

NEXThink®

refocusing information security on the human factor

OSSIR (Windows Security Group)

February 5th, Paris

Vincent Bieri, CEO

vincent.bieri@nexthink.com

nEXTHINK®

Copyright NEXThink® - PUBLIC INFORMATION

NEXThink in short



- Swiss company created in September 2004 on the campus of the Swiss Federal Institute of Technology (EPFL)
- Core technology based on research initially conducted at the Artificial Intelligence Laboratory by Pedro Bados co-founder and CTO
- 2 pending-patents
 - Method of detecting anomalous behaviour in a computer network
 - Method of visualizing anomalous behaviour in a computer network
- Awarded technology and business model
 - Start-up of the year 2005 by IMD Business School
 - PERL 2005 – Prix entreprendre région Lausanne
 - Swiss Technology Award 2006
 - Prix de l'Innovation 2006 des Assises de la Sécurité
 - CTI Start-up Label (Swiss government certification)
- The REFLEX™ solution is in operation at customer's site since October 2005 with deployments in large and multi-sites environments

Agenda



- Introduction
- Technology
- Examples
- Case Study
- Demo



REFLEX Introduction

nexTHink[®]

Copyright NEXThink[®] - PUBLIC INFORMATION

The human factor is the missing piece in today's security puzzle



Security solutions have a technological component, but security is fundamentally a people problem

Bruce Schneier, *Secrets & Lies*

- Billions of dollars spent on defending (efficiently) against technical vulnerabilities
- Failing to recognize the threats from **unintentional, unknown and careless behavior** lead to security incidents

Human factor essential for IT security
People and processes more important than technology
Robert Jaques, vnunet.com 26 Oct 2006

Global enterprises need to focus more time on policies, procedures and training, rather than on technology if they are to successfully secure IT infrastructure, according to a new survey by the International Information Systems Security Association (ISSA).

A poll of more than 4,000 information security professionals conducted by IDC on behalf of the International Information Systems Security Association (ISSA) found that organisations have traditionally overlooked the human factor in favour of trusting hardware and software to solve security problems.

However, survey respondents say organisations are now beginning to realize that human factor is an essential part of IT security.

Human factor biggest computer security risk, say hackers and safety experts
August 08, 2006 Edition 1

The most vexing weakness in computer security is not in the hardware or the software, it is in the people who use the machines, according to top hackers and cyber-safety specialists.

"It really is more of a human problem than a technical problem," said a security expert at the conference, DefCon, which ended in Las Vegas on August 7.

Staff are the weakest link
Posted by Guy Matthews at 10:27AM, Thursday 26th October 2006

All the IT security spending in the world won't protect your systems if the staff are stupid research finds

People are usually the weak link in information security, and not technology, concludes research by an independent think tank.

The three most important data protection are managed policies, users that follow them and recruitment of qualified security professionals.

SANS: Human error top security worry
Targeted attacks focus on humans, and they often work

Robert McMillan Today's Top Stories > or Other Security Stories >

November 15, 2006 (IDG News Service) -- The SANS Institute has some controversial advice for computer security professionals looking to lock down their networks: spear-phish your employees.

Managing the human factor is the opportunity to a better security

- You can't manage the human factor if you can't measure behavioral risk
- What are the key requirements?
 - **Common and measurable** risk definition
 - **Transversal diagnostics and metrics** that can be shared and compared across various organizational or geographical units
 - **Risk trajectory** versus status
 - Metrics at **individual and group level**
 - Behavioral risk integrated with **audit reports, policies & standards, and user awareness**
 - Risk mitigation processes integrated with **education programs and identity management**

The risk impact of the human factor is related to the behavior and usage of information technology

RISK = Critical Activity x Abnormal activity

Who am I for the company ?



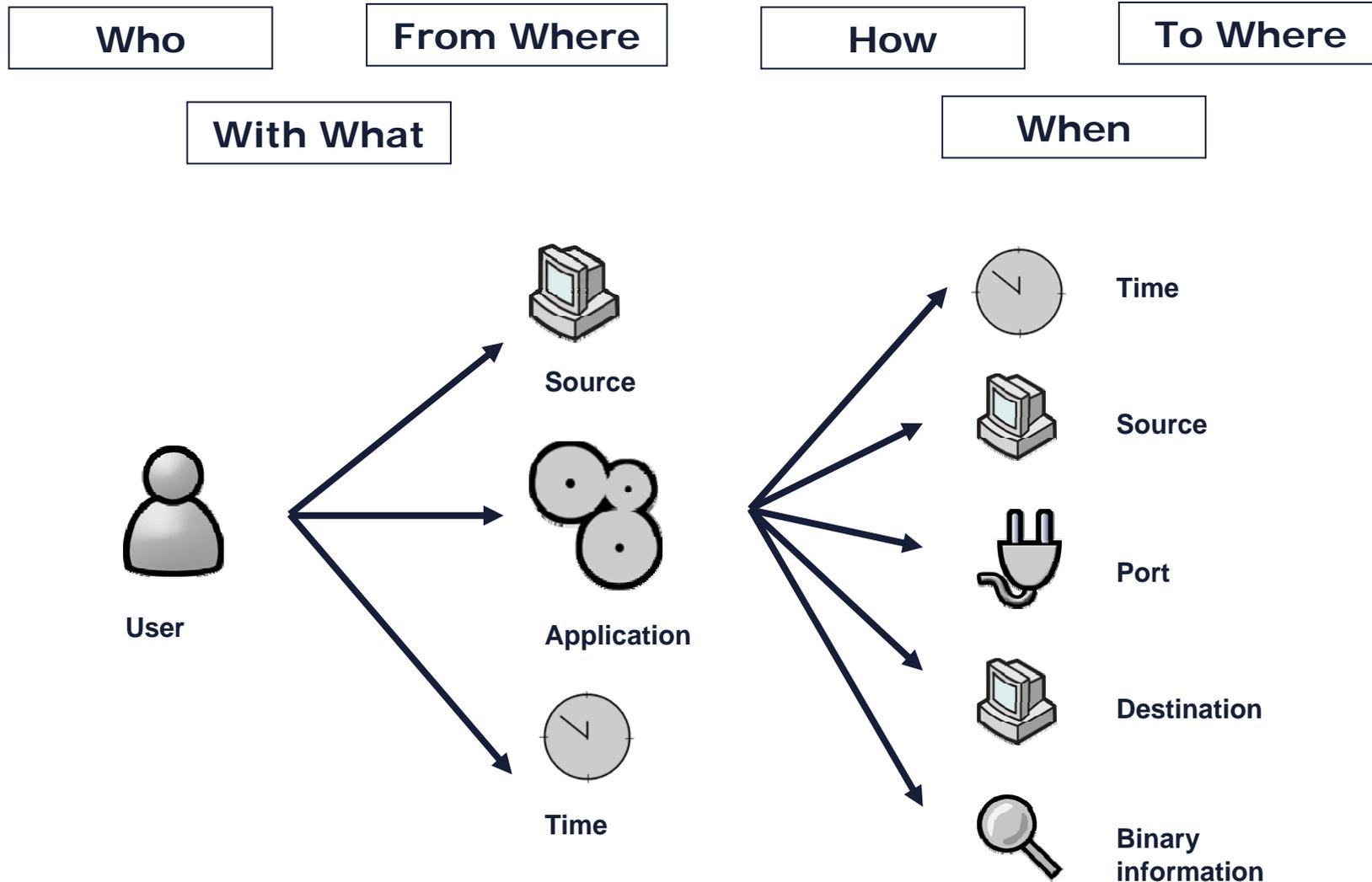
Critical Activity is related to the type of applications and destinations being accessed

Do I behave dangerously ?

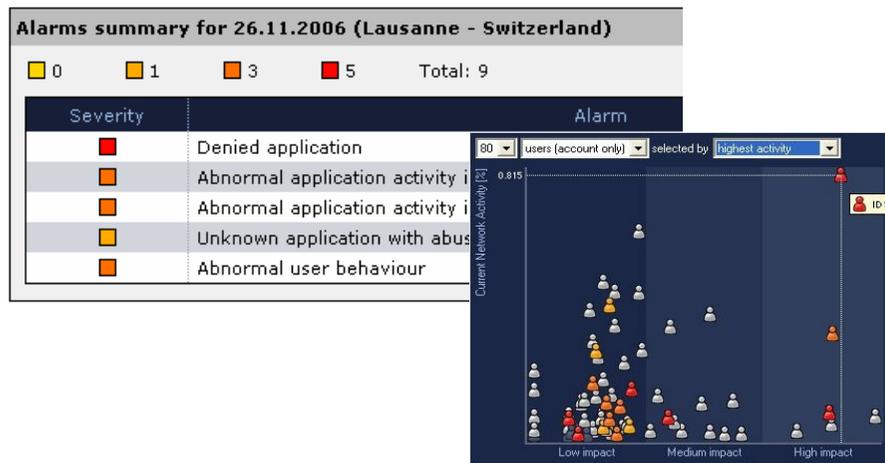
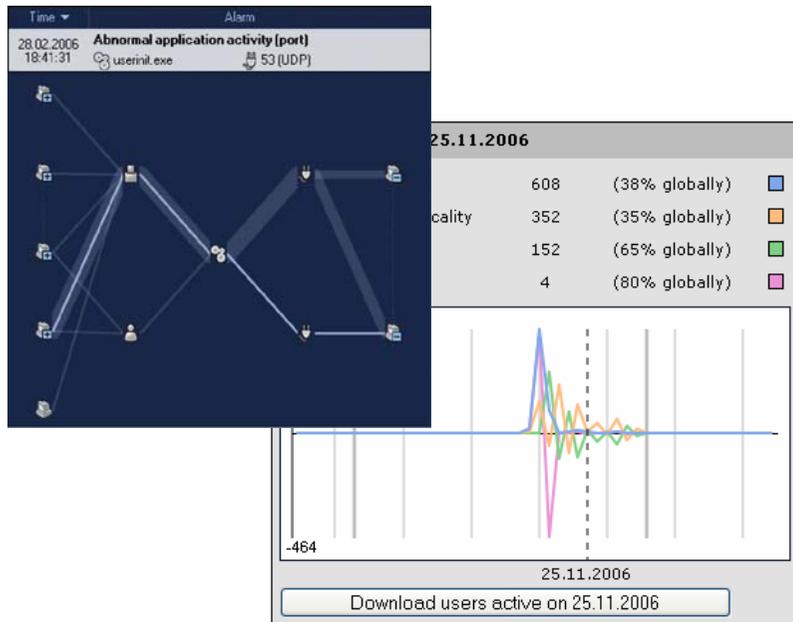


Abnormal activity is related to the level of abnormal behaviors for a user, an application or a source

The risk impact of the human factor is related to the behavior and usage of information technology

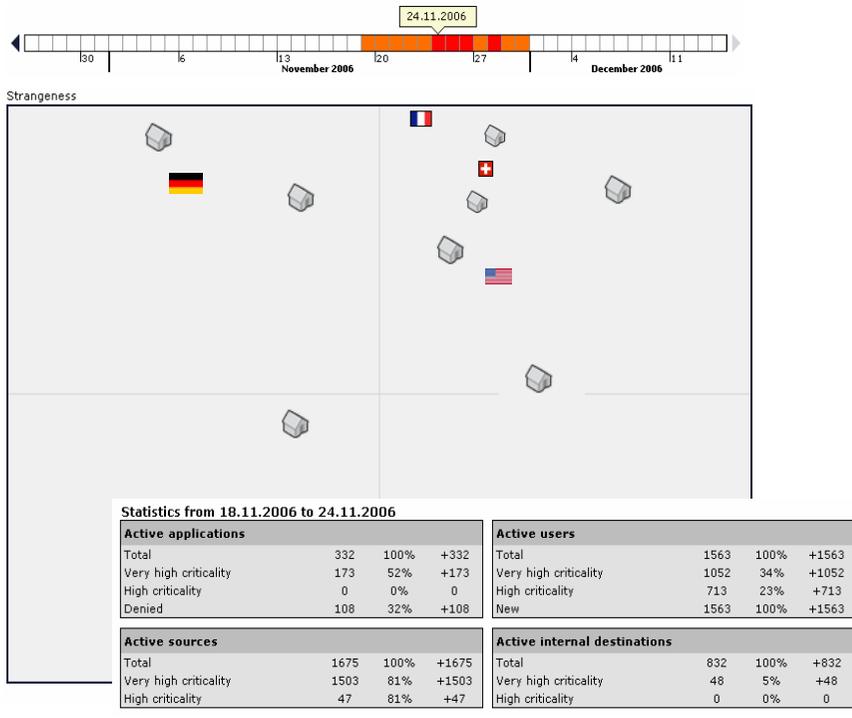


With REFLEX™ NEXThink refocuses information security on the human factor



- REFLEX™ **detects** identity's behavior changes
- REFLEX™ **warns** upon usage of denied applications (hash and version)
- REFLEX™ **identifies** abusive usage of network connections
- REFLEX™ **alerts** with meaningful information to allow immediate reactivity
- REFLEX™ **shows** hard data related to the human factor with powerful and intuitive visualizations

REFLEX™ delivers risk diagnostics at corporate level with capabilities to understand root cause up to the user



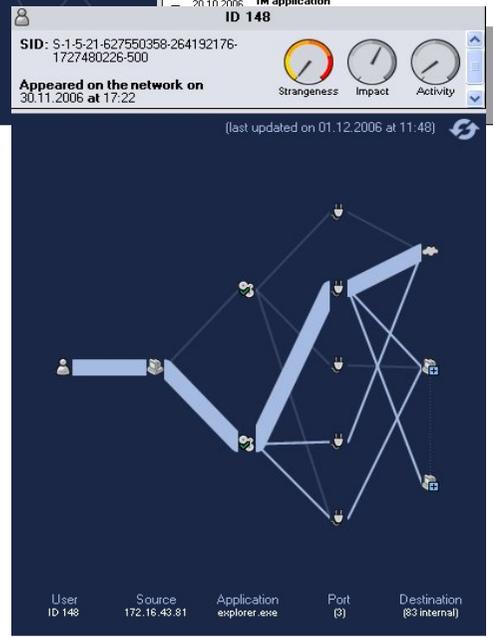
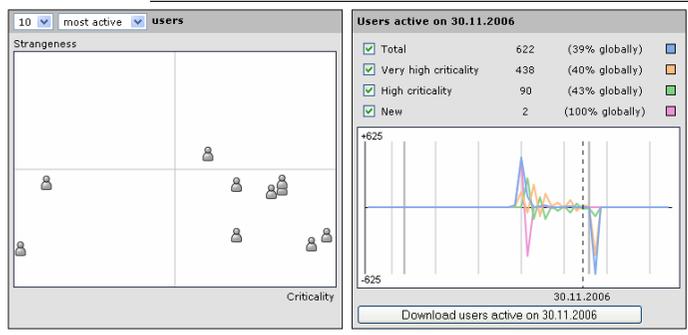
Alerts List:

Time	Alarm	Confidence	Severity
04.12.2006 10:51:57	IM application mmsgs.exe	Sure	Critical
30.11.2006 15:19:23	IM application mmsgs.exe	Sure	Critical
29.11.2006 15:05:44	IM application mmsgs.exe	Sure	Critical
14.11.2006 19:05:18	Abnormal application activity mmsgs.exe	Good	High
10.11.2006 10:59:24	Modified application binary mmsgs.exe (hash: 1e455b08870d4ac3bb6ab59...	Sure	Critical
02.11.2006 21:27:51	IM application mmsgs.exe	Sure	Critical
29.10.2006 22:35:38	IM application mmsgs.exe	Sure	Critical
20.10.2006	IM application	Sure	Critical

Alert Detail: ID 148
 SID: S-1-5-21-627550358-264192176-1727480226-500
 Appeared on the network on 30.11.2006 at 17:22

Connection Table:

Time	User	Source	Destination	Application	Port
10.11.2006 10:59:24	ID 68	172.16.43.81	172.16.42.15	mmsgs.exe	1900 (UDP)



REFLEX™ has various risk reporting data

Sources involved in alarms

1.	172.18	7	+7
2.			
3.			

Highly critical destinations involved in alarms

1.	172.18	7	+7
2.			
3.			

Highly critical users involved in alarms

1.	User 060 on REFLEX Engine "Engine-2"	5	+5
2.			
3.			

Denied applications

1.	firefox.exe	12167	+12167
2.			
3.			

Alarm types

1.	Denied application	781	+781
2.			
3.			

Highly critical applications involved in alarms

1.	launch~1.exe	22	+22
2.	pcsync2.exe	21	+21
3.	bmail.exe	18	+18
4.	msmsgs.exe	17	+17
5.	skype.exe	17	+17
6.	dw.exe	15	+15
7.	webshots.scr	15	+15
8.	windvd.exe	15	+15
9.	winamp.exe	14	+14
10.	btstac~1.exe	13	+13

Download list

Sources active on 25.11.2006

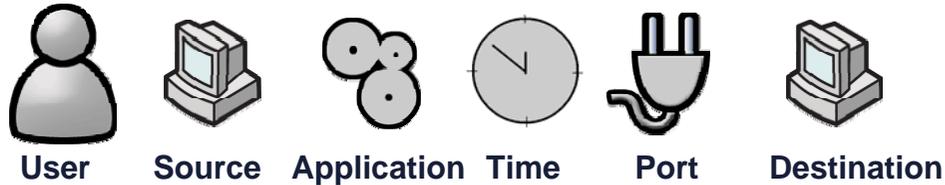
<input checked="" type="checkbox"/>	Total	1689	(100% globally)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Very high criticality	1527	(100% globally)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	High criticality	16	(100% globally)	<input type="checkbox"/>

Users active on 25.11.2006

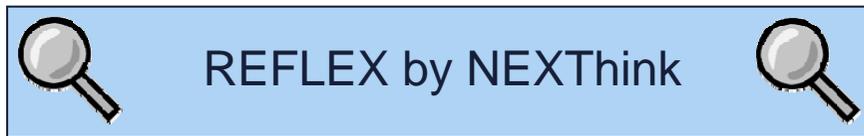
<input checked="" type="checkbox"/>	Total	1568	(100% globally)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Very high criticality	1002	(100% globally)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	High criticality	231	(100% globally)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	New	5	(100% globally)	<input type="checkbox"/>

Download users active on 25.11.2006

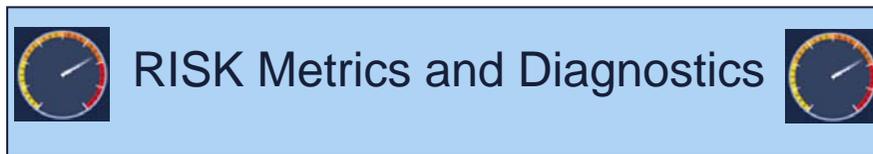
NEXThink has developed technologies and methodologies to measure, control and manage internal risks



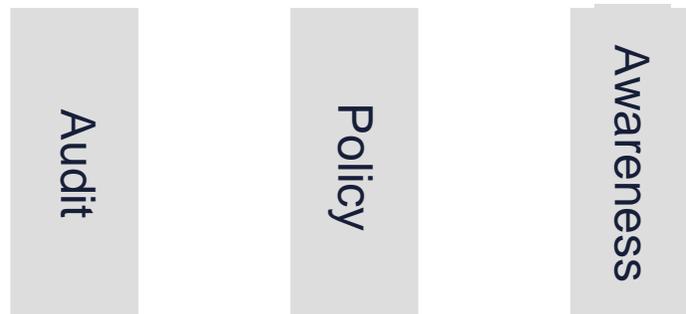
Behavioral Influencers



NEXThink Smart Technology



New Hard Data and Risk Analysis by NEXThink



Key Information Security Activities



NEXThink Methodologies

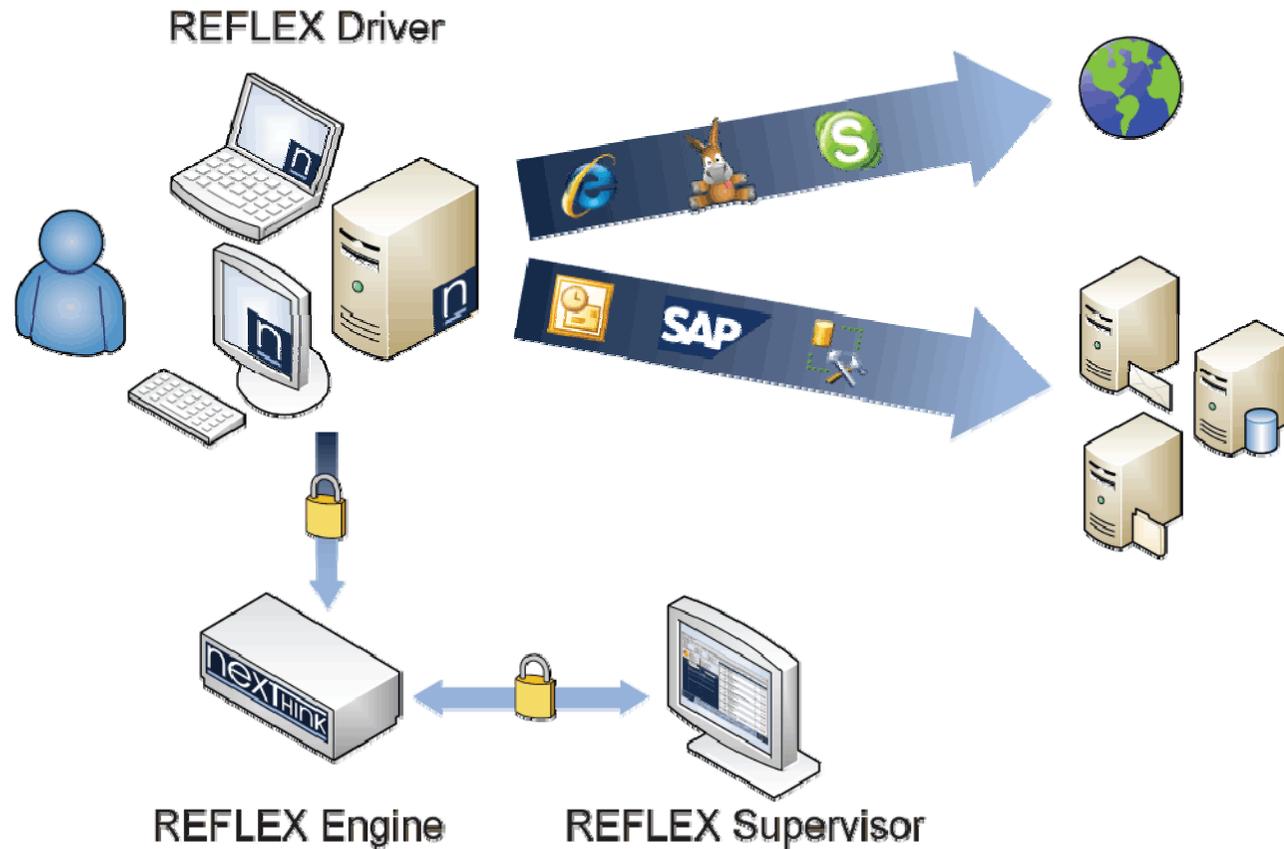


REFLEX Technology

nexTHink[®]

Copyright NEXThink[®] - PUBLIC INFORMATION

REFLEX technology is self-learning, non intrusive, simple to deploy, and patent pending



EPFL
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

CTI START-UP

Université de Fribourg
L'Université suisse bilingue

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

REFLEX components and innovations

REFLEX Driver

- **Minimized and meaningful information collection**
- Passive operation
- Silent installation
- Insignificant local and network performance impact

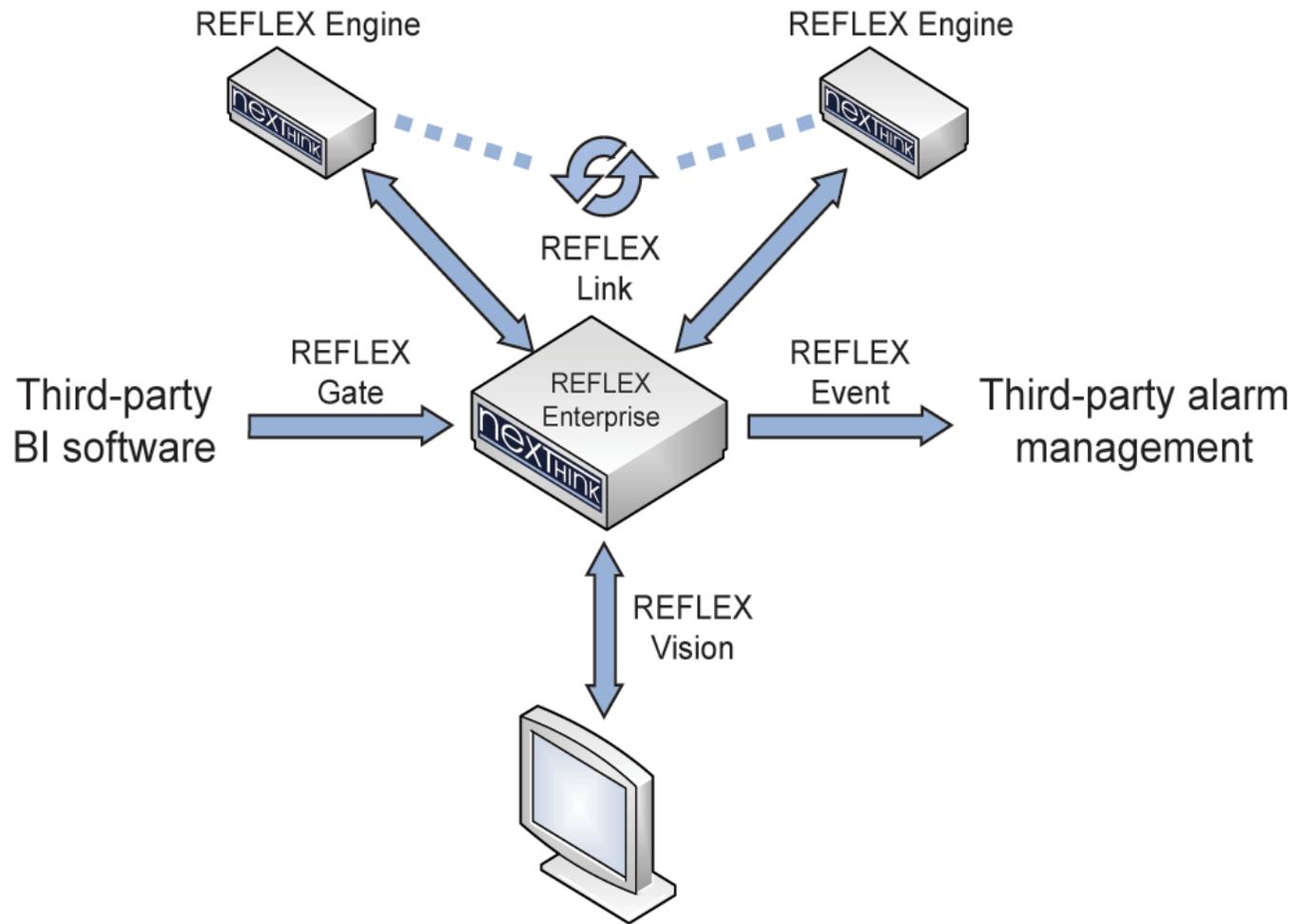
REFLEX Engine

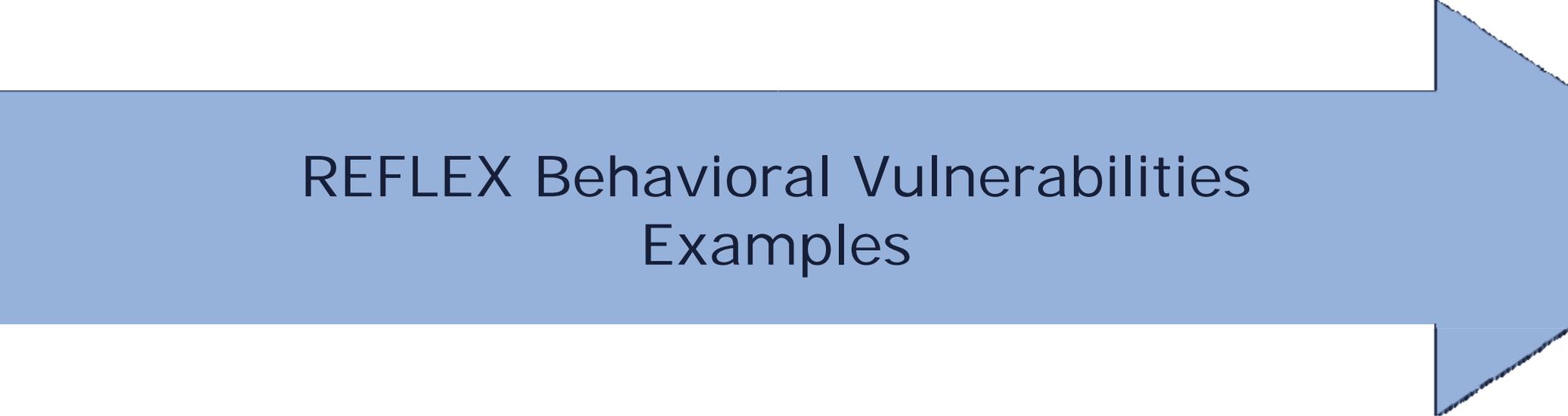
- Independent and deported intelligence
- 3-layer **Artificial Intelligence modelling and analysis applied to security**
- Unique users and applications interactions modelling

REFLEX Supervisor

- Visualization methods for network security events with new **graphical** and **metrics** concept
- **Understand exceptions in a matter of an eye-blink**
- Visualizations are tailored to security knowledge

REFLEX extended architecture for multi-Engine deployments





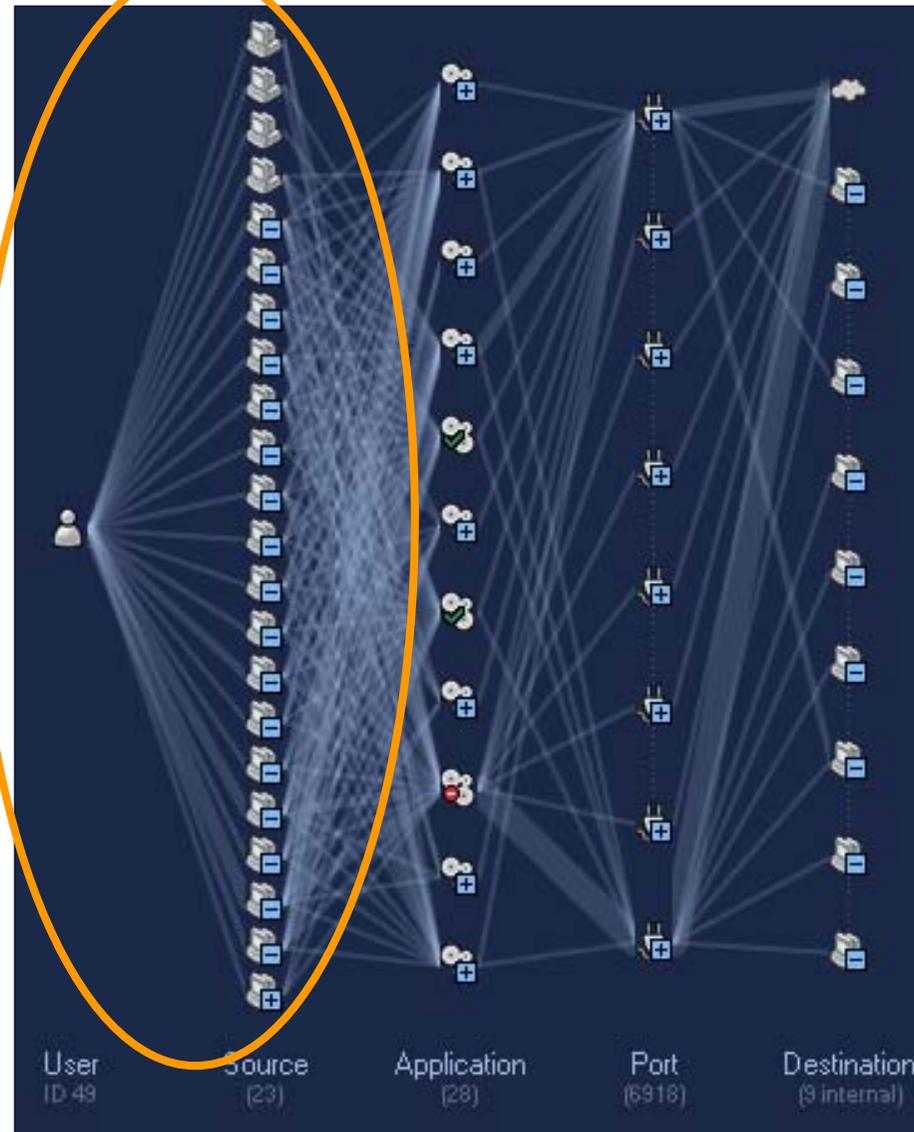
REFLEX Behavioral Vulnerabilities Examples

nexTHink[®]

Copyright NEXThink[®] - PUBLIC INFORMATION

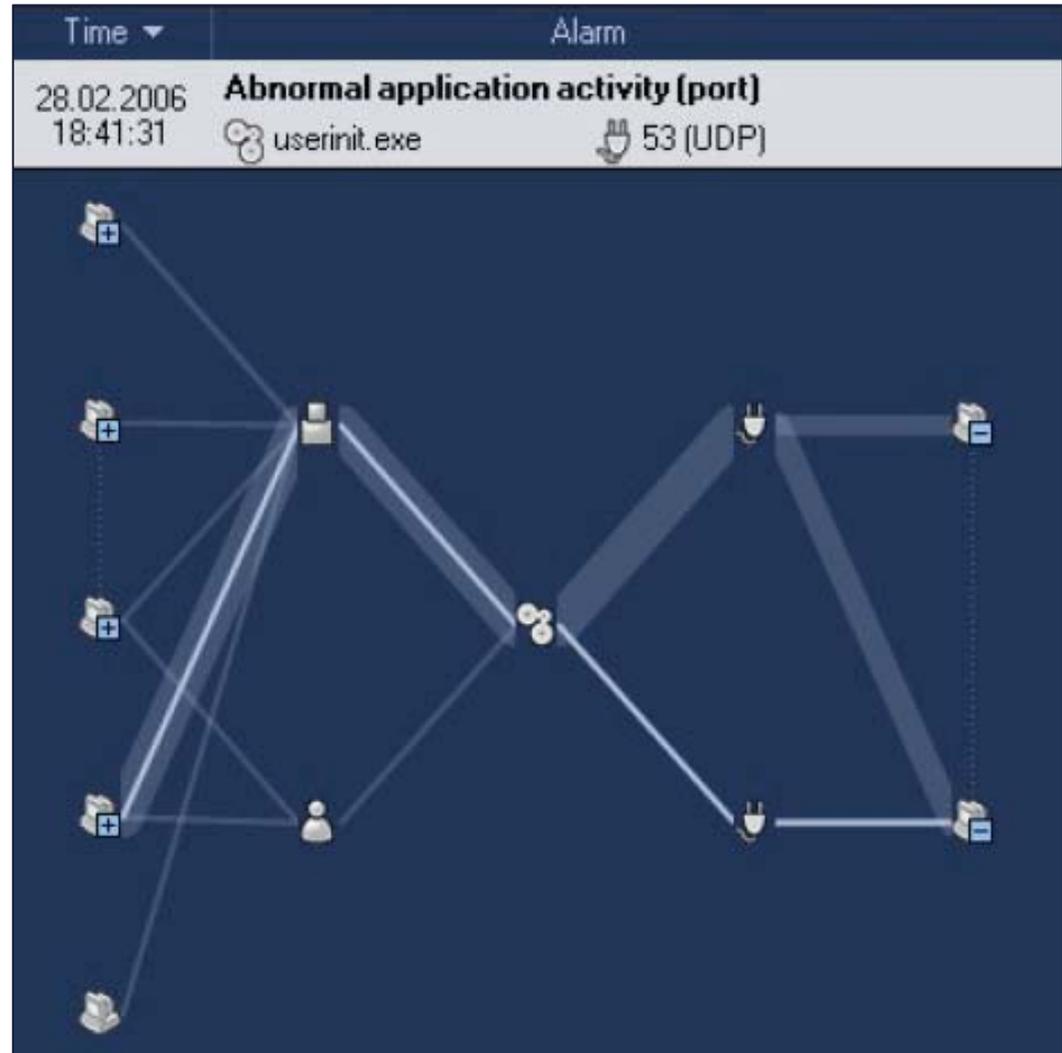
Example of behavioral vulnerabilities (user)

- User account connected to 23 sources!
- Potential abuse of access rights
- Username/pwd leakage



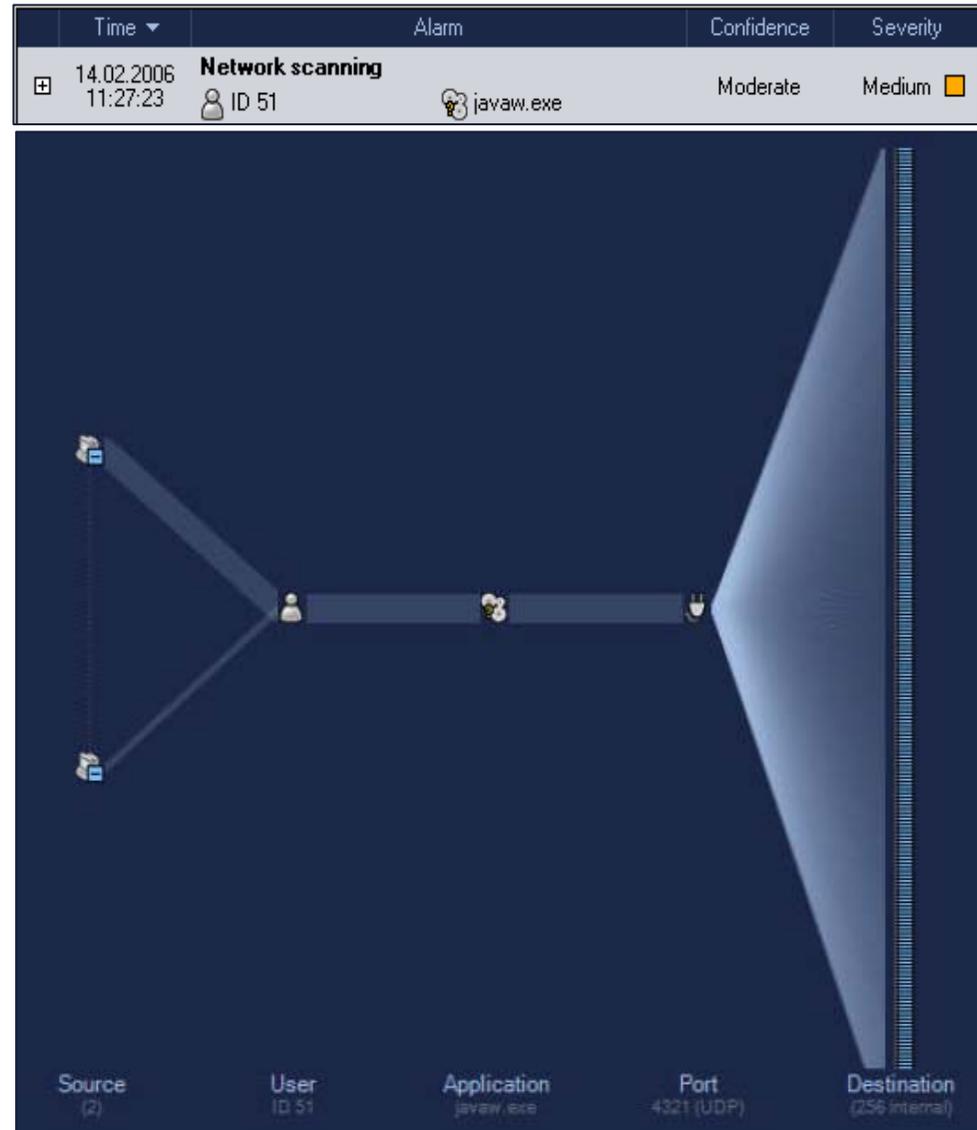
Example of behavioral vulnerabilities (application/network)

- Connection through a new port that was never used before by that application



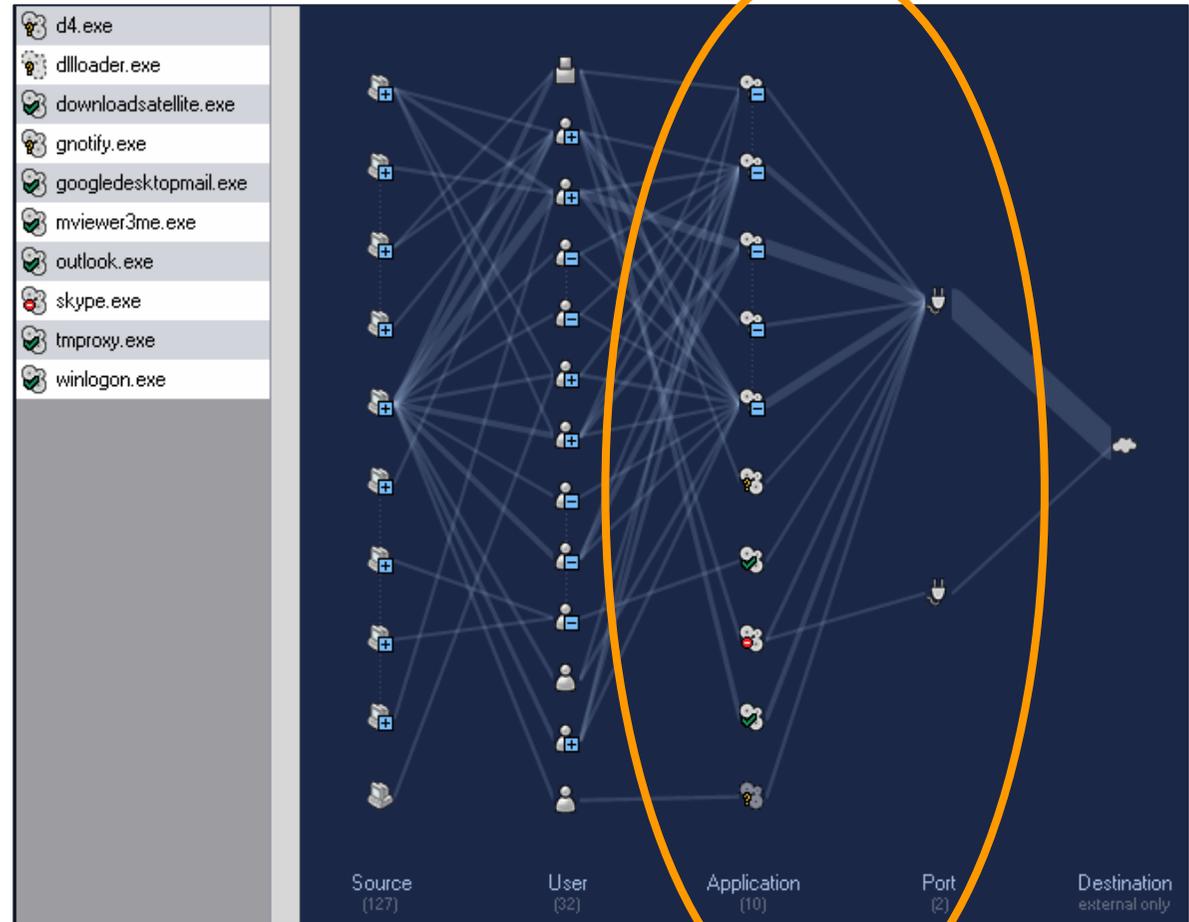
Example of behavioral vulnerabilities (internal scanning)

- Application (and user?) scanning the network



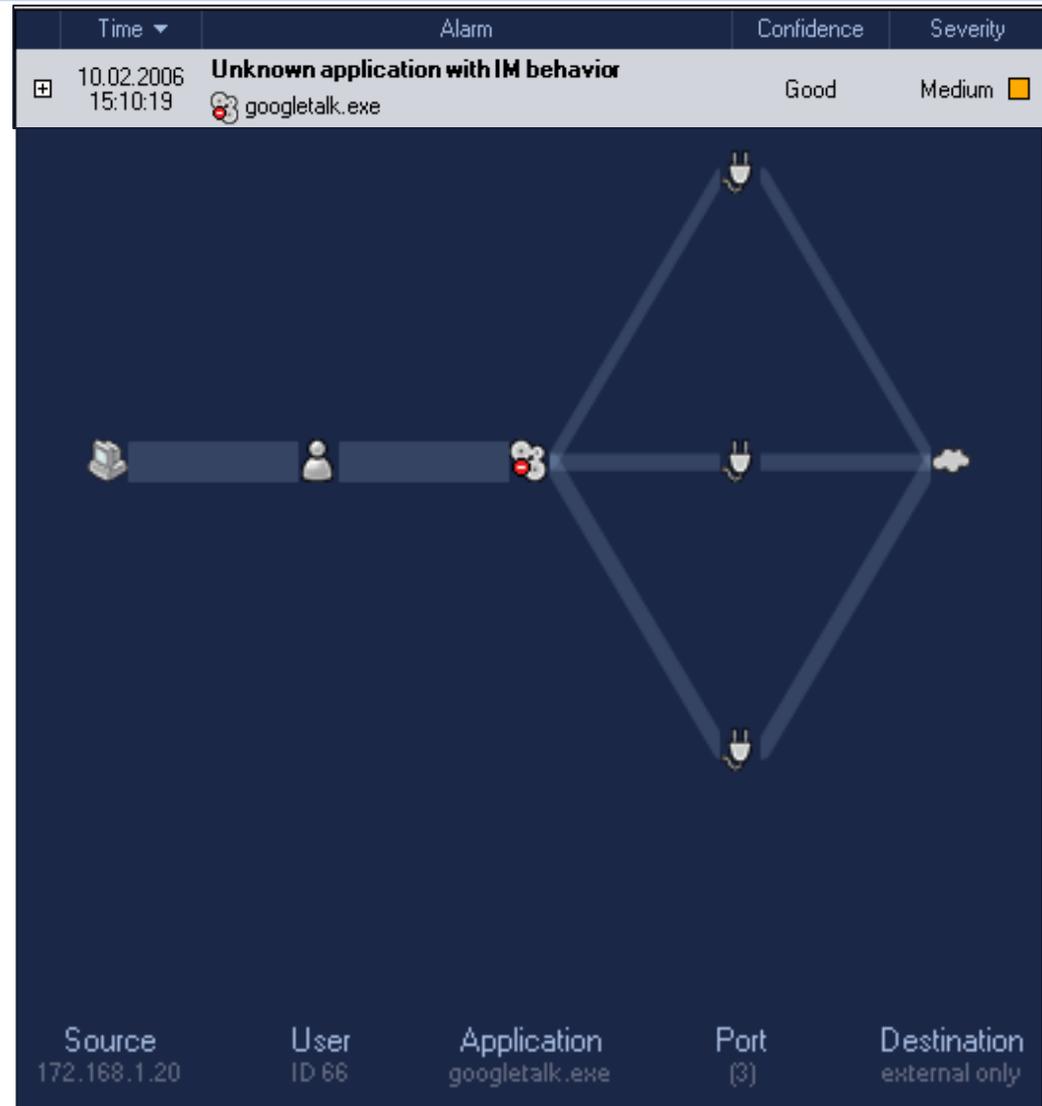
Example of behavioral vulnerabilities (port/network)

- Applications connecting to the outside over port 80 (TCP & UDP)
 - Misconfiguration security equipments
 - Untrusted or even unknown applications activities



Example of behavioral vulnerabilities (application)

- Instant messaging application usage



Example of behavioral vulnerabilities (malware)

- Silent / hidden malicious application (rootkit, spyware?) communicating with the outside (at non standard working hours)

23.02.2006 23:40:28 Malicious application Sure Critical

command.exe

Cause...
Threat level...

7 connections involving 1 users and 1 sources

Time	User	Source	Destination	Application	Port
24.02.2006 01:43:12	ID 17	192.168.10.3	69.42.70.12	command.exe	80 (TCP)
24.02.2006 01:41:20	ID 17	192.168.10.3	206.65.175.114	command.exe	80 (TCP)
24.02.2006 01:40:58	ID 17	192.168.10.3	69.42.70.12	command.exe	80 (TCP)
23.02.2006 23:42:22	ID 17	192.168.10.3	81.22.32.114	command.exe	80 (TCP)
23.02.2006 23:41:44	ID 17	192.168.10.3	69.42.70.12	command.exe	80 (TCP)
23.02.2006 23:40:49	ID 17	192.168.10.3	81.22.32.114	command.exe	80 (TCP)
23.02.2006 23:40:28	ID 17	192.168.10.3	69.42.70.12	command.exe	80 (TCP)

Example of behavioral vulnerabilities (unknown application) 1/2

Time	Alarm	Confidence	Severity		
26.06.2006 18:30:37	Unknown application with spyware behavior win3.tmp.exe	Good	Medium		
Cause...					
Threat level...					
1 connection					
Time	User	Source	Destination	Application	Port
26.06.2006 18:30:37	ID 1373	192.168.150.128	216.255.178.206	win3.tmp.exe	80 (TCP)

Complete scanning result of "windows_server_2003_enterprise_ed", received in VirusTotal at 06.26.2006, 12:11:47 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	6.35.0.16	06.26.2006	no virus found
Authentium	4.93.8	06.23.2006	no virus found
Avast	4.7.844.0	06.23.2006	no virus found
AVG	386	06.25.2006	no virus found
BitDefender	7.2	06.26.2006	Trojan.Mezz.A
CAT-QuickHeal	8.00	06.24.2006	(Suspicious) - DNAScan
ClamAV	devel-20060426	06.26.2006	no virus found
DrWeb	4.33	06.26.2006	BackDoor.Vocc
eTrust-InoculateIT	23.72.49	06.25.2006	no virus found
eTrust-Vet	12.6.2275	06.26.2006	no virus found
Ewido	3.5	06.26.2006	Dropper.Small.aqq
Fortinet	2.77.0.0	06.26.2006	suspicious
F-Prot	3.16f	06.23.2006	no virus found
Ikarus	0.2.65.0	06.26.2006	no virus found
Kaspersky	4.0.2.24	06.26.2006	Trojan-Dropper.Win32.Small.aqq
McAfee	4792	06.23.2006	no virus found
Microsoft	1.1481	06.25.2006	no virus found
NOD32v2	1.1623	06.26.2006	no virus found
Norman	5.90.21	06.26.2006	no virus found
Panda	9.0.0.4	06.25.2006	Suspicious file
Sophos	4.07.0	06.26.2006	no virus found
Symantec	8.0	06.26.2006	no virus found
TheHacker	5.9.8.165	06.26.2006	no virus found
UNA	1.83	06.23.2006	no virus found
VBA32	3.11.0	06.26.2006	no virus found
VirusBuster	4.3.7.9	06.25.2006	no virus found

Example of behavioral vulnerabilities (unknown application) 2/2

192.168.150.128

Appeared on the network on
26.06.2006 at 18:29



Strangeness



Activity

(last updated on 26.06.2006 at 18:53) 



User
ID 1373

Source
192.168.150.128

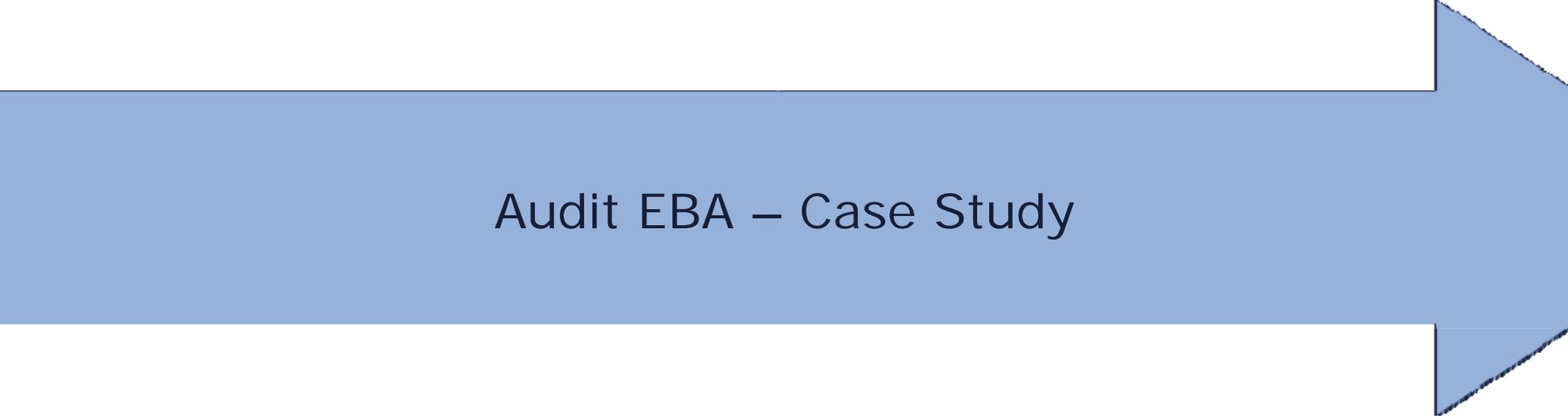
Application
(2)

Port
80 (TCP)

Destination
external only

.... last **pending alarms** where severity is any

Time	Alarm	Confidence	Severity		
26.06.2006 18:30:37	 win3.tmp.exe	Good	Medium ■		
Cause: A non identified application with possible spyware behavior is active (a category and a policy must be applied to any application)					
Threat level...					
1 connection					
Time	User	Source	Destination	Application	Port
26.06.2006 18:30:37	ID 1373	192.168.150.128	216.255.178.206	win3.tmp.exe	80 (TCP)



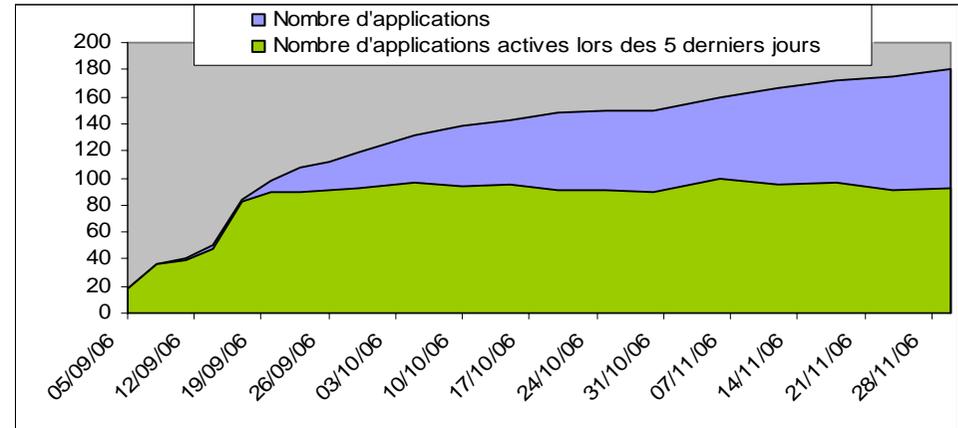
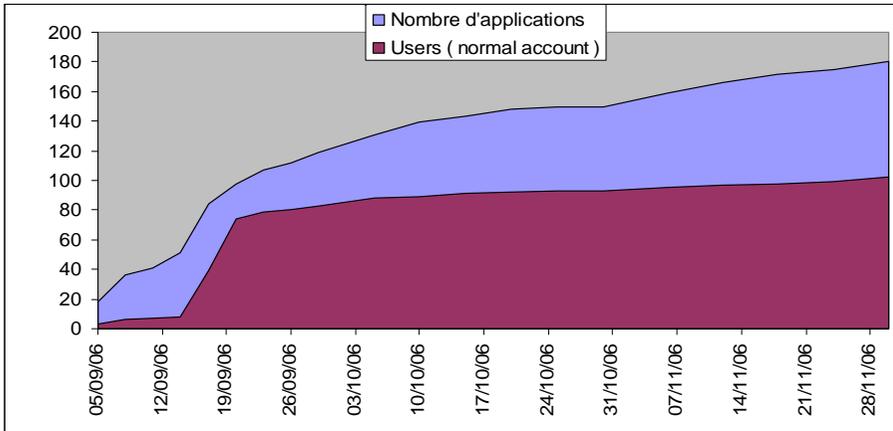
Audit EBA – Case Study

nexTHink[®]

Copyright NEXThink[®] - PUBLIC INFORMATION

Initial inventory of activity

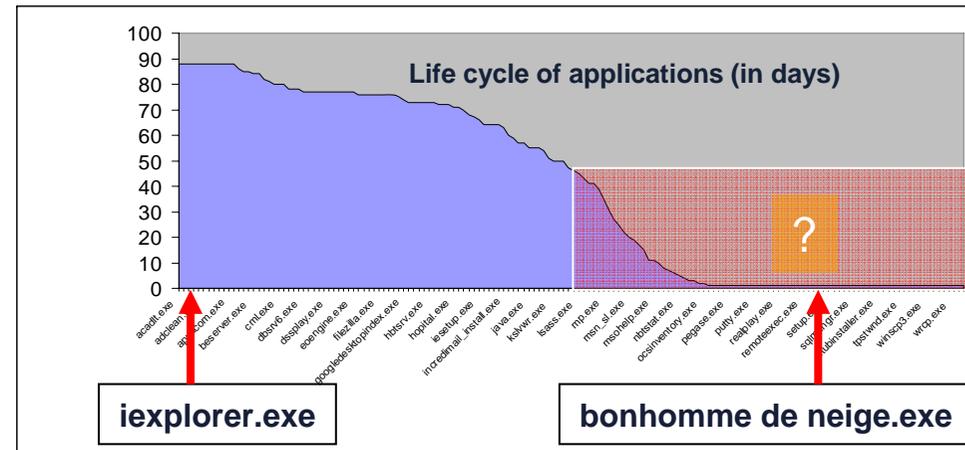
- Installation : **September 15th, 2006**
- Users : **110**
- Applications : **180**
- Sources : **160**



HotBar →

Incredimail →

Application	First time
sseasyscreensavers by hotbar.scr	30.11.2006 16:31:06
hbtsrv.exe	30.11.2006 16:29:10
hbtv.exe	30.11.2006 16:29:02
cml.exe	30.11.2006 16:29:01
glbb1.tmp	30.11.2006 14:00:14
iesetup.exe	30.11.2006 13:56:54
incredimail_install.exe	30.11.2006 12:23:36

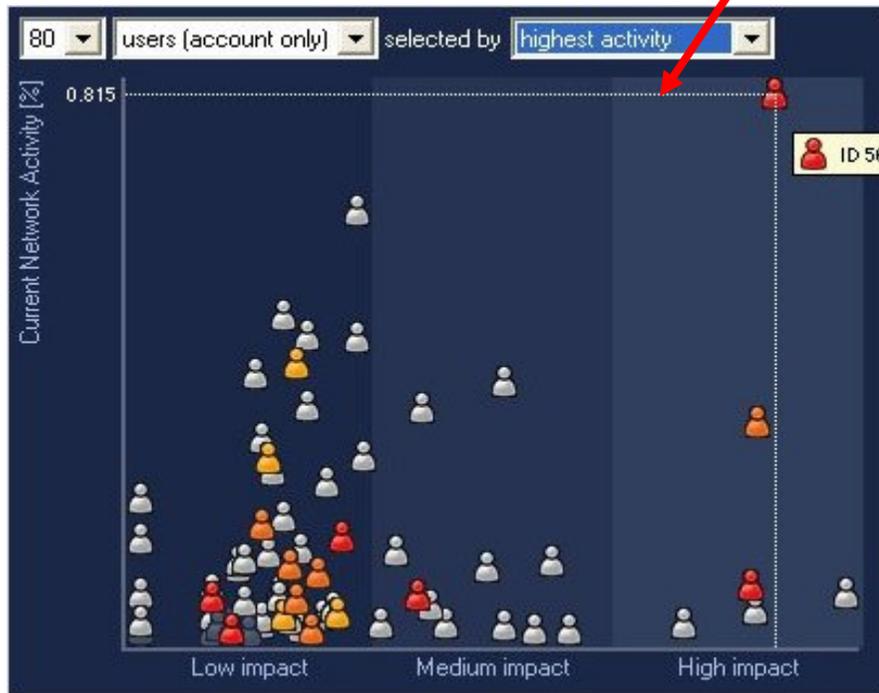


Reactivity based on intuitive visualizations

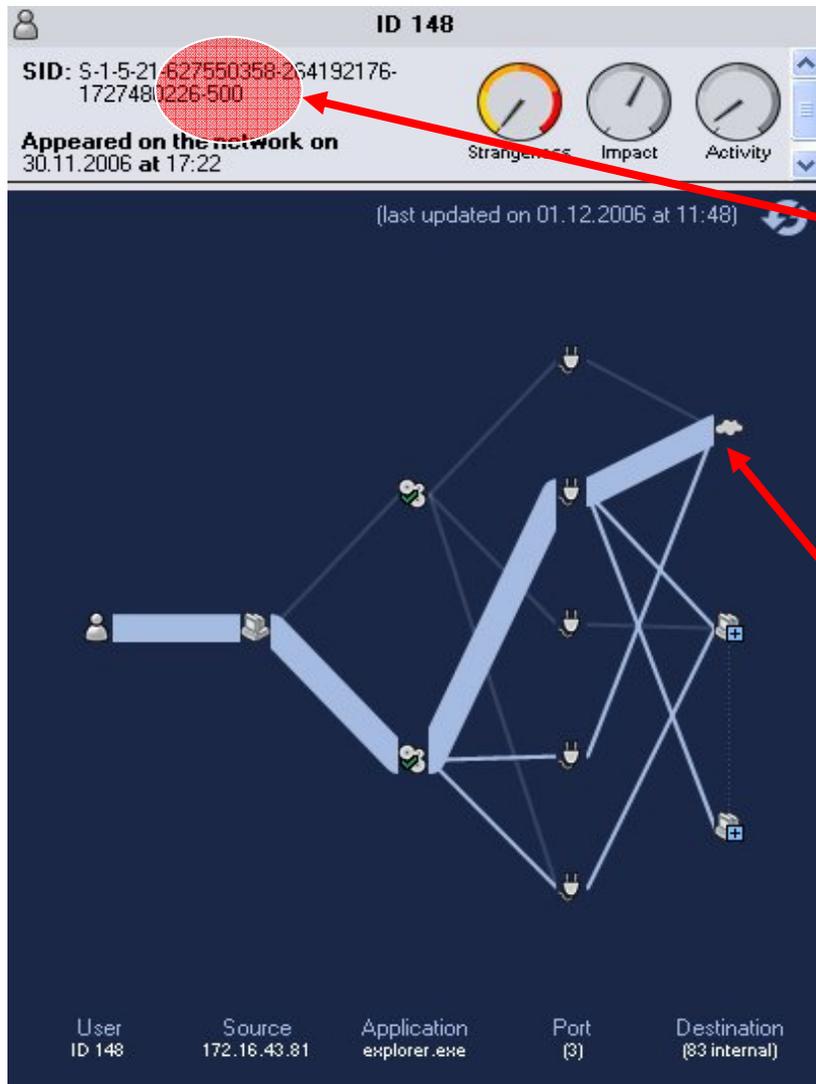
Network Activity (last 3 days)

Thursday November 30th

Friday December 1st (next day)



Immediate qualification of the potential problem



Event on Thursday Nov 30th 17:22

New Local Admin User

Heavy/abnormal traffic of this new "local admin user" with *explorer.exe* towards external destinations

Causal analysis based on time, user, application and source

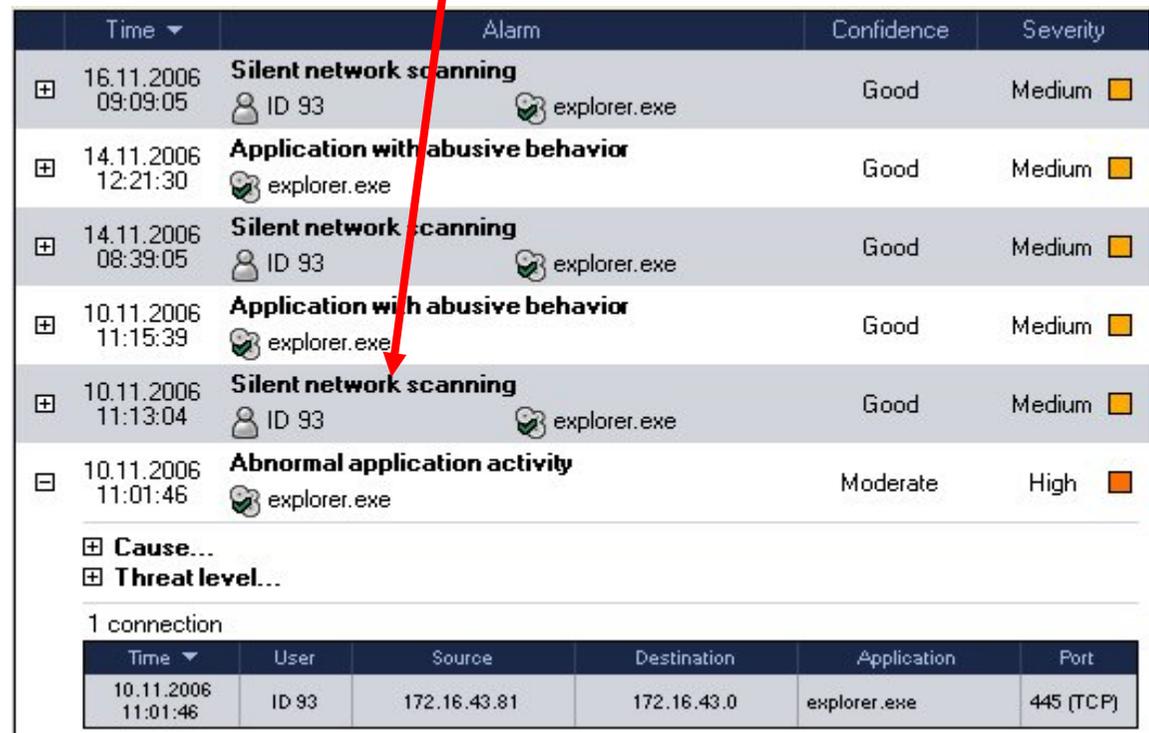
- 2 similar version of MSN Messenger are active
- ...but the binaries are different (hash not the same)

The screenshot displays a security analysis interface. On the left, a network diagram shows connections between various nodes, with a legend at the bottom identifying Source (11), User (12), Application (msmsgs.exe), Port (4), and Destination (3 internal). The main panel on the right shows a list of alarms for 'msmsgs.exe / MSN Messenger'. A red box highlights a specific entry in the 'Versions' tab, showing two different hashes for version 4.7.0.41. Another red box highlights an alarm entry for 'Modified application binary' with a 'Sure' confidence level and 'Critical' severity. Below this, a 'Cause...' section shows a 'Threat level...' and a table of connections involving 1 user and 1 source.

Time	User	Source	Destination	Application	Port
10.11.2006 10:59:24	ID 68	172.16.43.81	172.16.42.15	msmsgs.exe	1900 (UDP)

Impact alerting and full scope of the problem

- Successful buffer overflow against « *windows messenger* »
 - Local anti-virus did not react (although up to date)
 - Backdoor to exploit the process « *explorer.exe* » has been installed
 - To finally scan the whole internal network (silently)



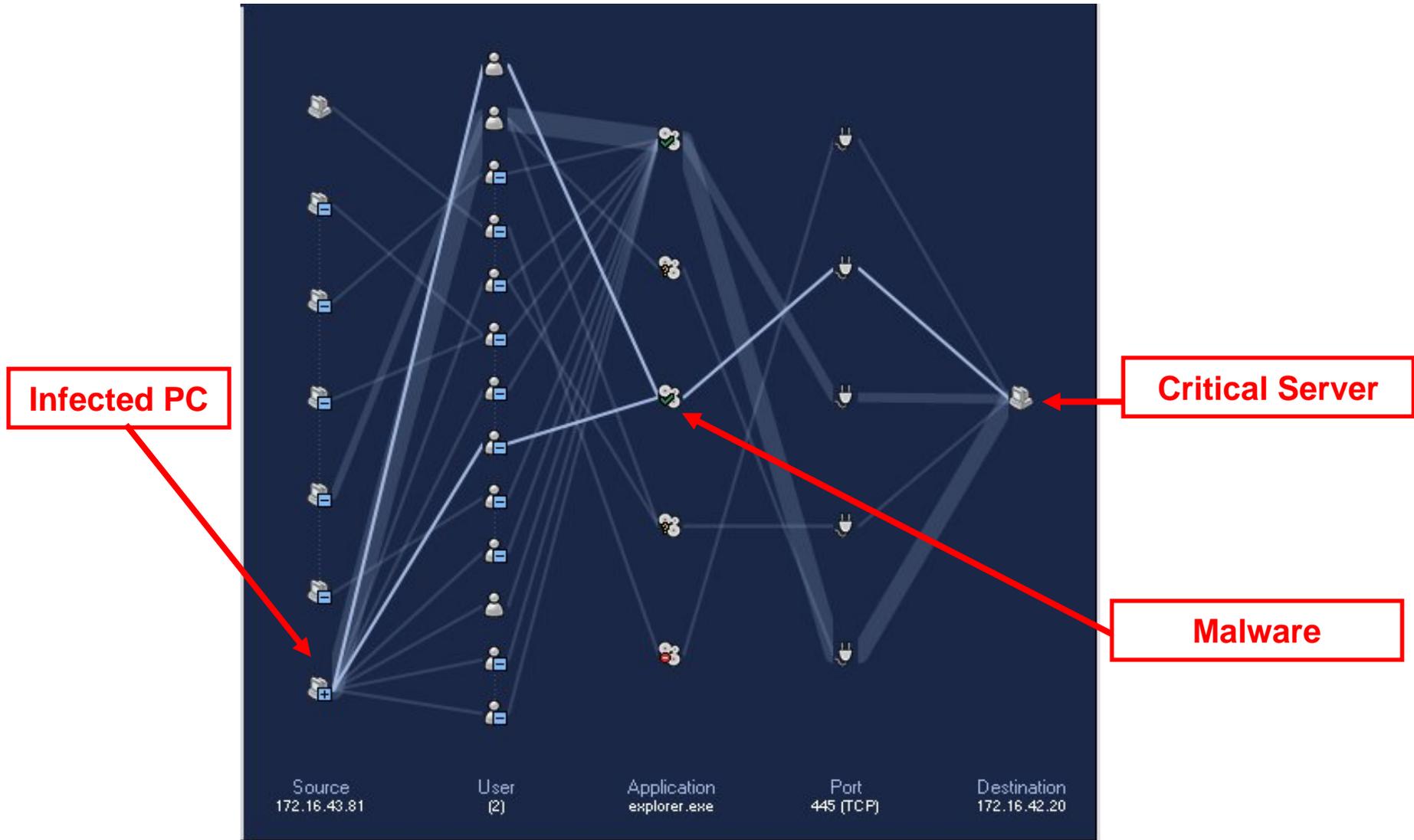
Time	Alarm	Confidence	Severity
16.11.2006 09:09:05	Silent network scanning ID 93 explorer.exe	Good	Medium
14.11.2006 12:21:30	Application with abusive behavior explorer.exe	Good	Medium
14.11.2006 08:39:05	Silent network scanning ID 93 explorer.exe	Good	Medium
10.11.2006 11:15:39	Application with abusive behavior explorer.exe	Good	Medium
10.11.2006 11:13:04	Silent network scanning ID 93 explorer.exe	Good	Medium
10.11.2006 11:01:46	Abnormal application activity explorer.exe	Moderate	High

Cause...
Threat level...

1 connection

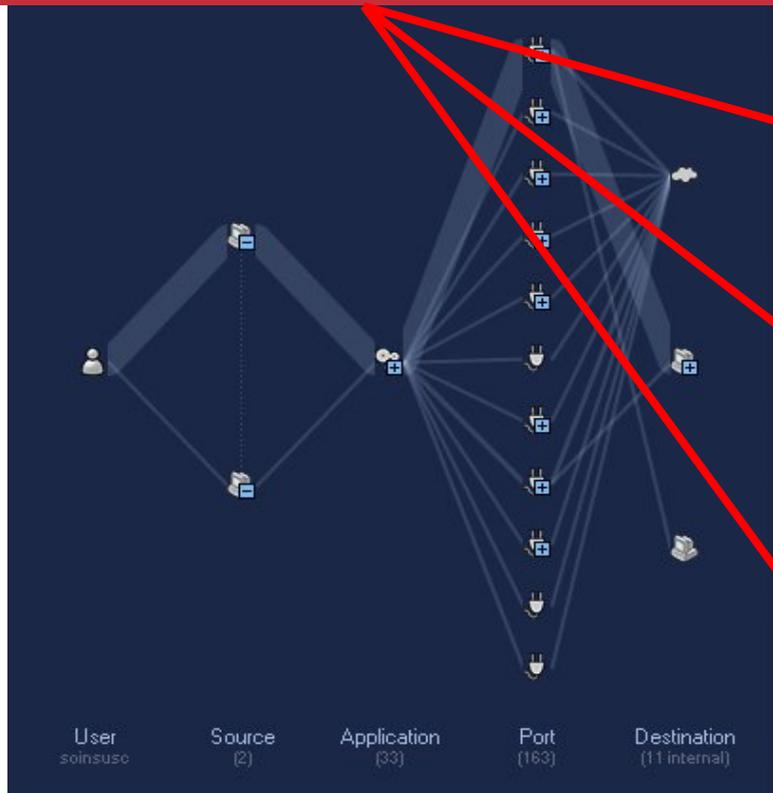
Time	User	Source	Destination	Application	Port
10.11.2006 11:01:46	ID 93	172.16.43.81	172.16.43.0	explorer.exe	445 (TCP)

Risk analysis of a highly critical destination



Risk analysis of a shared computer

- o Poste XYZ
- o Dimanche 26 novembre
- o Apparition de :
 - emule.exe (peer-to-peer)
 - limewire.exe (peer-to-peer)
 - shareaza.exe (peer-to-peer)



Alarm	Confidence	Severity
IM application msnmsgr.exe	Sure	Critical
Application with abusive behavior shareaza.exe	Moderate	Medium
Abusive network usage soinsusc	Moderate	High
Unknown application with P2P behavior shareaza.exe	Good	Medium
Abusive network usage soinsusc	Moderate	High
Abusive network usage soinsusc	Moderate	High
Denied application limewire.exe	Sure	Critical
Unknown application with spyware behavior stubbinstaller.exe	Good	Medium
P2P application emule.exe	Sure	Critical
New application binary version emule.exe (version: 0.47.2.66)	Sure	High
Abnormal application activity emule.exe	Good	High
IM application msnmsgr.exe	Sure	Critical
IM application msn_sl.exe	Sure	Critical
IM application	Sure	Critical

Conclusion and proposed actions



- Well secured organization
 - Update and patch management
 - Anti-Virus updates tested every day
 - Application proxies
 - Firewalls on the perimeters
 - On going log monitoring
- Human factor remains a threat not to be overlooked
- Leverage user risk perception with focused awareness programs and assess their efficiency



REFLEX Demo

nEXThink[®]

Copyright NEXThink[®] - PUBLIC INFORMATION

nextTHINK®
