Aalto University
School of Science
and Technology

On the use of name server log data as input for security measurements

Christian Frühwirth
SBL, Aalto University, Finland
christian.fruehwirth@tkk.fi

Christian Proschinger
CERT.at , Austria
proschinger@cert.at

Otmar Lendl
CERT.at , Austria
lendl@cert.at

Austrian national Computer Emergency Response Team

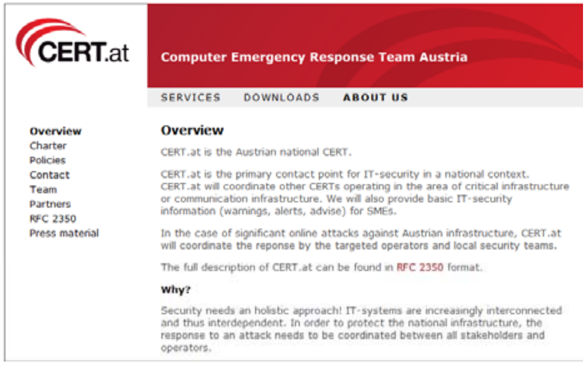
- Mission Statement

  “The purpose of CERT.at is to coordinate security efforts and incident response for IT-security problems on a national level in Austria. “

- Constituency

  “The constituency are IT-security teams and local CERTs in Austria. Pro-active and educational material will be provided for SMEs and the general public as well.”

- Initiative from Nic.at – the Austrian registry



Overview

CERT.at is the Austrian national CERT.

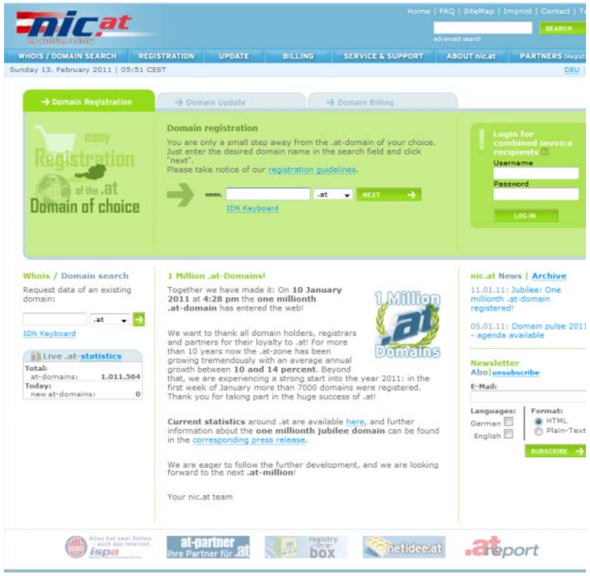
CERT.at is the primary contact point for IT-security in a national context. CERT.at will coordinate other CERTs operating in the area of critical infrastructure or communication infrastructure. We will also provide basic IT-security information (warnings, alerts, advise) for SMEs.

In the case of significant online attacks against Austrian infrastructure, CERT.at will coordinate the reponse by the targeted operators and local security teams.

The full description of CERT.at can be found in RFC 2350 format.

Why?

Security needs an holistic approach! IT-systems are increasingly interconnected and thus interdependent. In order to protect the national infrastructure, the response to an attack needs to be coordinated between all stakeholders and operators.



Sunday 13. February 2011 | 05:51 CEST

Domain registration

You are only a small step away from the .at-domain of your choice. Just enter the desired domain name in the search field and click "next".
Please take notice of our registration guidelines.

Whois / Domain search

Request data of an existing domain:

Live .at-statistics

Total:
at-domains: 1.011.564
Today:
new at-domains: 0

1 Million .at-Domains!

Together we have made it: On **10 January 2011** at **4:28 pm** the **one millionth .at-domain** has entered the web!

We want to thank all domain holders, registrars and partners for their loyalty to .at! For more than 10 years now the .at-zone has been growing tremendously with an average annual growth between **10 and 14 percent**. Beyond that, we are experiencing a strong start into the year 2011: in the first week of January more than 7000 domains were registered. Thank you for taking part in the huge success of .at!

Current statistics around .at are available here, and further information about the **one millionth jubilee domain** can be found in the corresponding press release.

We are eager to follow the further development, and we are looking forward to the next **.at-million**!

Your nic.at team

nic.at News | Archive

11.01.11: Jubilee: One millionth .at-domain registered!

05.01.11: Domain pulse 2011 - agenda available

Newsletter
Abo | unsubscribe

E-Mail:

Languages: German □ English □

Format: ● HTML ○ Plain-Text

Motivation

- National CERT's mission is to inform its constituency about security issues and facilitate communication between its partners (ISPs, companies, universities, end-users, other CERTs)

- DNS logs are a rich, and readily available, data source for security measurement (from large organizations->companies -> end users).

→ Individual analysis of DNS Logs proved useful in the past, but without **cooperation** between organizations, our (CERT's) field of view is limited.

→ We **wanted an overview** of how and where the Analysis of DNS logs for security measurement purposes is already working well, and **where we should focus** our improvement (i.e. cooperation) efforts.

Goal

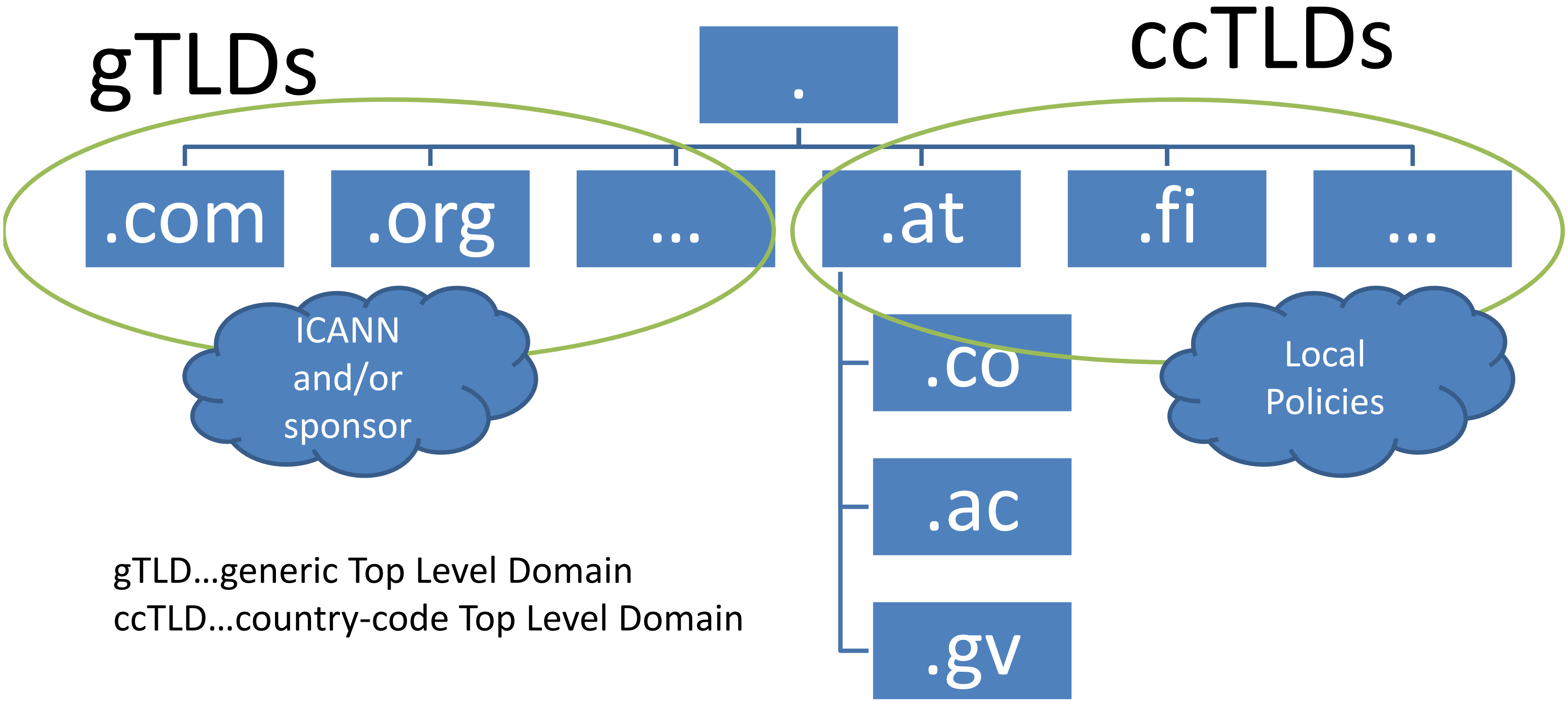
- Give a **high-level overview** of how DNS is & can be used for practical security measurement by members of CERTs' constituency

- Help CERT stakeholders understand where cooperation is beneficial.

→ **Encourage more companies & organizations to partner with CERTs** and improve security trend monitoring

Quick DNS 101

DNS hierarchy



gTLD…generic Top Level Domain
ccTLD…country-code Top Level Domain

Passive DNS

- Passive collection of DNS server replies
  - Allows to determine
    - Change of IP adresses behind domains
    - Change of nameservers
    - Domains hosted at the same IP
  - Major **limitation**: Passive DNS requires sensors in different networks

Approach

How to structure a high-level overview of DNS use in sec. measurement?

Our approach:

- DNS log analysis is used for security measurement by
  - different entities (**stakeholders**) with
  - different measurement capabilities (**fields of view**) on
  - different measurement elements in the security vulnerability-threat-incident chain of events.

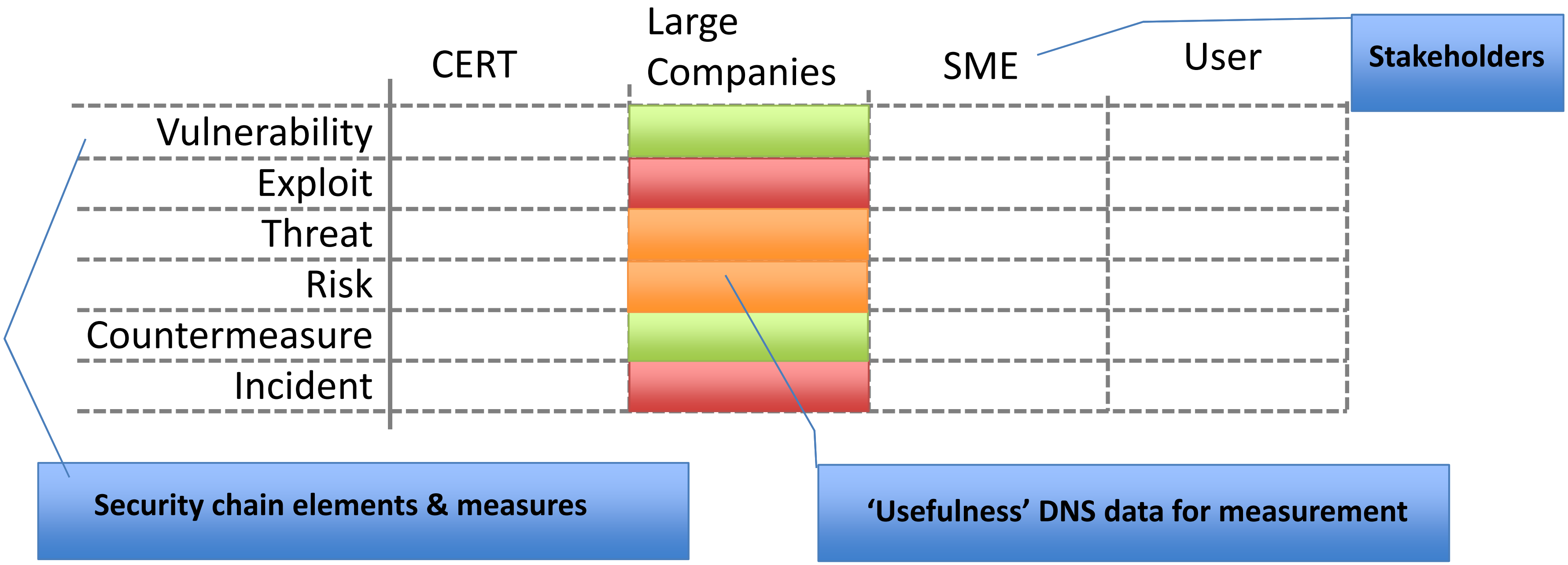
→We organize the use of DNS for sec. measurement by

1.) **Stakeholder type** & **field of view**

2.) Security measurement elements (Based on: security relationship, in CISSP All-in-one-Guide Fourth Edition, S. Harris, p.63)

1.) Create matrix for stakeholders and security chain / measurements

2.) Fill cells with color-coded description of possible DNS log data use



	CERT	Large Companies	SME	User
Vulnerability		🟩		
Exploit		🟥		
Threat		🟧		
Risk		🟧		
Countermeasure		🟩		
Incident		🟥		

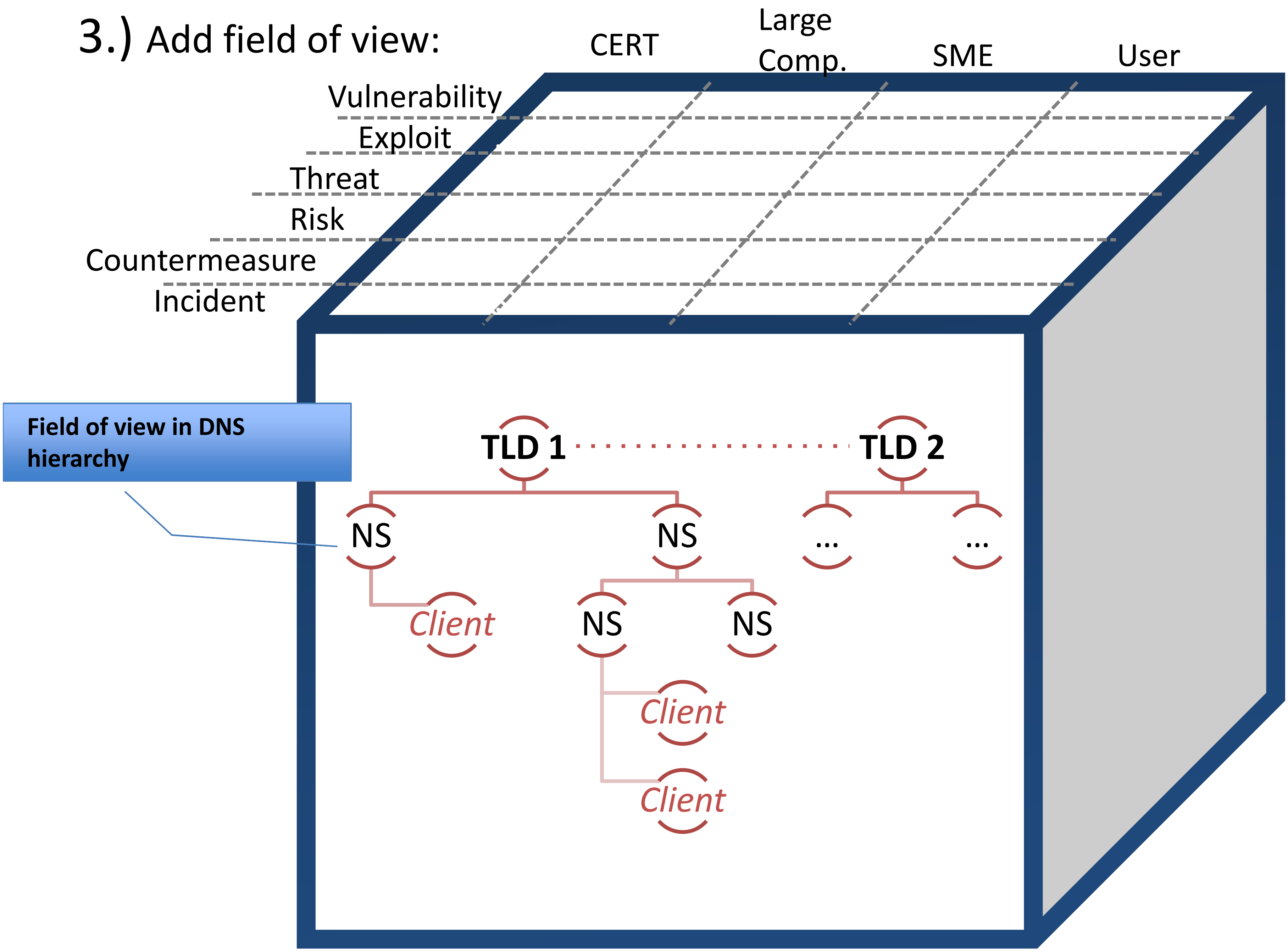
Stakeholders
Security chain elements & measures
'Usefulness' DNS data for measurement

Vulnerability	# of vulnerable Systems
Exploit	Signs of exploited vulnerabilities
Threat	Severity of threat (based on V, E)
Risk	Risk for group of stakeholders
Countermeasure	# of countermeasures deployed / Vuln. Fixed
Incident	# of incidents that occurred

Color coded cells:

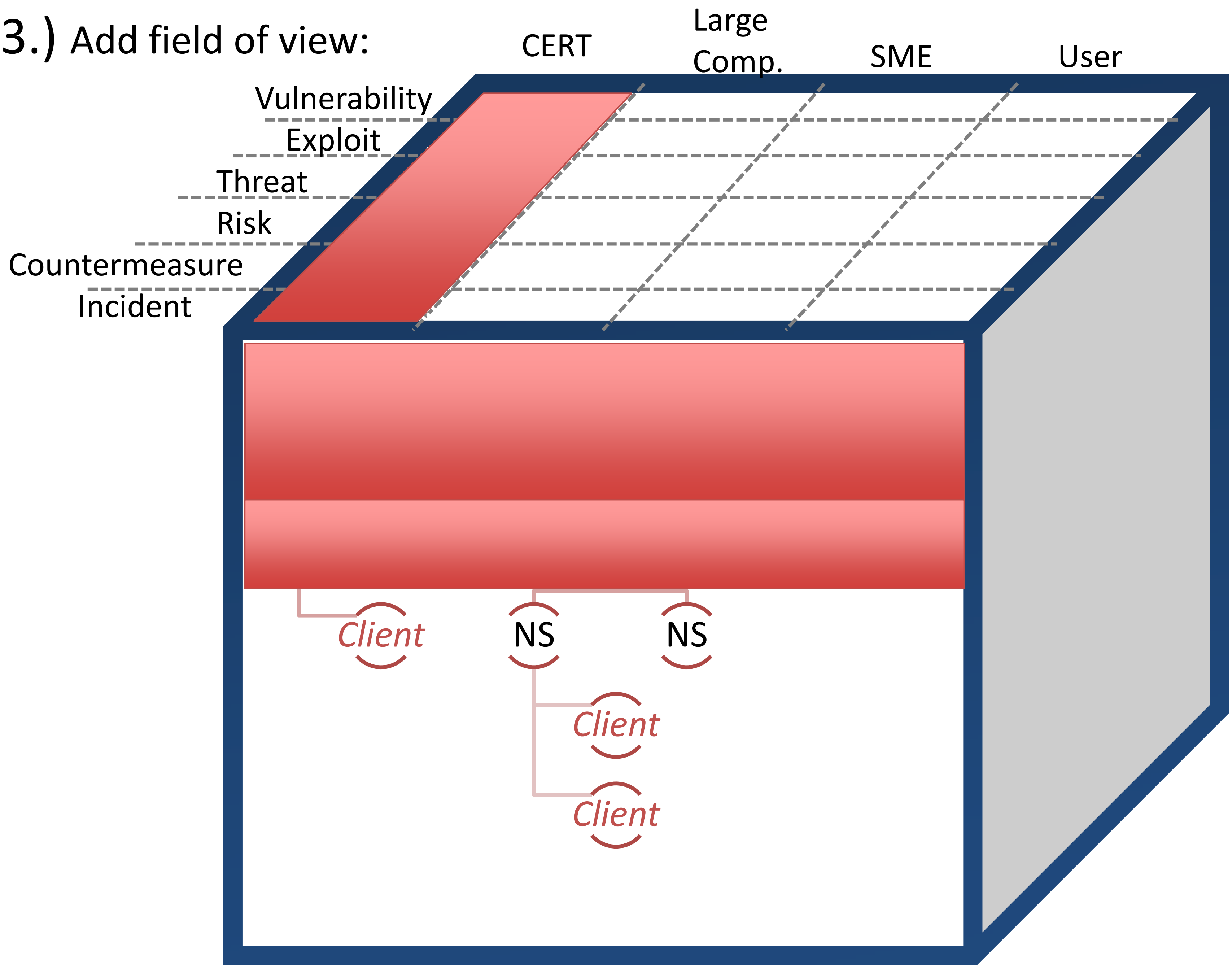
🟥	Cooperation with 3rd party required
🟧	Sucessfull measurement depends on cooperation with 3rd party at earlier stage
🟩	Measurement is possible
⬜	Measurement not possible or N/A

3.) Add field of view:

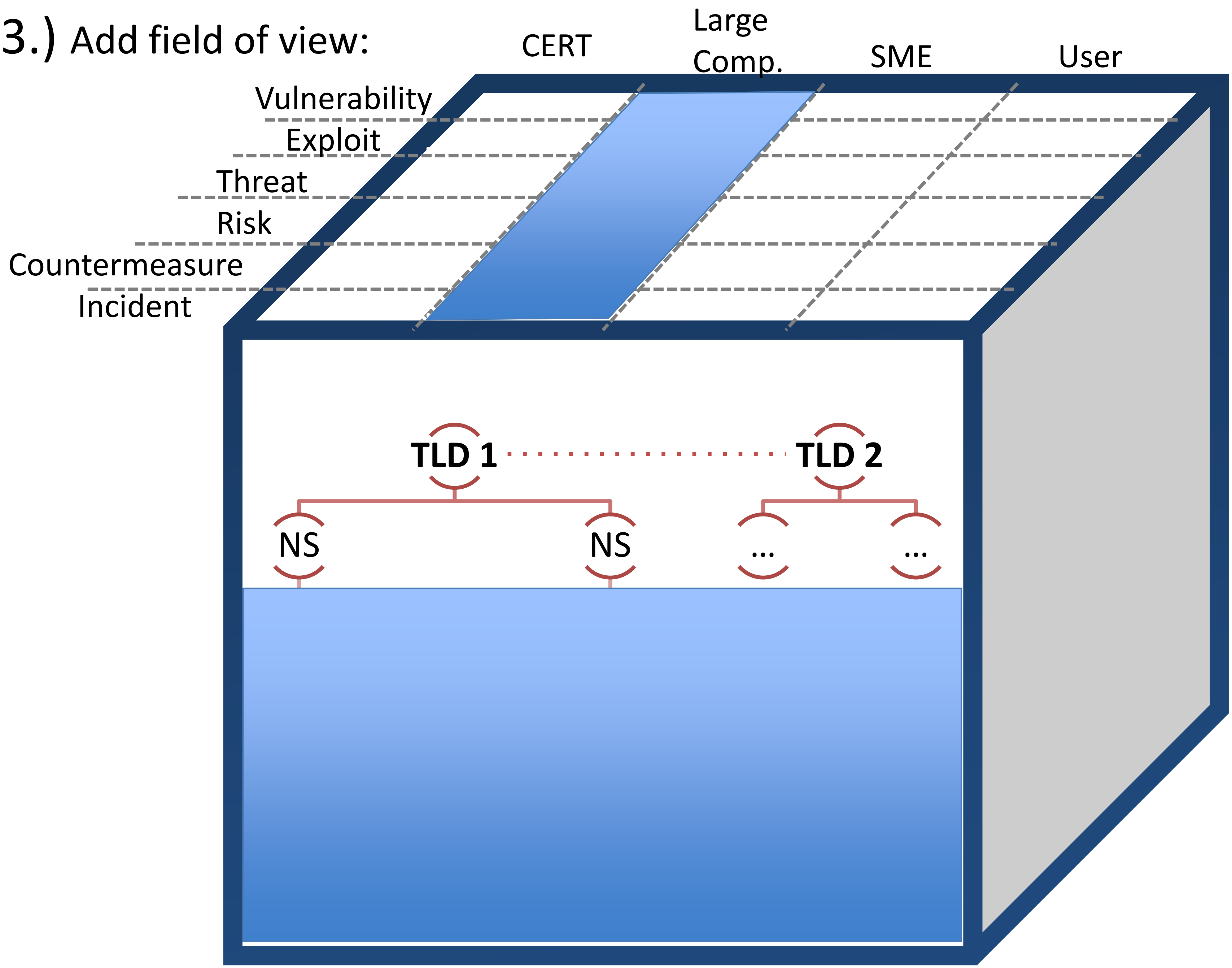


Field of view in DNS hierarchy

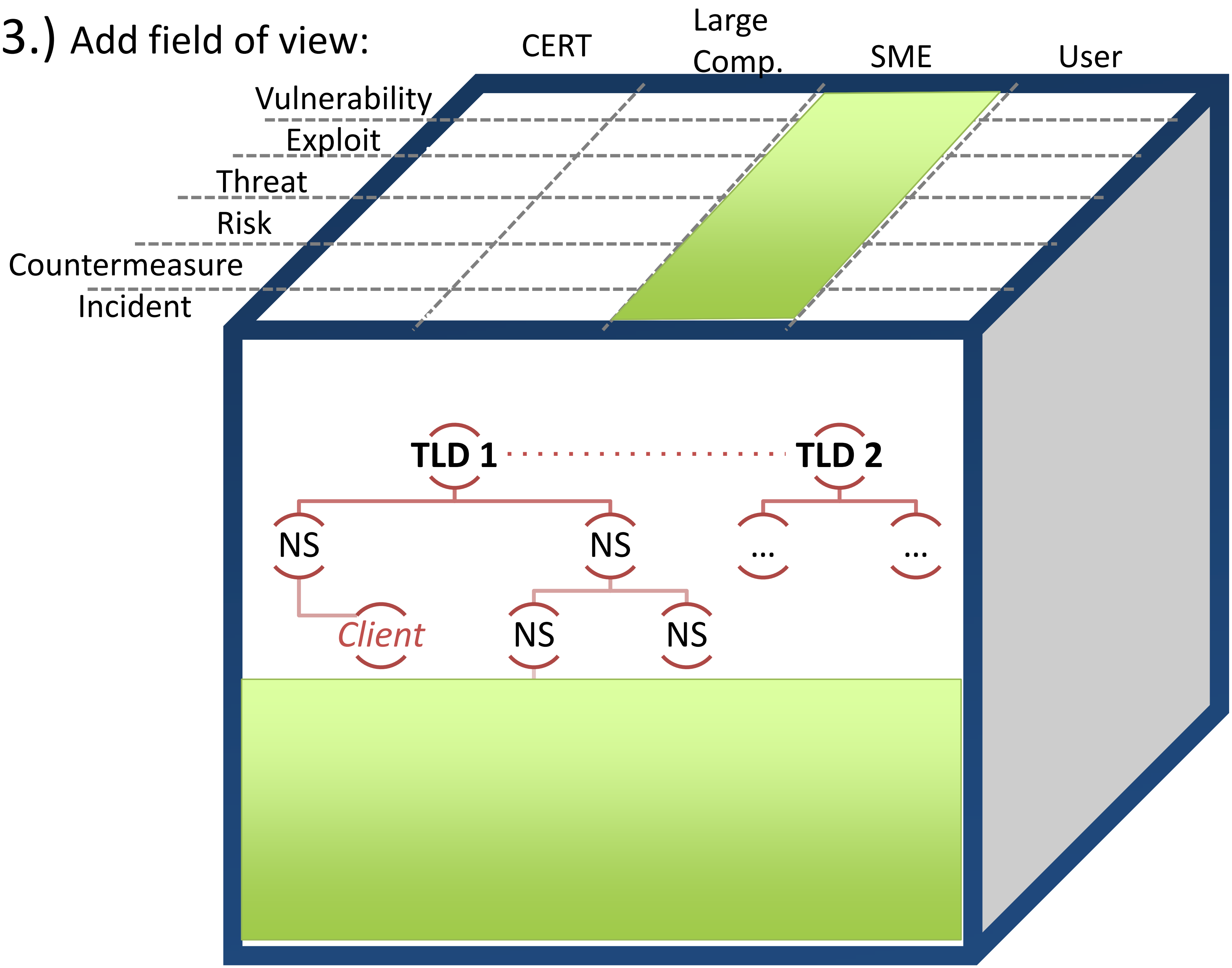
3.) Add field of view:



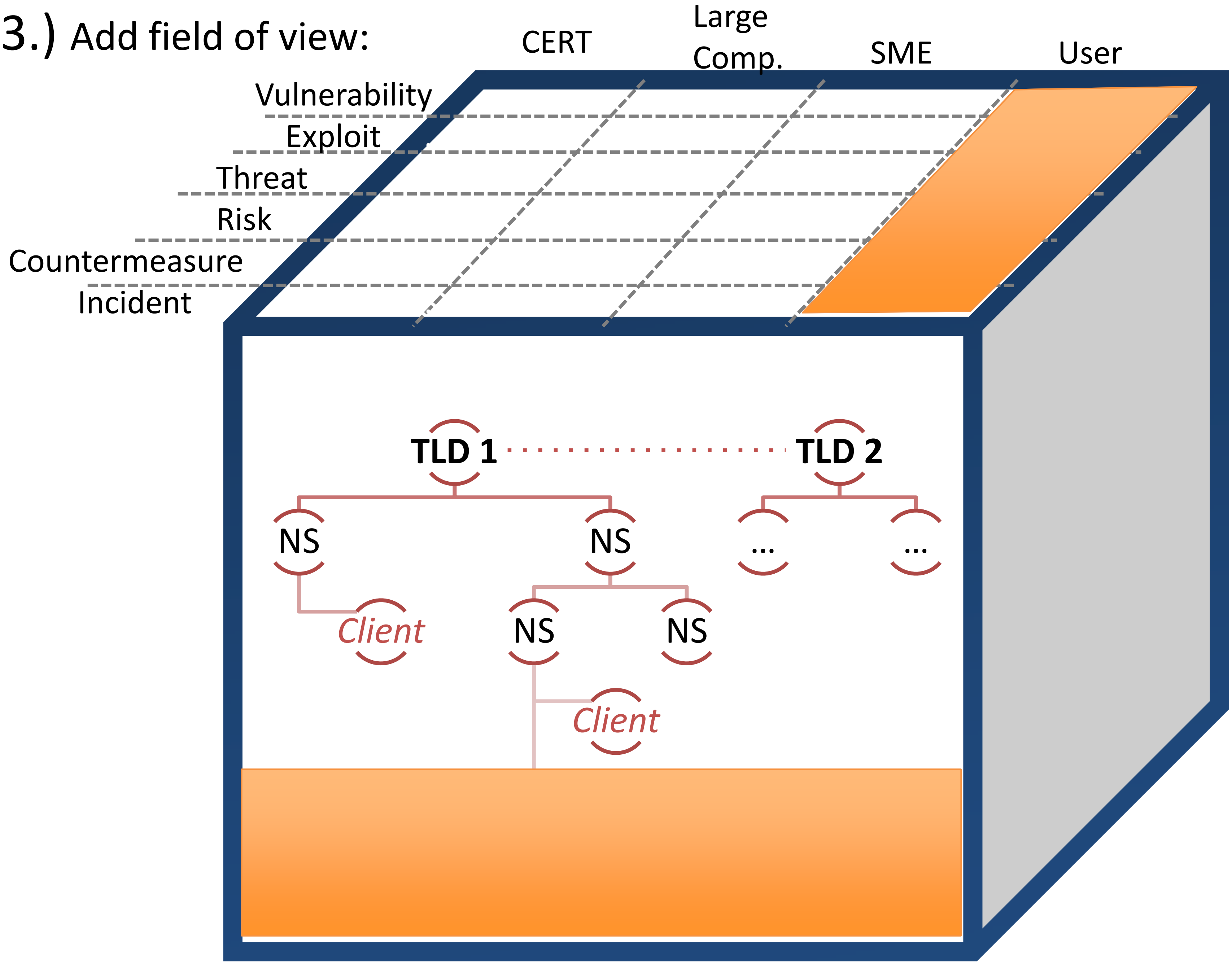
3.) Add field of view:



3.) Add field of view:



3.) Add field of view:



4.) Apply to use cases:

We applied the categorization to 4 cases where DNS played an important role in understanding and measuring the security issue at hand.

- Targeted Attack: **Aurora**
- Worm: **Conficker**
- Technology issue: **DNS Kaminsky Bug**
- Industrial Malware: **Stuxnet**

DNS log analysis use cases
Experiences - Results

Aurora

- 12.1.2010 – Google announced attack

  -over 30 other organization affected too
- Infection by
  - drive-by download
  - Zero day exploit
- CnC Server
  - Based on DynamicDNS

Aurora

Stage	Measure	CERT	Large Company	SME	EndUser
Vulnerability	# of vulnerable Systems				
Exploit	Signs of exploited vulnerabilities	A (if info from DDNS providers is available)	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party
Threat	Severity of threat (based on V, E)	A (if info from DDNS providers is available)			
Risk	Risk for group of stakeholders				
Countermeasure	# of countermeasures deployed / Vuln. Fixed	A *	A *	A (*)	A (*)
Incident	# of incidents that occured	A (if info from DDNS providers or victims is available)	A (visible in NS and local cache)	A (visible in local cache)	A (visible in local cache)

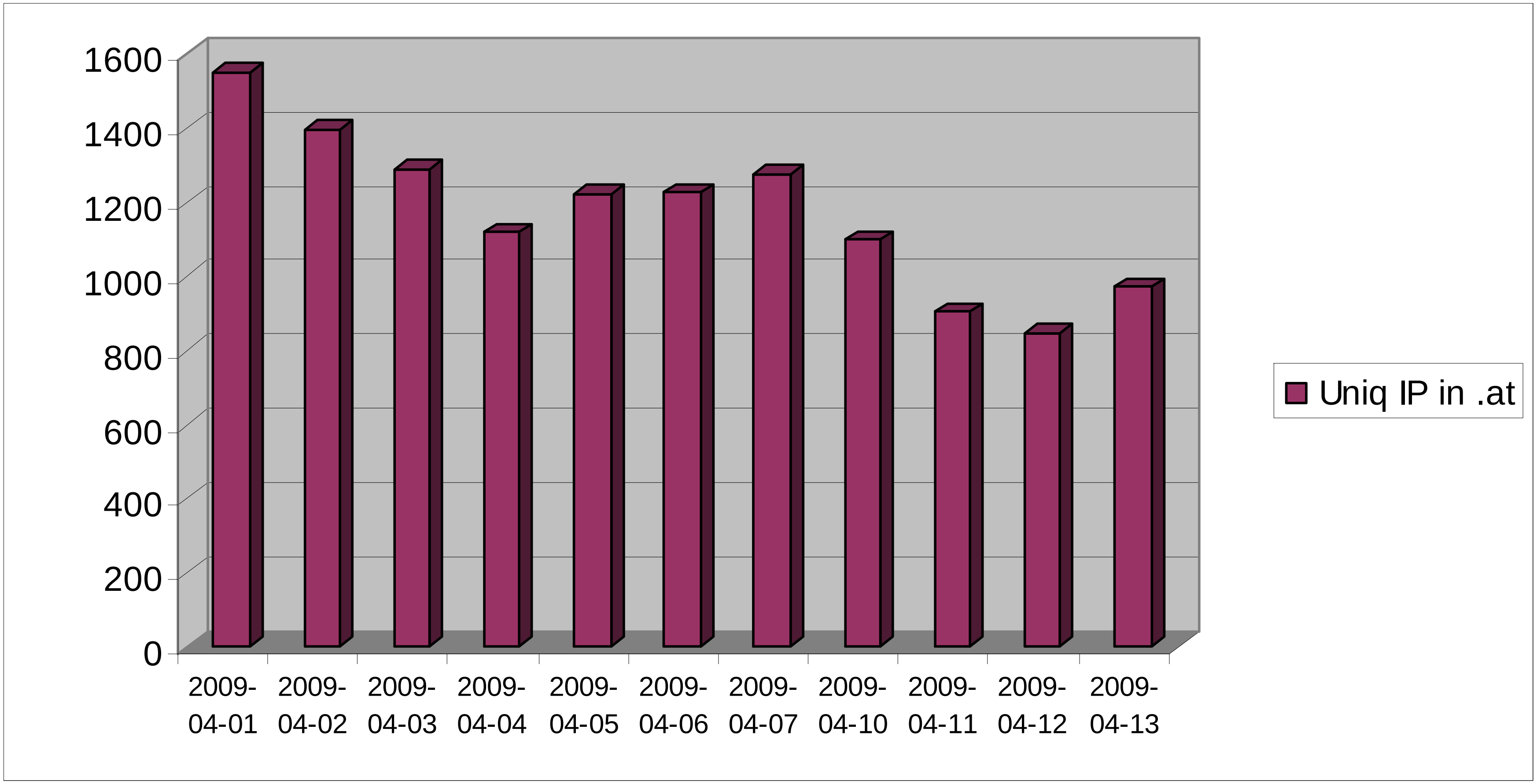
Conficker and DNS

AutoPlay
Removable Disk (E:)
□ Always do this for software and games:
Install or run program
Open folder to view files
Published by Microsoft Windows
General options
Open folder to view files
using Windows Explorer
Speed up my system
using Windows ReadyBoost
Set AutoPlay defaults in Control Panel

- Pseudorandom domains
  - Conficker.B: 250 / day
  - Conficker.C: 450 .at domains / day
- Large Scale
  - Aconet CERT runs nameservers and a sinkhole
  - CERT.at uses Data to generate Warnings
  - nic.at is sponsoring the domain costs
  - Cooperation with the international Conficker Working Group
- Small Scale
  - By looking at DNS Queries
  - Manipulation local DNS Cache

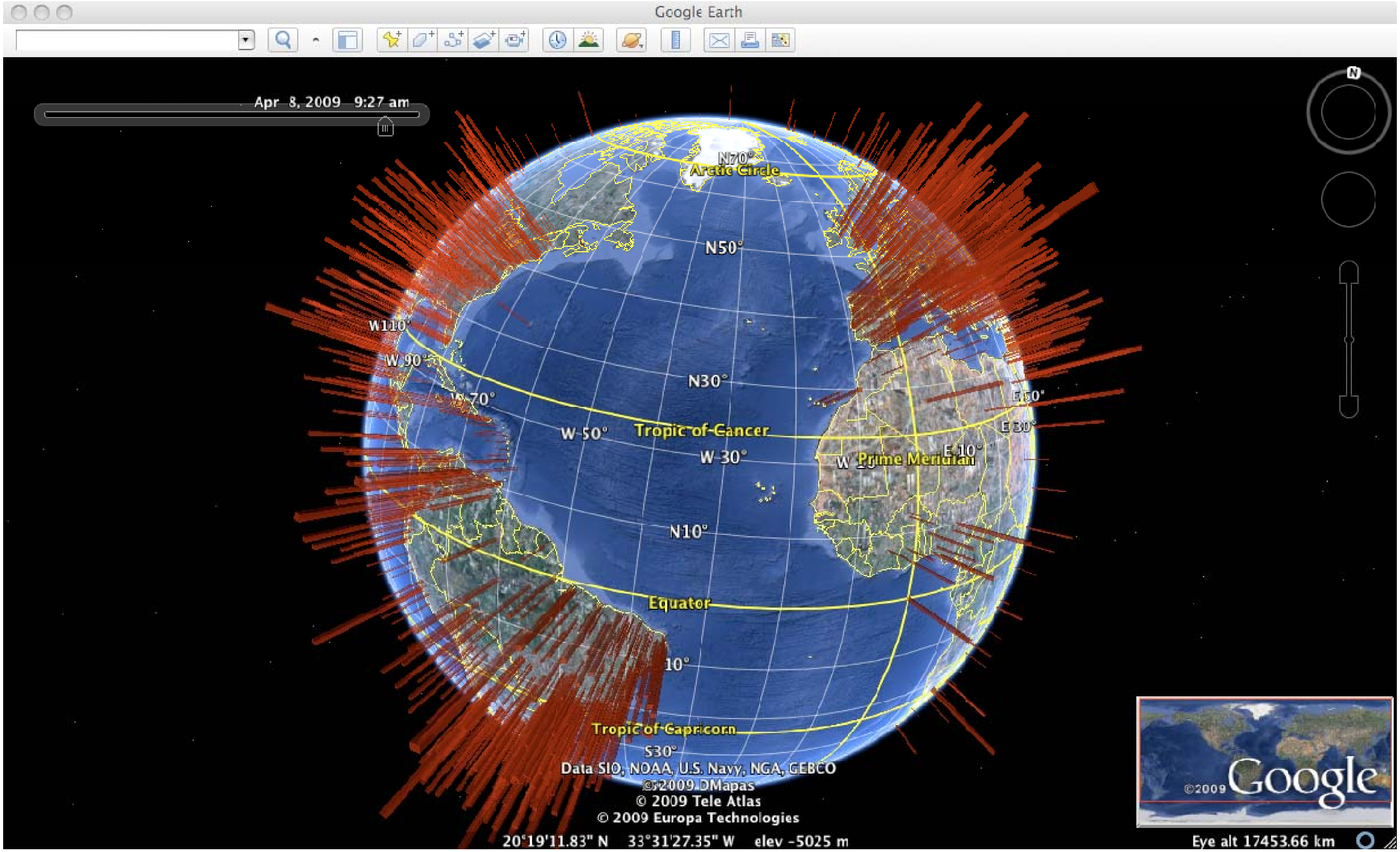
Conficker measurement example:

Unique infected IPs in Austria over time



Conficker measurement example:

Infected IPs Worldwide by location

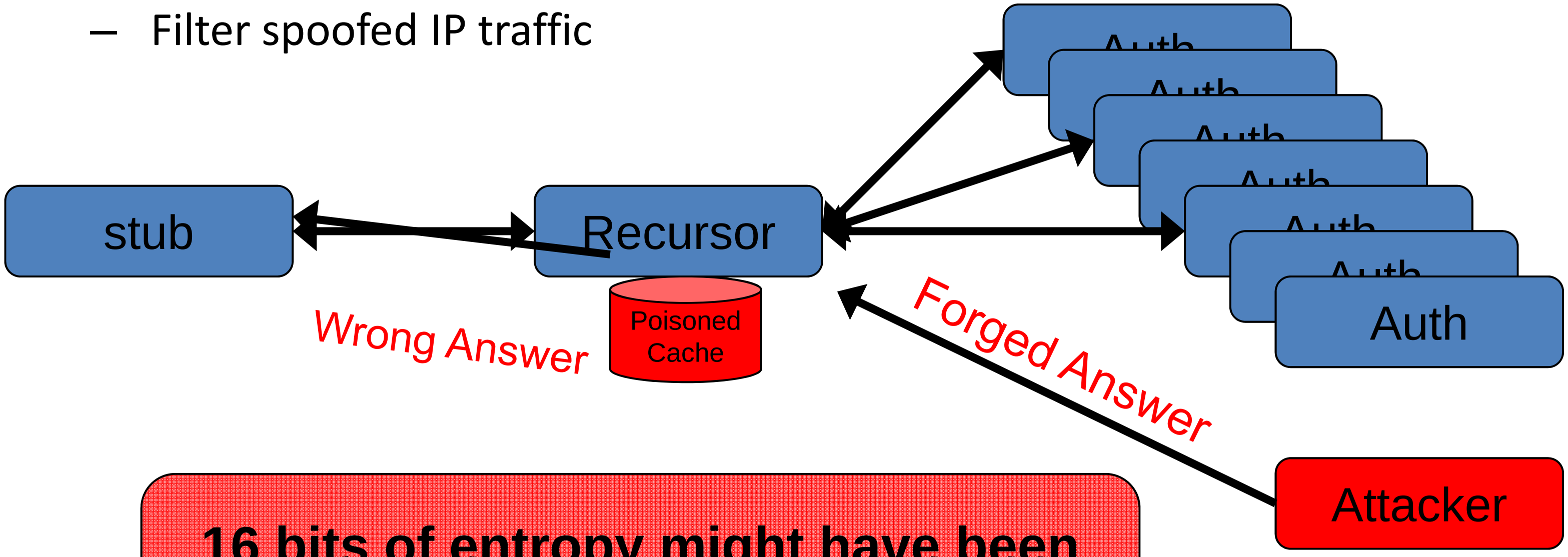


Conficker

Stage	Measure	CERT	Large Company	SME	EndUser
Vulnerability	# of vulnerable Systems				
Exploit	Signs of exploited vulnerabilities	C, Quality improvement through 3rd party info	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party
Threat	Severity of threat (based on V, E)	S, cooperation with Large ISPs required			
Risk	Risk for group of stakeholders				
Countermeasure	# of countermeasures deployed / Vuln. Fixed	C *	C *	C*	C *
Incident	# of incidents that occured	C (visible in NS cache)	C (visible in NS cache)	C (visible in local cache)	C (visible in local cache + ability to access antivir domains)

„Kaminsky“ DNS Bug

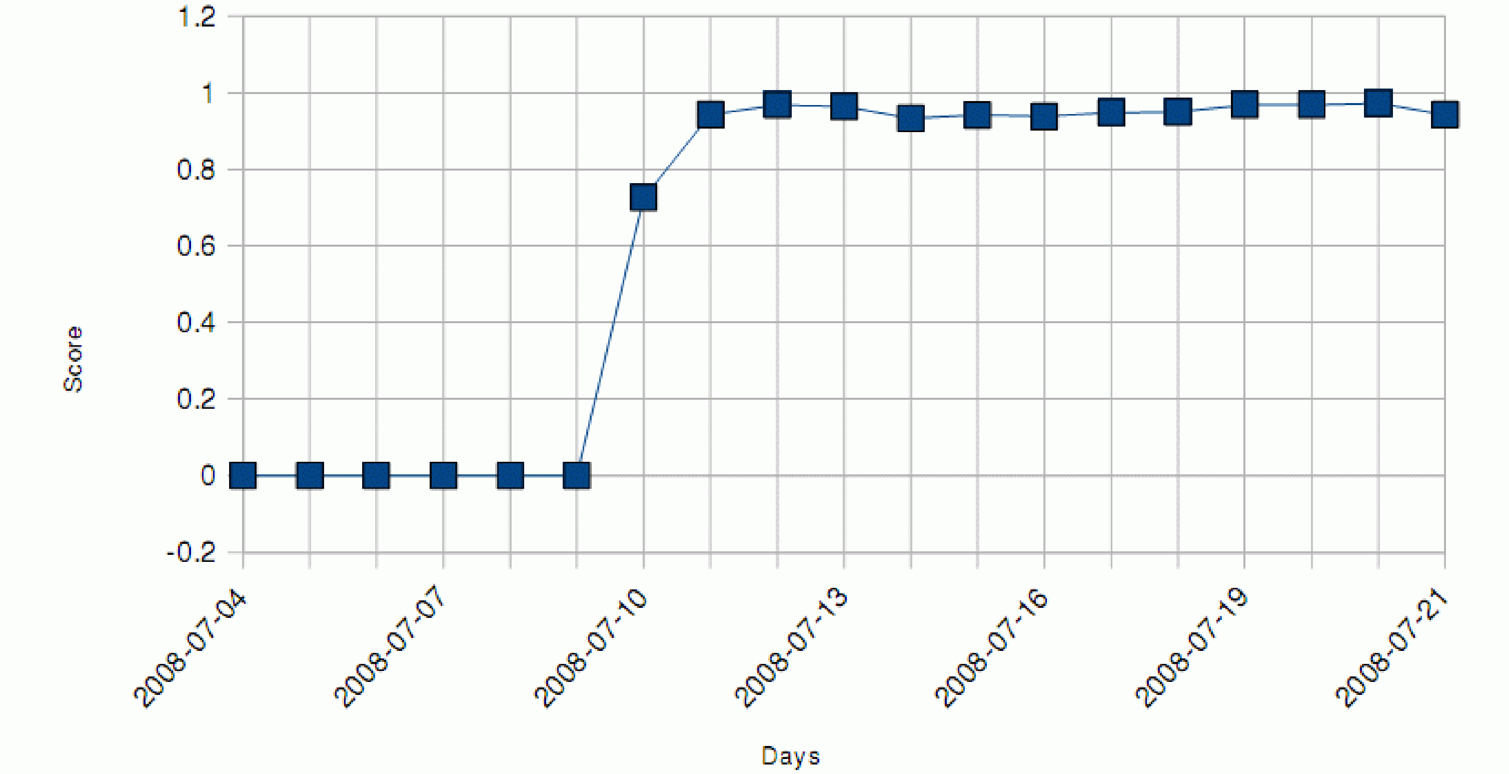
- VU#800113
- Dire Warning: Insufficient entropy in ID
- Recommendation were
  - Update Software
  - Implement Source Port Randomization
  - Restrict Recursion
  - Filter spoofed IP traffic



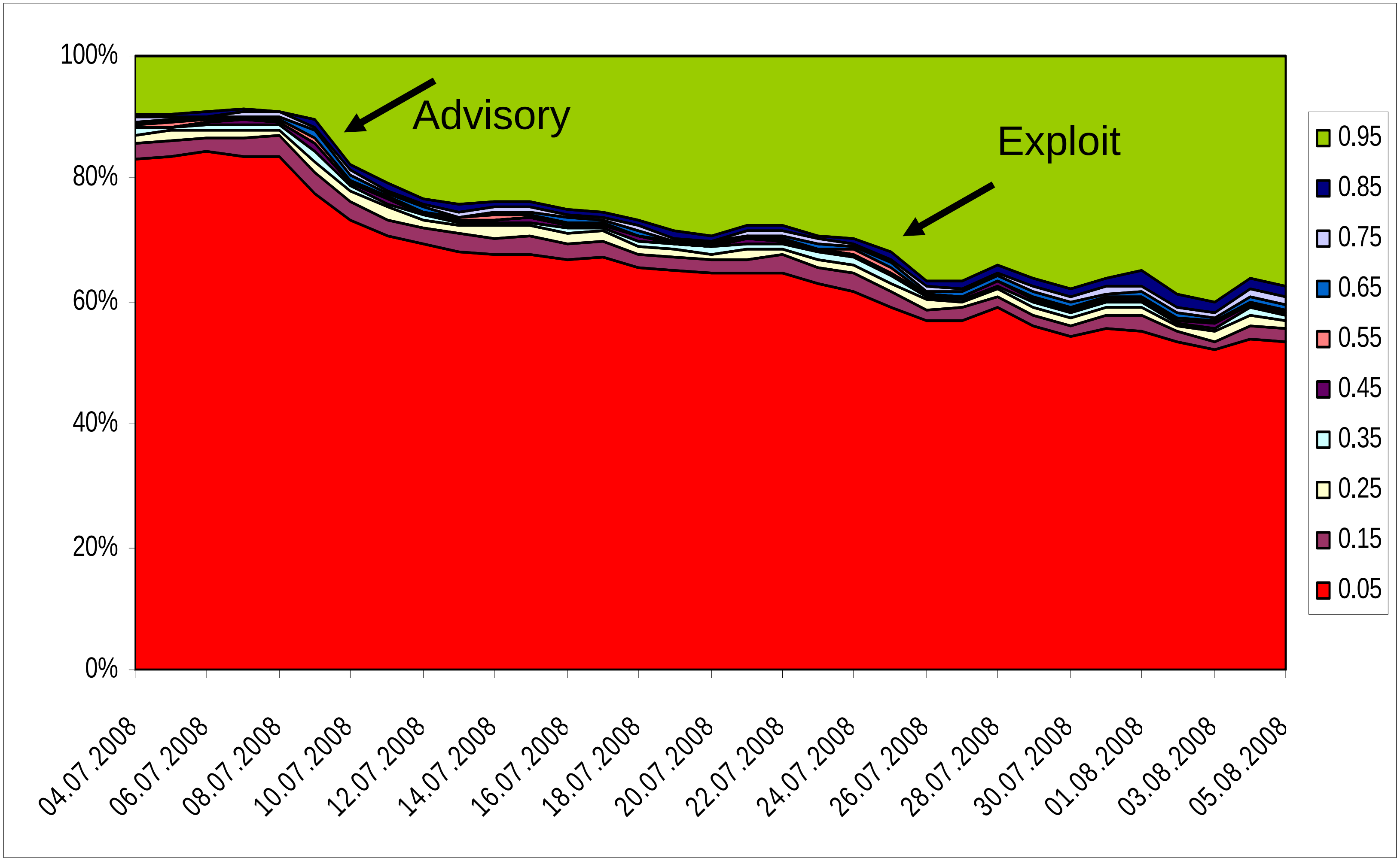
16 bits of entropy might have been enough in 1987, but not in 2008.

Scoring Resolvers

$$score = \frac{portchanges}{queries} * \frac{ports}{\min(queries, 65536)}$$

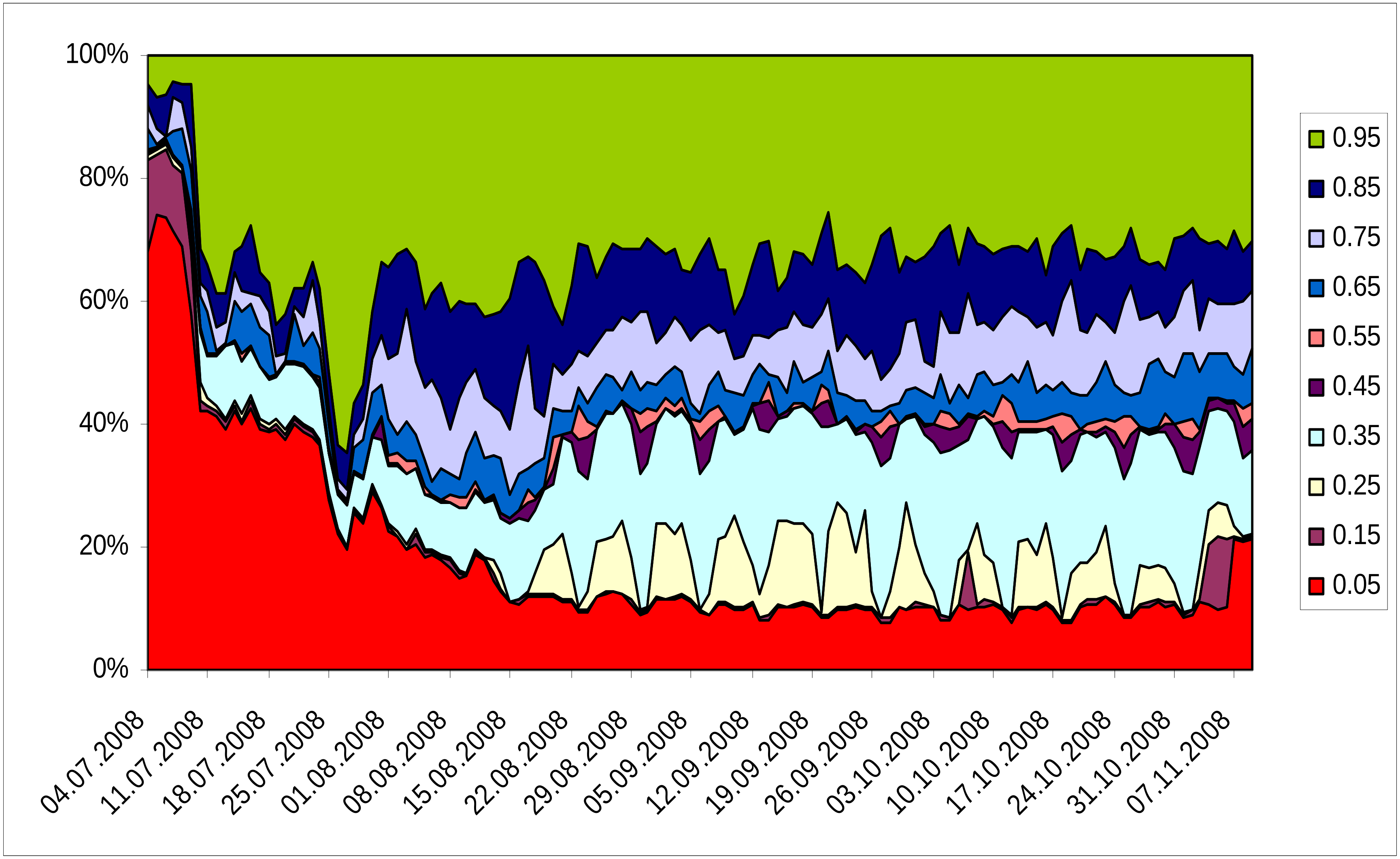


Patching by Server (short term)



Source: http://www.cert.at/static/downloads/papers/cert.at-0802-DNS-patchanalysis.pdf

By request, not by server:



Source: http://www.cert.at/static/downloads/papers/cert.at-0802-DNS-patchanalysis.pdf

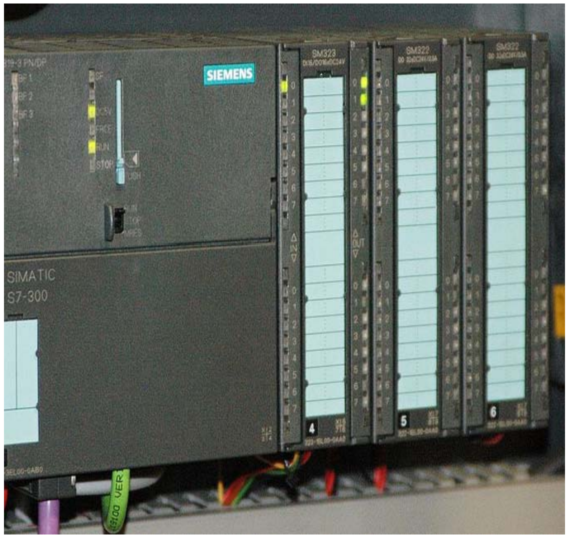
Kaminsky

Stage	Measure	CERT	Large Company	SME	EndUser
Vulnerability	# of vulnerable Systems	K	K	K	K
Exploit	Signs of exploited vulnerabilities	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party
Threat	Severity of threat (based on V, E)	K (if info from 3rd party is available)	K (given V+E is known)	info delivered FROM 3rd party	info delivered FROM 3rd party
Risk	Risk for group of stakeholders	K (if info from 3rd party is available)	K (given V+E+T is known)	info delivered FROM 3rd party	info delivered FROM 3rd party
Countermeasure	# of countermeasures deployed / Vuln. Fixed	K	K (on known NS)	K	K
Incident	# of incidents that occured	K (if info from 3rd party is available)	K (access to cache + passive DNS)	K (access to cache + passive DNS)	K (access to cache + passive DNS)

Stuxnet

- Targeted Siemens Simatic industrial control systems
  - Point of entry Windows Systems

- CnC connection attempts visible in DNS logs:
  - mypremierfutbol.com
  - todaysfutbol.com



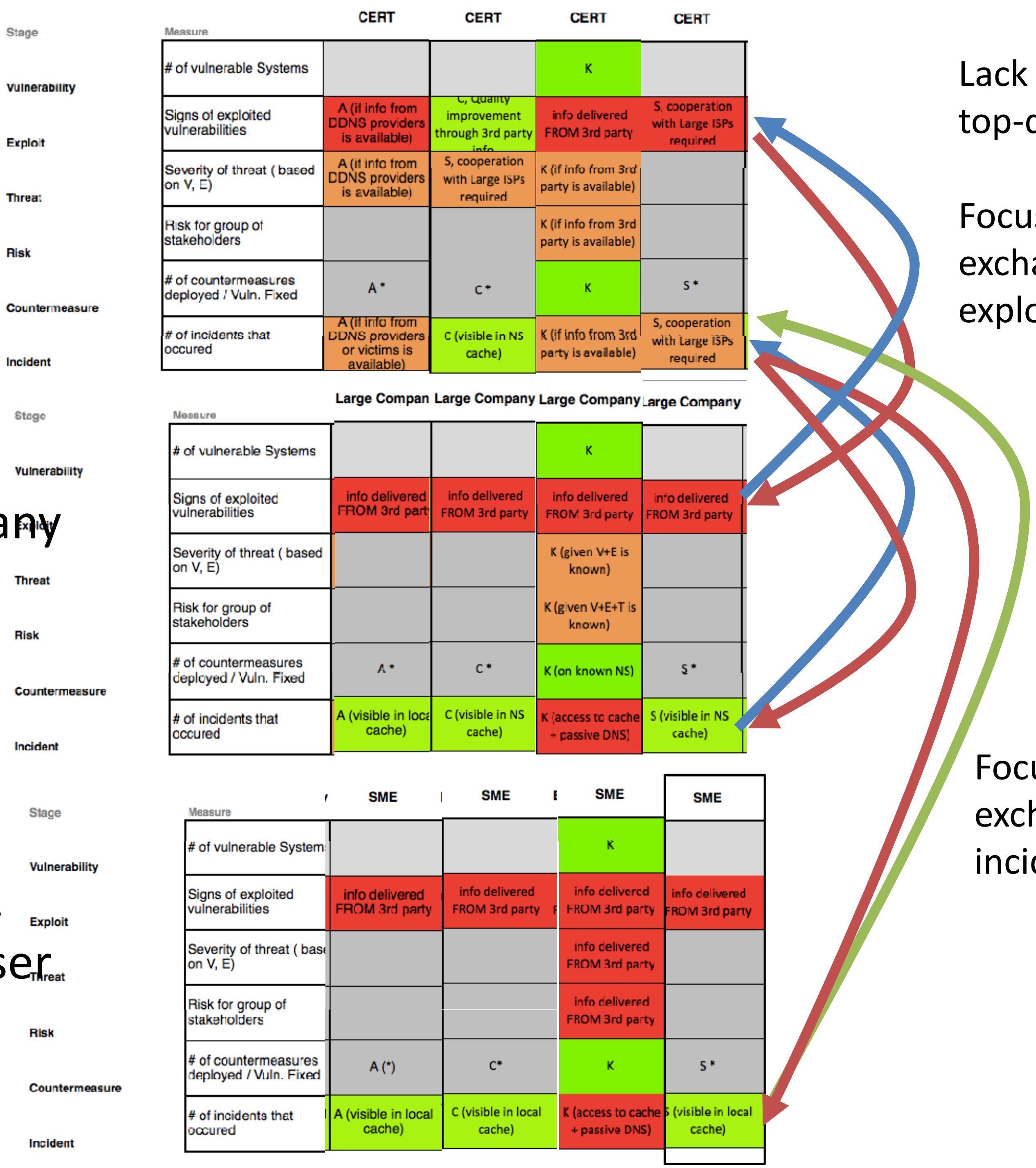
Siemens Simatic S7-300

Source: Wikimedia commons
Ulli 1105
http://en.wikipedia.org/wiki/File:S7300.JPG

Stuxnet

Stage	Measure	CERT	Large Company	SME	EndUser
Vulnerability	# of vulnerable Systems				
Exploit	Signs of exploited vulnerabilities	S, cooperation with Large ISPs required	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party
Threat	Severity of threat (based on V, E)				
Risk	Risk for group of stakeholders				
Countermeasure	# of countermeasures deployed / Vuln. Fixed	S *	S *	S *	S *
Incident	# of incidents that occured	S, cooperation with Large ISPs required	S (visible in NS cache)	S (visible in local cache)	S (visible in local cache)

Conclusions



CERT

Stage	Measure	CERT	CERT	CERT	CERT
Vulnerability	# of vulnerable Systems			K	
Exploit	Signs of exploited vulnerabilities	A (if info from DDNS providers is available)	C, Quality improvement through 3rd party info	info delivered FROM 3rd party	S, cooperation with Large ISPs required
Threat	Severity of threat (based on V, E)	A (if info from DDNS providers is available)	S, cooperation with Large ISPs required	K (if info from 3rd party is available)	
Risk	Risk for group of stakeholders			K (if info from 3rd party is available)	
Countermeasure	# of countermeasures deployed / Vuln. Fixed	A *	C *	K	S *
Incident	# of incidents that occured	A (if info from DDNS providers or victims is available)	C (visible in NS cache)	K (if info from 3rd party is available)	S, cooperation with Large ISPs required

Large Company

Stage	Measure	Large Compan	Large Company	Large Company	Large Company
Vulnerability	# of vulnerable Systems			K	
Exploit	Signs of exploited vulnerabilities	info delivered FROM 3rd part	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party
Threat	Severity of threat (based on V, E)			K (given V+E is known)	
Risk	Risk for group of stakeholders			K (given V+E+T is known)	
Countermeasure	# of countermeasures deployed / Vuln. Fixed	A *	C *	K (on known NS)	S *
Incident	# of incidents that occured	A (visible in loca cache)	C (visible in NS cache)	K (access to cache + passive DNS)	S (visible in NS cache)

SME & End User

Stage	Measure	SME	SME	SME	SME
Vulnerability	# of vulnerable System			K	
Exploit	Signs of exploited vulnerabilities	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party	info delivered FROM 3rd party
Threat	Severity of threat (base on V, E)			info delivered FROM 3rd party	
Risk	Risk for group of stakeholders			info delivered FROM 3rd party	
Countermeasure	# of countermeasures deployed / Vuln. Fixed	A (*)	C*	K	S *
Incident	# of incidents that occured	A (visible in local cache)	C (visible in local cache)	K (access to cache + passive DNS)	S (visible in local cache)

Lack of visibility due to top-down view.

Focus on information exchange on signs of exploited vulnerabilities

Focus on information exchange on local incidents

Conclusions

- National CERTs
  - can gain large scale view - but need cooperation
  - Able to compile/distribute information for other organizations
  - Top-Down view – only information from „victims“ allows detailed observation
  - Special Situation @ DNS Technical issues – possibility of countermeasure control
- Large Scale Companies
  - DNS is a good possibility for the detection and analysis (patient 0) of security incidents and control of countermeasures
  - They can benefit from CERT information
  - National CERTs can benefit from there nameserver logs
- SME, EndUser
  - Strength in local DNS cache analysis
  - Can benefit from CERT Incident Reports (Technical Guides)

Aalto University
School of Science
and Technology

CERT.at

Thank you!

Comments, Questions!

proschinger@cert.at - christian.fruewirth@tkk.fi - lendl@cert.fi

Special credit to:

Reijo Savola (VTT)

Aaron Kaplan

Florian Weimar

AcoNet CERT

Sources

Patching Nameservers: Austria reacts to VU#800113
http://www.cert.at/static/downloads/papers/cert.at-0802-DNS-patchanalysis.pdf

Detecting Conficker in your Network
http://www.cert.at/static/downloads/papers/TR_Conficker_Detection.pdf

Erkennung von Stuxnet im eigenen Unternehmen
http://www.cert.at/static/downloads/specials/stuxnet-report_public.pdf

The Command Structure of the Aurora Botnet,
http://www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf

W32.Stuxnet Dossier, Symantec

Passive DNS Replication
http://www.first.org/conference/2005/papers/florian-weimer-slides-1.pdf