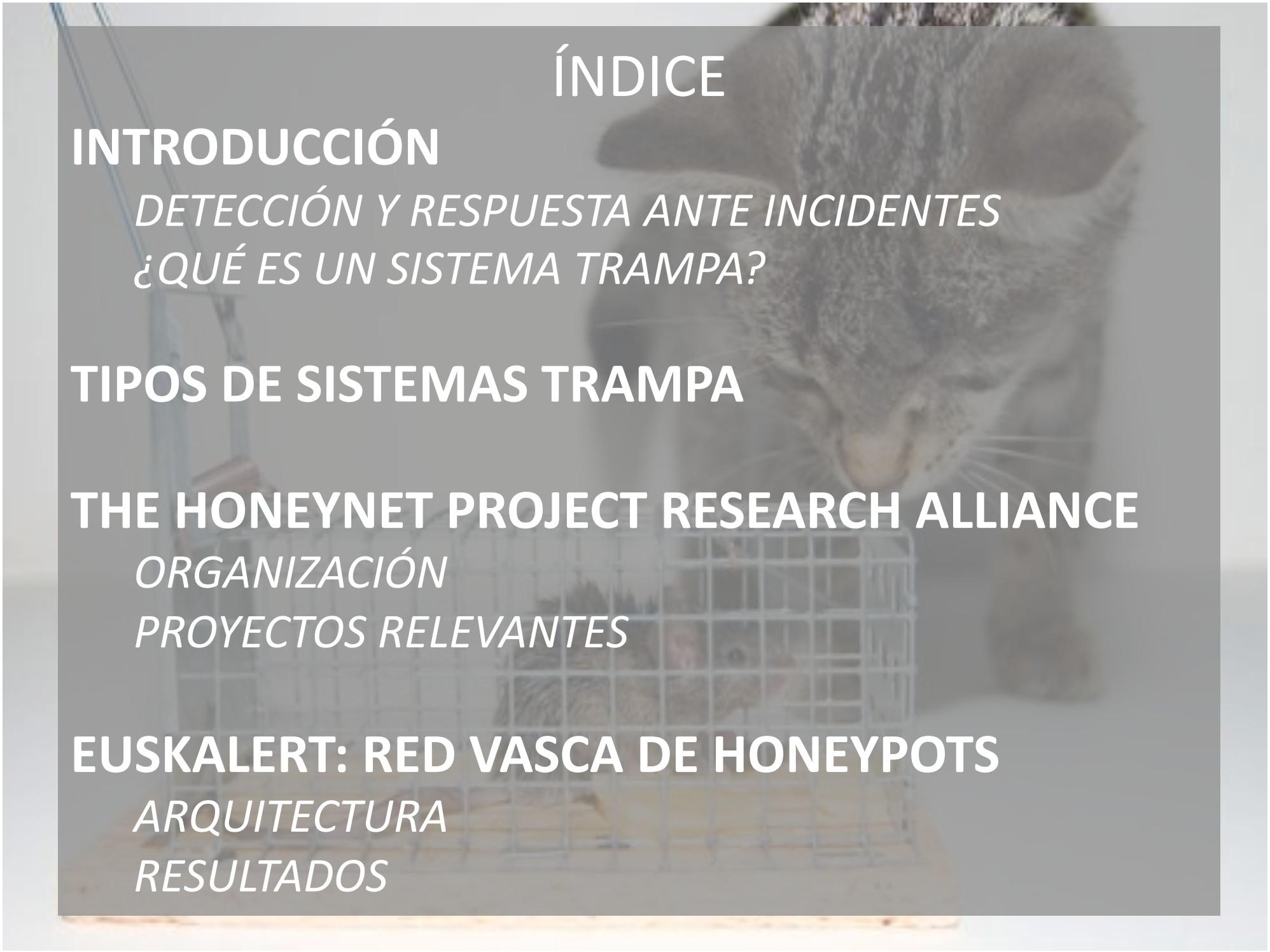
Máquinas trampa: Conoce a tu enemigo

Urko Zurutuza

Mondragon Unibertsitatea

Miramon Enpresa Digitala, Donostia, 18/03/2010

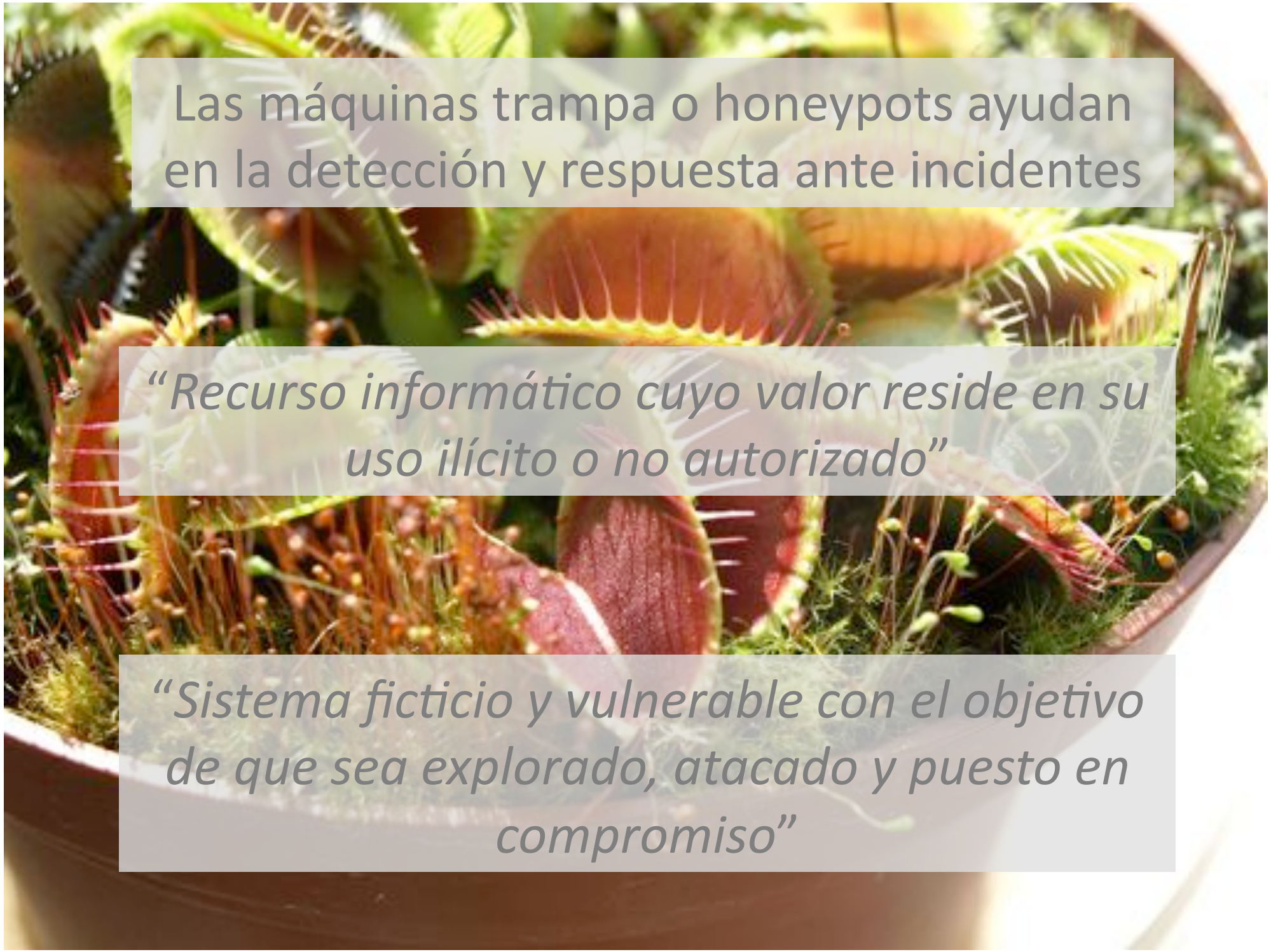


ÍNDICE


INTRODUCCIÓN

Dificultad para analizar los métodos y técnicas de atacantes

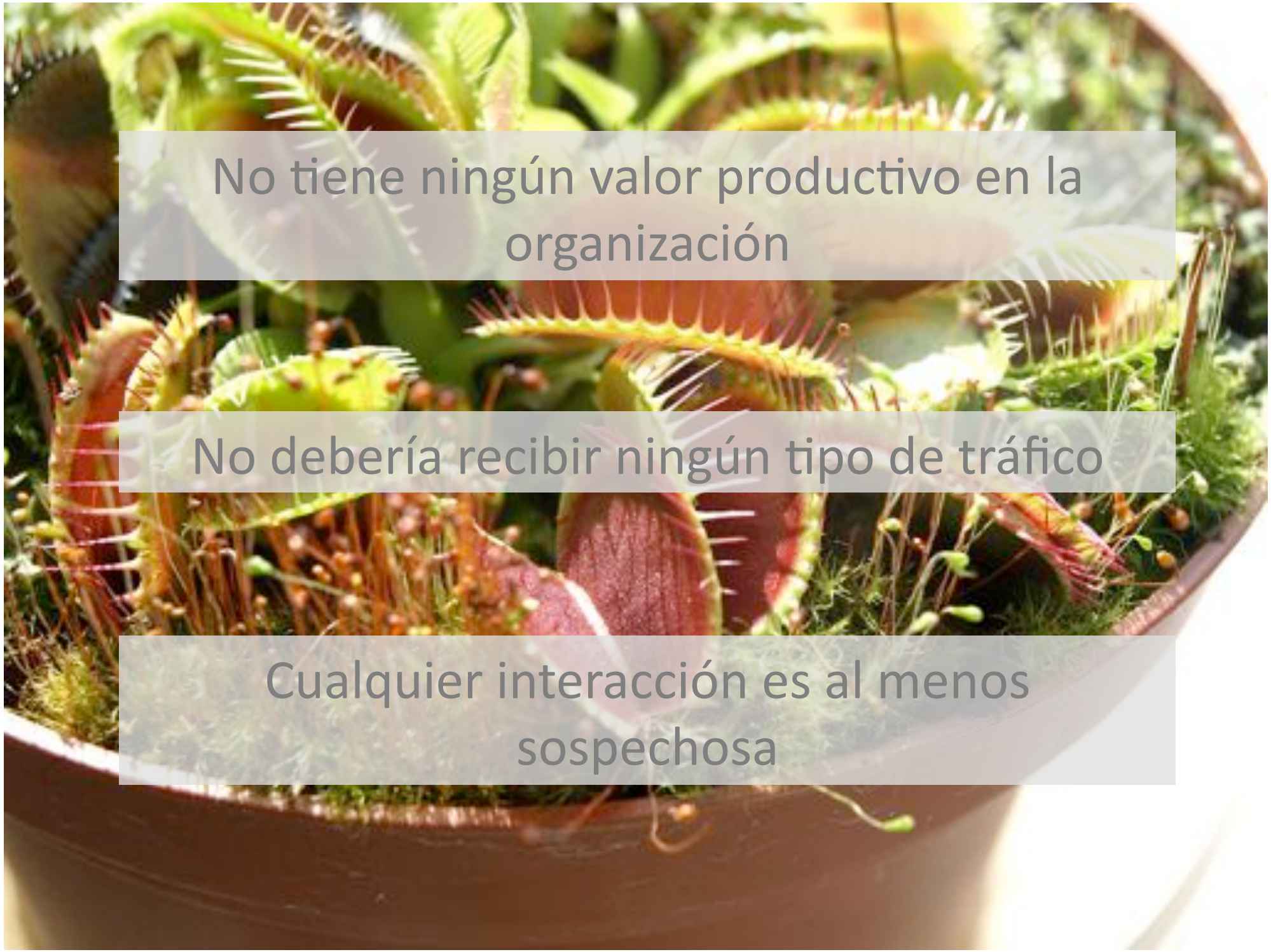
Detección y respuesta ante Incidentes: Logs y más logs



Las máquinas trampa o honeypots ayudan en la detección y respuesta ante incidentes

"Recurso informático cuyo valor reside en su uso ilícito o no autorizado"

"Sistema ficticio y vulnerable con el objetivo de que sea explorado, atacado y puesto en compromiso"

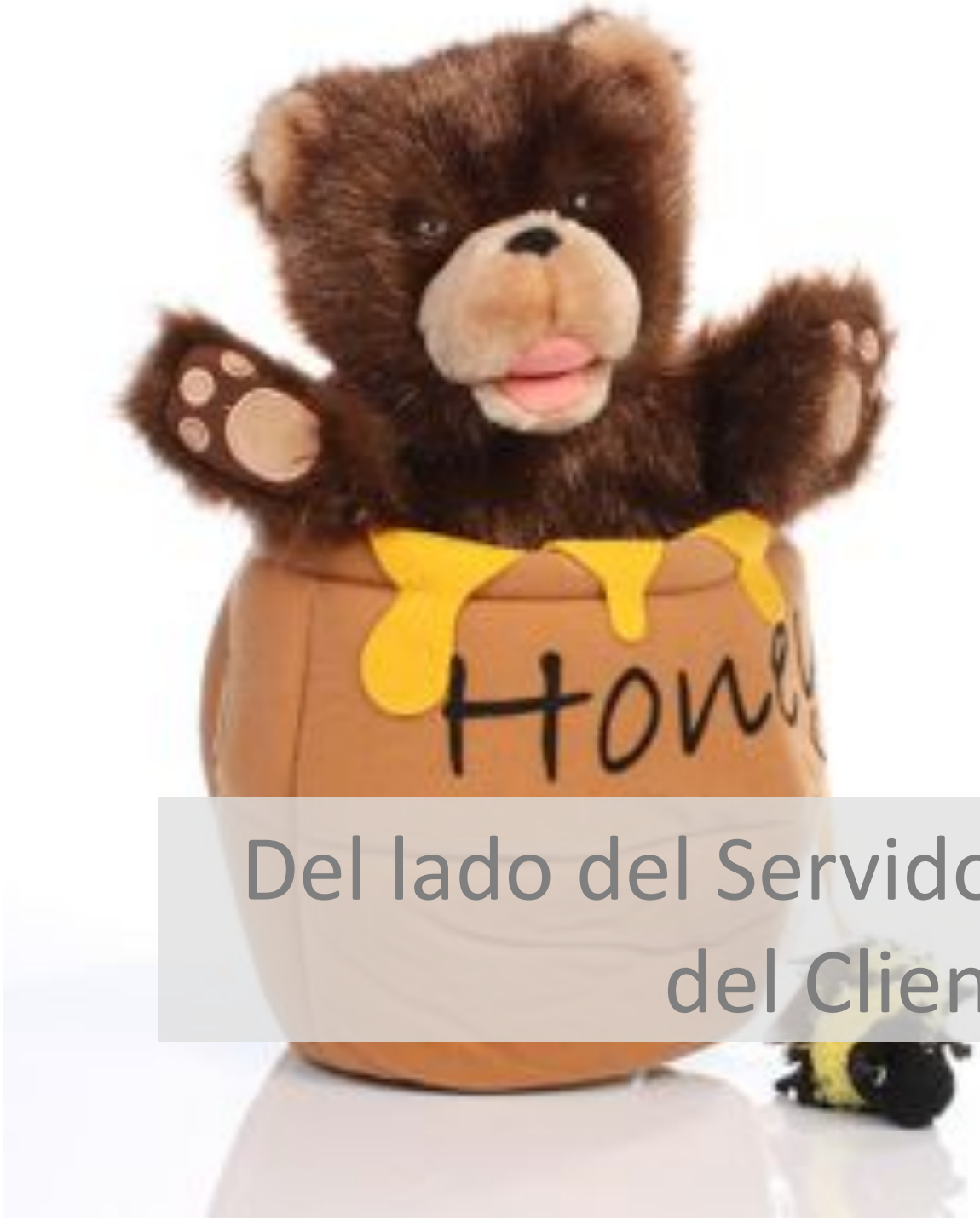

No tiene ningún valor productivo en la organización
No debería recibir ningún tipo de tráfico
Cualquier interacción es al menos sospechosa


TIPOS

Alta Interacción Vs. Baja Interacción

- *honeyd*
- *nepenthes*
- *Amun*
- *honeytrap*
- *…*

Máquinas Reales Vs. Máquinas Virtuales



- *Capture HPC*
- *HoneyC*
- *phoneyc*
- *MonkeySpider*
- *…*

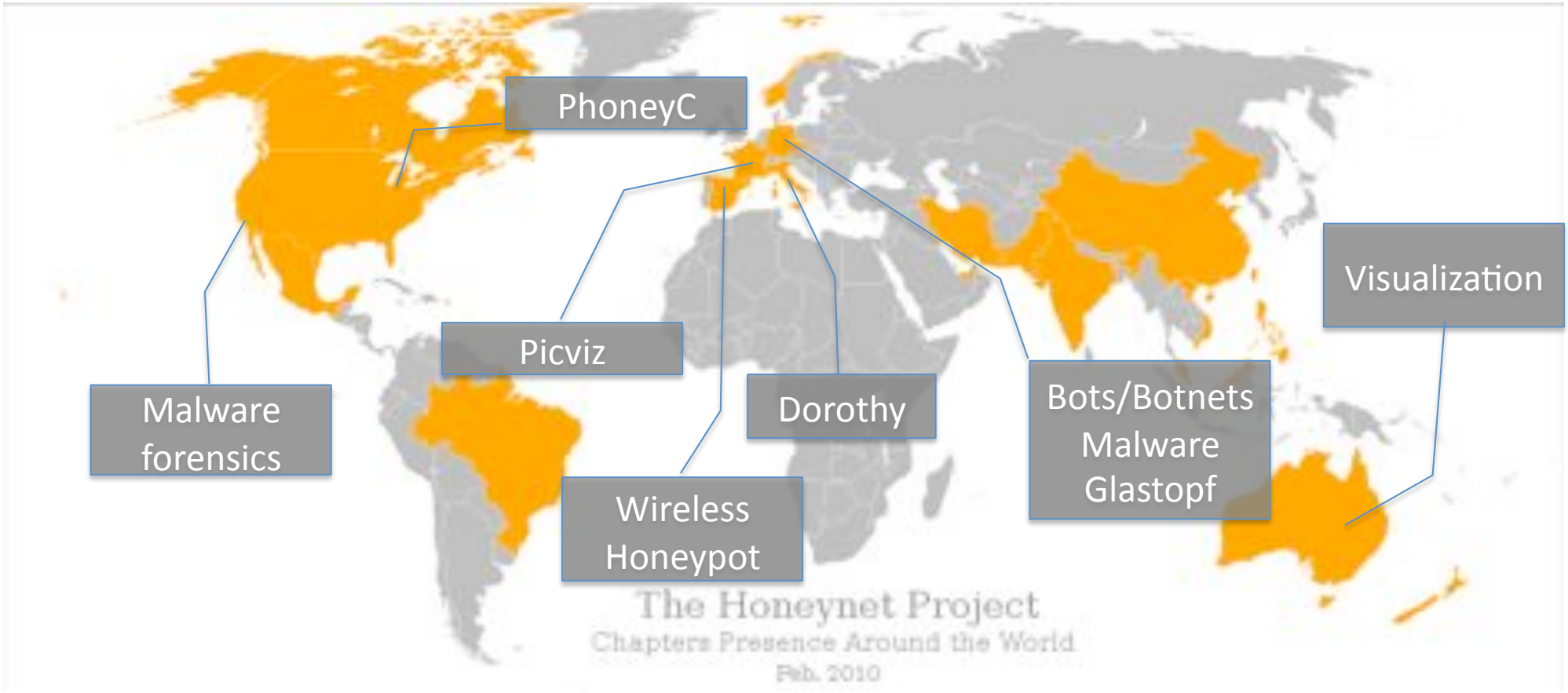
Del lado del Servidor Vs. del lado del Cliente


HONEYNET
PROJECT
HN/P

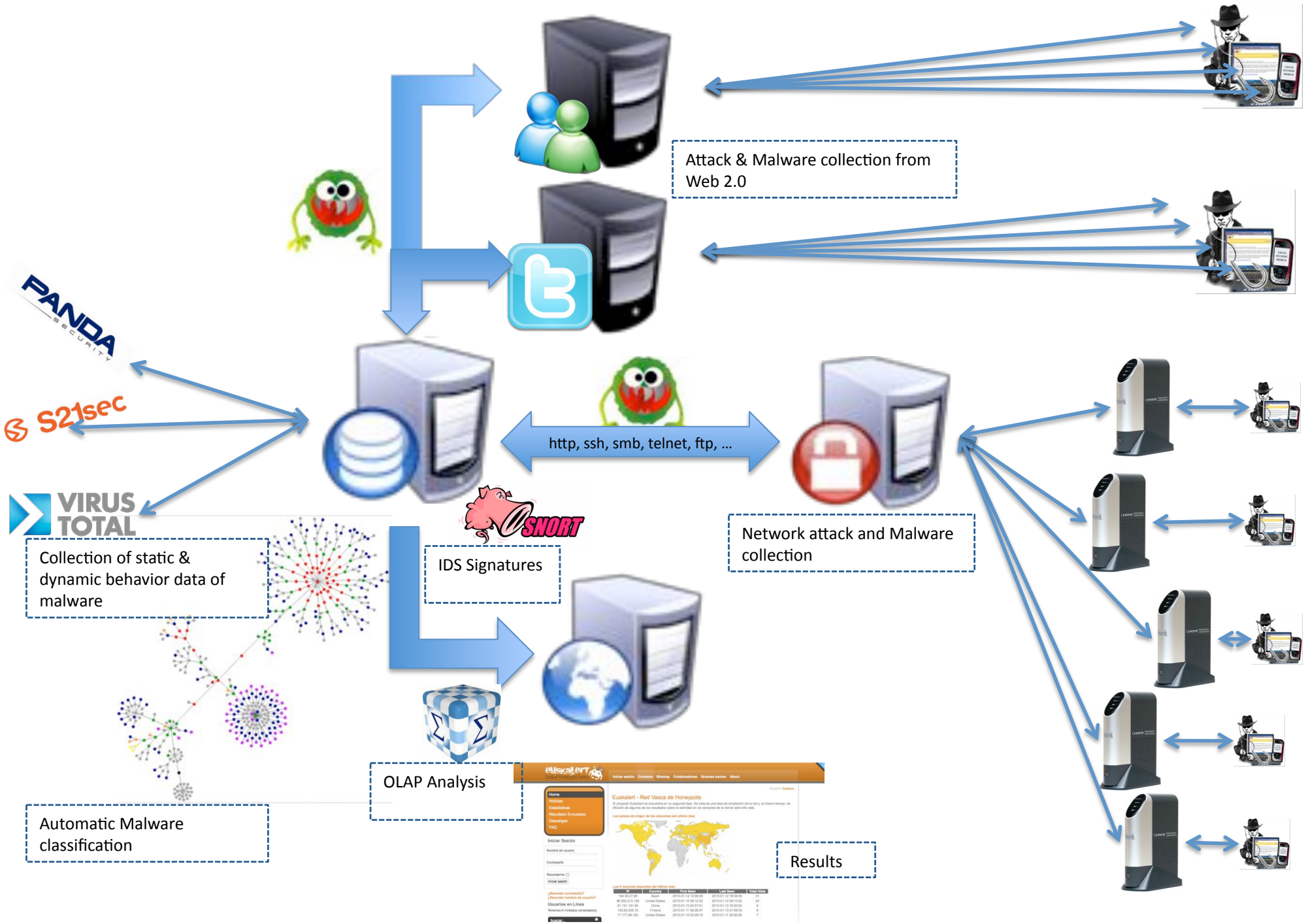

GenI
Honeynets
GenII
Honeynets
GenIII
Honeynets

The Honeynet PROJECT

Grupos distribuidos en el mundo
Cada grupo debe hacer algo diferente
Compartir las lecciones aprendidas




EUSKALERT
www.euskalert.net


Attack & Malware collection from Web 2.0
PANDA SECURITY
S21sec
VIRUS TOTAL
http, ssh, smb, telnet, ftp, ...
SNORT
Network attack and Malware collection
Collection of static & dynamic behavior data of malware
IDS Signatures
OLAP Analysis
Automatic Malware classification
Results

www.euskalert.net

Intentos de accesos Vía FTP:

"RMD sarcaxxo”
"PASS .”
"USER administrator”
"PASS NULL”
"MKD 090713182104p”
"CWD /public/”
"PASS Pgpuser@home.com”
"USER anonymous PASS ftp@example.com PWD EPSV PASV CWD pub PASV CWD publicPASV CWD pub CWD incoming PASV CWD incoming PASV CWD _vti_pvt PASV CWDupload PASV QUIT”

Ataques / pruebas vía HTTP:

GET /twiki/bin/statistics HTTP/1.1 Accept: */* Accept-Language: en-usAccept-Encoding: gzip, deflate User-Agent: Toata dragostea mea pentrudiavola Host: ***.***.***.49 Connection: Close

OPTIONS / HTTP/1.1 translate: f User-Agent:Microsoft-WebDAV-MiniRedir/5.1.2600 Host: ***.***.***.61 Content-Length: 0Connection: Keep-Alive

GET /roundcube/program/js/list.js HTTP/1.1 Accept: */* Accept-Language:en-us Accept-Encoding: gzip, deflate User-Agent: Toata dragostea mea pentrudiavola Host: ***.***.***.49 Connection: Close

GET/unauthenticated/..%01/..%01/%01/..%01/..%01/..%01/..%01/..%01/etc/passwdHTTP/1.1 Accept: */* Accept-Language: en-us Accept-Encoding: gzip, deflateUser-Agent: Toata dragostea mea pentru diavola Host: ***.***.***.49Connection: Close

POST /webmail/bin/html2text.php HTTP/1.0 Host: ***.***.***.69 User-Agent:Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2)Content-length: 54 Accept: ZWNobygiU3VjY2VlZGVkISA6KSlcclxuXHJcbi4iKTsK{${EVAL(BASE64_DECODE($_SERVER[HTTP_ACCEPT]))}}

Máquinas trampa: Conoce a tu enemigo

uzurutuza@eps.mondragon.edu

Mondragon Unibertsitatea

Miramon Enpresa Digitala, Donostia, 18/03/2010