

Att veta eller tro

- Validering av nätverksstrukturen -

Internetdagarna
2005-10-24 – 25

Alf Lundström
Koncerninformationssäkerhetschef
Vattenfall

alf.lundstrom@vattenfall.com

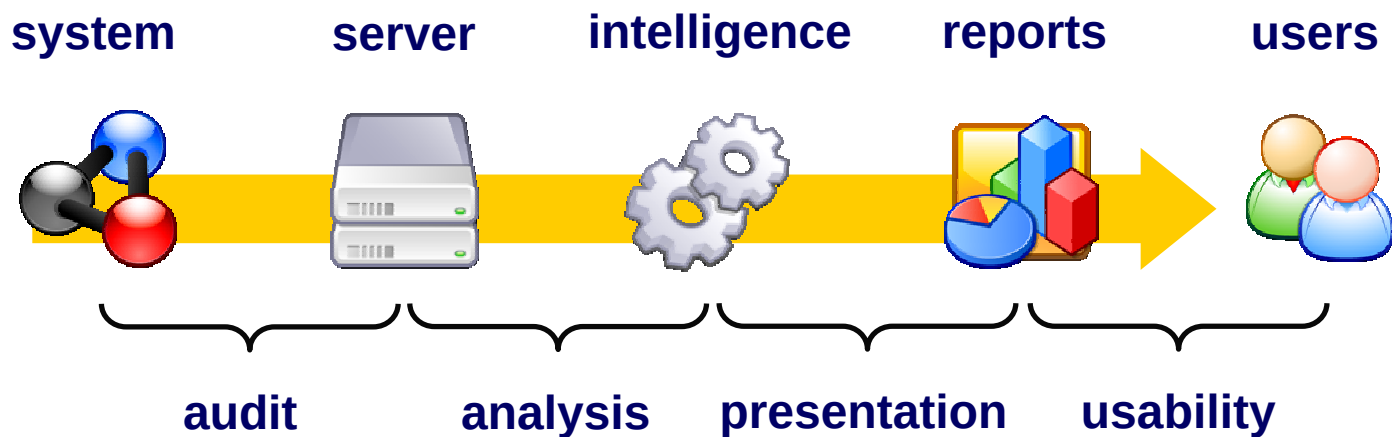
Något om Vattenfall

- Ca 37 000 anställda
- I huvudsak verksam i följande länder
 - Sverige
 - Finland
 - Danmark
 - Tyskland
 - Polen
- Ca 32 000 datorer (MS 2000, XP, UNIX)
- Ca 5 000 servrar (MS 2000, 2003, UNIX m fl)
- Stort antal övrig utrustning som routrar, switchar etc

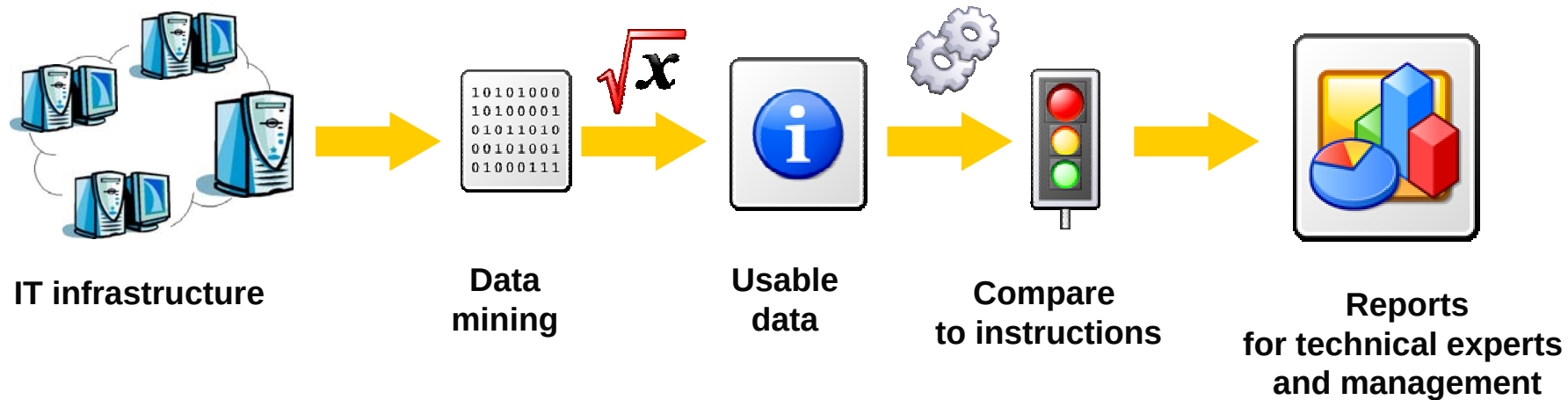
Vattenfall IT Security Scanner

(VITSS)

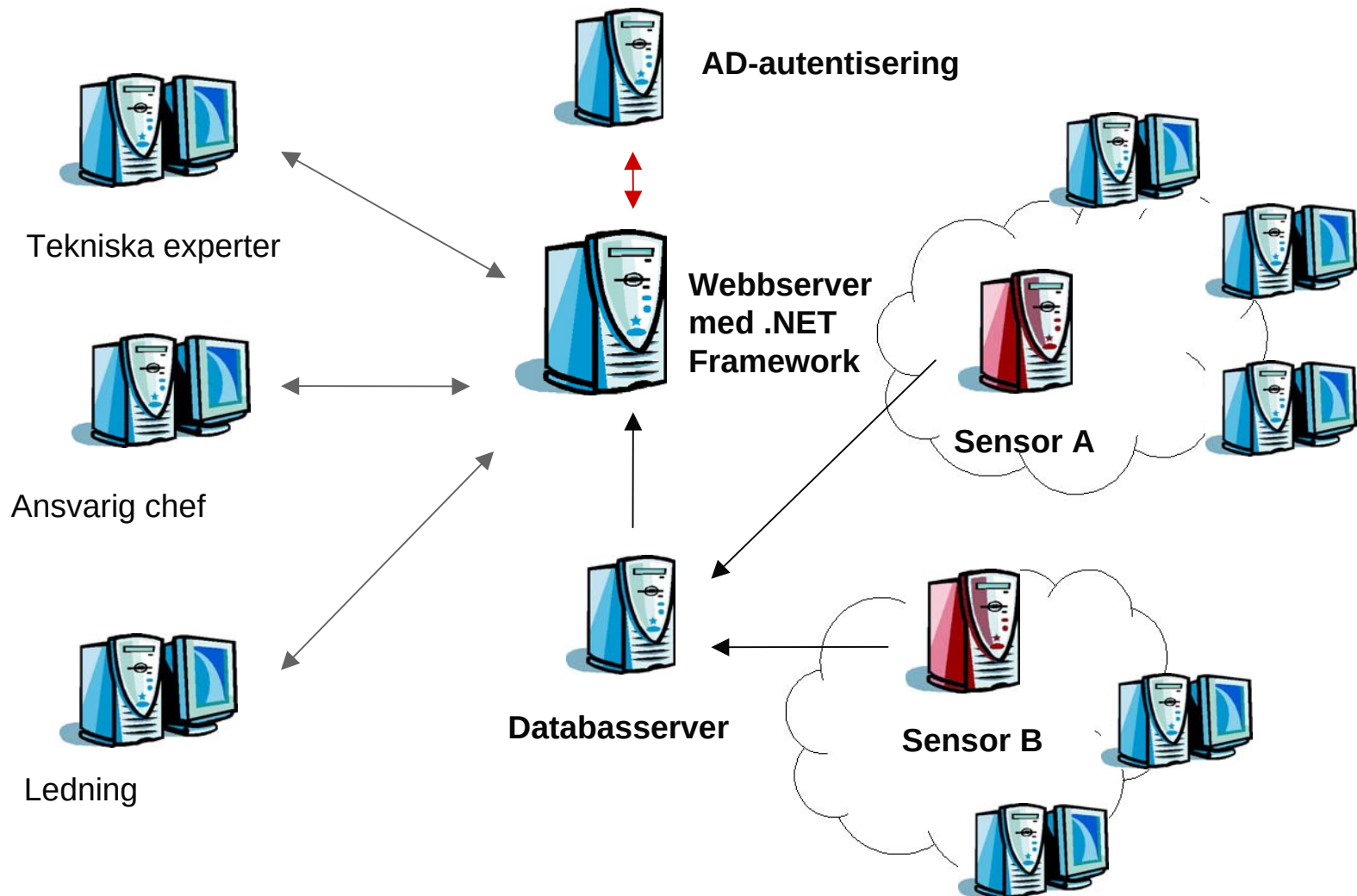
Funktionell vy över VITSS



Teknisk vy över VITSS (1)



Teknisk vy över VITSS (2)



Vad ingår i sensordelen?

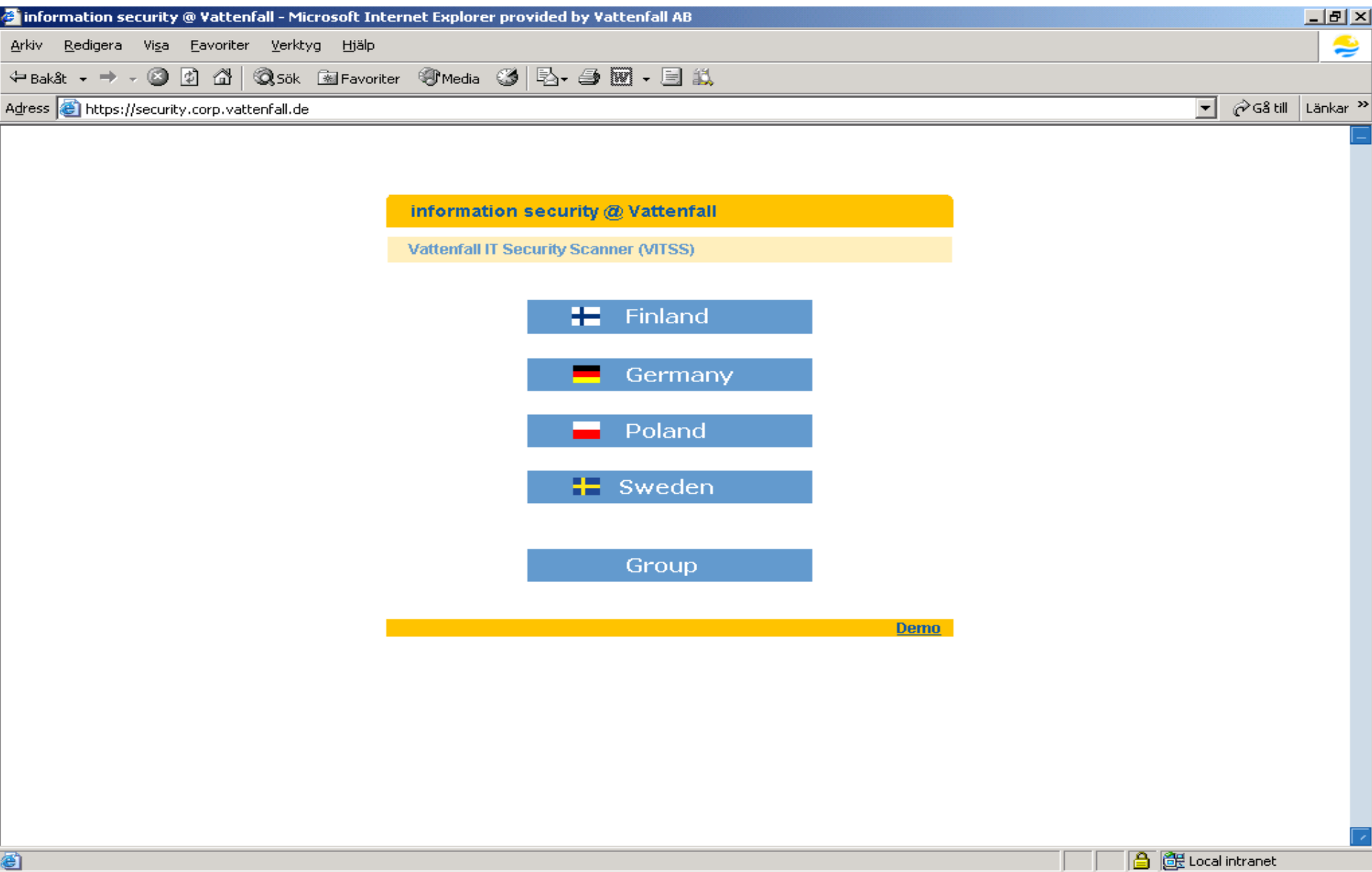
- **Skannerdel**

- LanGuard
- Nessus
- MBSA
- Jass
- Hyena
- AV interface
- Tivoli (WMI)
- SMS
- Perl Scripts f
- nmap

Vad som skannas

Windows + windowssäkerhetshål
Sårbarheter/säkerhetshål
Windows
Sun Solaris
AD, Windows
AV software
Client, Server
Windows
lexible
network discov.

- ... more coming soon



Welcome to the Vattenfall IT Security Scanner (VITSS)

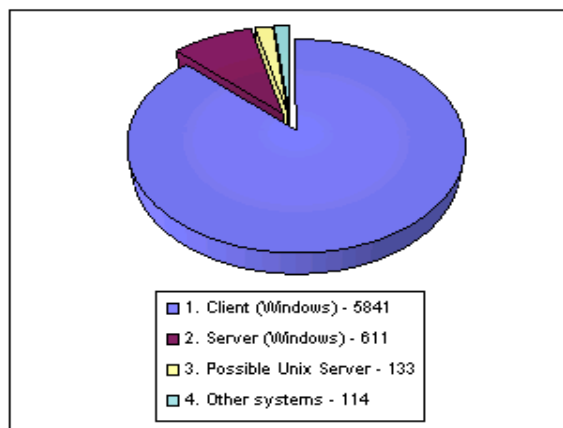
The **Vattenfall IT Security Scanner (VITSS)** is a single point of visibility of the IT security status in the Vattenfall group.

Based on the guidelines of the Vattenfall group (e.g. [Group Instruction 26](#)) and the Best Practice (ISO 17799) the target of **VITSS** is

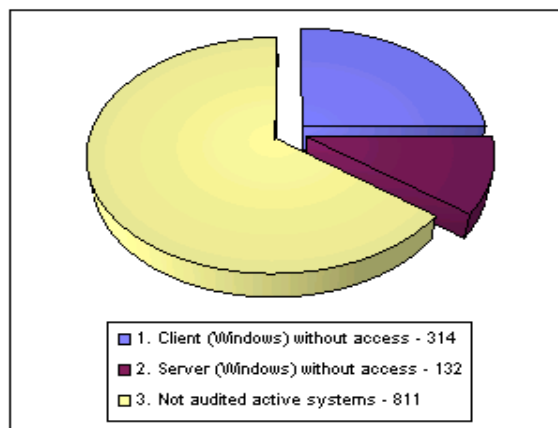
- to [identify vulnerabilities](#) and non-compliances of IT systems
- to inventory the IT infrastructure concerning security facts
- to support the risk and threat management with reliable information
- to enable an efficient and measurable minimization of risk
- to control und prioritize actions based on hard technical facts

Current status of the audit

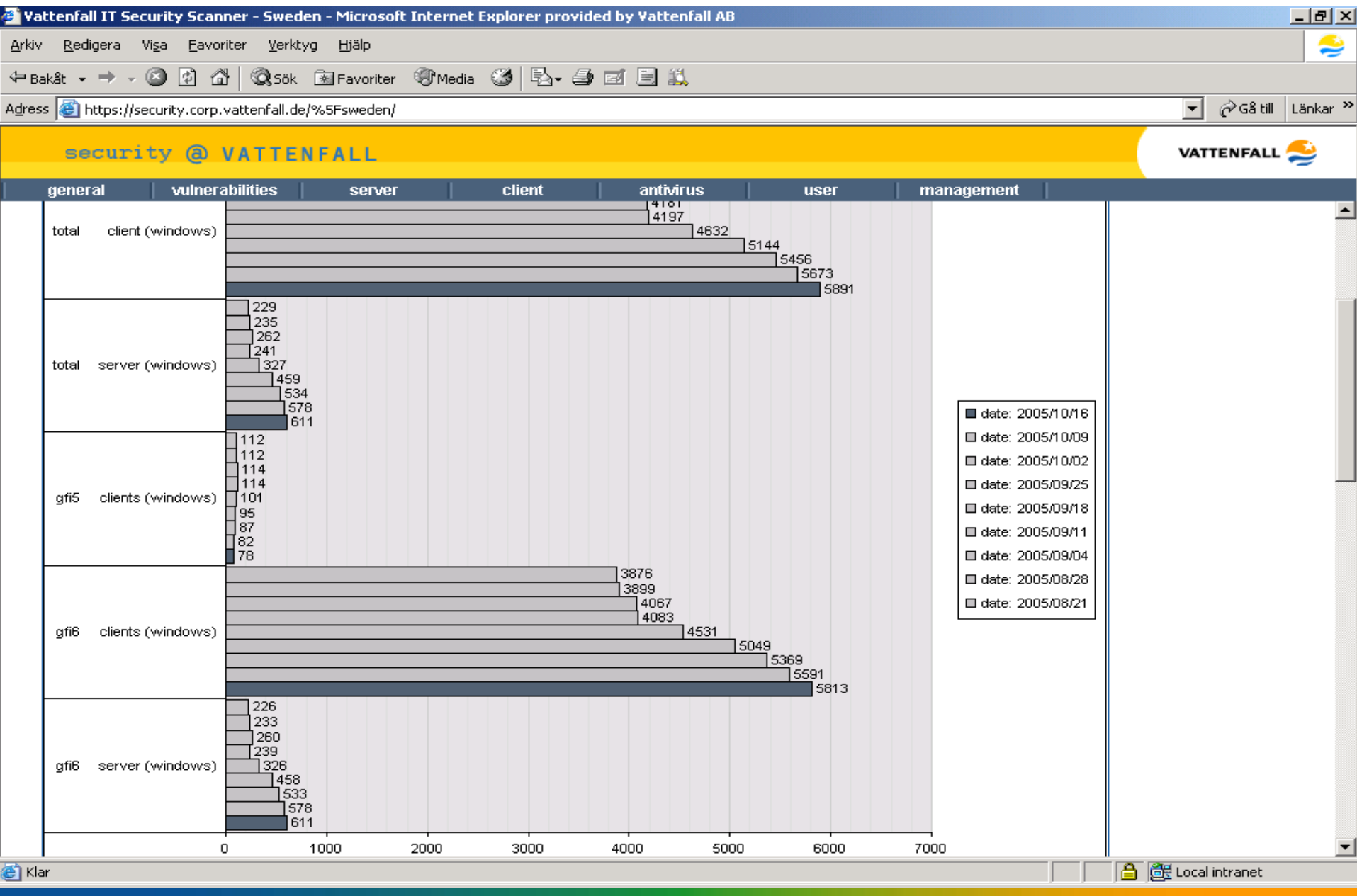
Identificated systems



Not audited systems



= 7 986



Vattenfall IT Security Scanner - Sweden - Microsoft Internet Explorer provided by Vattenfall AB

Arkiv Redigera Visa Favoriter Verktyg Hjälp

Bakåt → ↻ ↗ Sök Favoriter Media

Adress <https://security.corp.vattenfall.de/%5Fsweden/> Gå till Länkar »

security @ VATTENFALL **VATTENFALL**

general vulnerabilities server client antivirus user management

<< 1 >> vulnerabilities - alerts ... (1 - 21 / 21) Set Filter Export FAQ all

alertlevel	alertname	alrtdescription	cnt	details	note	link	date	account	delete
0	Administrator account without password!	You MUST set a password for the administrator account.	14	details	test av kommentarsfält	edit	2005-09-26 10:33:55.087	EUR\RTMN	delete
0	Auto Logon (1)	Auto Logon is enabled	11	details		edit			delete
0	KnownDLLs List Vulnerability	An attacker can replace system dll's with trojaned ones	25	details		edit			delete
0	Nachi Worm	A trojan horse is likely to be installed on this computer	5	details		edit			delete
0	NT Screen Saver Vulnerability	An attacker can replace the screen server with a trojaned executable gaining administrative level privileges	25	details		edit			delete
0	Old Openssh	old openssh versions prior to 3.7.1 had a vulnerability which allowed people to excute commands remotely	72	details		edit			delete
0	POP3 server might be vulnerable to a remote buffer overflow exploit	Contains a buffer overflow that could result in the overwriting of process memory, including the return address within the stack, and code execution.	2	details		edit			delete
0	Possible snmpXdmid SunOS buffer overflow	Some versions of this service are vulnerable (Run arbitrary commands as root)	8	details		edit			delete
0	Possible statd format string attack	Some versions of this service are vulnerable (Run arbitrary commands as root)	51	details		edit			delete
0	Remote Buffer Overflow in Sendmail	Sendmail versions from 5.79 to 8.12.7 are vulnerable to this buffer overflow.	47	details		edit			delete
0	Remote OpenSSH Vulnerability	A remotely exploitable vulnerability exists in OpenSSH prior to version 3.3 (Version 3.3 is affected only if UsePrivilegeSeparation is disabled)	10	details		edit			delete
0	Sendmail is older than 8.12.9	Various buffer overflows can be found in old Sendmail version including some that allow remote users to gain root privileges.	39	details		edit			delete
0	SWAT - Samba Web Administration Tool	The SWAT service is listening on port 901. It is not recommended to allow access from outside to this service as	1	details		edit			delete

Local intranet

VATTENFALL



security @ VATTENFALL



general		vulnerabilities	server	client	antivirus	user	management					
<< < 1 > >>				alerts	Alerts ... (1 - 21 / 21)		Set Filter Export FAQ					
alertlevel		alertname			no access	cnt	details	note	link	date	account	delete
0	Administrator account without password!	You MUST set a password		missing hotfixes	Administrator account.	14	details	test av kommentarsfält	edit	2005-09-26 10:33:55.087	EUR\RTMN	delete
0	Auto Logon (1)	Auto Logon is enabled		antivirus		11	details		edit			delete
0	KnownDLLs List Vulnerability	An attacker can replace DLLs		no tivoli	with trojaned ones	25	details		edit			delete
0	Nachi Worm	A trojan horse is like a worm		info	on this computer	5	details		edit			delete
0	NT Screen Saver Vulnerability	An attacker can replace the screen saver with a trojaned one		local admins	over with a trojaned one	25	details		edit			delete
0	Old Openssh	old openssh versions are vulnerable		open ports	privileges	72	details		edit			delete
0	POP3 server might be vulnerable to a remote buffer overflow exploit	Contains a buffer overflow		serviceinfo	a vulnerability which can be exploited remotely	2	details		edit			delete
0	Possible snmpXdmid SunOS buffer overflow	Some versions of this service are vulnerable (Run arbitrary commands as root)		shares		8	details		edit			delete
0	Possible statd format string attack	Some versions of this service are vulnerable (Run arbitrary commands as root)		statistic	result in the overwriting of process memory, including the return address within the stack, and code execution.	51	details		edit			delete
0	Remote Buffer Overflow in Sendmail	Sendmail versions from 5.79 to 8.12.7 are vulnerable to this buffer overflow.				47	details		edit			delete
0	Remote OpenSSH Vulnerability	A remotely exploitable vulnerability exists in OpenSSH prior to version 3.3 (Version 3.3 is affected only if UsePrivilegeSeparation is disabled)				10	details		edit			delete
0	Sendmail is older than 8.12.9	Various buffer overflows can be found in old Sendmail version including some that allow remote users to gain root privileges.				39	details		edit			delete
0	SWAT - Samba Web Administration Tool	The SWAT service is listening on port 901. It is not recommended to allow access from outside to this service as				1	details		edit			delete

no av (mcafee) ... (1 - 20 / 265)										
Set Filter Export FAQ 20										
hostname	domain	os	ip	usage	no_mcafeeframework	no_mcshield	antivirus	createdon	audit	Location
WIND01	EUR	Windows 2000	151.156	Member Server	no_mcafeeframework	-	mcafee	17.10.2005 13:44:04	perl	
DOMINOLAB	EUR	Windows XP	151.156	Workstation	no_mcafeeframework	-	mcafee	12.03.2005 11:52:36	gfi6	
HD0927	EUR	Windows 2000	192.168	Workstation	no_mcafeeframework	-	mcafee	14.10.2005 00:37:48	gfi6	
LICALV01	EUR	Windows Server 2003	151.156	Member Server	no_mcafeeframework	no_mcshield	-	17.10.2005 13:46:55	perl_wmi	
MAPSGEABDB1	EUR	Windows 2000	151.156	Member Server	-	no_mcshield	mcafee	17.10.2005 14:07:27	perl_wmi	
SE002086	EUR	Windows 2000	151.156	Workstation	-	no_mcshield	mcafee	14.10.2005 12:46:40	perl_wmi	
COGNOS2	EUR	Windows Server 2003	151.156	Member Server	-	no_mcshield	mcafee	17.10.2005 19:45:40	perl_wmi	
C-CL3-3	EUR	Windows Server 2003	151.156	Member Server	no_mcafeeframework	no_mcshield	-	17.10.2005 13:52:28	perl	
C-CL3-1	EUR	Windows Server 2003	151.156	Member Server	no_mcafeeframework	no_mcshield	-	17.10.2005 13:51:29	perl	
SWP0684	EUR	Windows 2000	151.156	Workstation	-	no_mcshield	mcafee	09.03.2005 00:00:00	perl	
HM3075	EUR	Windows 2000	151.156	Workstation	no_mcafeeframework	-	mcafee	18.01.2005 22:15:49	gfi5	
CASTORW	EUR	Windows 2000	151.156	Workstation	no_mcafeeframework	no_mcshield	-	17.10.2005 19:44:41	perl_wmi	
SE006829	EUR	Windows 2000	151.156	Workstation	-	no_mcshield	mcafee	10.10.2005 16:05:29	perl_wmi	
VWSQC01	EUR	Windows 2000	10.50.1	Member Server	no_mcafeeframework	no_mcshield	-	17.10.2005 19:44:23	perl_wmi	
AD0581	EUR	Windows 2000	151.156	Workstation	-	no_mcshield	mcafee	17.10.2005 19:43:25	perl_wmi	
CAPP8	EUR	Windows 2000	151.156	Member Server	no_mcafeeframework	no_mcshield	-	17.10.2005 14:32:16	perl_wmi	
SE005703	EUR	Windows 2000	151.156	Workstation	no_mcafeeframework	-	mcafee	17.10.2005 13:09:45	perl_wmi	
SE004354	EUR	Windows 2000	151.156	Workstation	-	no_mcshield	mcafee	14.10.2005 18:34:17	perl_wmi	
CAPP9	EUR	Windows 2000	151.156	Member Server	no_mcafeeframework	no_mcshield	-	17.10.2005 14:32:10	perl_wmi	
XD0826	EUR	Windows 2000	10.50.1	Workstation	no_mcafeeframework	-	mcafee	23.03.2005 05:48:32	gfi6	

security @ VATTENFALL



general vulnerabilities server client antivirus **user** management

local admins

user - local admins ... (1 - 20 / 1671)

Set Filter

Export

FAQ

20

localadmin	Anzahl	details	note	link	date	account	delete	hide
EUR\A1ADCH	1	details		edit			delete	7 days
EUR\A1JSAM	12	details		edit			delete	7 days
EUR\A1Imar	2	details		edit			delete	7 days
EUR\A1obrosius	1	details		edit			delete	7 days
EUR\A1PBOR	3	details		edit			delete	7 days
EUR\A1ROBI	7	details		edit			delete	7 days
EUR\A1TOLS	3	details		edit			delete	7 days
EUR\A2frkb	4	details		edit			delete	7 days
EUR\A2oschuett	1	details		edit			delete	7 days
EUR\A2smolibocki	2	details		edit			delete	7 days
EUR\AADN	1	details		edit			delete	7 days
EUR\Aago	2	details		edit			delete	7 days
EUR\AAKI	12	details		edit			delete	7 days
EUR\Aakm	18	details		edit			delete	7 days
EUR\Aapn	1	details		edit			delete	7 days
EUR\AAWG	1	details		edit			delete	7 days
EUR\Aaxb	1	details		edit			delete	7 days
EUR\ABAU	1	details		edit			delete	7 days
EUR\Abru	2	details		edit			delete	7 days
EUR\ABVL	1	details		edit			delete	7 days

Framtida utveckling

- Anpassning till gällande krav, policies, standarder etc
 - GI 26 – Vattenfalls Group Instruction "Informationssäkerhet"
 - ISO/IEC 1 77 99
 - BASEL 2
 - KontaG
 - PCI
 - etc
- Fortsatt teknisk utveckling
 - Nya tester
 - Bättre integrering mot andra databaser: inventariesystem, personalregister
 - Bättre integrering mot andra säkerhetssystem: informationsklassningsdatabas, andra skanningsverktyg

Erhållen information

- Teknisk information
 - Tekniska brister och svagheter
 - "TODO"-listor till IT-operation
 - Viktigt med information och förståelse för att åtgärda de anmärkningar och avvikelser som framkommit i VITSS
- "Överskottsinformation"
 - Personliga oegentligheter t ex nedladdning av program och funktioner som strider mot företagets policy och regelverk
 - Rutiner måste finnas och vara avstämda med personalorganisationer m fl, hur denna information får hanteras och av vem.

Avslutning !

Frågor ?