



The network of knowledge

# The BELNET Vulnerability Scanner

**TF-CSIRT**

**25-26 Sept 2008, Vienna**



The network of knowledge

# agenda

## **BELNET CERT**

- customers
- services

## **call for tender**

- requirements
- evaluation criteria
- results

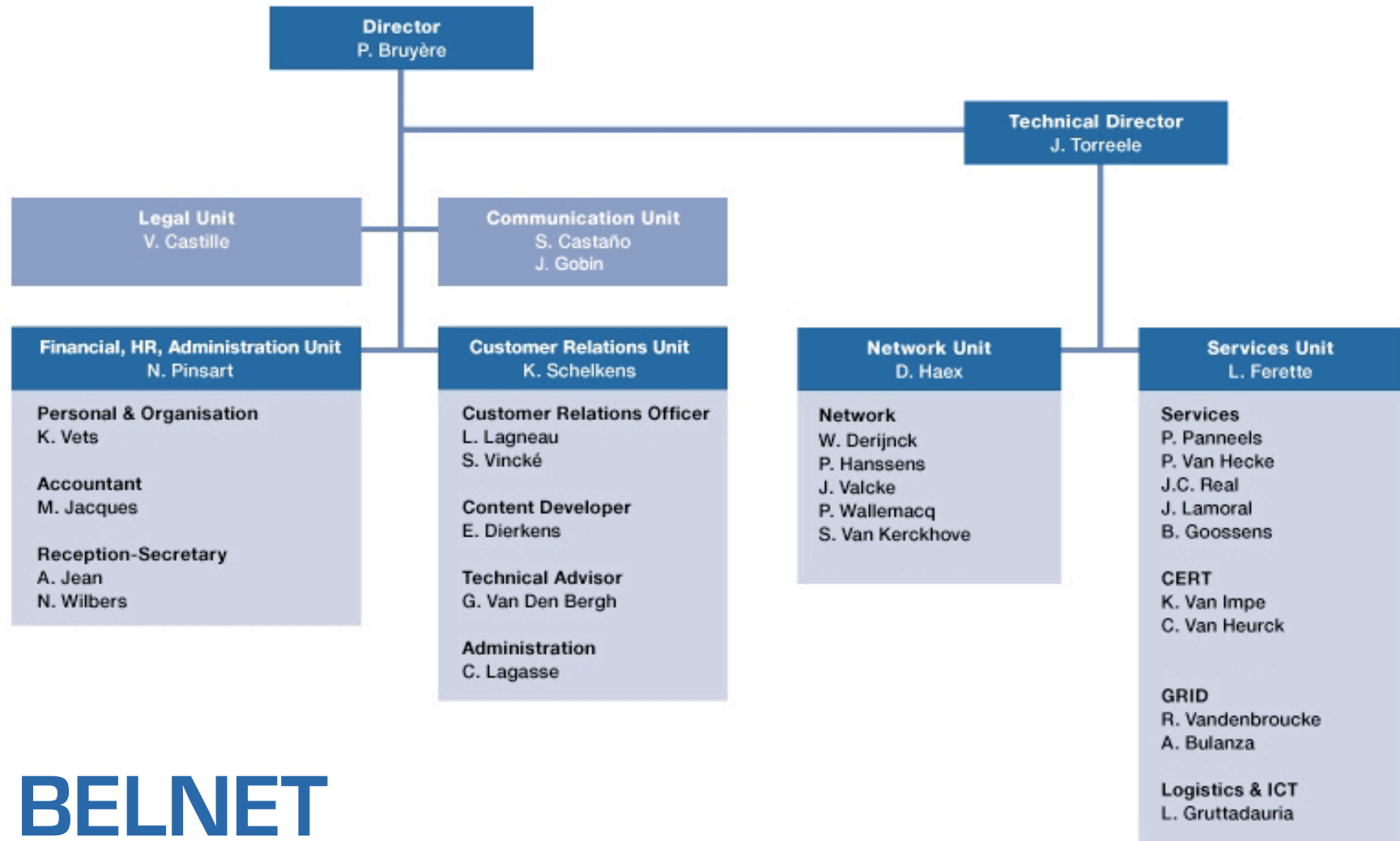
## **scanner.belnet.be**

- pilot
- features, figures & examples
- future
- lessons learned

## **Q&A**



The network of knowledge



# BELNET





The network of knowledge

# BELNET CERT

we offer **services** to our constituency:

**classic** services:

website [ <http://cert.belnet.be> ]

alerting

incident coordination - handling

vulnerability handling

awareness

training

**new** services:

projects



The network of knowledge

# demand from customers

the need for **automated** scanning  
a couple of “ad-hoc” demands for a scan

BELNET CERT initiates **project** within Services unit  
vendor neutral  
knowledge - expertise  
size *does* matter  
pilot free for BELNET customers  
allows for serious testing & evaluation



The network of knowledge

# call for tender

BELNET = government  
= rules & regulations  
= comply or ... *reboot*

**initial study & demo's**  
**technical requirements**  
**budget**

149.000\* € for one year \* excl. VAT

**legal & administrative requirements**  
**call for tender**

**European publication**



The network of knowledge

# call for tender

continued

14-09-2007

**publication of call for tender**

06-11-2007

**closing date for offers**

60 days for evaluation

end 01-2008

**publication of evaluation result**

1 week for complaints

early 02-2008

**90 days to implement the solution**

10-06-2008

**final delivery by subcontractor**



The network of knowledge

# technical requirements

non intrusive

easy and automatic updating

external support services (phone, e-mail)

training

central management via a secured website

7500 IP's but extensible to 100K

scans from different locations (firewall)

scheduling of scans

trends-reporting

strong encryption between components



The network of knowledge

# technical requirements continued

different user roles

various platforms

computers & operating systems

routers

applications

ticketing

backup strategy

rebranding

remote interface (XML)

IPv6 not required



The network of knowledge

# evaluation criteria

“official” evaluation document is used to:

**choose** between the proposals

**justification** of the choice

governmental financial control bodies

**Koen Van Impe** for more details



The network of knowledge

# evaluation criteria continued

9 different criteria with a total of 61 points

ratio cost/features	12 points
support services	8 points
scalability	8 points
data quality & data protection	8 points
SLA for maintenance, etc...	5 points
integration with BELNET look & feel	5 points
training	5 points
report quality	5 points
integration in BELNET environment	5 points



The network of knowledge

# evaluation results

5 contenders

1 wasn't accepted because of  
administrative mistakes by supplier

2 competitive offers with  
similar features  
different approach

Qualys & Dimension Data :: SAS

nCircle & VerizonBusiness :: in house



The network of knowledge

# winner

## Qualys & Dimension Data

margin less than **10%**

- + **training**
- + **integration** with BELNET “look & feel”
- + **integration** in BELNET environment
- + excellent **XML** interface



The network of knowledge

# scanner.belnet.be continued

one central **SOC** in Germany (Qualys)

two scanner **appliances** at BELNET

one BELNET **Back Office** account

- manage user accounts

- review the access logs

- review activity

every user gets a **Front Office** account

- 32 IP's per account

- “teaser” :: pilot ends in April 2009



The network of knowledge

# Back Office

Home ▾ Subscription ▾ Administrator ▾ Setup ▾ Help ▾ Logout

## QUALYS GUARD ADMIN @EU



[Quick Help](#)

### Scan and Map Statistics

▼ Search

Find:

Type:  Vulnerability Scan  Compliance Scan  Map  Scheduled Vulnerability Scan  Scheduled Compliance Scan  Scheduled Map

Status:  Running  Finished  Canceled  Error  No results  No host alive  Interrupted  Paused

Account:  Customer  Prospect

Range:  -  View:

◀ ◀ 1 to 2 of 2 ▶ ▶

Date Range ▾	Type	Total	Hosts	Duration	Avg Time	Finished	Canceled	Paused
<a href="#">08/19/2008 - 08/26/2008</a>	map	15	2854	1 day 02:43:04	01:46:52	100%	0%	0%
<a href="#">08/19/2008 - 08/26/2008</a>	scan	21	650	17:38:15	00:50:24	95%	0%	0%





The network of knowledge

# Front Office

## BELNET Vulnerability Scanner

New Search View Setup Help

VM PCI PC CERT CERT (benet-cc) | [Log Out](#)

### Navigation

- Dashboard
- Map
- Scan
- Schedule
- Report
- Remediation
- Asset Search
- Risk Analysis

### Tools

- Asset Groups
- Report Templates
- User Accounts
- Option Profiles
- Scanner Appliances
- Host Assets
- Domain Assets
- Remediation Policy
- Authentication
- Business Units
- Virtual Hosts
- KnowledgeBase
- Activity Log

### Vulnerabilities

1 - 20 of 6099

Info	Edit	QID	Title	Authentication	Category	Patch	Edited	Severity	CVE ID	Vendor Reference	Bugtraq ID	Modified
		6	DNS Host Name		Information gathering				1			12/31/1997
		9	Open RPC Services List		RPC				2			N/A
		11	Hidden RPC Services		RPC				2			12/31/1997
		32	Darxite Banner		General remote services				2			11/22/2000
		1000	Potential UDP Backdoor		Backdoors and trojan horses				4	CVE-1999-0660		11/04/2005
		1001	"Back Orifice" Backdoor		Backdoors and trojan horses				5	CVE-1999-0660		11/22/2005
		1002	"GirlFriend" Backdoor		Backdoors and trojan horses				5	CVE-1999-0660		11/22/2005
			Potential TCP		Backdoors							

Please click on an item in above datalist to view its preview.

0 of 6099 Items Shown, 0 selected

Powered By Qualys



The network of knowledge

# Front Office features

**rebranding** :: only *“Powered by Qualys”*

a customer account is created as a “manager” (top)

every customer can then create their **own accounts**

scanner

reader

manager (backup)

**delegated** user management

less work for BELNET staff



The network of knowledge

# scans & maps

**mapping** :: discovery

detecting the hosts on the network

unlimited in frequency

unlimited number of IP's (map the Internet)

**scanning** :: detect vulnerabilities

stored encrypted at SOC

loose credentials :: game over

unlimited in frequency

limited to 32 IP's



The network of knowledge

# scanning

returns a **list of vulnerabilities**

QID's

references to CVE, Bugtraq, ...

tips for patching, ...

scan for **all** vulnerabilities

takes longer – data stored in database

filter your reports

query results database for fresh vulnerabilities



The network of knowledge

# reporting

**summary** reports

by *assets* and-or by *vulnerabilities*

**detailed** reports

by *assets* and-or by *vulnerabilities*

**scorecard** reports

*asset group* vulnerabilities

most *vulnerable hosts*

**vulnerability management**

returning issues

follow-up



The network of knowledge

# API

## QualysGuard API sample code (Perl scripts)

### XML reports:

```
<SCAN value="scan/1192210826.26584">
  <HEADER>
</HEADER>
  <IP value="64.41.134.60" name="demo02.qualys.com">
    <OS>Windows 2000 SP2</OS>
    <NETBIOS_HOSTNAME>DEMO02</NETBIOS_HOSTNAME>
    <INFOS>
      <CAT value="CGI" port="80" protocol="tcp">
        <INFO number="12059" severity="2">
          <TITLE>
            Web Server Probed For Various URL-Encoding Schemes Supported
          </TITLE>
```



The network of knowledge

# documentation

BELNET created **own introduction**

integrator released a detailed “**how-to**” document once the setup phase was finished

documents on the BELNET support website only available from within our network

**welcome pack**

**getting started**

**training** on site (BELNET) and hands-on



The network of knowledge

# current status

fully **operational**

62 primary **accounts**

83 user accounts

since the start 201 **maps** for 81874 hosts

since the start 335 **scans** for 4864 hosts

interesting for our own LAN – DMZ ...



The network of knowledge

## to be continued ...

pilot phase ends April 2009.

??? renewal ???

??? **paid** service ???

extra training session after nonuser **feedback**

maybe such a service needs more **publicity**?

Integration in a new BELNET portal (XML)



The network of knowledge

**thank you for your attention!**

**any questions?**

