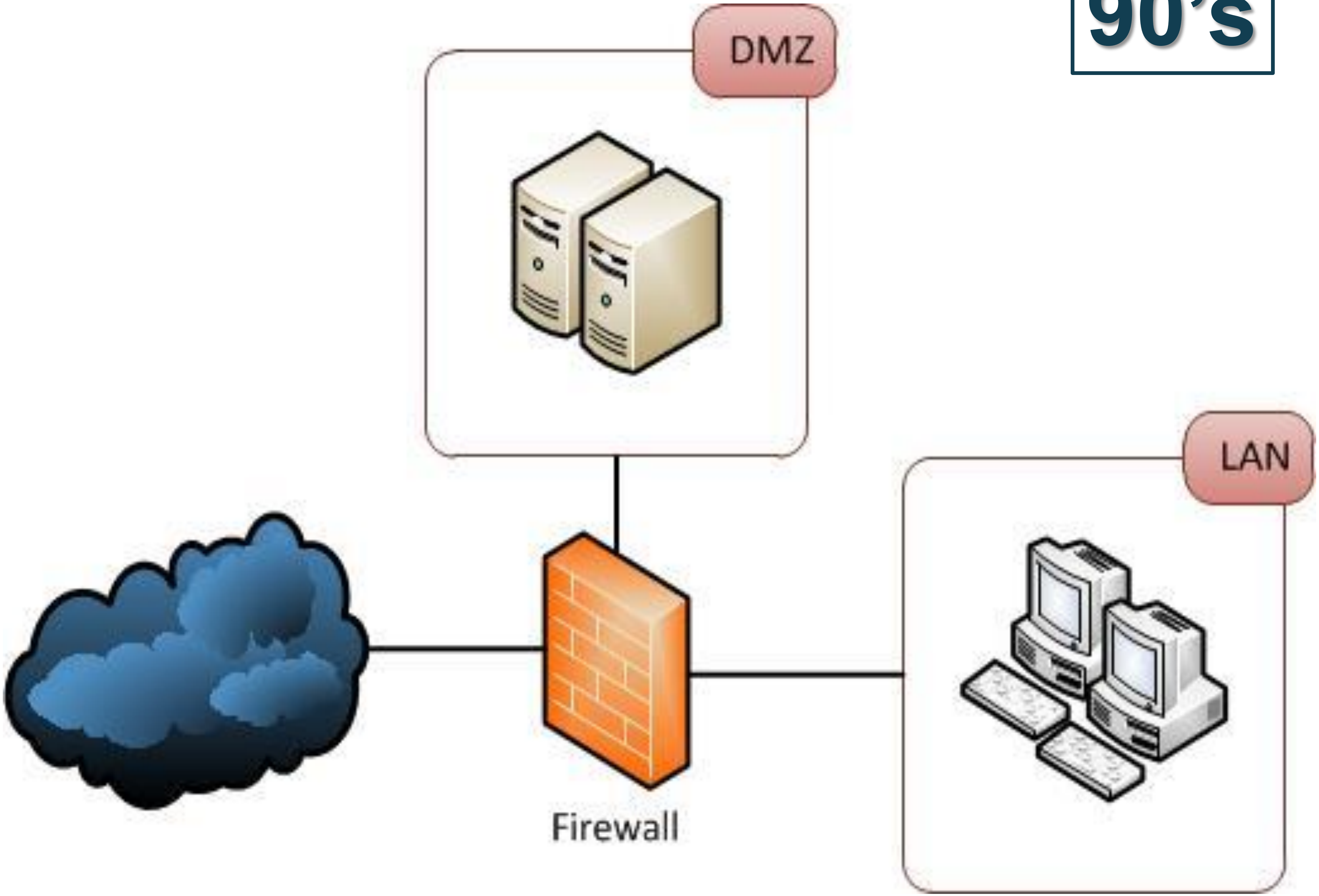
Better laughter through electronics: Steven Jobs (left) and Stephen Wozniak examine their latest creation.

80’s

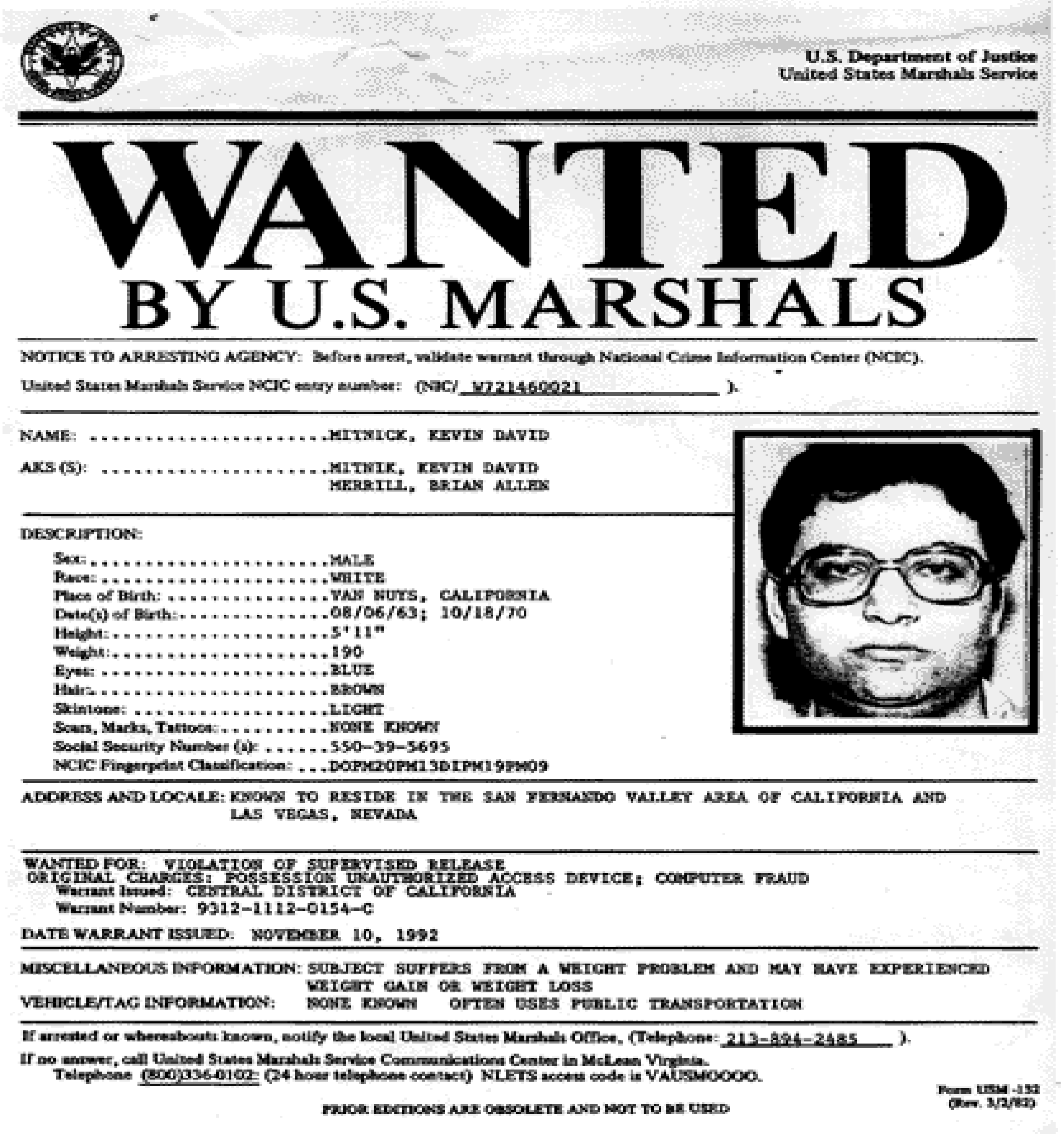
80’s

80’s

90’s



90's



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

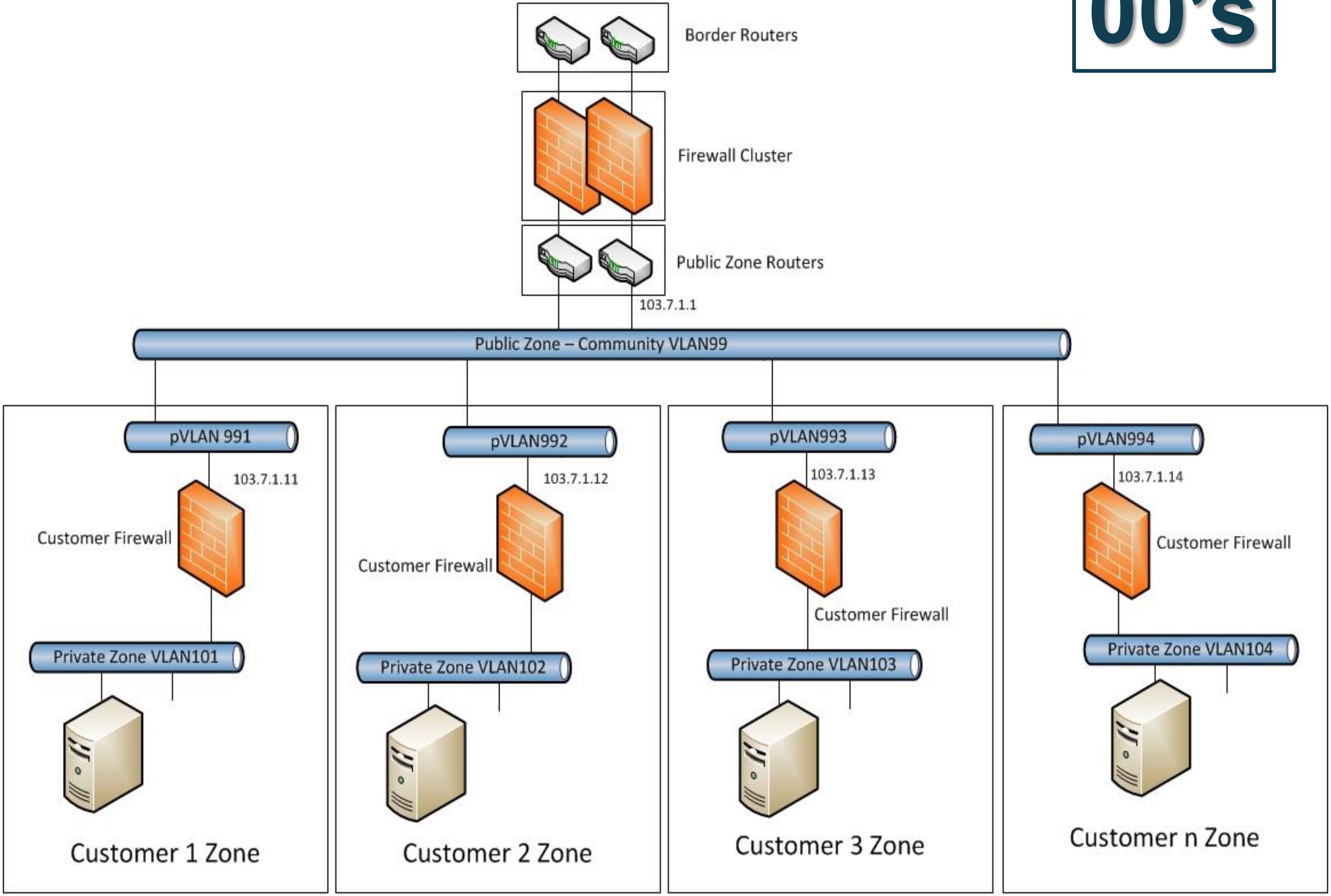
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSMOOOO.

Form USM -132
(Rev. 3/2/82)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

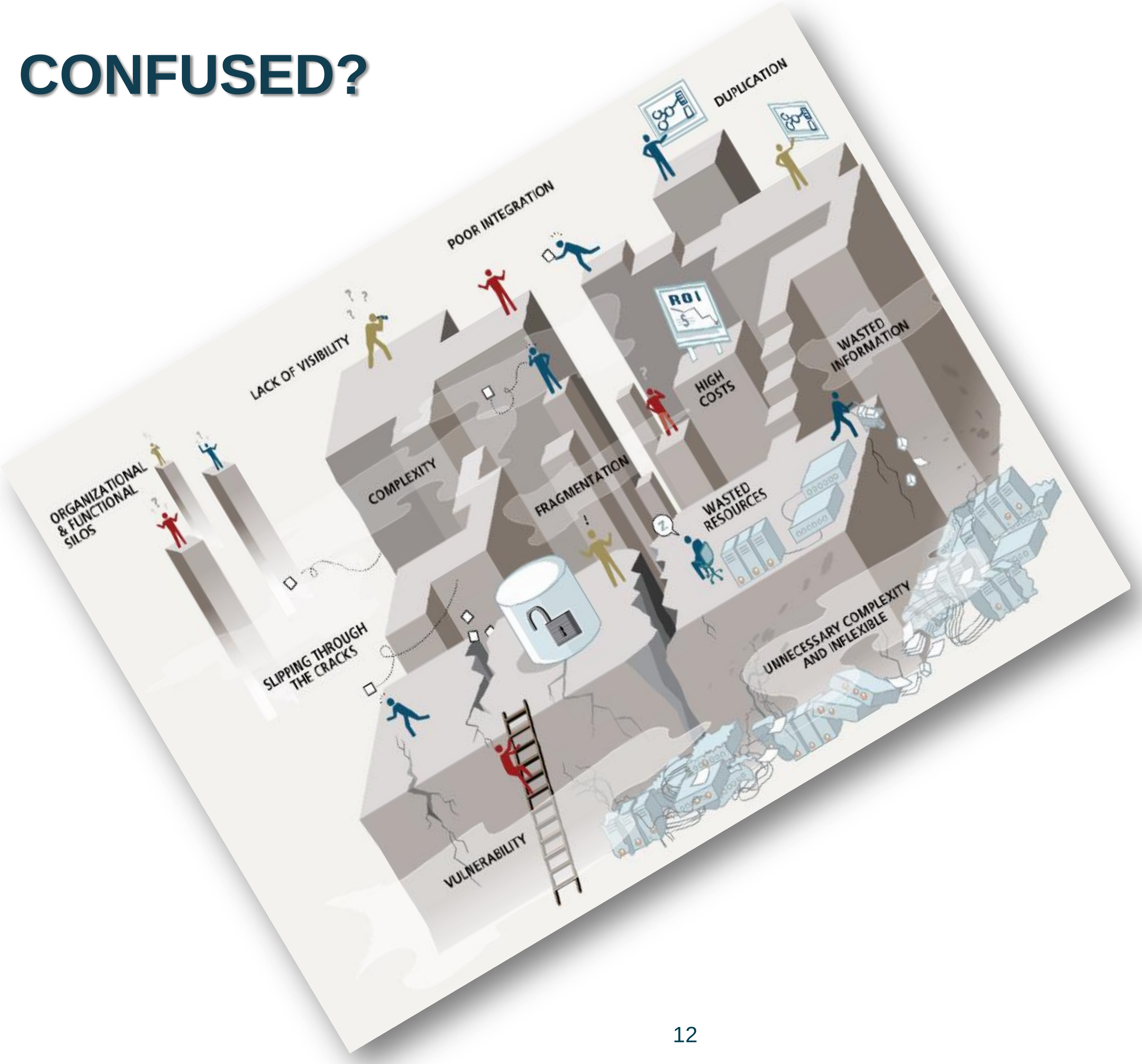
00's



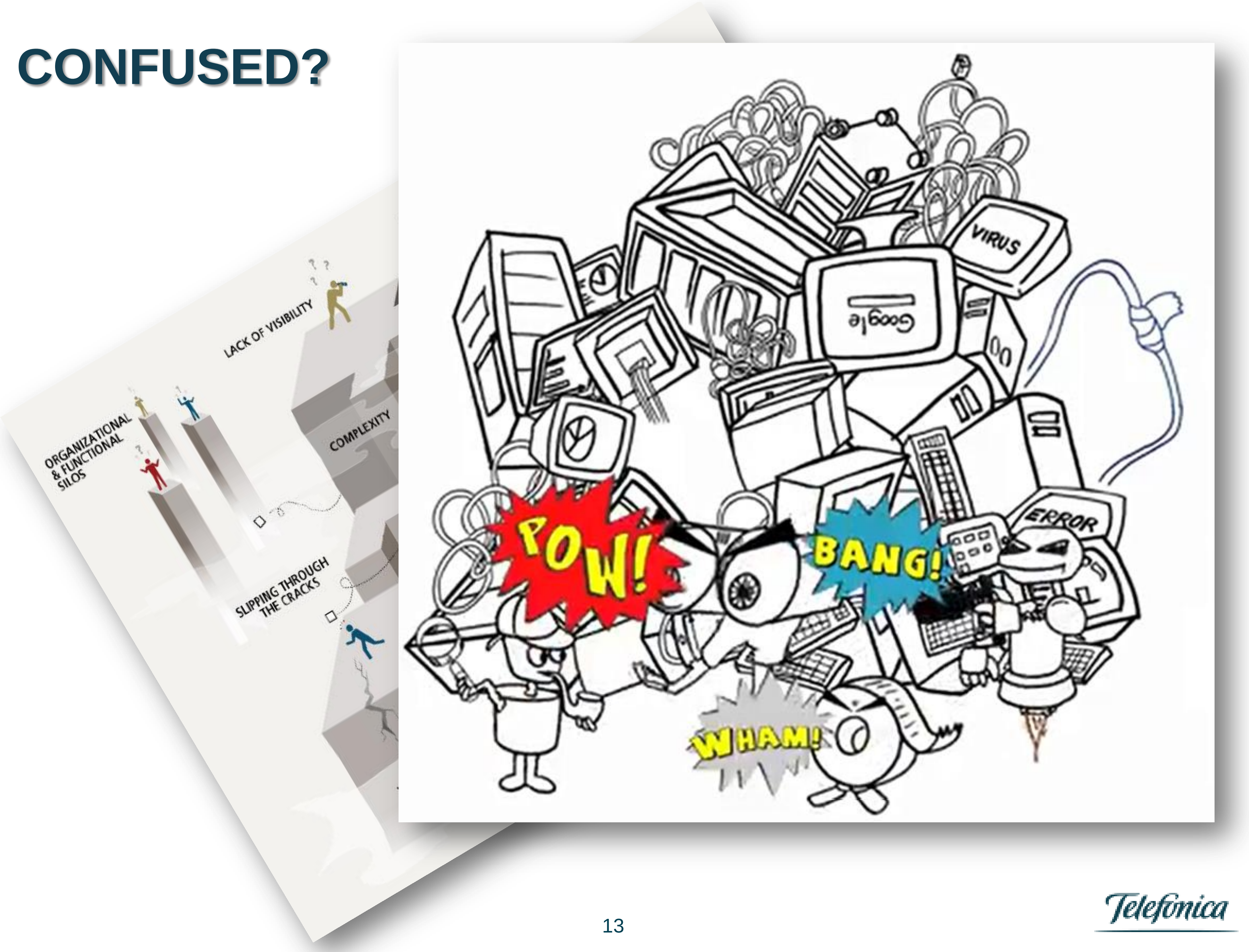
Border Routers
Firewall Cluster
Public Zone Routers
103.7.1.1
Public Zone – Community VLAN99
pVLAN 991
103.7.1.11
Customer Firewall
Private Zone VLAN101
Customer 1 Zone
pVLAN992
103.7.1.12
Customer Firewall
Private Zone VLAN102
Customer 2 Zone
pVLAN993
103.7.1.13
Customer Firewall
Private Zone VLAN103
Customer 3 Zone
pVLAN994
103.7.1.14
Customer Firewall
Private Zone VLAN104
Customer n Zone

00’s

CONFUSED?

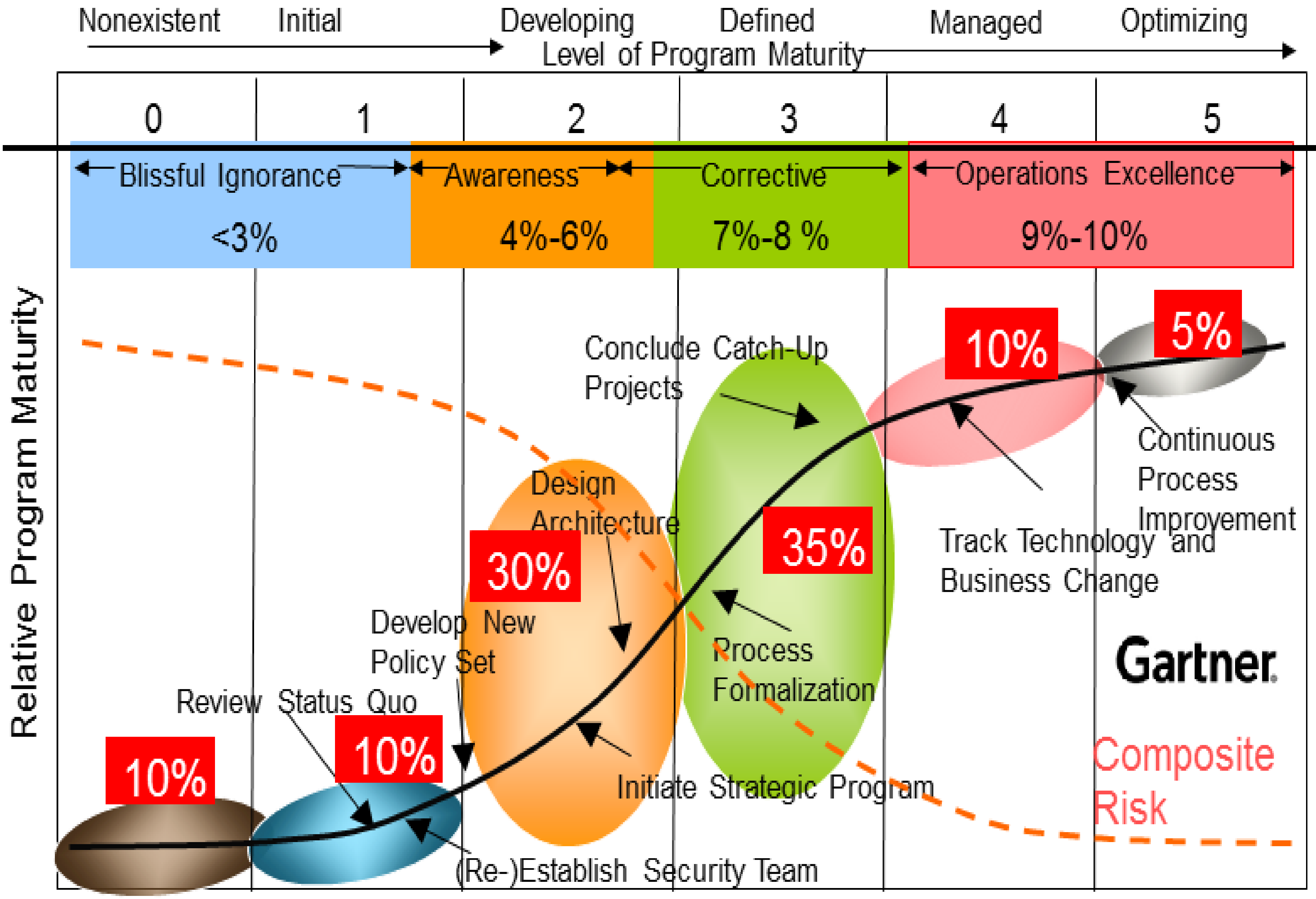

DUPLICATION
POOR INTEGRATION
LACK OF VISIBILITY
ROI
HIGH COSTS
WASTED INFORMATION
ORGANIZATIONAL & FUNCTIONAL SILOS
COMPLEXITY
FRAGMENTATION
WASTED RESOURCES
SLIPPING THROUGH THE CRACKS
UNNECESSARY COMPLEXITY AND INFLEXIBLE
VULNERABILITY

CONFUSED?


LACK OF VISIBILITY
ORGANIZATIONAL & FUNCTIONAL SILOS
COMPLEXITY
SLIPPING THROUGH THE CRACKS
VIRUS
Google
ERROR
POW!
BANG!
WHAM!

CONFUSED?

CONFUSED?


Nonexistent
Initial
Developing
Defined
Managed
Optimizing
Level of Program Maturity
0
1
2
3
4
5
Blissful Ignorance
<3%
Awareness
4%-6%
Corrective
7%-8 %
Operations Excellence
9%-10%
Relative Program Maturity
Conclude Catch-Up Projects
10%
5%
Continuous Process Improvement
Design Architecture
30%
35%
Track Technology and Business Change
Develop New Policy Set
Process Formalization
Review Status Quo
10%
10%
Initiate Strategic Program
(Re-)Establish Security Team
Gartner
Composite Risk

2. New Challenges

1

Companies and information

The leaky corporation

Digital information is easy not only to store but also to leak. Companies must decide what they really need to keep secret, and how best to do so

Feb 24th 2011 | from the print edition

Is already happening…

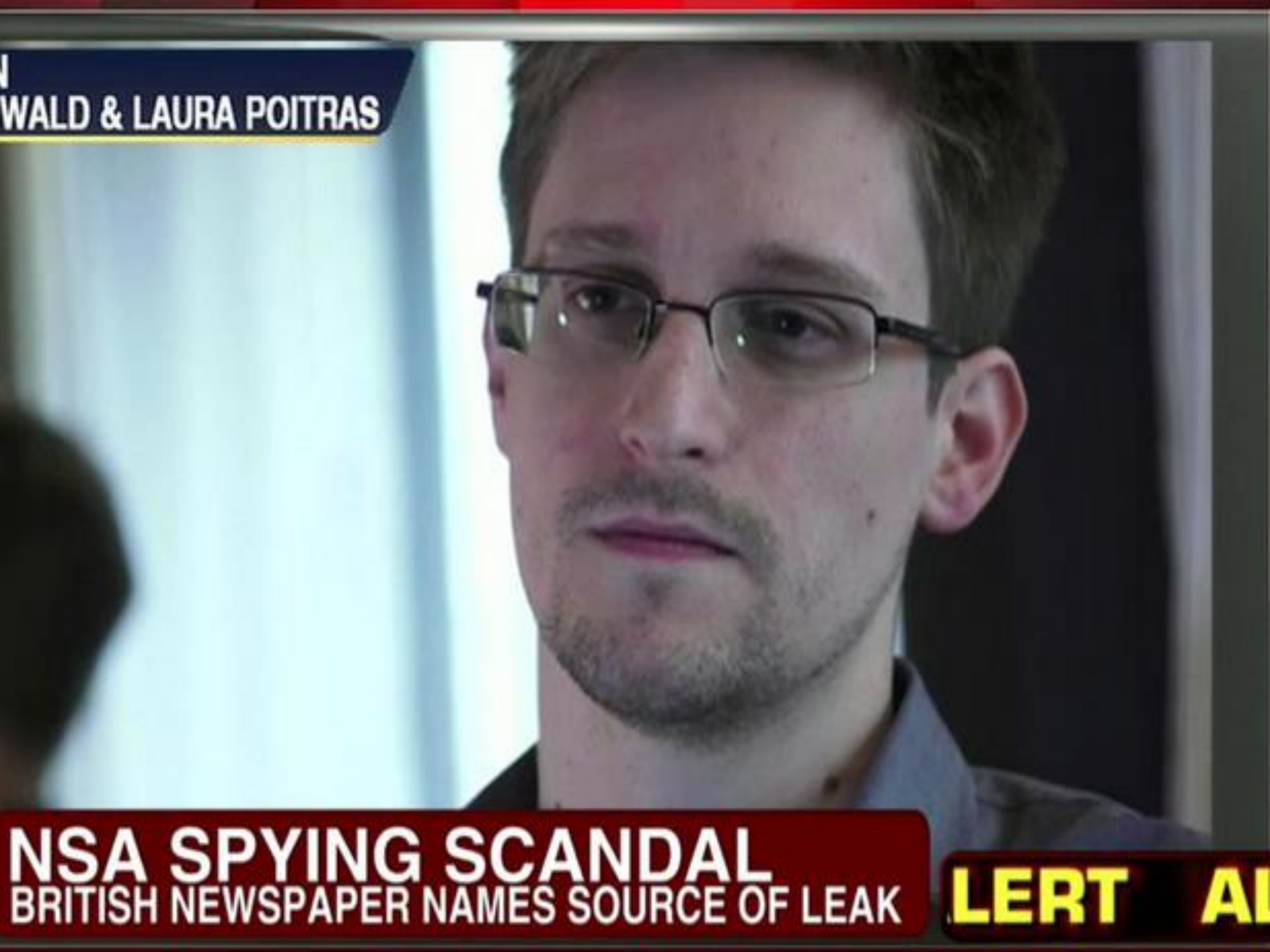
The 2012 combined dataset represents the largest we have ever covered in any single year, spanning 47,000+ reported security incidents, 621 confirmed data disclosures, and at least 44 million compromised records

VERIZON 2013 DataBreach Report

WANTED

BY THE FBI

ANONYMOUS


N
WALD & LAURA POITRAS
NSA SPYING SCANDAL
BRITISH NEWSPAPER NAMES SOURCE OF LEAK
LERT AL

TIME

THE INFORMERS

WHY A NEW GENERATION OF HACKTIVISTS IS DRIVEN TO SPILL THE GOVERNMENT'S SECRETS

BY MICHAEL SCHERER

Aaron Swartz
Bradley Manning

“A picture of your DATACENTER Today”

The Endless Datacenter

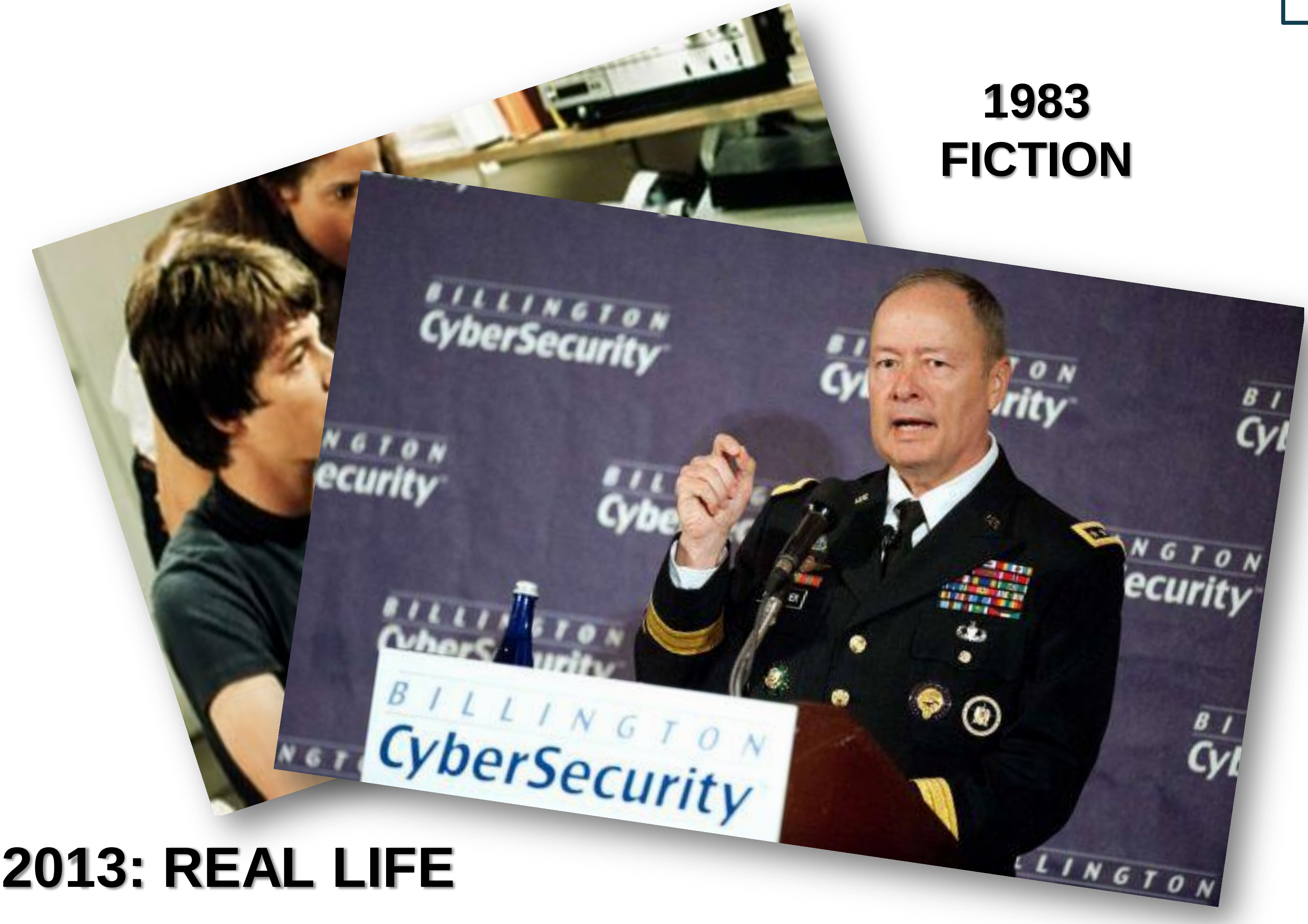
4

“Wild Wild West 3.0”

The Internet Landscape

FROM … TO …

5

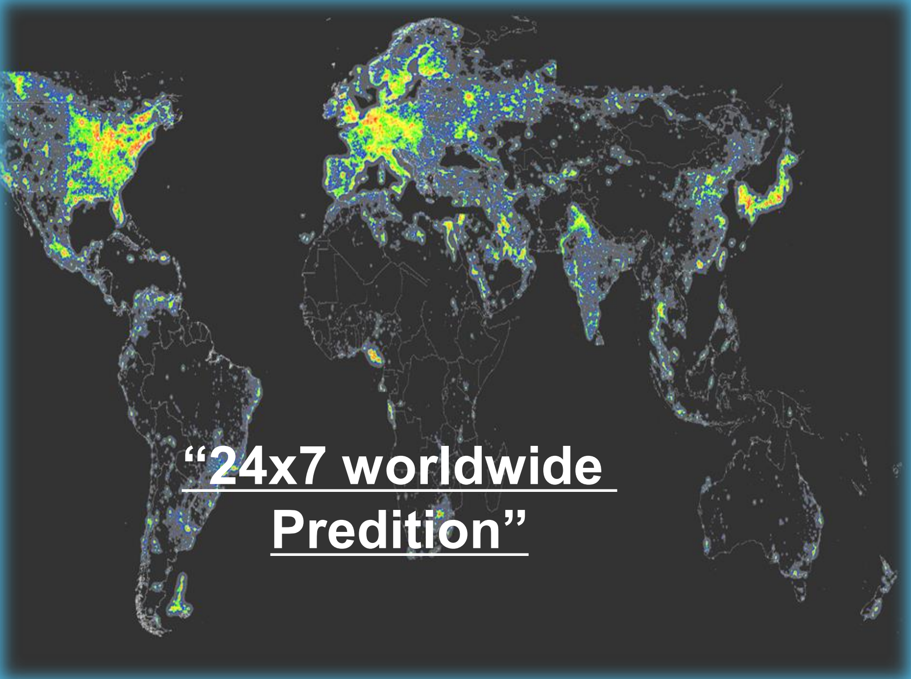


1983
FICTION

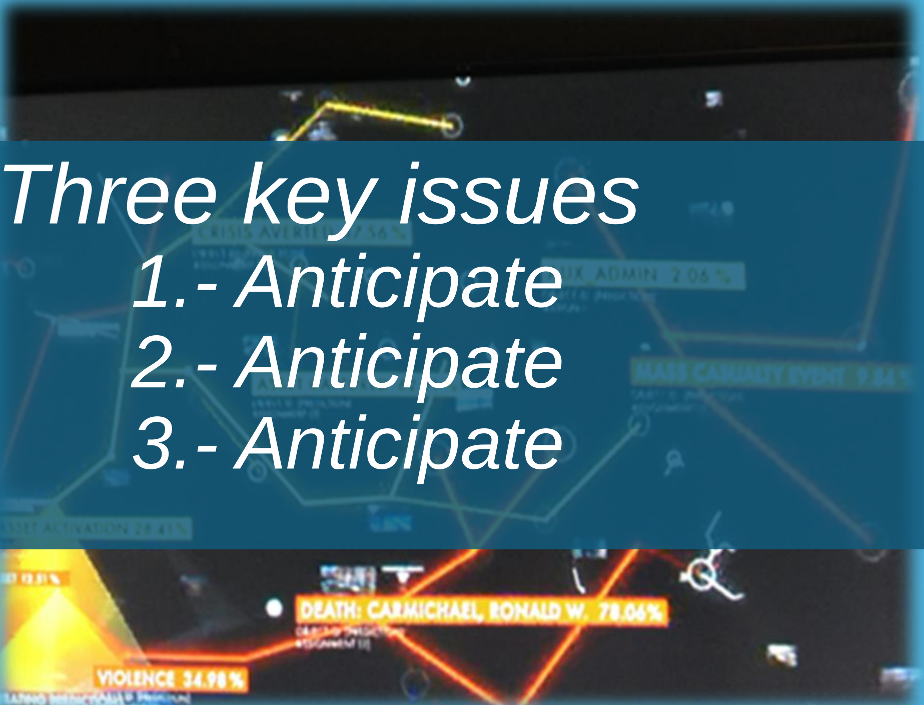
2013: REAL LIFE

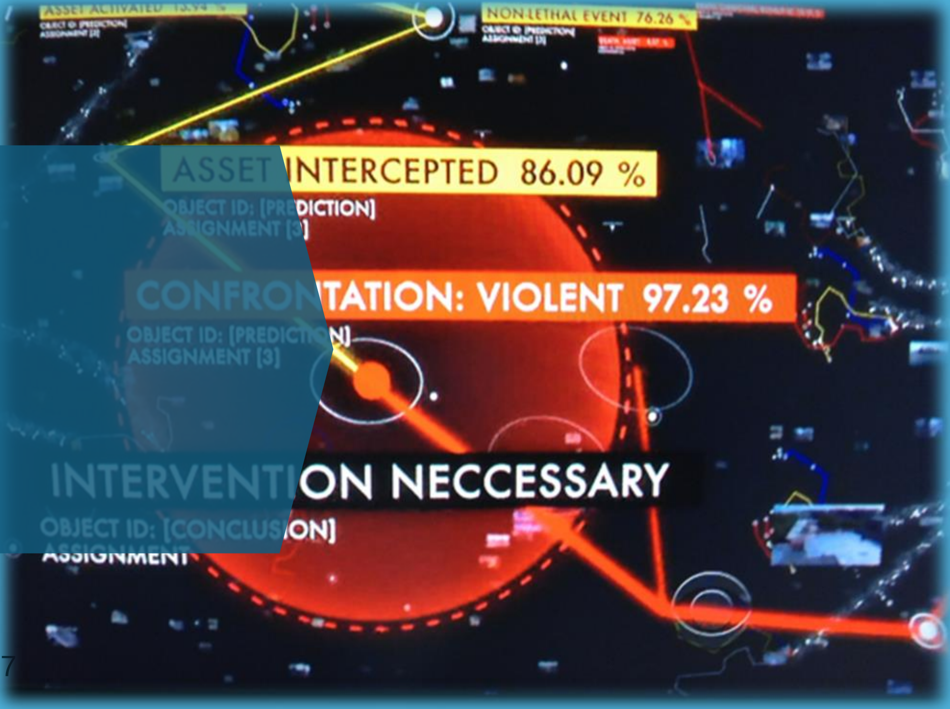
Index

1. History
2. New Challenges
3. CBS: Threat Prevention
4. CBS: Continuous Pentesting



“24x7 worldwide Predition”





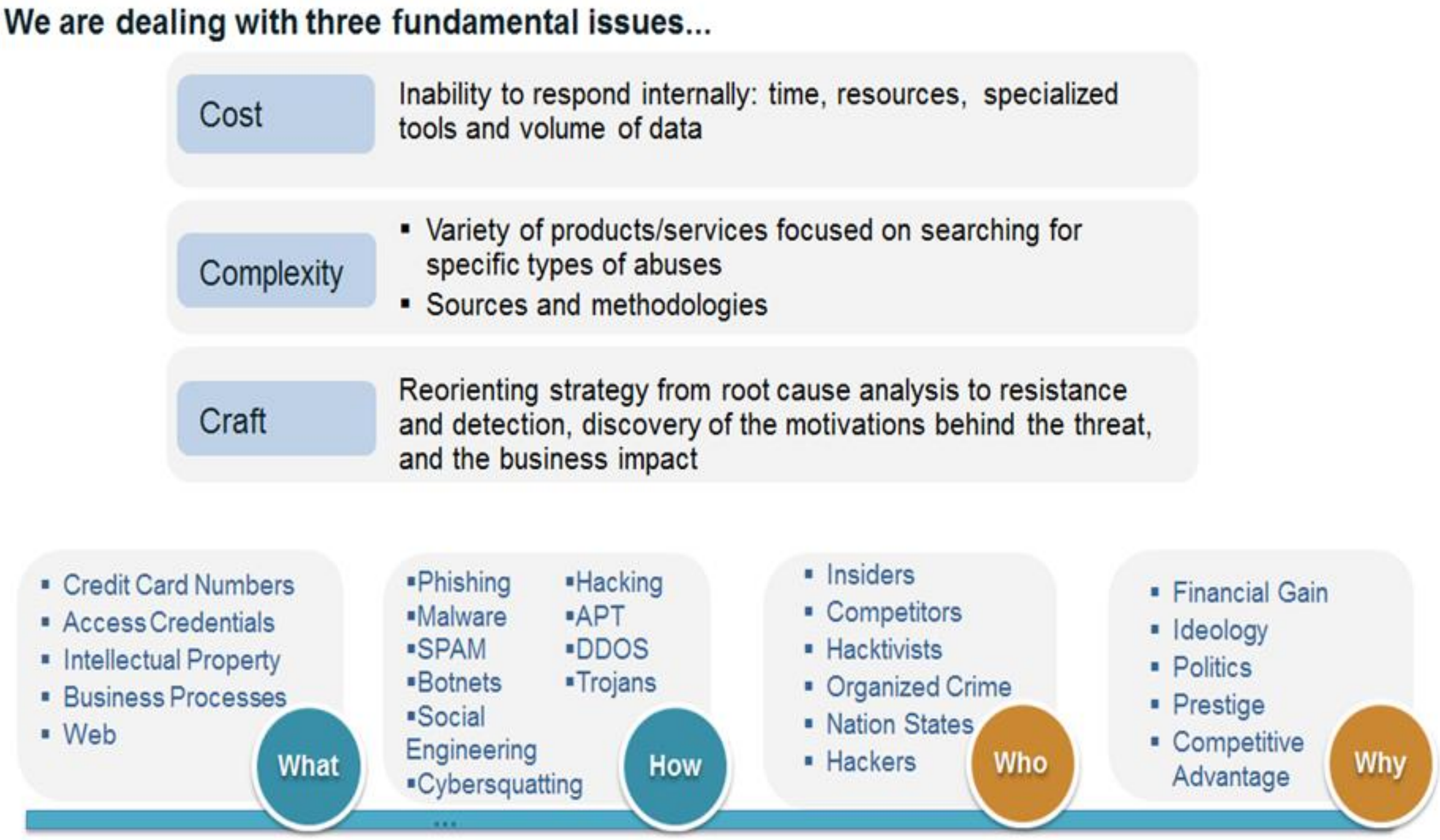
Three key issues

1.- Anticipate

2.- Anticipate

3.- Anticipate

CYBER DETECT: Threats



We are dealing with three fundamental issues...

Cost: Inability to respond internally: time, resources, specialized tools and volume of data

Complexity:
- Variety of products/services focused on searching for specific types of abuses
- Sources and methodologies

Craft: Reorienting strategy from root cause analysis to resistance and detection, discovery of the motivations behind the threat, and the business impact

What
- Credit Card Numbers
- Access Credentials
- Intellectual Property
- Business Processes
- Web

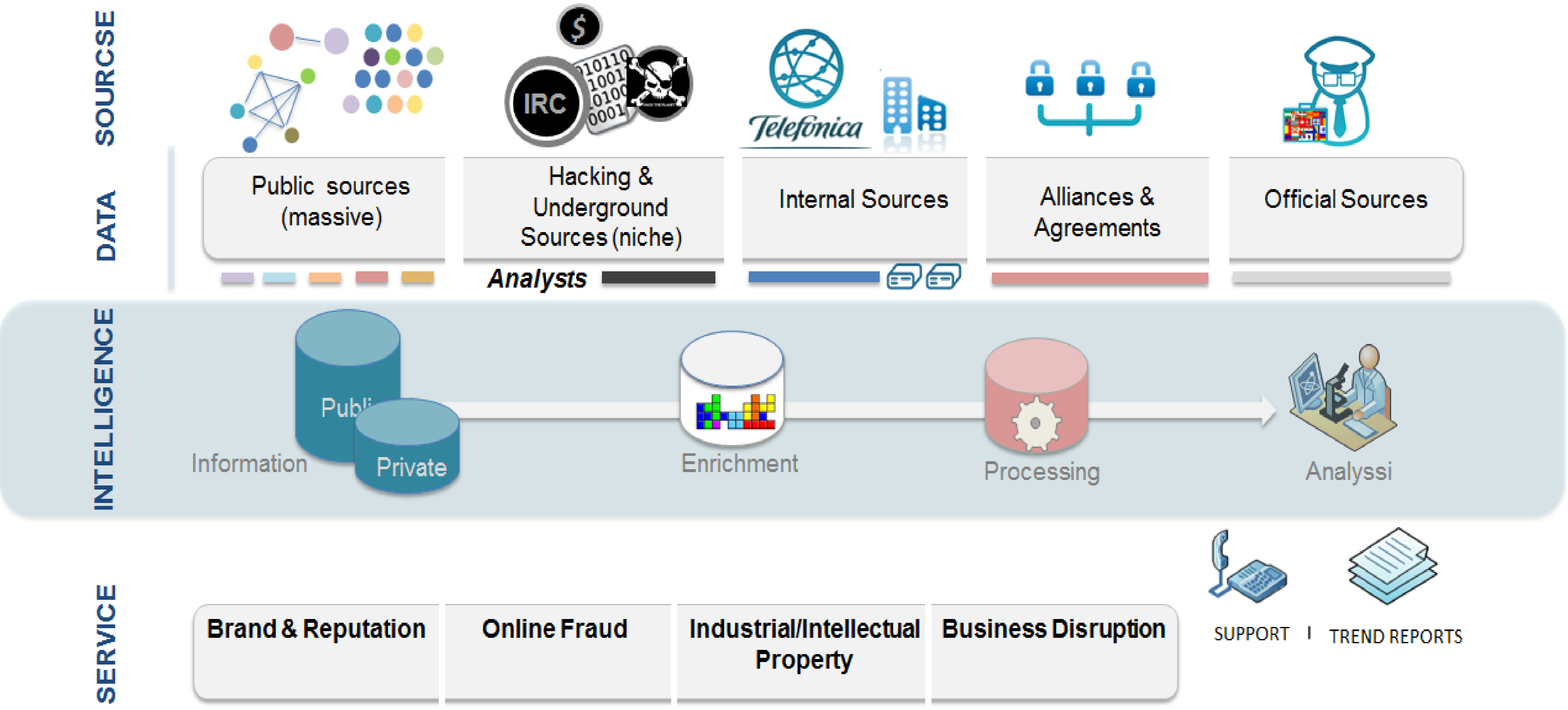
How
- Phishing
- Malware
- SPAM
- Botnets
- Social Engineering
- Cybersquatting
- Hacking
- APT
- DDOS
- Trojans

Who
- Insiders
- Competitors
- Hacktivists
- Organized Crime
- Nation States
- Hackers

Why
- Financial Gain
- Ideology
- Politics
- Prestige
- Competitive Advantage

...

CYBER DETECT: Threats



SOURCSE

DATA

Public sources (massive)

Hacking & Underground Sources (niche)

Internal Sources

Alliances & Agreements

Official Sources

Analysts

INTELLIGENCE

Information

Publi

Private

Enrichment

Processing

Analyssi

SERVICE

Brand & Reputation

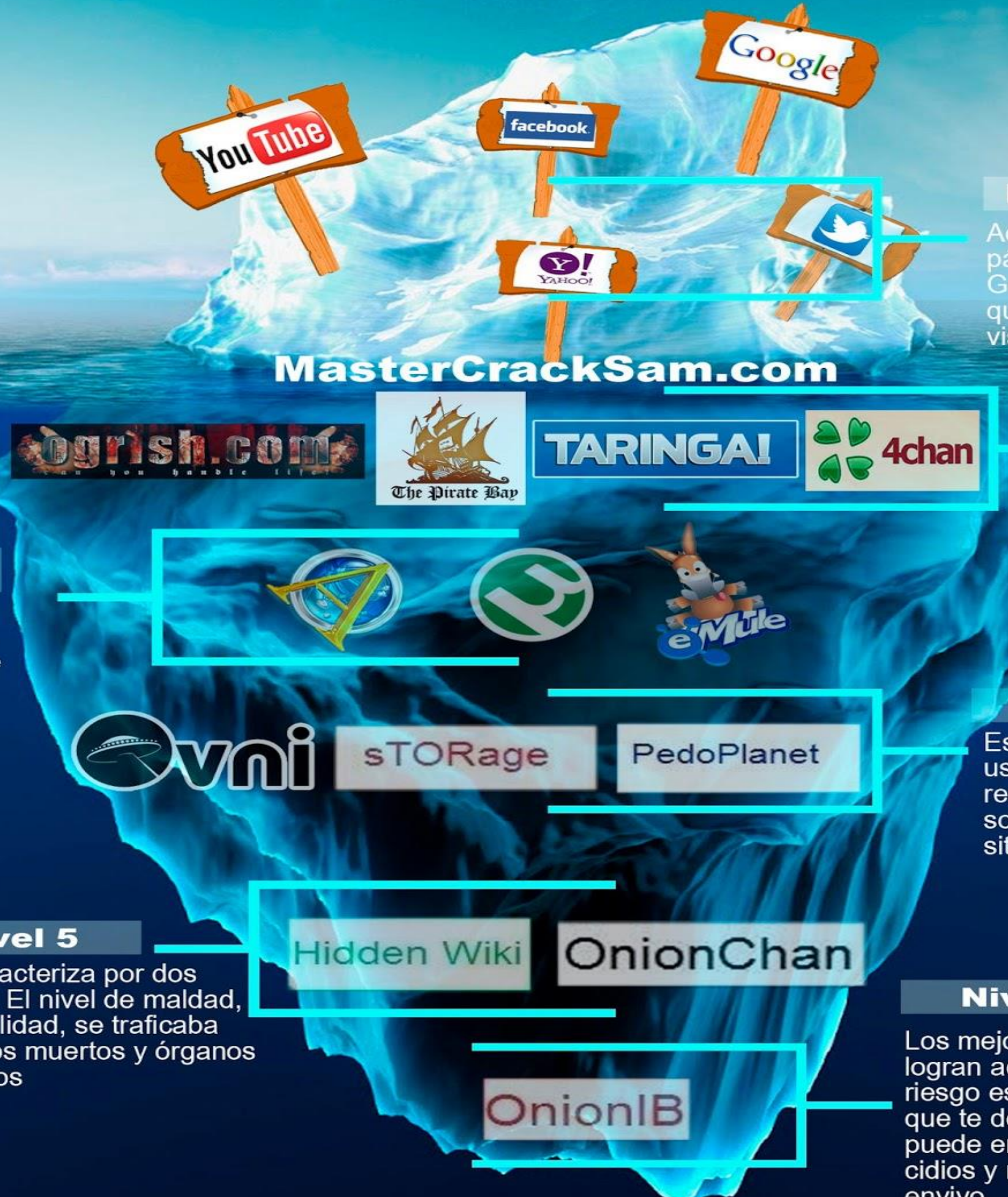
Online Fraud

Industrial/Intellectual Property

Business Disruption

SUPPORT I TREND REPORTS

LA DEEP WEB
LA WEB PROFUNDA



Nivel 1

Aquí estamos nosotros páginas comunes, Google o Facebook que estan en el mundo visible de la internet

Nivel 2

Entramos resultados que Google ha suprimido, paginas con H0neypots, Pornografía, Freehive, canales como 4Chan y Video Stream.

Nivel 3

Los usuarios rosan lo ilegal usando programas como Ares,Utorrent, este nivel ya se encuentra dentro del Deep Web.

Nivel 4

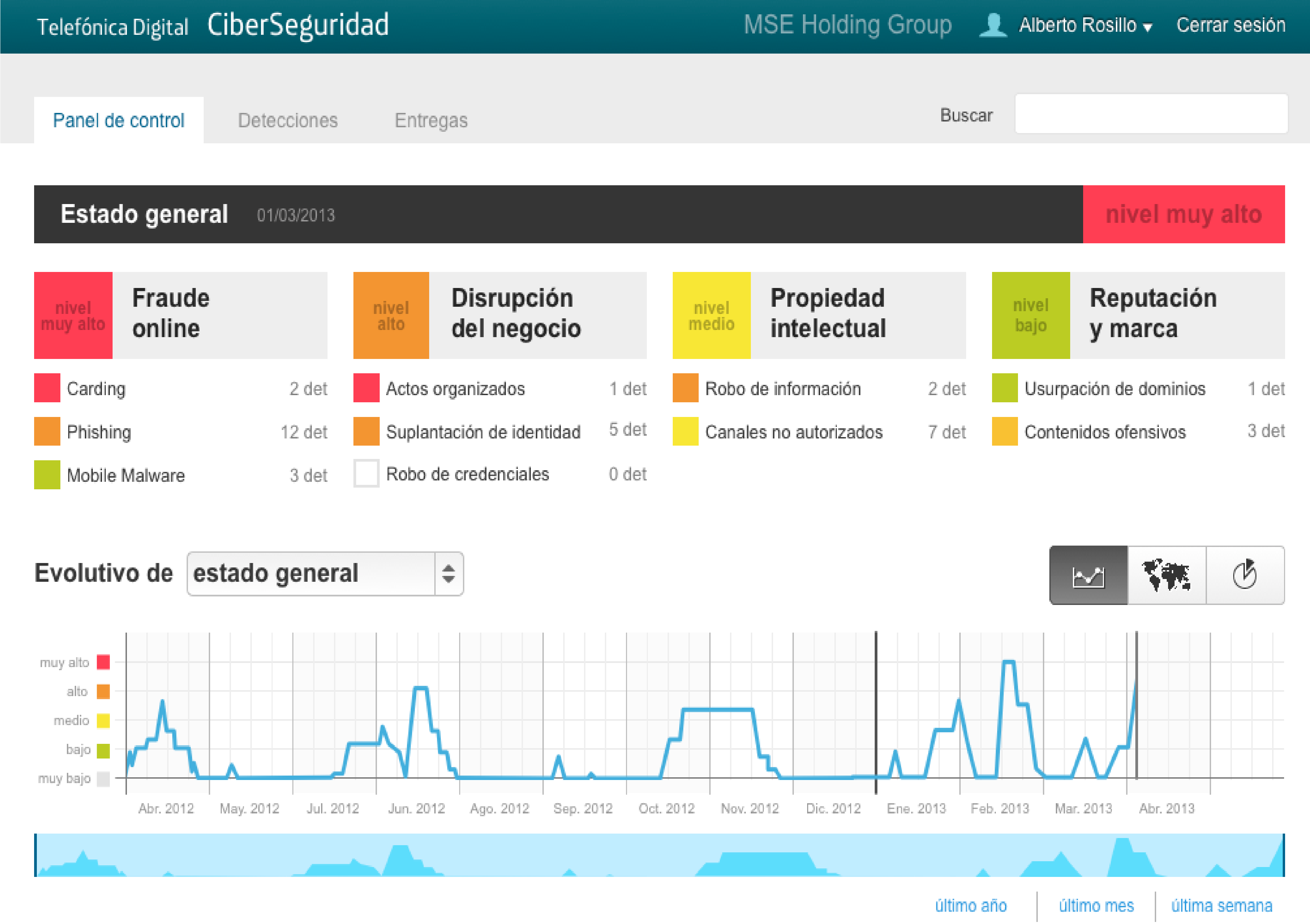
Es un nivel peligroso si el usuario es detectado, puede recibir años de cárcel por el solo hecho de estar en estos sitios con Pornografía infantil.

Nivel 5

Se caracteriza por dos cosas: El nivel de maldad, o ilegalidad, se traficaba cuerpos muertos y órganos de niños

Nivel 6

Los mejores hackers logran acceder el riesgo es muy alto a que te descubran se puede encontrar suicidios y muertes envivo



Telefónica Digital CiberSeguridad

MSE Holding Group

Alberto Rosillo ▾ Cerrar sesión

Panel de control | Detecciones | Entregas

Buscar

Estado general 01/03/2013

nivel muy alto

nivel muy alto	**Fraude online**
🟥 Carding	2 det
🟧 Phishing	12 det
🟩 Mobile Malware	3 det

nivel alto	**Disrupción del negocio**
🟥 Actos organizados	1 det
🟧 Suplantación de identidad	5 det
□ Robo de credenciales	0 det

nivel medio	**Propiedad intelectual**
🟧 Robo de información	2 det
🟨 Canales no autorizados	7 det

nivel bajo	**Reputación y marca**
🟩 Usurpación de dominios	1 det
🟨 Contenidos ofensivos	3 det

Evolutivo de estado general

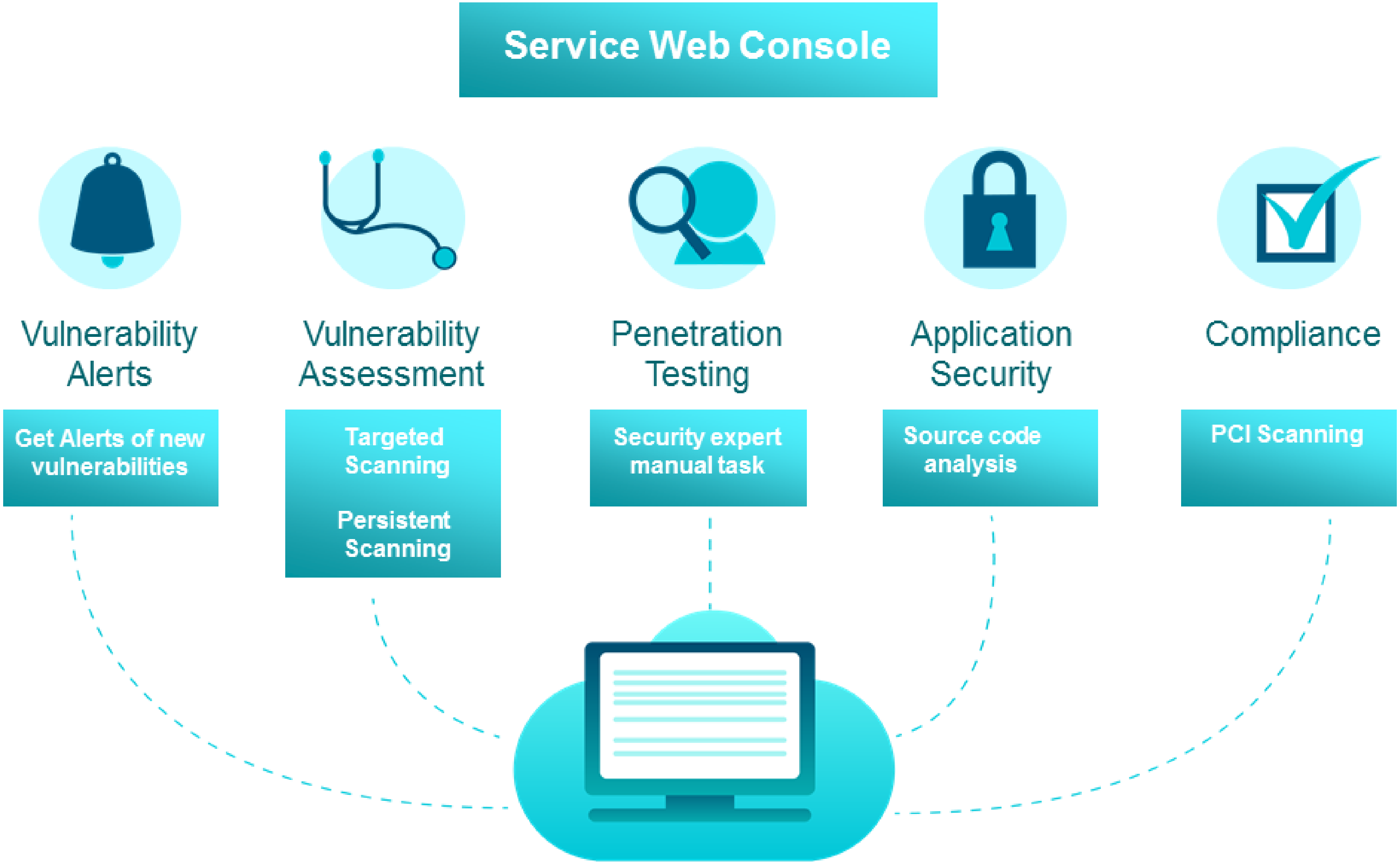
último año | último mes | última semana

Index

1. History
2. New Challenges
3. CBS: Threat Prevention
4. CBS: Continuous Pentesting

Why do we think that “the bad guys” will be targeting us when we are prepared for it….

CBS: Continuous Pentesting



Service Web Console

Vulnerability Alerts

Get Alerts of new vulnerabilities

Vulnerability Assessment

Targeted Scanning

Persistent Scanning

Penetration Testing

Security expert manual task

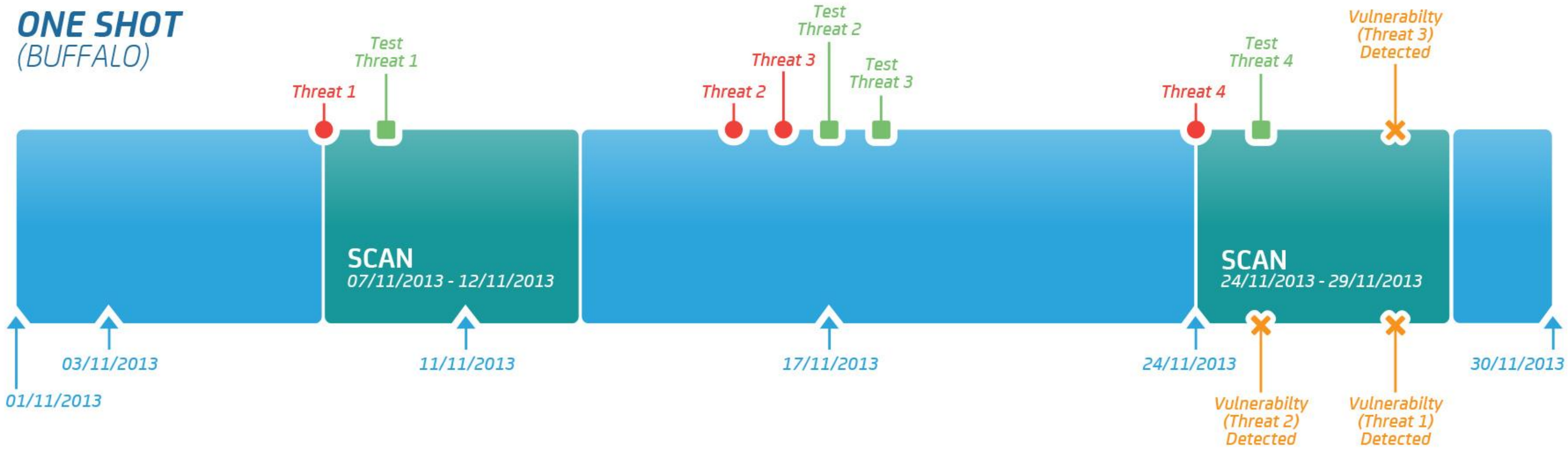
Application Security

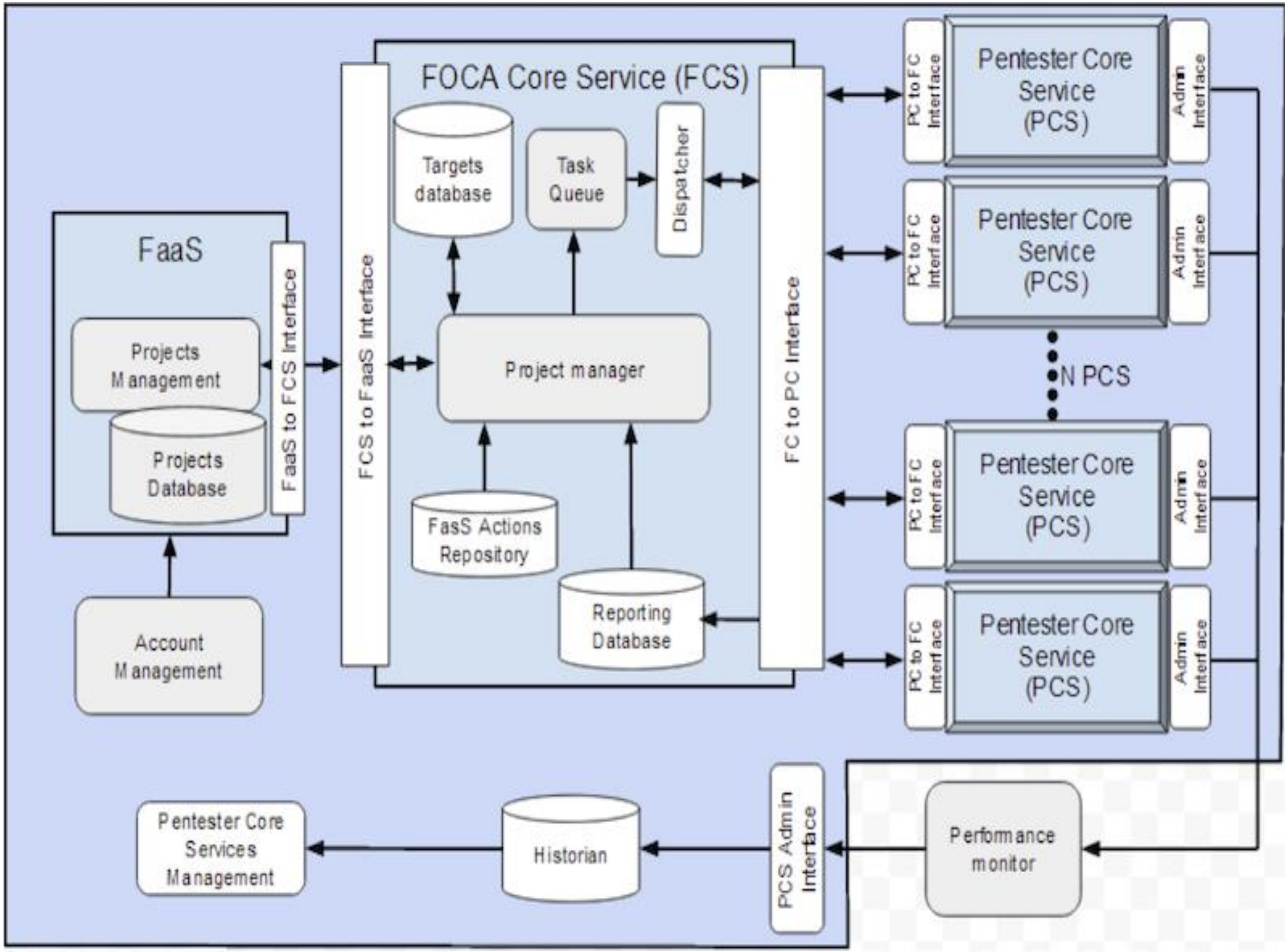
Source code analysis

Compliance

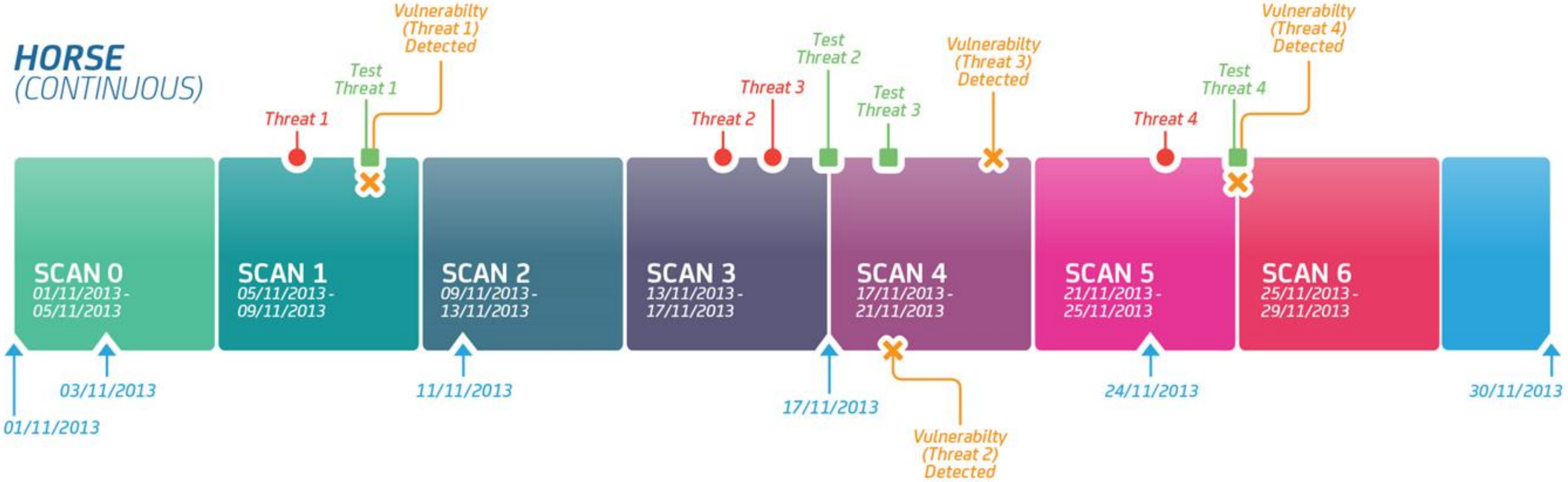
PCI Scanning

Traditional Pentesting

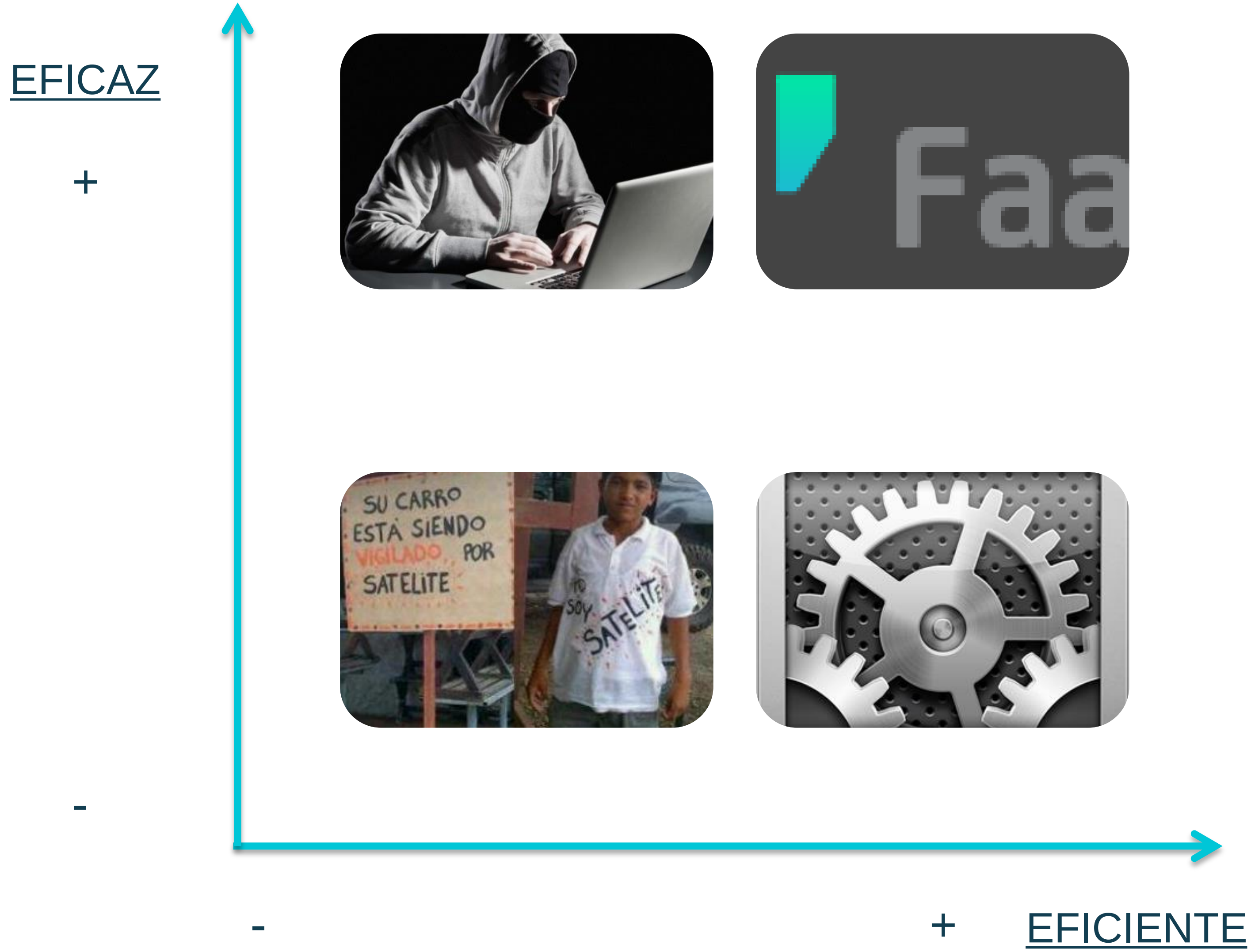



FOCA Core Service (FCS)
Targets database
Task Queue
Dispatcher
FaaS
FaaS to FCS Interface
FCS to FaaS Interface
FC to PC Interface
Projects Management
Projects Database
Project manager
FasS Actions Repository
Reporting Database
Account Management
PC to FC Interface
Pentester Core Service (PCS)
Admin Interface
PC to FC Interface
Pentester Core Service (PCS)
Admin Interface
N PCS
PC to FC Interface
Pentester Core Service (PCS)
Admin Interface
PC to FC Interface
Pentester Core Service (PCS)
Admin Interface
Pentester Core Services Management
Historian
PCS Admin Interface
Performance monitor

Continuos Pentesting


HORSE
(CONTINUOUS)
Threat 1
Test Threat 1
Vulnerabilty (Threat 1) Detected
Threat 2
Threat 3
Test Threat 2
Test Threat 3
Vulnerabilty (Threat 3) Detected
Threat 4
Test Threat 4
Vulnerabilty (Threat 4) Detected
SCAN 0 01/11/2013 - 05/11/2013
SCAN 1 05/11/2013 - 09/11/2013
SCAN 2 09/11/2013 - 13/11/2013
SCAN 3 13/11/2013 - 17/11/2013
SCAN 4 17/11/2013 - 21/11/2013
SCAN 5 21/11/2013 - 25/11/2013
SCAN 6 25/11/2013 - 29/11/2013
01/11/2013
03/11/2013
11/11/2013
17/11/2013
Vulnerabilty (Threat 2) Detected
24/11/2013
30/11/2013

Pentesting 2.0



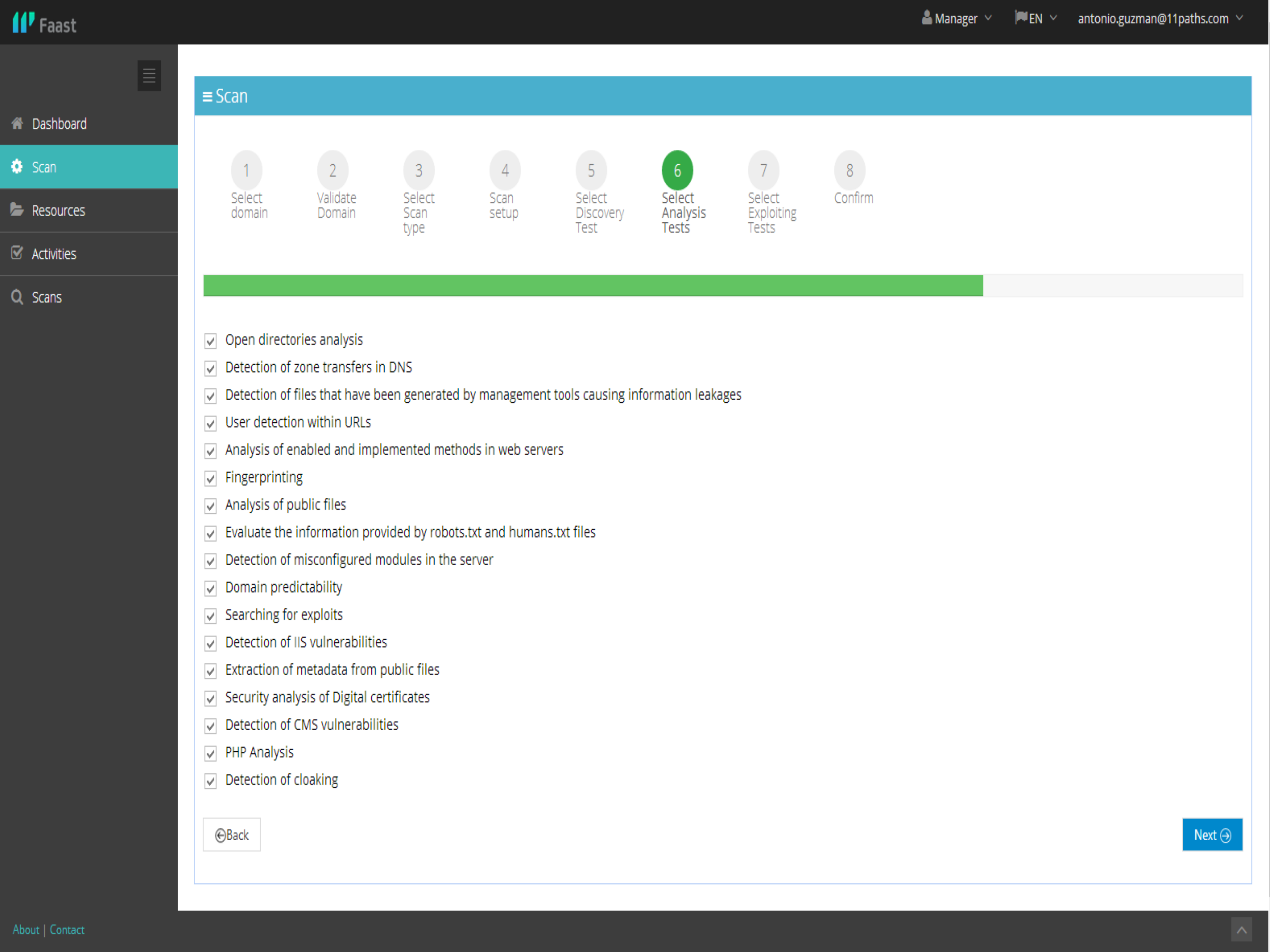
EFICAZ

+

-

-

+ EFICIENTE



≡ Scan

- ☑ Open directories analysis
- ☑ Detection of zone transfers in DNS
- ☑ Detection of files that have been generated by management tools causing information leakages
- ☑ User detection within URLs
- ☑ Analysis of enabled and implemented methods in web servers
- ☑ Fingerprinting
- ☑ Analysis of public files
- ☑ Evaluate the information provided by robots.txt and humans.txt files
- ☑ Detection of misconfigured modules in the server
- ☑ Domain predictability
- ☑ Searching for exploits
- ☑ Detection of IIS vulnerabilities
- ☑ Extraction of metadata from public files
- ☑ Security analysis of Digital certificates
- ☑ Detection of CMS vulnerabilities
- ☑ PHP Analysis
- ☑ Detection of cloaking

Telefonica