Seguridad en Redes Corporativas
Detectando al Intruso

José Camacho

Departamento de Teoría de la Señal, Telemática y Comunicaciones

Organiza: Grupo en Ciberseguridad de la UGR

Network Engineering & Security Group
http://nesg.ugr.es

Universidad de Granada

ÍNDICE

- ✓ Seguridad en Cifras
- ✓ Seguridad en Redes Corporativas
- ✓ Docencia:
  - ✓ Laboratorio Virtual de Seguridad en Red
- ✓ Investigación:
  - ✓ Detectando al intruso con Análisis Multivariante
  - ✓ Aplicación en Redes y Servicios Avanzados (Proyecto VERITAS)

- Seguridad en 2013
  - Enero
    - Red-October Cyber-Espionage Campaign
    - DDoS en EEUU
  - Febrero
    - Citadel Trojan en POS
    - Breaches en Facebook, Twitter, Apple, Microsoft…
  - Marzo
    - 5M Evernote
    - Cyberbunker-CloudFlare-Spamhaus
      - (85-300 Gbps)
    - BlackPOS

Verizon Data Breach Investigation Report 2014

- Seguridad en 2013
  - Abril:
    - Syrian Electronic Army

Verizon Data Breach Investigation Report 2014

- Seguridad en 2013
  - Abril:
    - Syrian Electronic Army

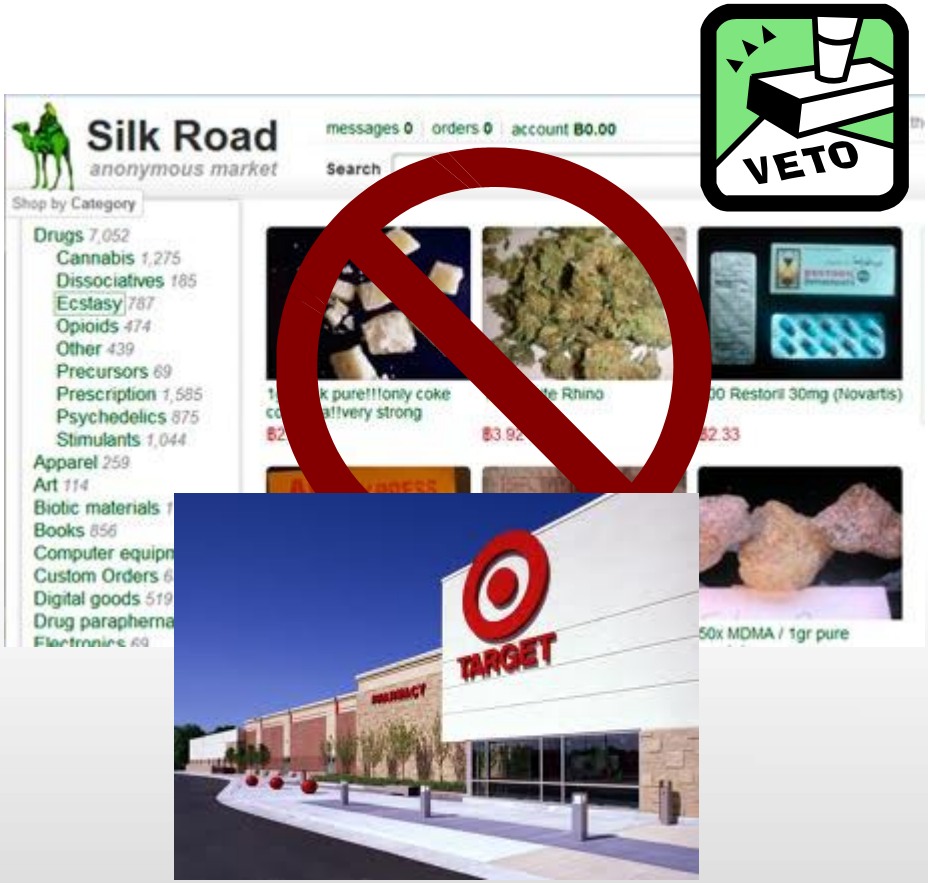
  - Mayo
    - Ciber-espionaje en EEUU, Pakistán, Tibet…
    - SEA – Twitter
  - Junio
    - Raley's Breach
    - NetTraveller
    - Snowden

Verizon Data Breach Investigation Report 2014

- Seguridad en 2013
  - Julio
    - SEA
    - Breaches
  - Agosto
    - SEA – Twitter
    - Calc-Team – G20
  - Septiembre
    - Vodafone Breach (2M)
    - Espionaje
    - Cryptolocker

Verizon Data Breach Investigation Report 2014

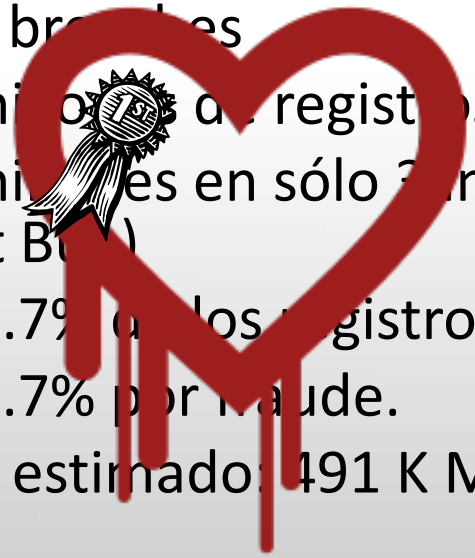
- Seguridad en 2013
  - Octubre
    - Adobe Breach (38M)
    - Nordstrom
    - Silk Road
  - Noviembre
    - …
  - Diciembre
    - TARGET Breach (70M)



Verizon Data Breach Investigation Report 2014

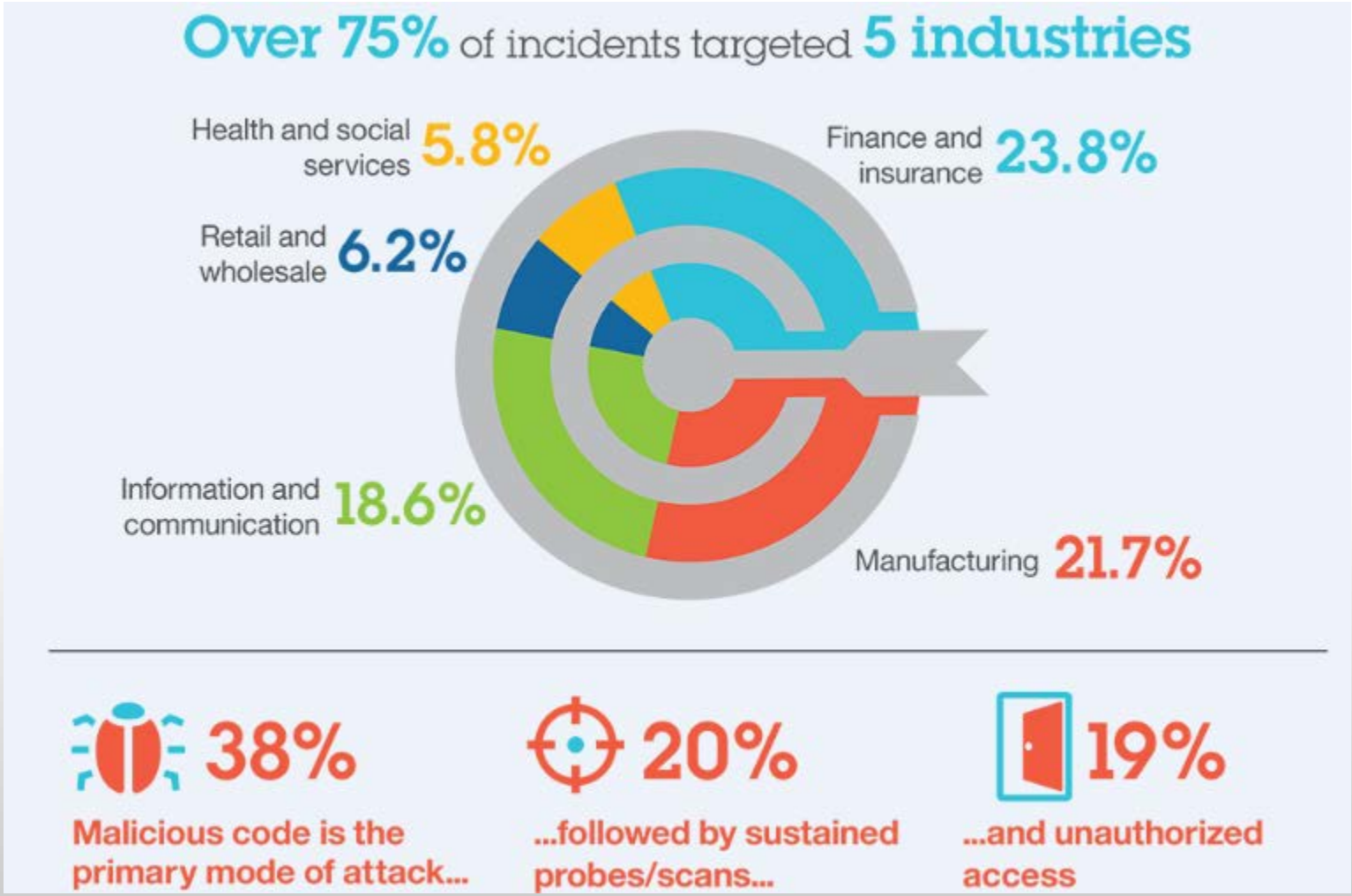
- Seguridad Corporativa de 2013 en números
  - 63.437 incidentes de seguridad
  - 1.367 breaches
  - 500-814 millones de registros (IBM, RBS)

- En 2014… primera mitad
  - 1.331 brechas
  - 502 millones de registros
  - 422 millones en sólo 3 incidentes (NYC Taxi, Adobe, Korea Credit Bureau)
  - Un 78.7% de los registros fueron obtenidos por Hacking.
  - Un 20.7% por fraude.
  - Gasto estimado: 491 K M$ (IDM, SU, Microsoft)

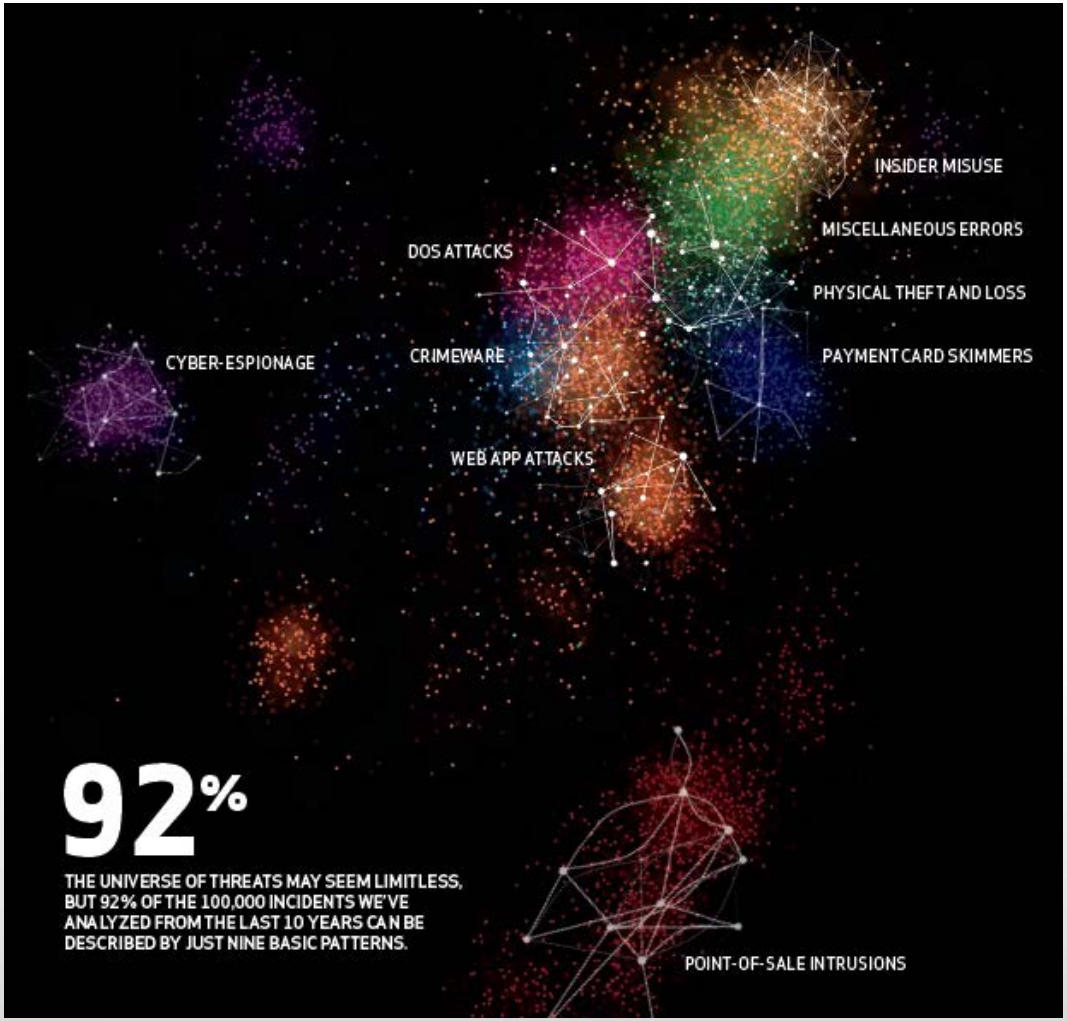


http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

IBM CyberSecurity Intelligence Index 2014



SEGURIDAD EN CIFRAS

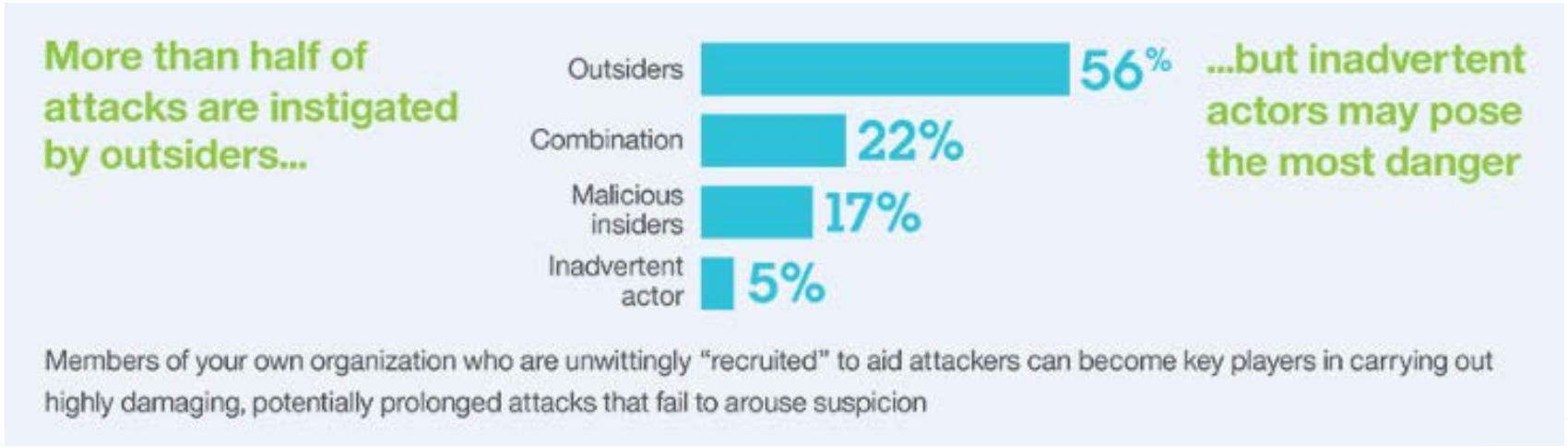


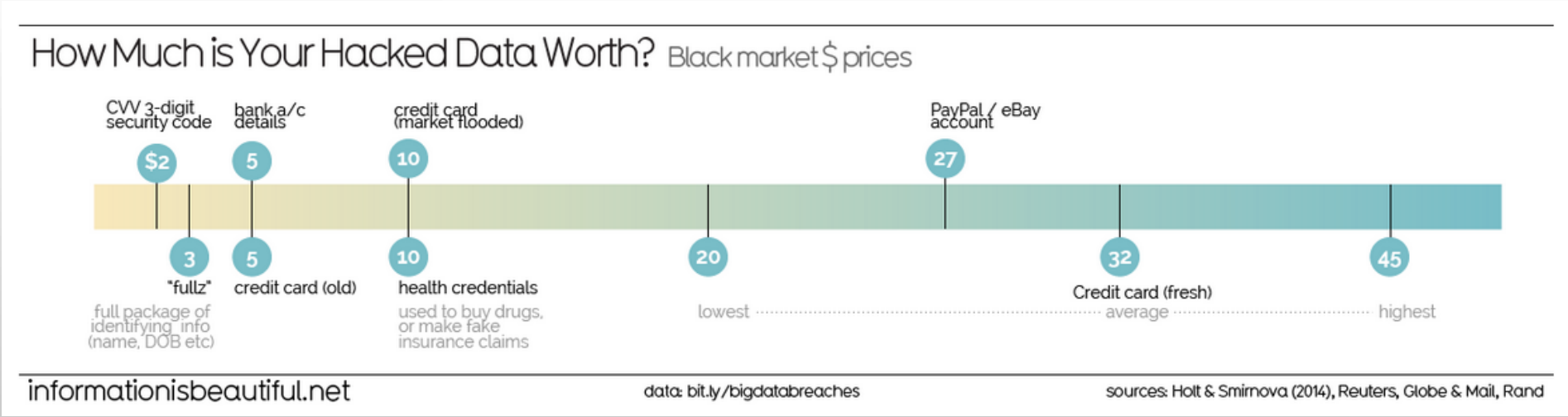
Verizon Data Breach Investigation Report 2014

SEGURIDAD EN CIFRAS

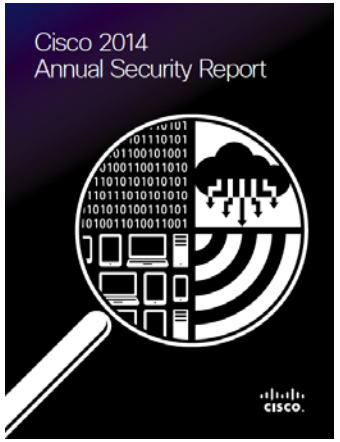
ObserveIt

IBM CyberSecurity Intelligence Index 2014





- Cisco: Security Experts Shortage 2014
  - 1.000.000
  - Conocimientos valorados
    - Big Data
    - BYOD



- Tendencias de contratación profesional 2014
  - Big Data
  - Comunicaciones móviles
  - La nube
  - Seguridad

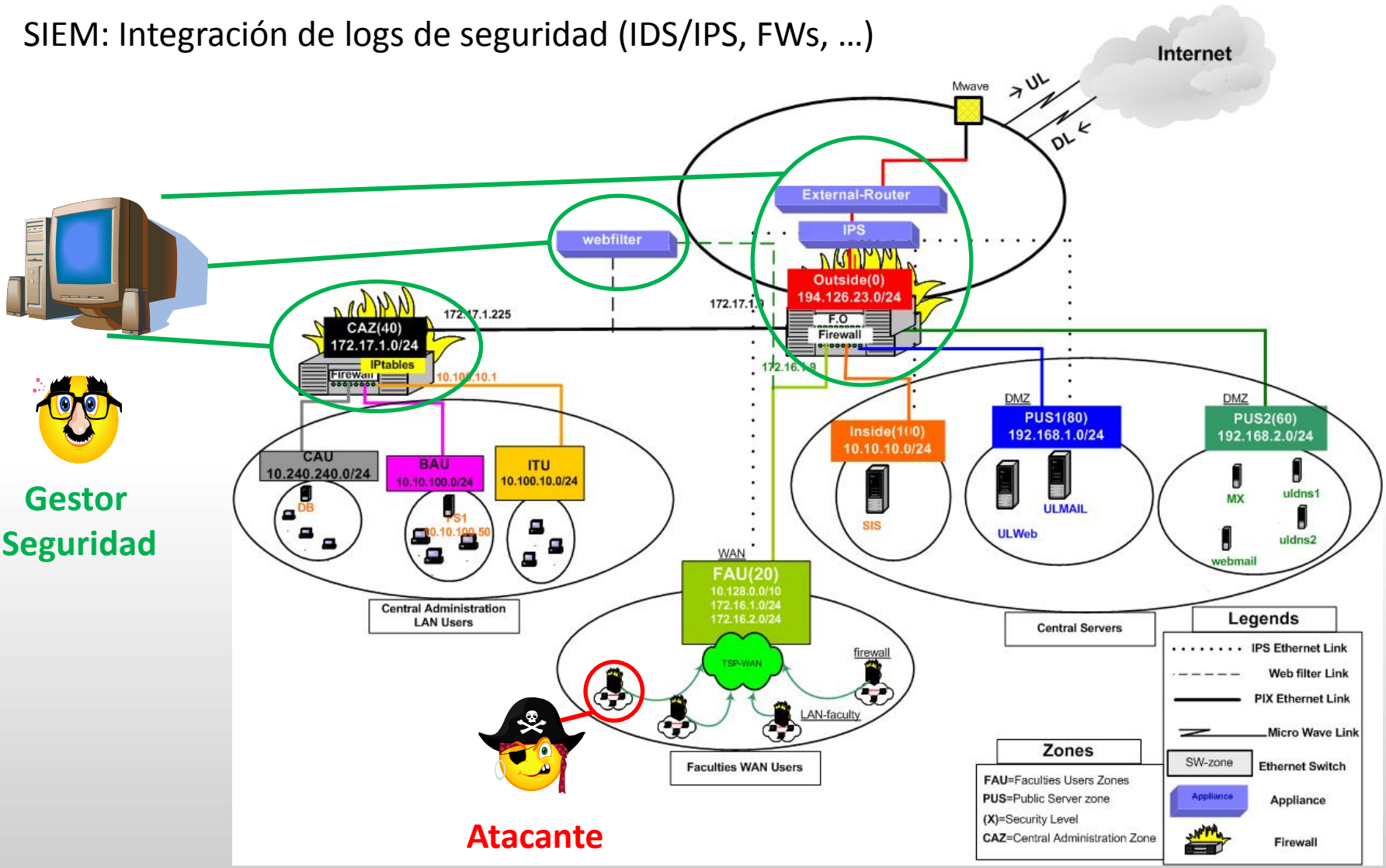
TechRepublic

- ✓ Seguridad en Cifras
- ✓ **Seguridad en Redes Corporativas**
- ✓ Docencia:
  - ✓ Laboratorio Virtual de Seguridad en Red
- ✓ Investigación:
  - ✓ Detectando al intruso con Análisis Multivariante
  - ✓ Aplicación en Redes y Servicios Avanzados (Proyecto VERITAS)

- Dimensiones de Seguridad
  - Prevención
    - Seguridad Física
    - Criptografía ➔Protocolos Seguros (WPA, IPSEC, TLS, ..)
    - Acceso ➔RADIUS, VPNs …
    - Seguridad Perimetral ➔ FWs, NAT …
    - Otros…

  - Detección
    - Intrusion Detection System (IDSs)
    - Security Information & Event Management Systems (SIEMs)
  - Respuesta
    - IRSs
    - Políticas y Procedimientos
    - Incident Response Teams

SIEM: Integración de logs de seguridad (IDS/IPS, FWs, …)

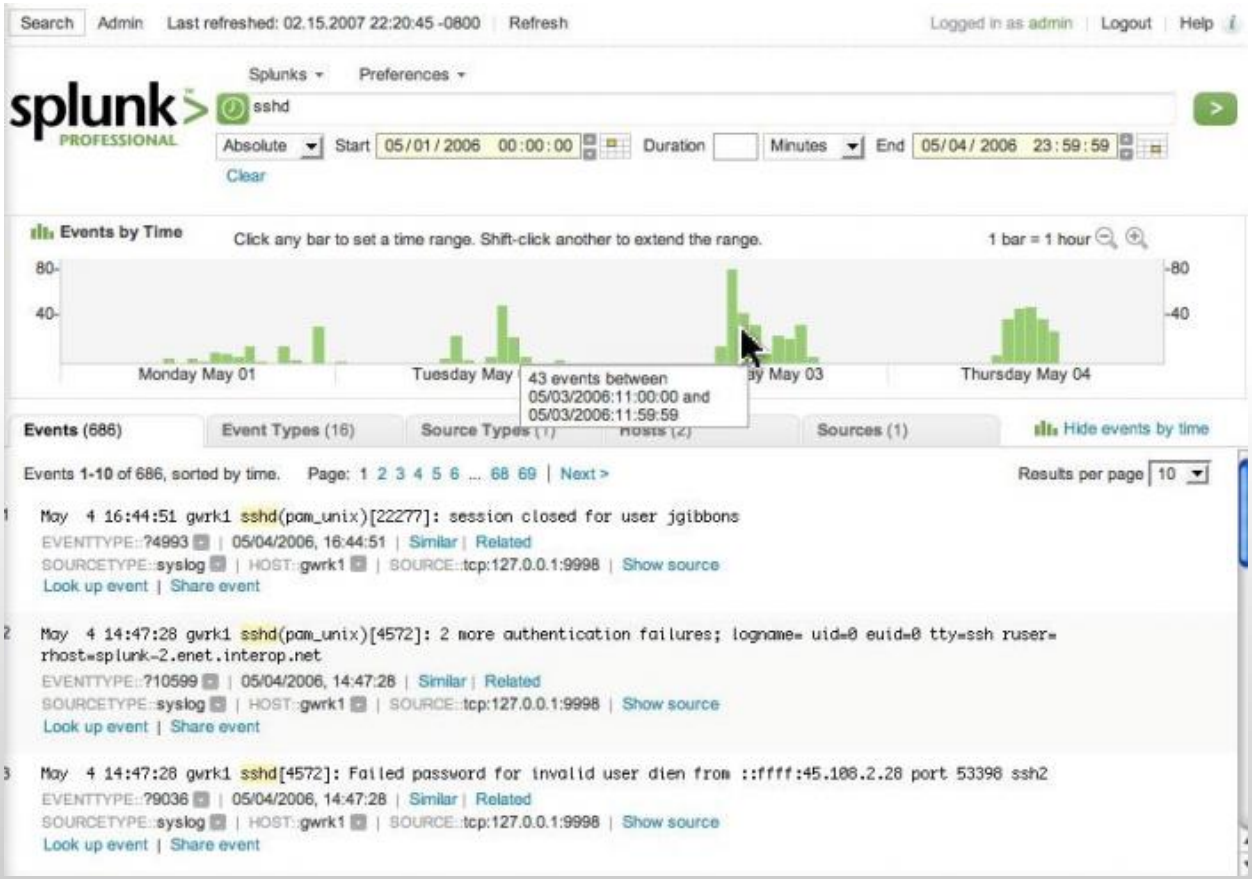


Gestor Seguridad

Atacante

- Ej. RSA Security Analytics
  https://www.youtube.com/watch?v=RzscmZ-UtCY

- Splunk
- Symantec
- IBM
- ....




Syslog
Firewalls
IDS
Netflow
SNMP
Traffic
App
logs
Big Data

Variedad

Veracidad

Velocidad

Syslog

Firewalls

IDS

Netflow

SNMP

Traffic

App logs

VOLUMEN

Una mirada a los datos

estructurados
y
desestructurados

IDS-03292012-1hr.txt

```
[**] [1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
03/29-14:48:31.019982 172.23.0.216:1251 -> 172.23.0.10:445
TCP TTL:128 TOS:0x0 ID:1696 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xA9B345B0  Ack: 0x4522D27D  Win: 0xFF3A  TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12065][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12052][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0818][Xref =>
http://www.securityfocus.com/bid/9635][Xref => http://www.securityfocus.com/bid/9633]

[**] [1:2102466:9] GPL NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
03/29-14:48:31.024896 172.23.0.216:1251 -> 172.23.0.10:445
TCP TTL:128 TOS:0x0 ID:1698 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0xA9B35020  Ack: 0x4522D402  Win: 0xFDB5  TcpLen: 20

[**] [1:2103003:7] GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
03/29-14:48:32.421373 172.23.0.211:1308 -> 172.23.0.10:445
TCP TTL:128 TOS:0x0 ID:1843 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xA1B4DB42  Ack: 0x5D2556D8  Win: 0xFF3A  TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12065][Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12052][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0818][Xref =>
http://www.securityfocus.com/bid/9635][Xref => http://www.securityfocus.com/bid/9633]
```

For Help, press F1 | 30 | 1 | Read | Ovr | Block | Sync | Rec | Caps

TextPad -

File Edit Search View Tools Macros Configure Window Help

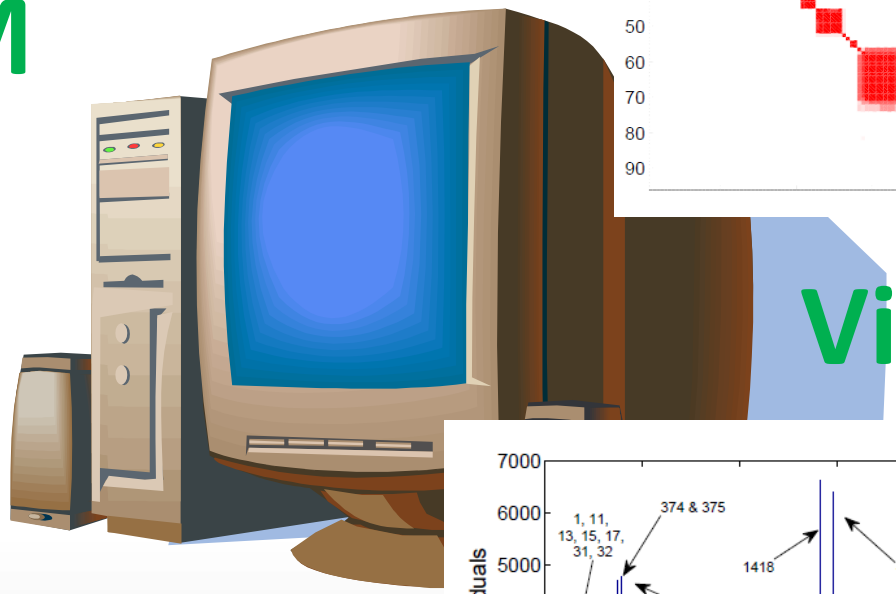
Find incrementally | Match case

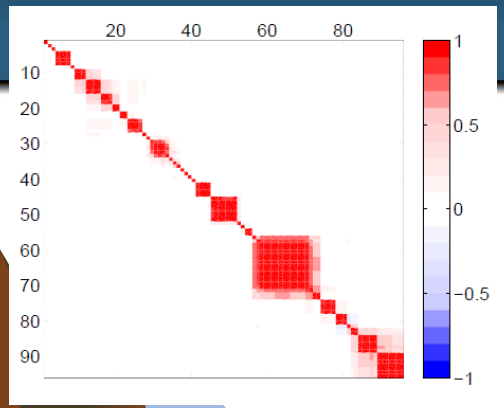
syslog-03292012-1hr-parsed.csv *

```
Date/time,Logging device,Syslog priority,Operation,Message,Message code,Protocol,Source IP,Source MAC address,Destination IP,Source port,Destination port,Source side,
Destination side,Destination service,Interface,Direction
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.39",(empty),"10.32.0.100",1212,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.45",(empty),"10.32.0.100",1213,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.47",(empty),"10.32.0.100",1214,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.52",(empty),"10.32.0.100",1215,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.63",(empty),"10.32.0.100",1216,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.54",(empty),"10.32.0.100",1217,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.44",(empty),"10.32.0.100",1218,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.60",(empty),"10.32.0.100",1219,80,inside,outside,http,(empty),outbound
29/Mar/2012 14:37:44,"172.23.0.1",Info,Built,[message removed],ASA-6-302013,TCP,"172.23.4.36",(empty),"10.32.0.100",1220,80,inside,outside,http,(empty),outbound
```

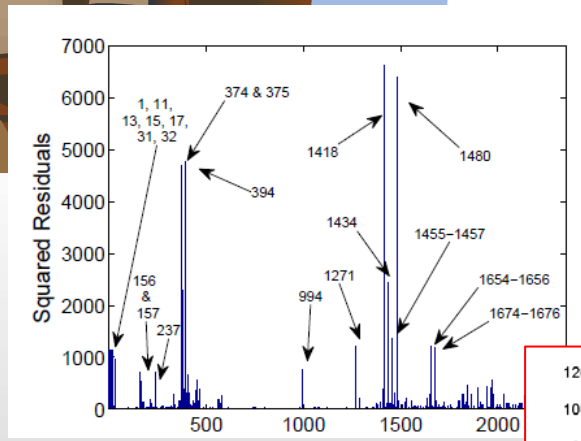
For Help, press F1 | 2 | 1 | Read | Ovr | Block | Sync | Rec | Caps

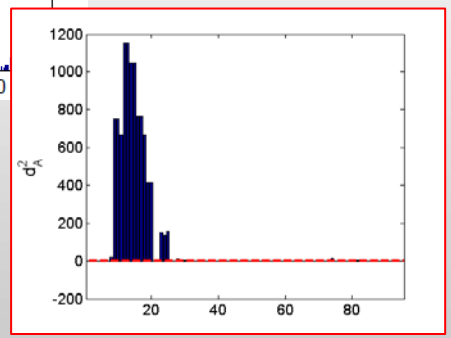
SIEM





Visualizations





VISUAL ANALYTICS

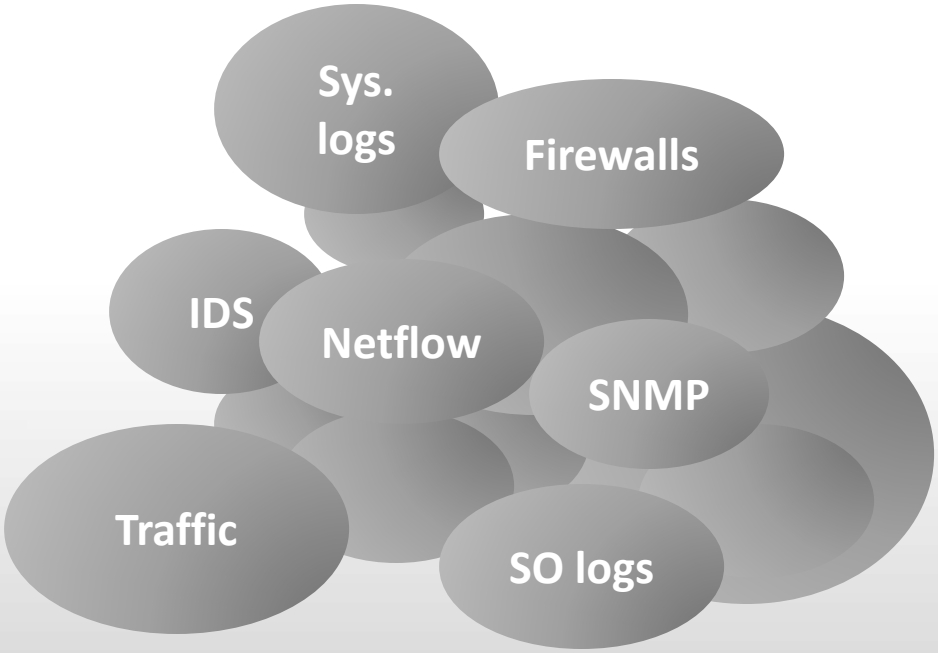
DAVIX

afterglow

Big Data

mahout

hadoop



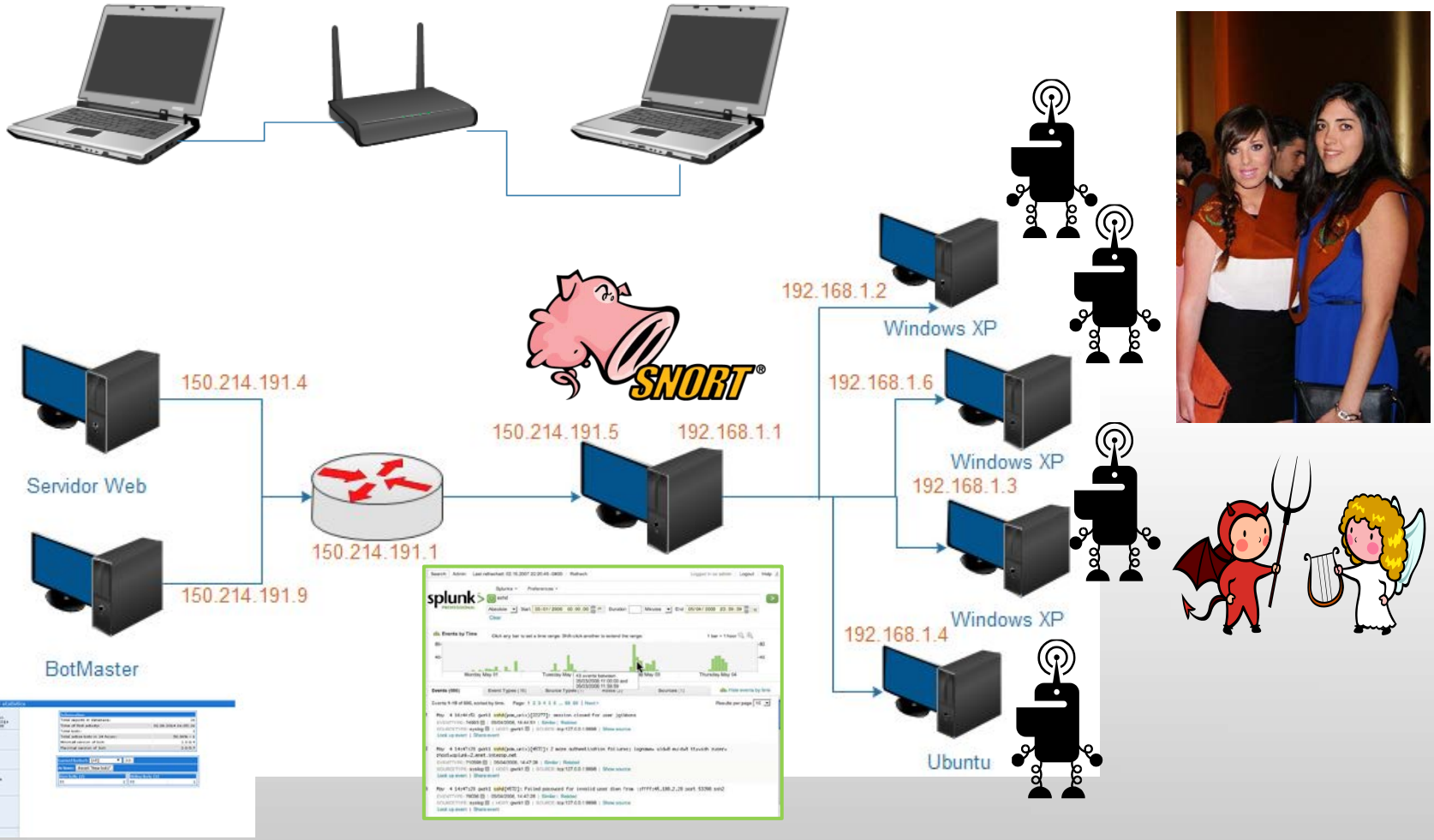
RSA SilverTail Systems

SIEM

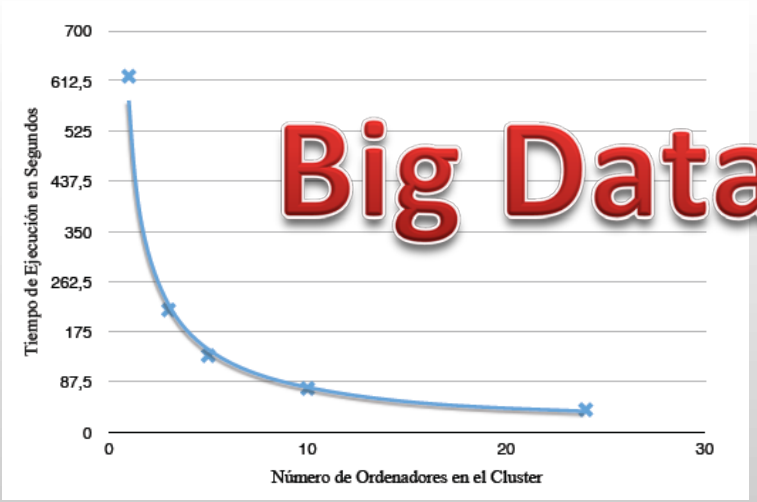
splunk> listen to your data™

- ✓ Seguridad en Cifras
- ✓ Seguridad en Redes Corporativas
- ✓ **Docencia:**
  - ✓ **Laboratorio Virtual de Seguridad en Red**
- ✓ Investigación:
  - ✓ Detectando al intruso con Análisis Multivariante
  - ✓ Aplicación en Redes y Servicios Avanzados (Proyecto VERITAS)

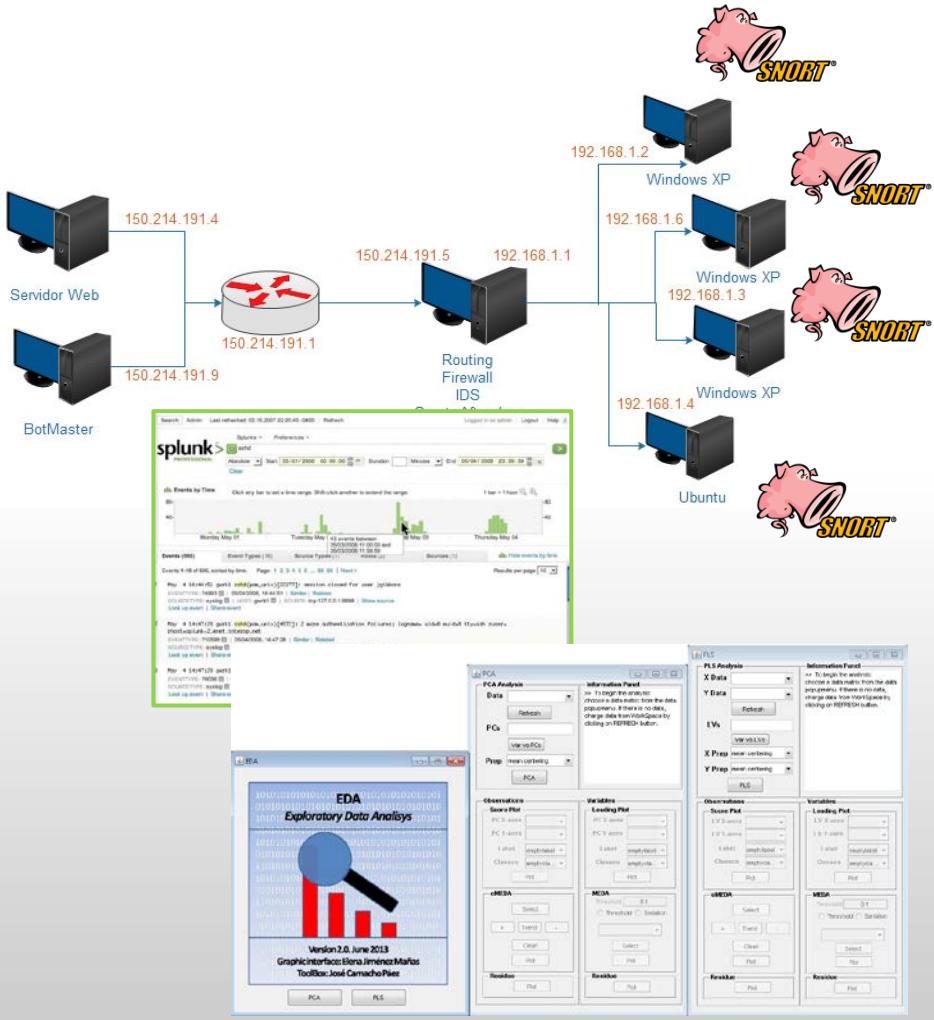
- Virtualización + Hardware de interconexión



- Virtualización + Hardware de interconexión



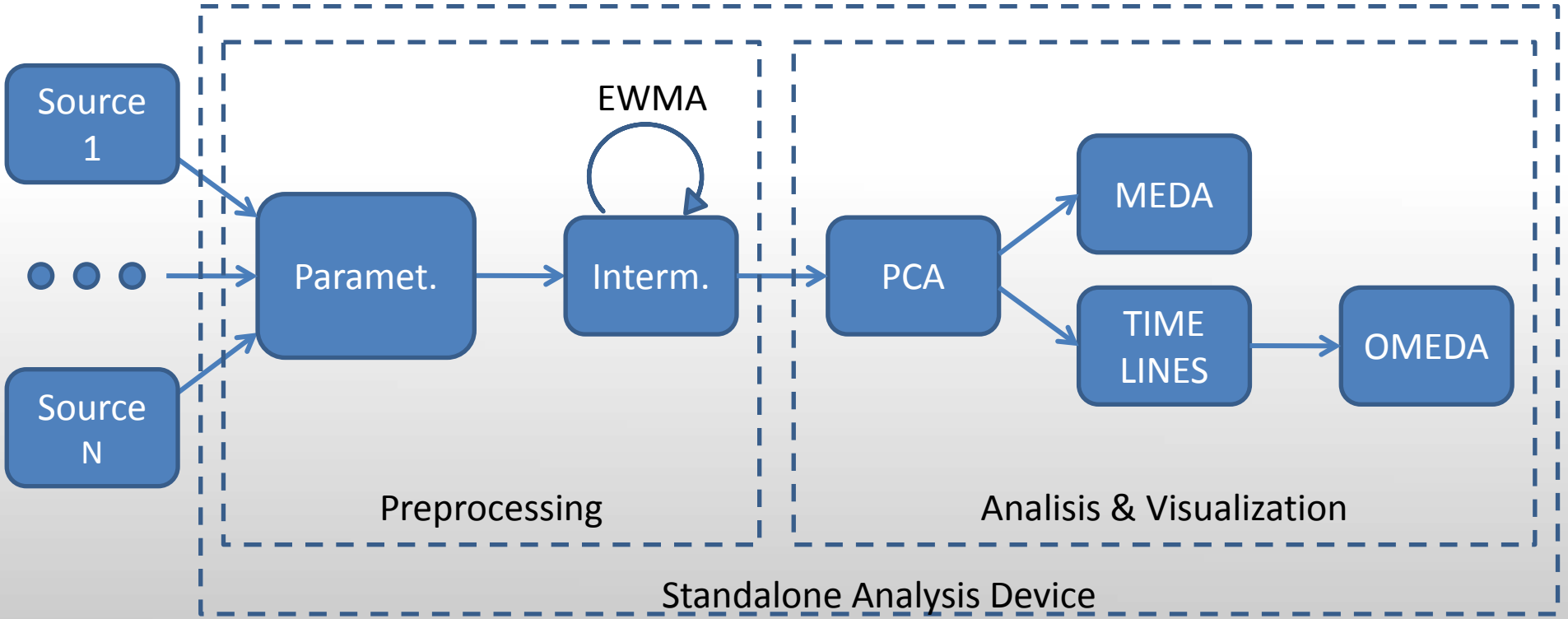
- Virtualización + Hardware de interconexión



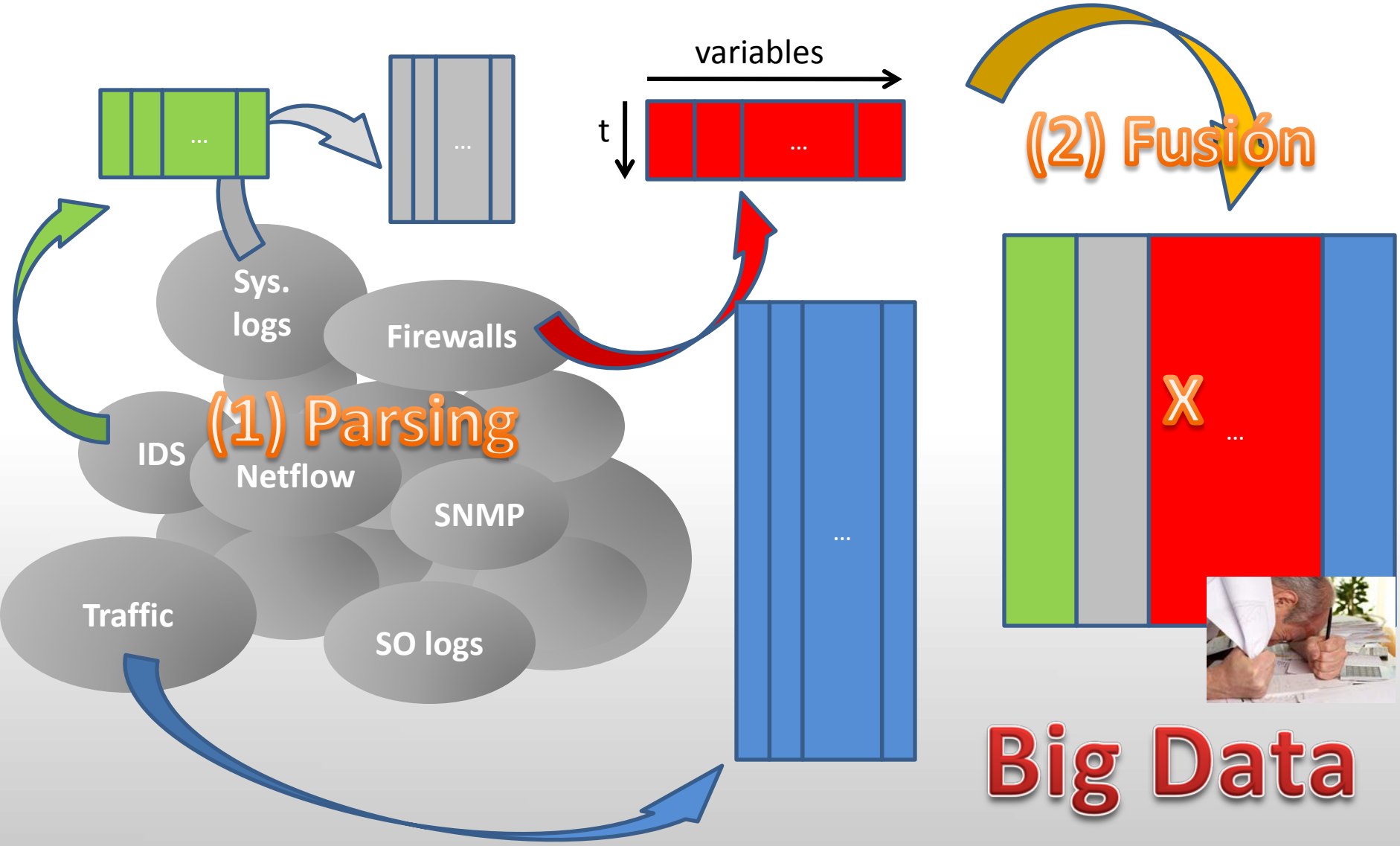
- ✓ Seguridad en Cifras
- ✓ Seguridad en Redes Corporativas
- ✓ Docencia:
  - ✓ Laboratorio Virtual de Seguridad en Red
- ✓ **Investigación:**
  - ✓ **Detectando al intruso con Análisis Multivariante**
  - ✓ Aplicación en Redes y Servicios Avanzados (Proyecto VERITAS)

MULTIVARIATE ANALYSIS

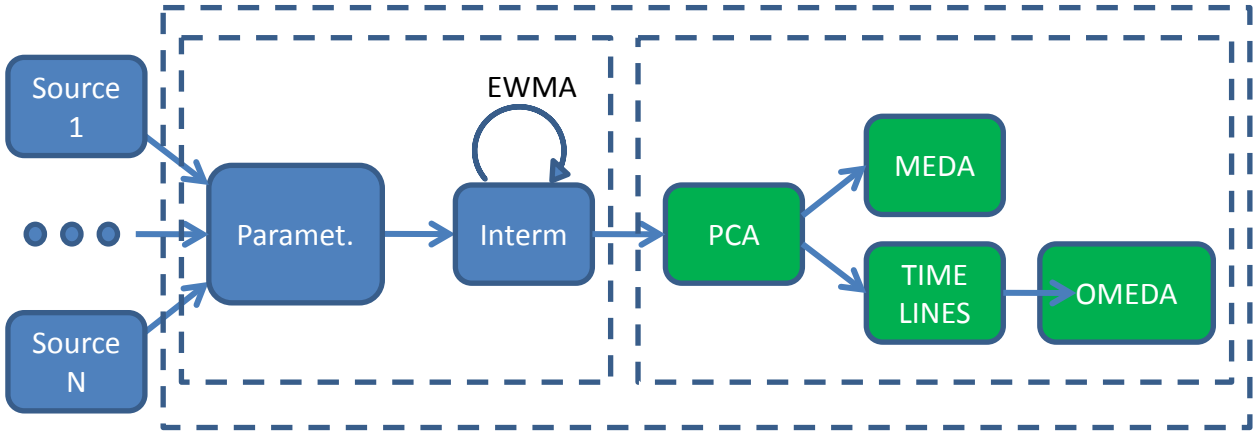
- Ventaja: ¡¡Maneja miles de variables!!



DETECTANDO AL INTRUSO CON ANÁLISIS MULTIVARIANTE

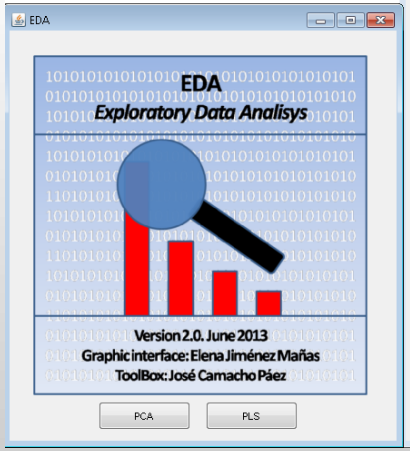


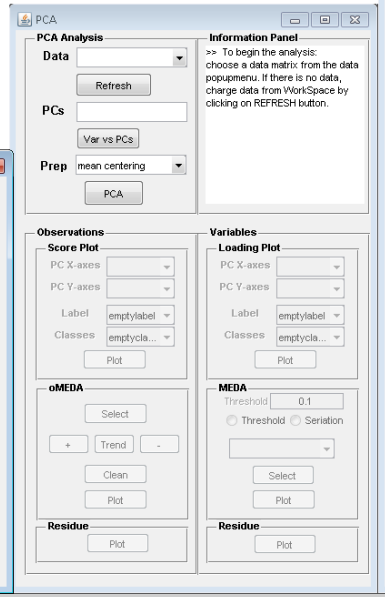
DETECTANDO AL INTRUSO CON ANÁLISIS MULTIVARIANTE

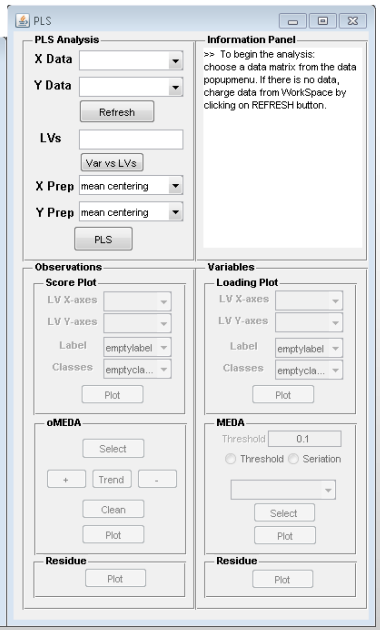


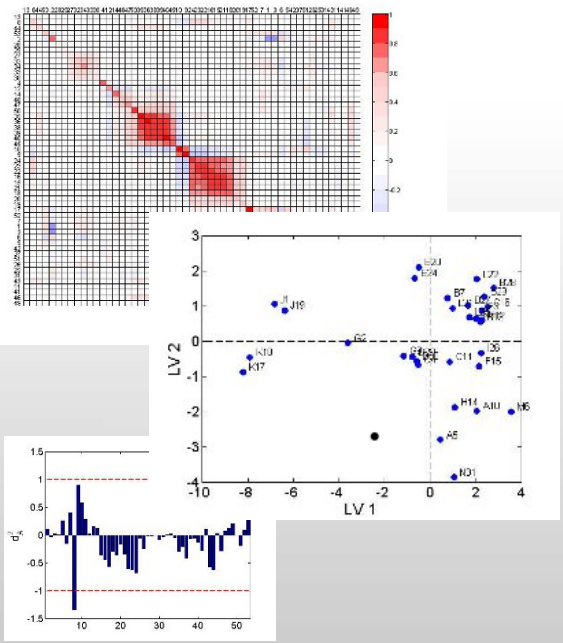
MEDA Toolbox

MATLAB MathWorks





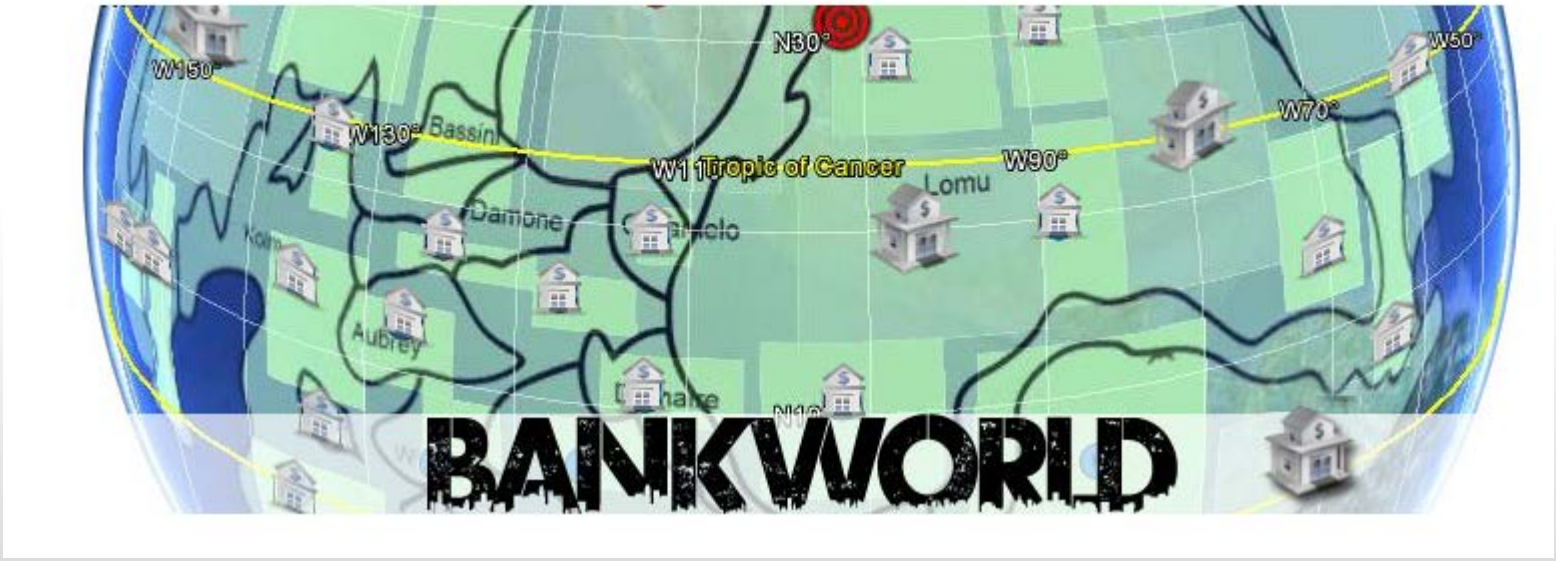




https://github.com/josecamachop/MEDA-Toolbox

VAST Challenge 2012

Visual Analytics Community
DISCOVERY THROUGH COLLABORATION AND SHARING



Mini-Challenge 2: Bank of Money Regional Office Network Operations Forensics

During a time period that is NOT overlapping with MC 1, a Region within the Bank of Money is experiencing operational difficulties. This becomes a challenge for the operations staff, particularly as they attempt to deploy their limited number of skilled administrators to address issues occurring in the enterprise.

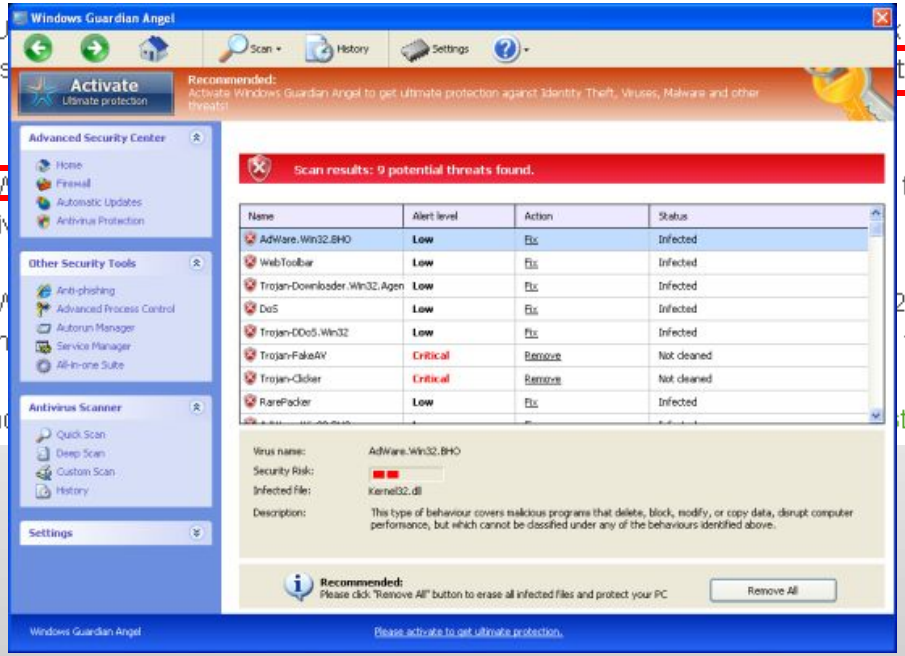
You will be provided with Firewall and IDS logs from one of the BOM networks of approximately 5000 wall and IDS logs you worked on during the VAST 2011 MC 2, and so the tools you used there will come in ha encouraged). You will also be provided with a description of the network to guide your investigation.

MC 2.1 U k place for the ti gs?
Provide s thy events of se ach
event.

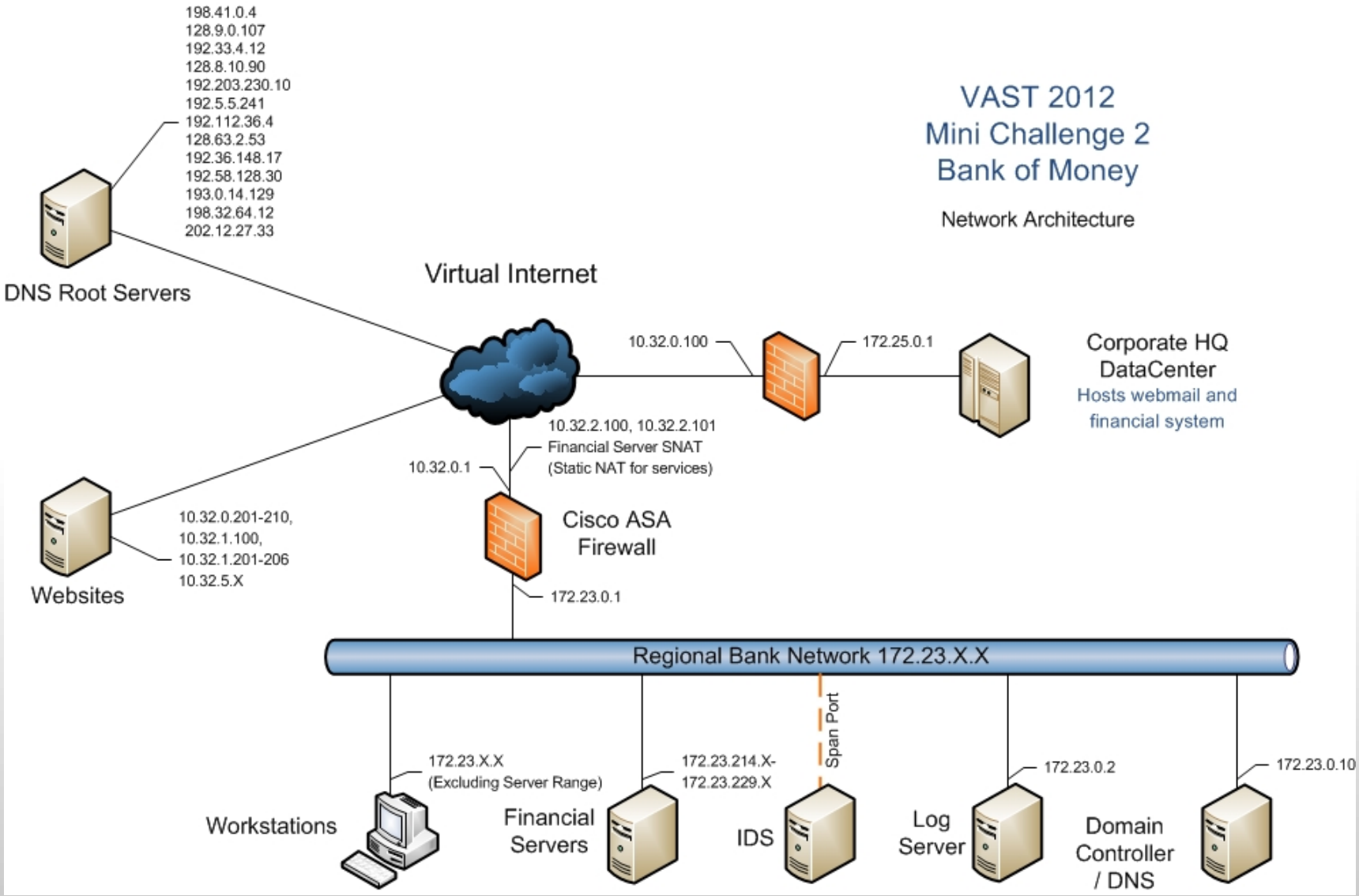
MC 2.2 W the two days in ith an
informati

MC 2.3 W 2.1? Understanding that you cannot shut down the corporate network
or discon to mitigate the root cause problem(s)?

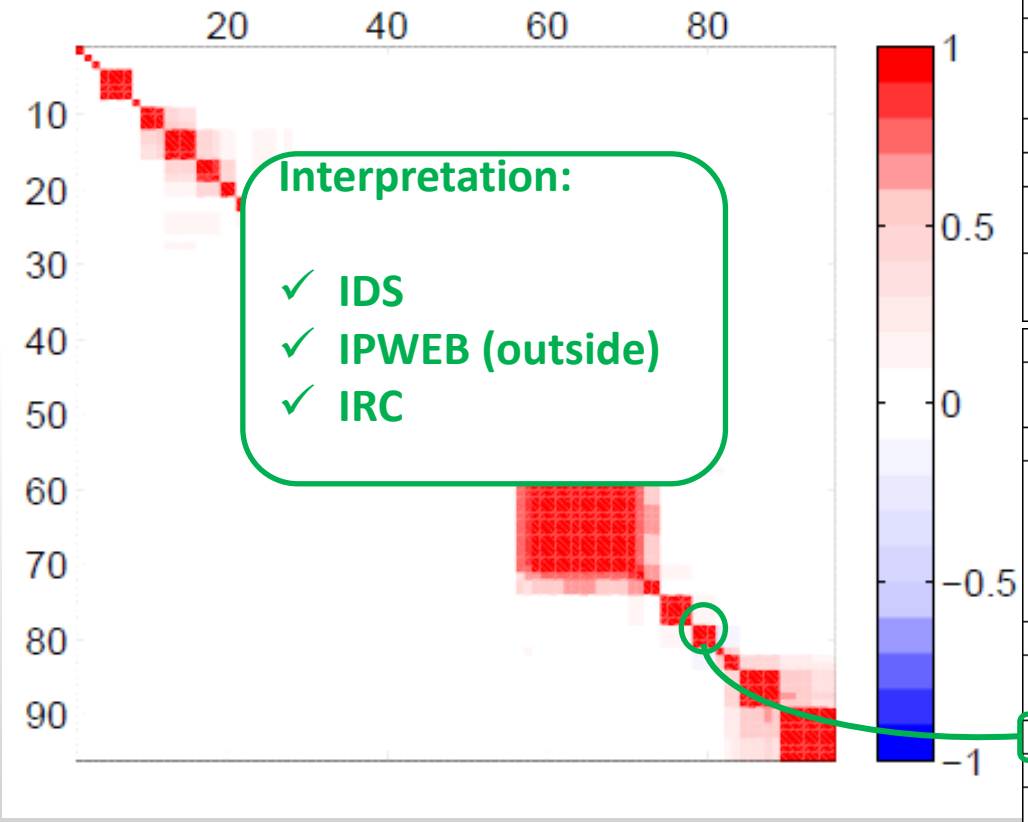
Downloa tructions and Downloads page.



DETECTANDO AL INTRUSO CON ANÁLISIS MULTIVARIANTE

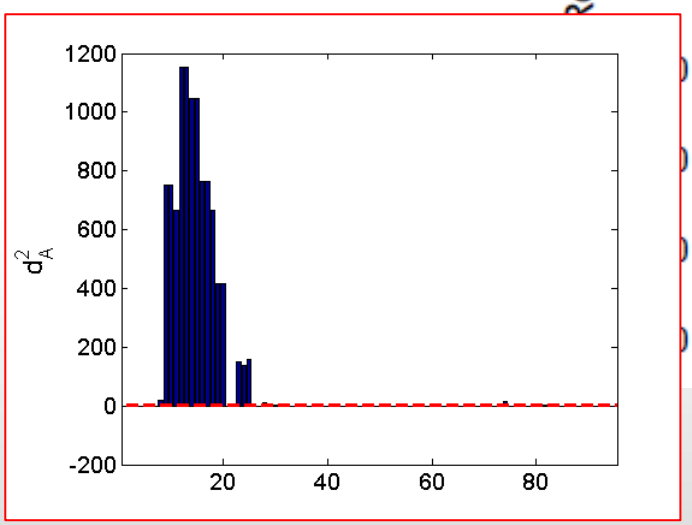


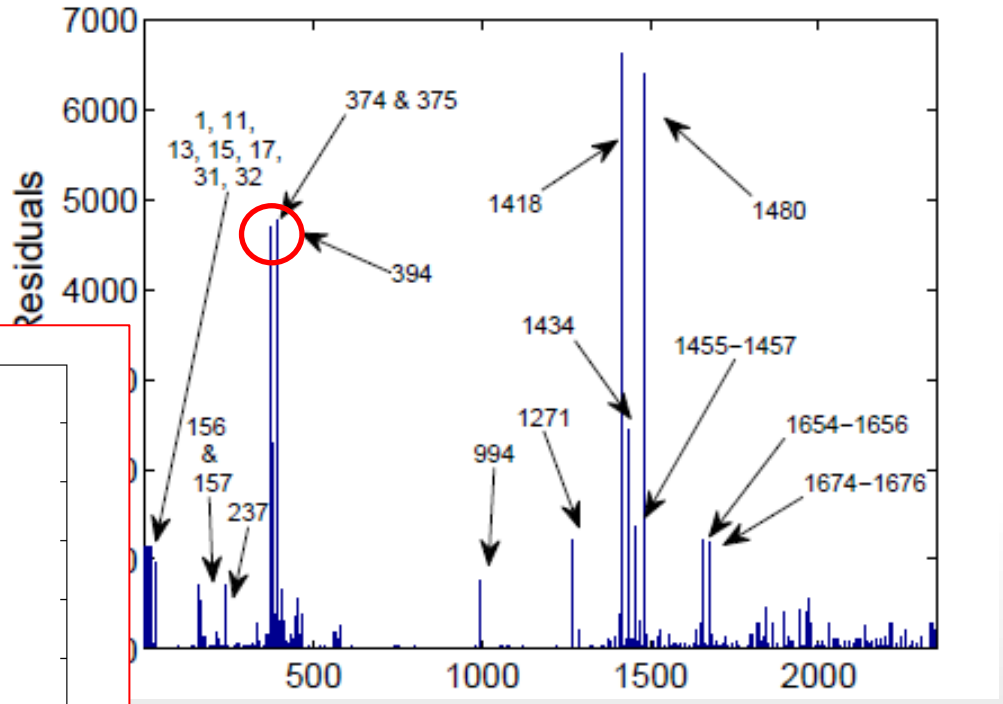
- MEDA:
  - Bird view of the network state



#	Int.	Relevant features
1	4-7	fw_syswarn fw_asa4 fw_pftp fw_asa41
2	9-11	ids_lssh ids_pssh fw_ptelnet
3	12-15	fw_opdenyacl fw_asa37 fw_asa3 fw_syserror
4	16-18	ids_lsnmp ids_psnmp fw_psnmp
5	19-20	ids_limap ids_lpop3
6	21-22	ids_badtraffic ids_lsql
7	23-26	ids_ipfwhq ids_prio2 ids_leak ids_lvnc
8	29-33	fw_asa635 fw_pdns fw_udp fw_ipdc fw_asa636
9	41-44	ids_ldns ids_privacy ids_pdns ids_prio1
10	45-51	ids_pnstd ids_ipws ids_ipdc ids_psmb ids_command ids_lnetbios ids_prio3
11	54-55	fw_iplog fw_psyslog
12	56-71	fw_ipfwr fw_ipout fw_phttp fw_asa634 fw_opteardown fw_condown fw_sysinfo fw_asa6 fw_tcp fw_ipws fw_conbuilt fw_opbuilt fw_asa633 fw_outbound fw_pnstd fw_ipweb
13	72-73	fw_opdeny fw_asa610
14	74-77	fw_ipfwhq fw_inbound fw_syscritical fw_asa21
15	78-80	ids_misc ids_ipweb ids_lirc
16	82-83	fw_opempty fw_empty
17	84-88	fw_asa66 fw_asa671 fw_asa672 fw_asa673 fw_asa677
18	89-95	fw_opcommand fw_asa518 fw_sysnotice fw_asa5 fw_asa6310 fw_asa639 fw_asa517

- Time lines
- oMEDA



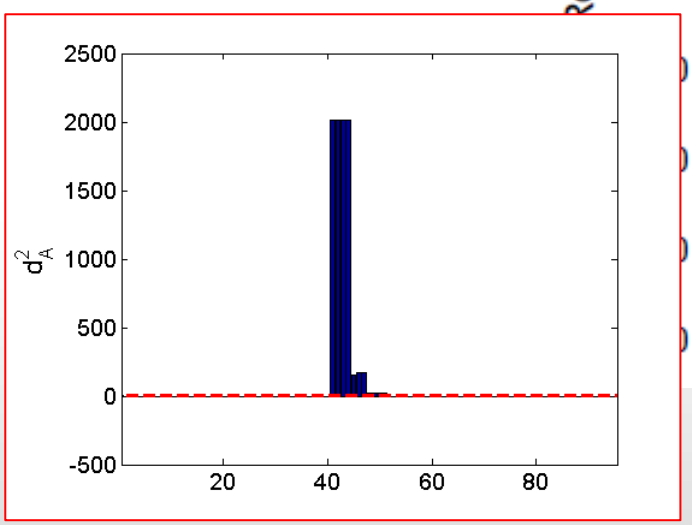


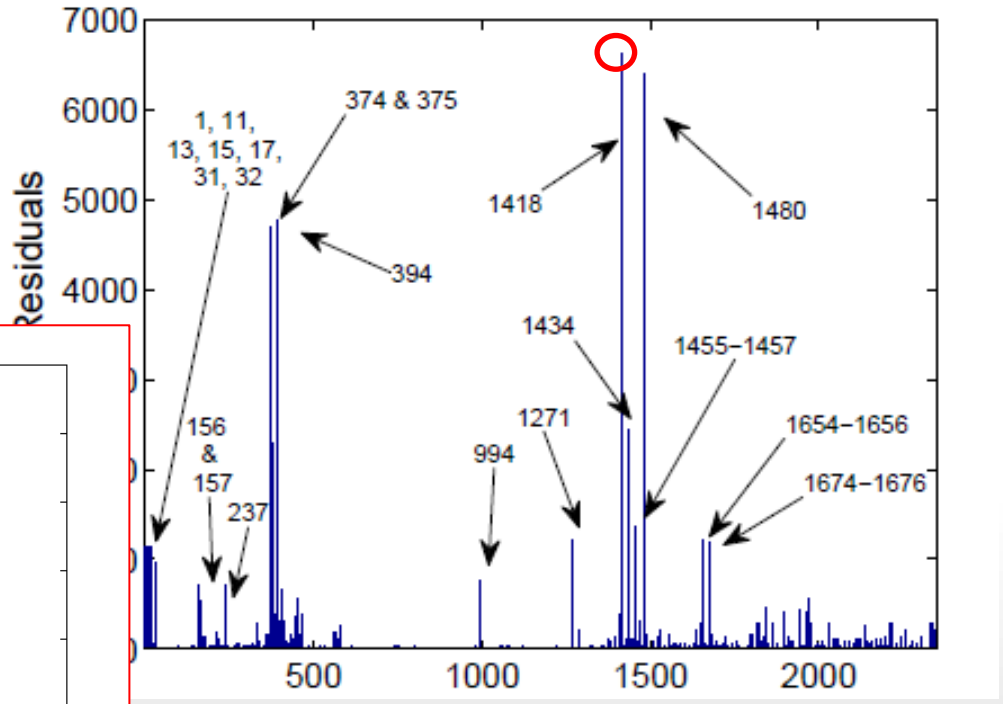
'ids_lssh' 'ids_pssh' 'fw_ptelnet' 'fw_asa37' 'fw_opdenyacl' 'fw_syserror' 'fw_asa3' 'ids_lsnmp' 'ids_psnmp' 'fw_psnmp' 'ids_limap' 'ids_lpop3' 'ids_ipfw' 'ids_prio2' 'ids_leak'

- Interpretación: Scanning en el firewall.

DETECTANDO AL INTRUSO CON ANÁLISIS MULTIVARIANTE

- Time lines
- oMEDA

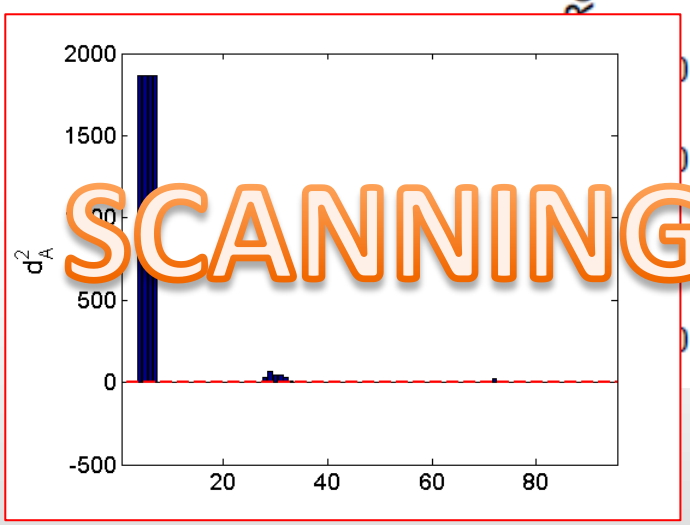


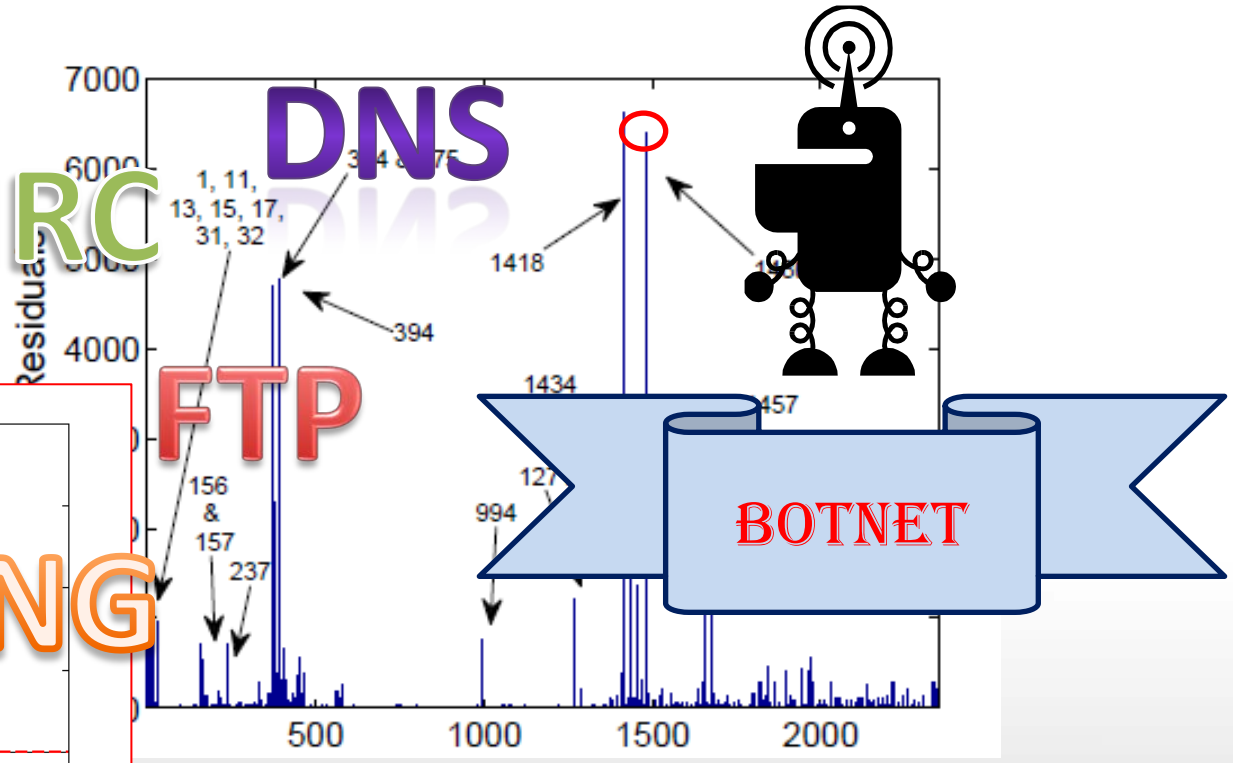


'ids_ldns' 'ids_pdns' 'ids_privacy' 'ids_prio1' 'ids_pnstd' 'ids_ipws' 'ids_ipdc'

- Interpretación: Ataques al servicio DNS desde el interior de la red

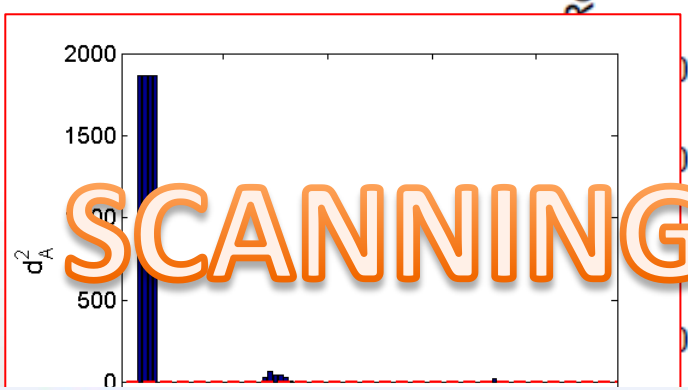
- Time lines
- oMEDA

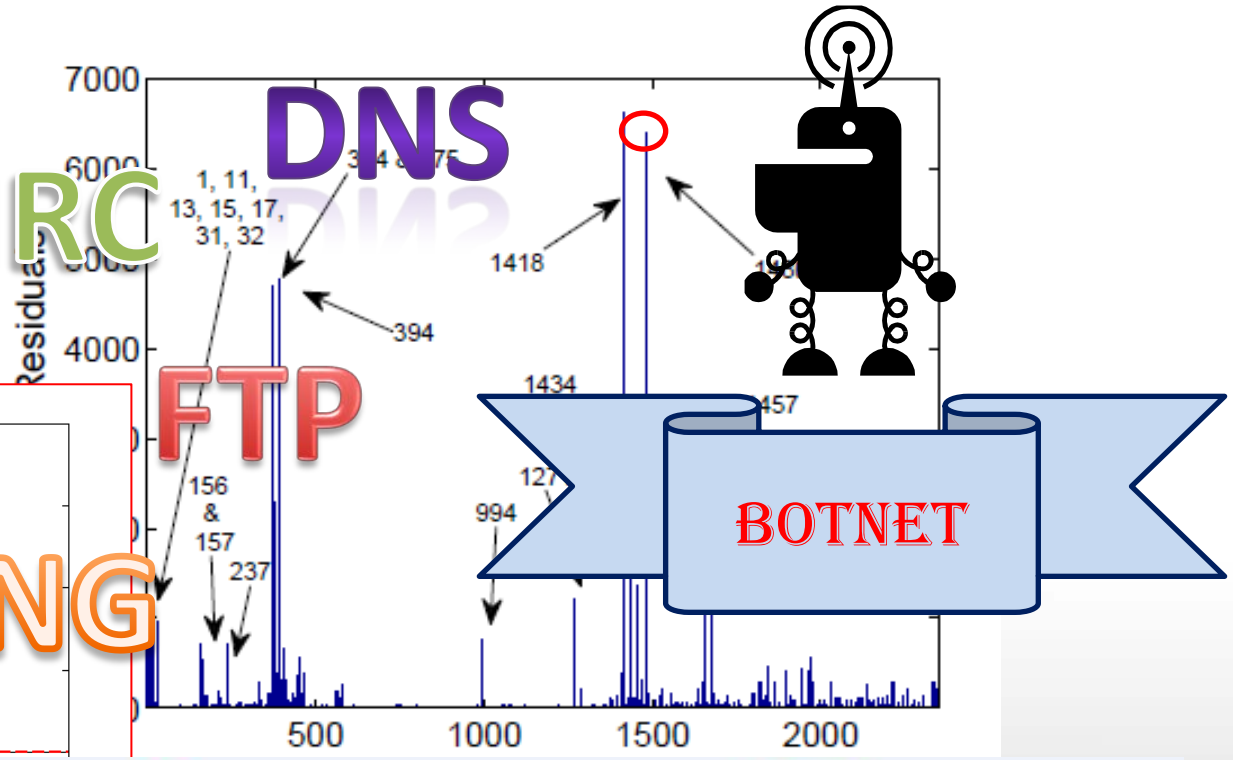




- Interpretación: intentos de conexión FTP bloqueado por el firewall

- Time lines
- oMEDA





38%

Malicious code is the primary mode of attack...

20%

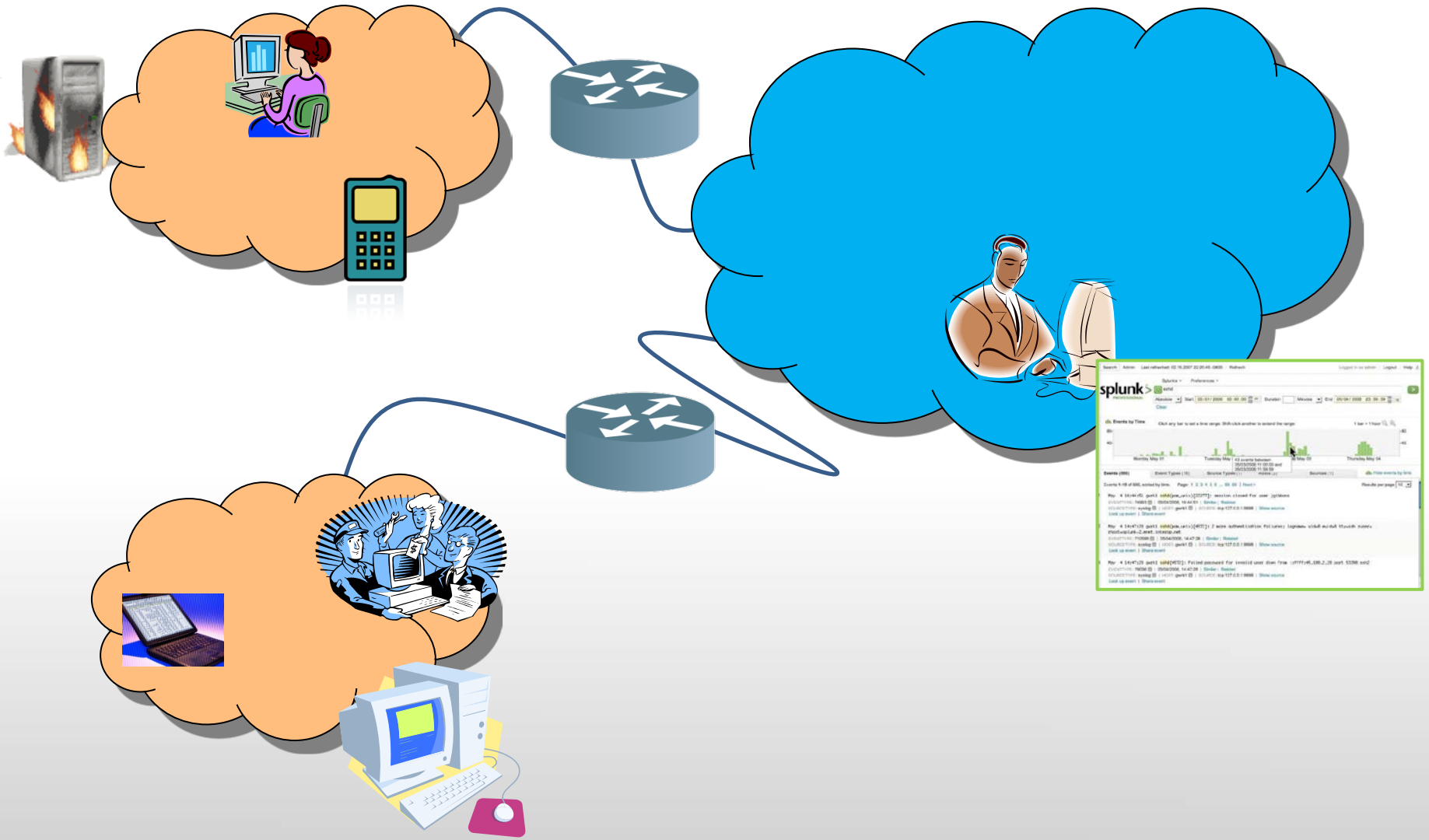
...followed by sustained probes/scans...

19%

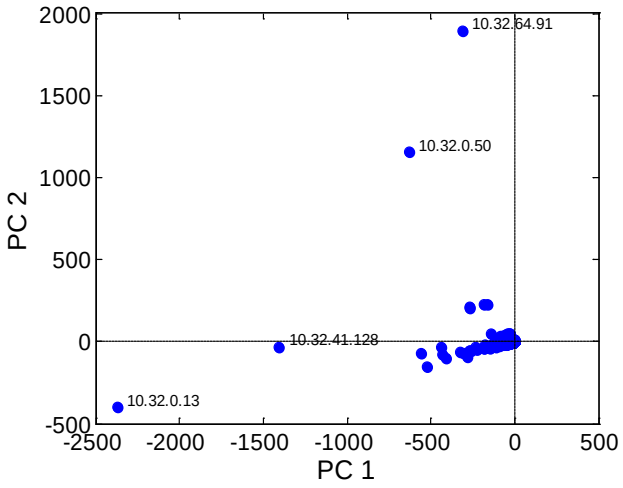
...and unauthorized access

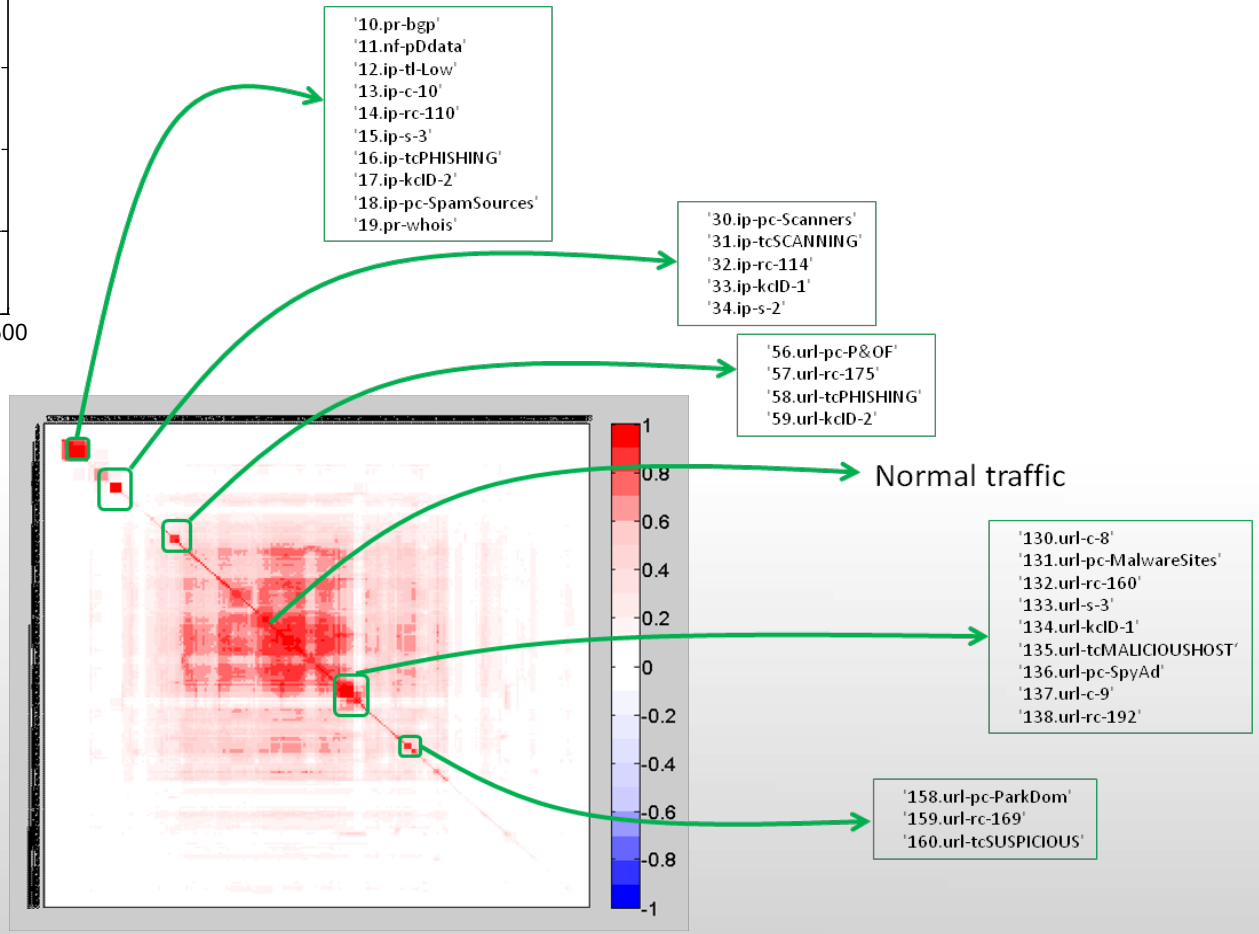
IBM CyberSecurity Intelligence Index 2014

DETECTANDO AL INTRUSO CON ANÁLISIS MULTIVARIANTE

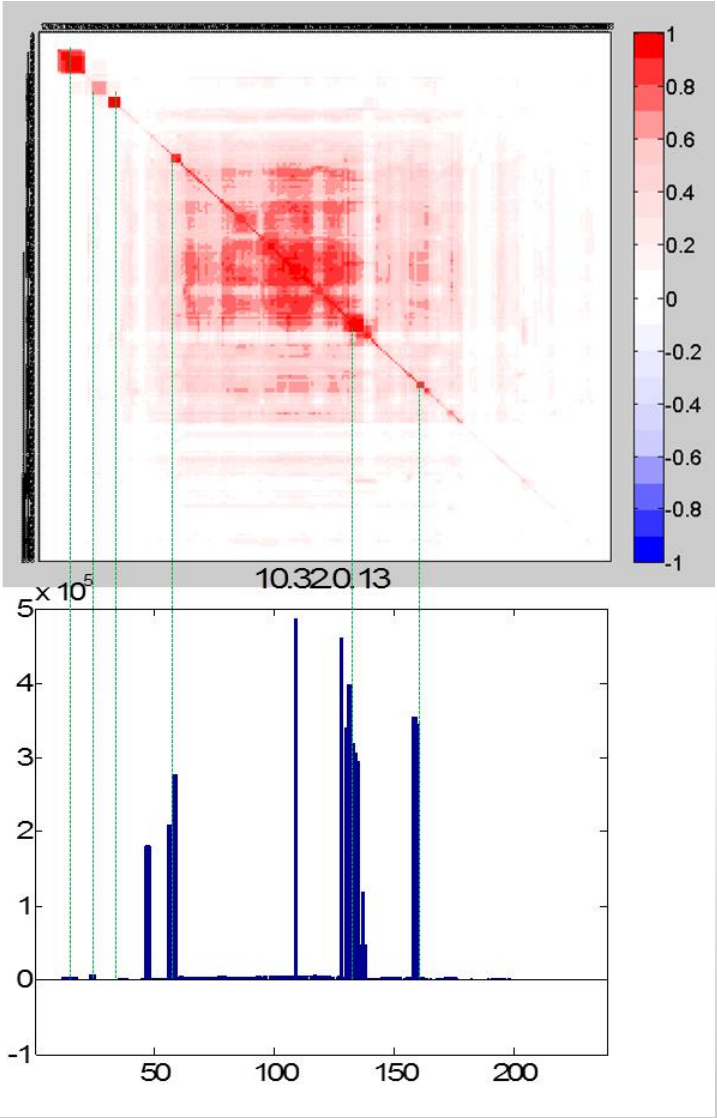


DETECTANDO AL INTRUSO CON ANÁLISIS MULTIVARIANTE



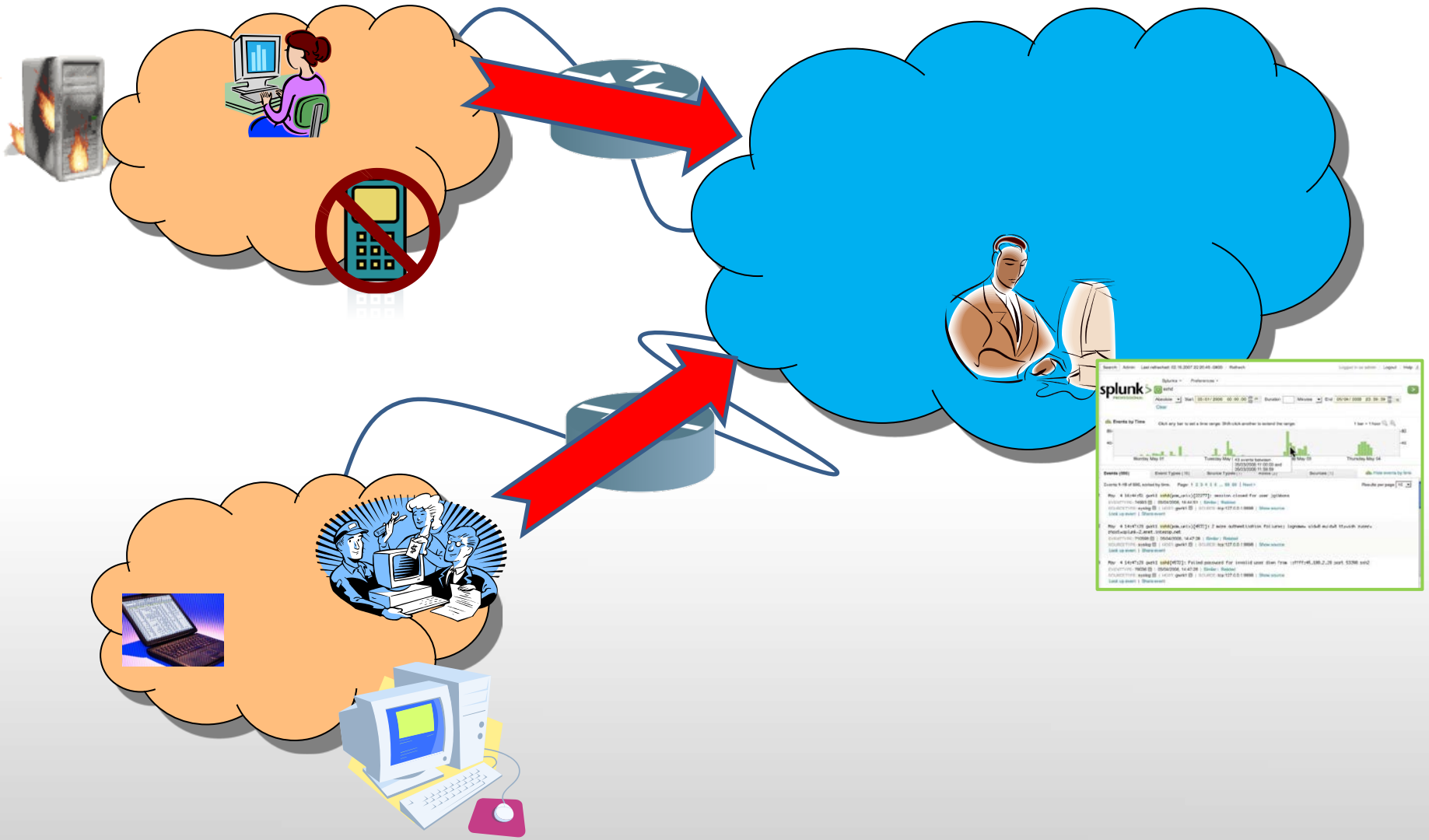


DETECTANDO AL INTRUSO CON ANÁLISIS MULTIVARIANTE

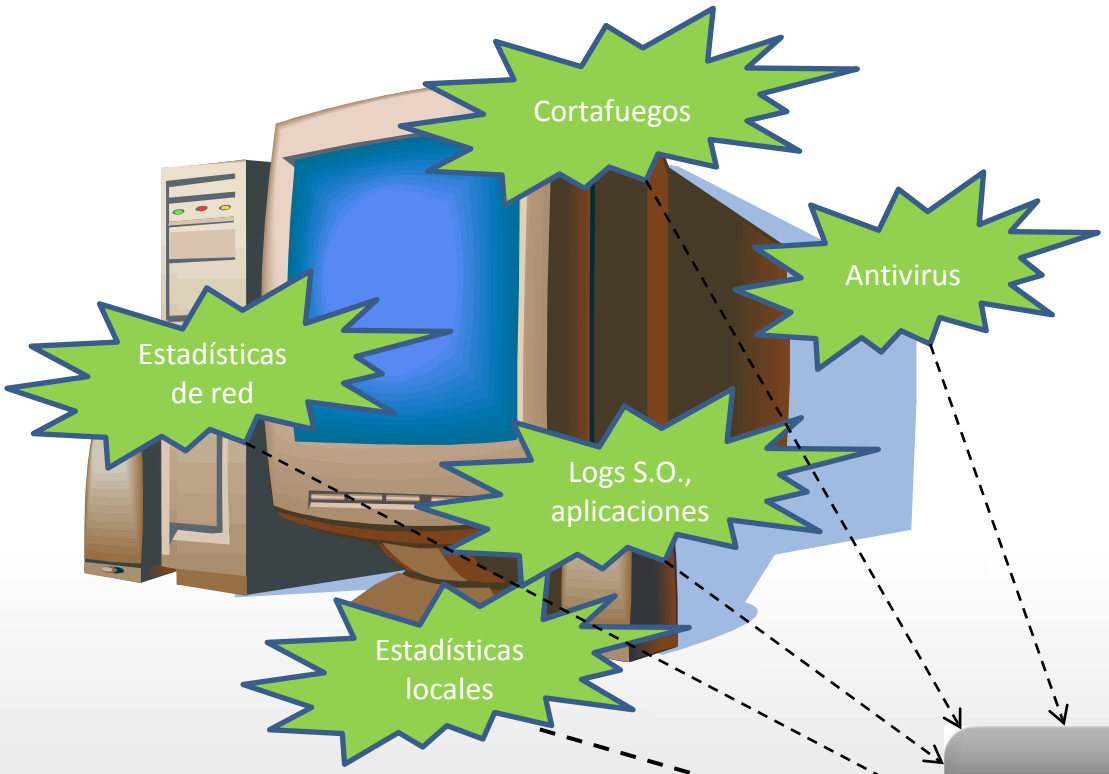


'10.32.0.13'	'10.32.0.50'	'10.32.41.128'
'47.url-pc-SPAMURLs' '58.url-tcPHISHING' '131.url-pc-MalwareSites' '135.url-tcMALICIOUSHOST' '160.url-tcSUSPICIOUS'	'30.ip-pc-Scanners' '31.ip-tcSCANNING'	'30.ip-pc-Scanners' '31.ip-tcSCANNING' '131.url-pc-MalwareSites' ‘135.url-tcMALICIOUSHOST' '136.url-pc-SpyAd'

- ✓ Seguridad en Cifras
- ✓ Seguridad en Redes Corporativas
- ✓ Docencia:
  - ✓ Laboratorio Virtual de Seguridad en Red
- ✓ Investigación:
  - ✓ Detectando al intruso con Análisis Multivariante
  - ✓ **Aplicación en Redes y Servicios Avanzados (Proyecto VERITAS)**

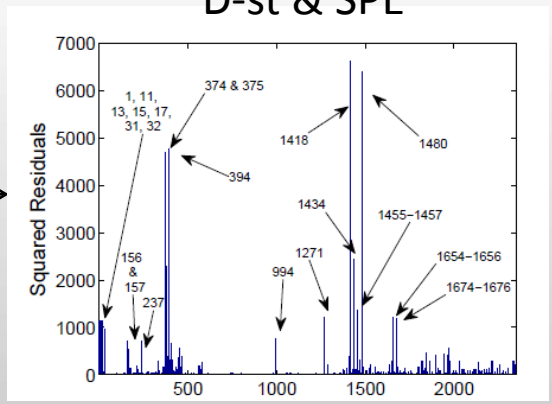

splunk>

APLICACIÓN EN REDES Y SERVICIOS AVANZADOS: PROYECTO VERITAS

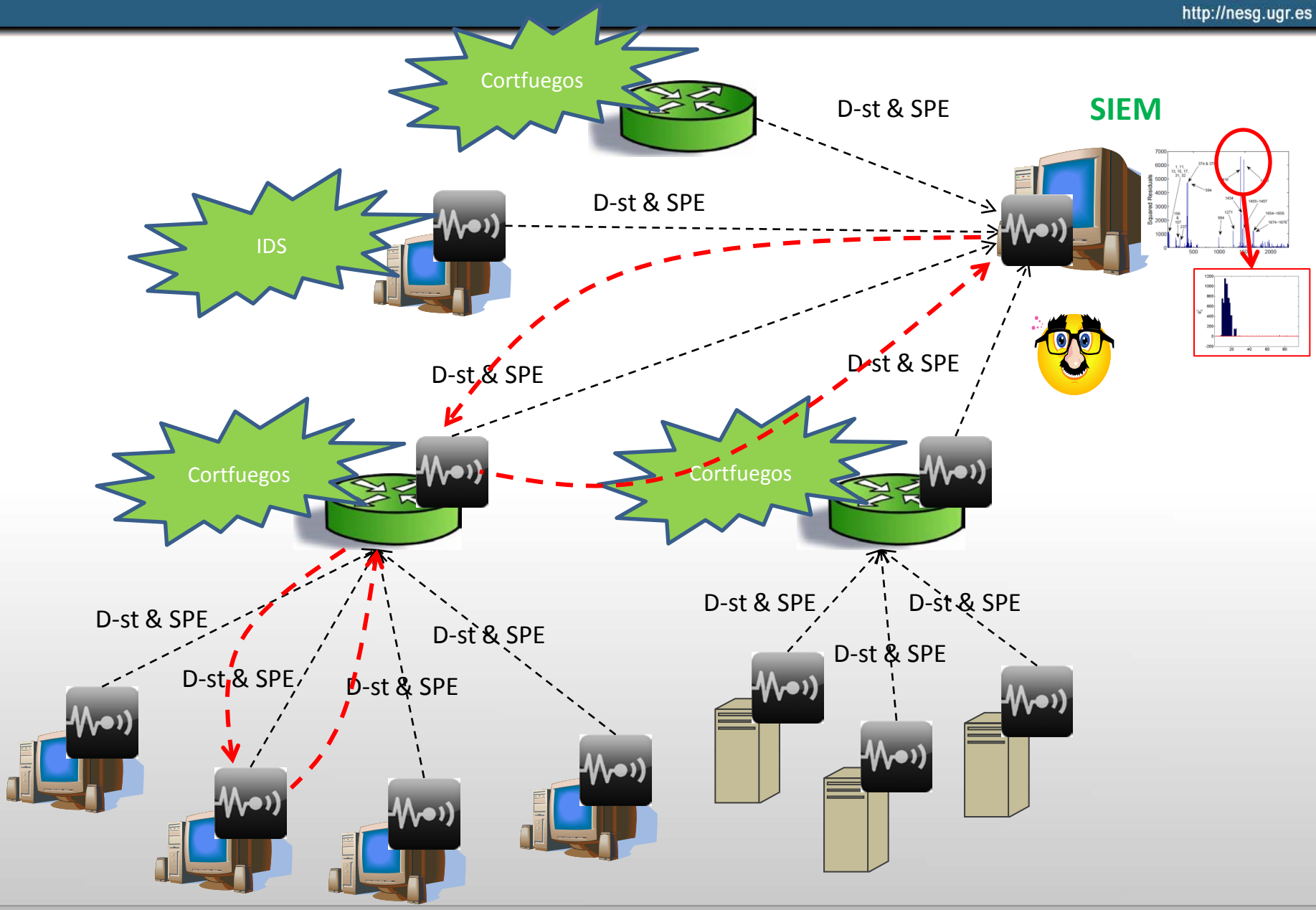


Sensor PCA

D-st & SPE



APLICACIÓN EN REDES Y SERVICIOS AVANZADOS: PROYECTO VERITAS



Grupo Trevenque

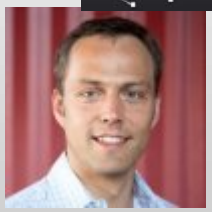
VNiVERSiDAD D SALAMANCA

VERITAS

Visualización de Eventos en Red Inteligente para el Tratamiento y Análisis de la Seguridad

VIS-SENSE

pixlcloud



Seguridad en Redes Corporativas
Detectando al Intruso

José Camacho

Departamento de Teoría de la Señal, Telemática y Comunicaciones

Organiza: Grupo en Ciberseguridad de la UGR

Network Engineering & Security Group
http://nesg.ugr.es

Universidad de Granada