NEXThink®

refocusing information security on the human factor

OSSIR (Windows Security Group)

February 5th, Paris

Vincent Bieri, CEO

vincent.bieri@nexthink.com

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 Assisses 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

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

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

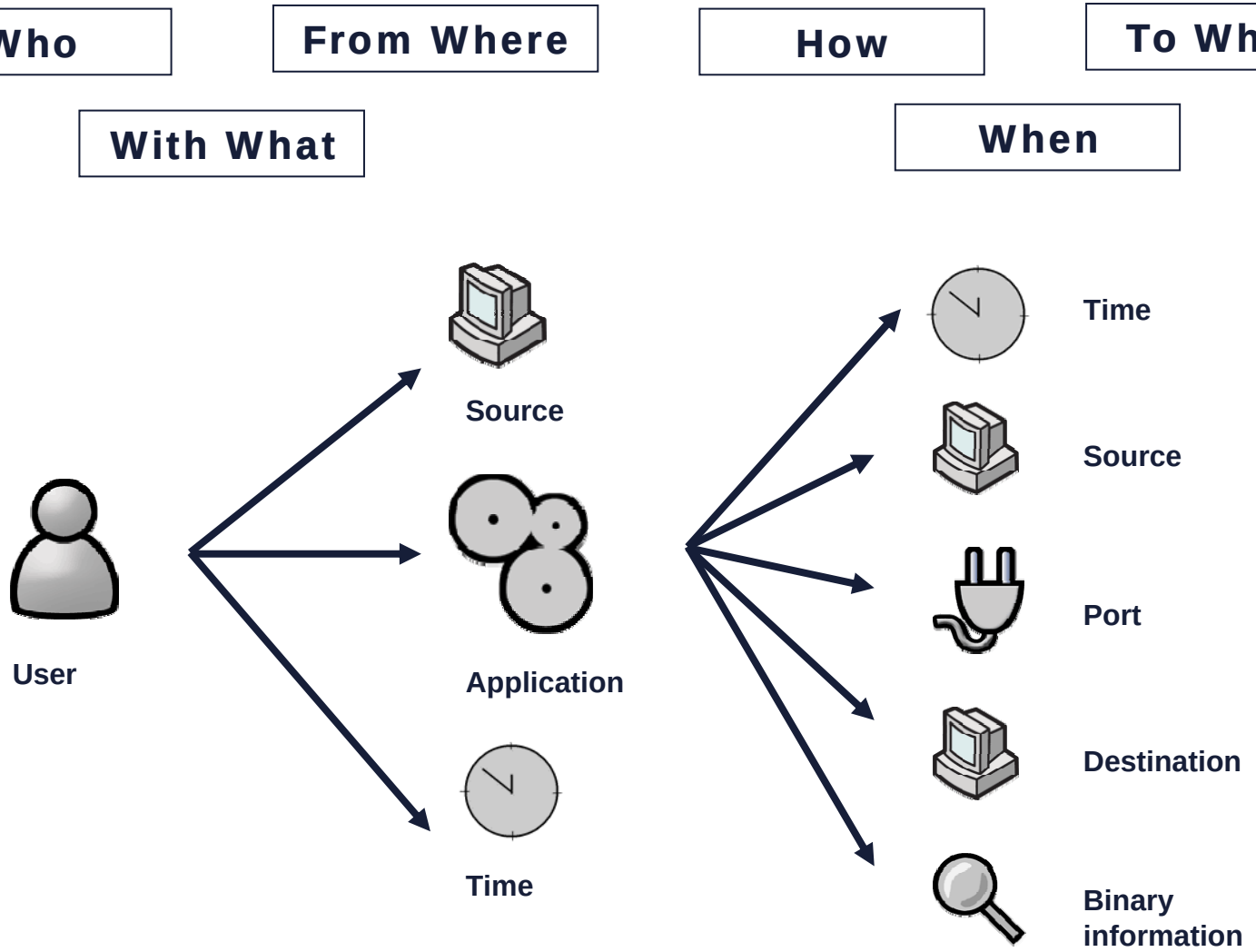
Who am I for the company ?

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

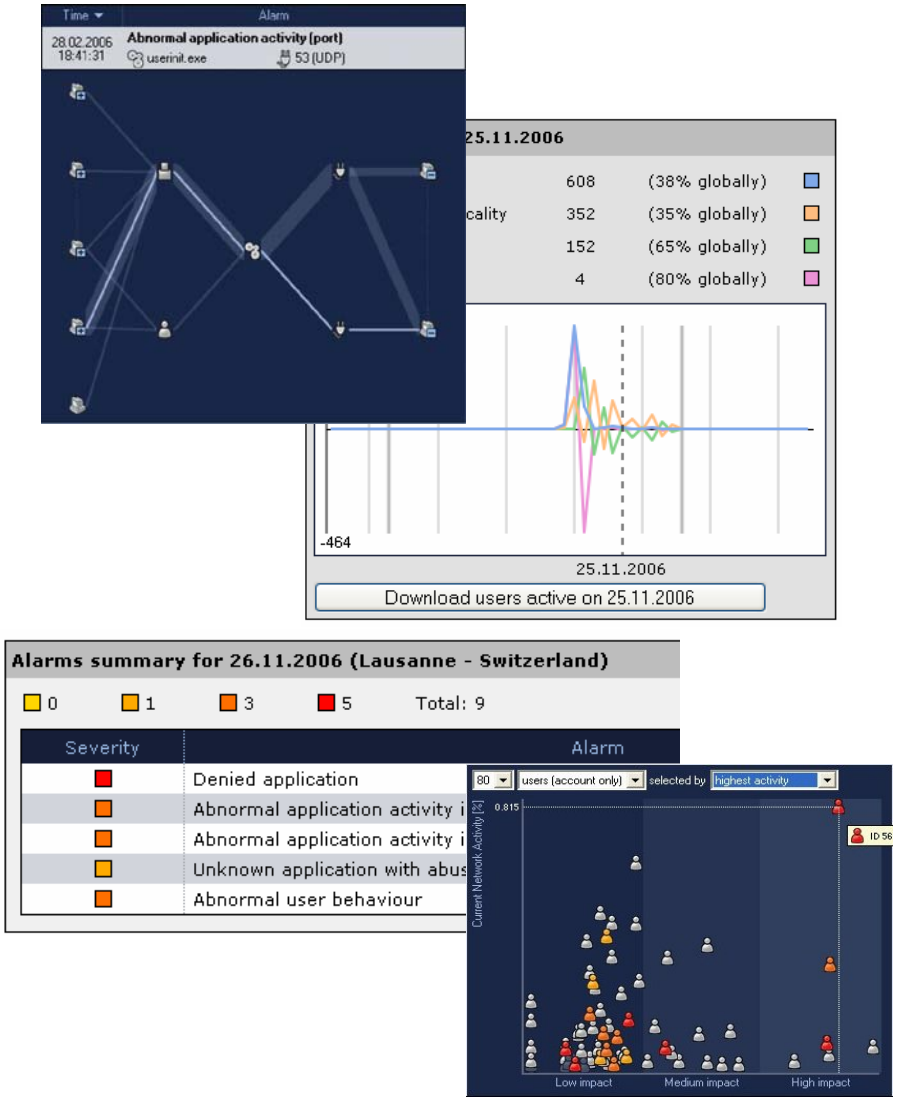
Do I behave dangerously ?

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

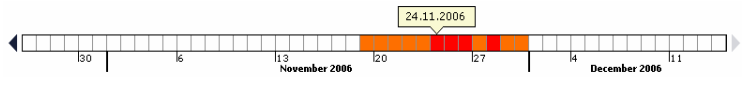


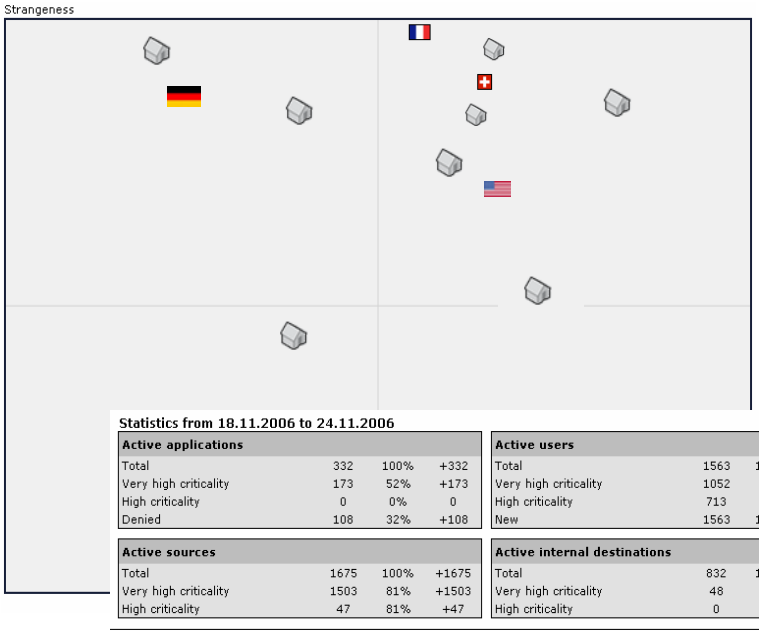
With REFLEX™ NEXThink refocuses information security on the human factor



- 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





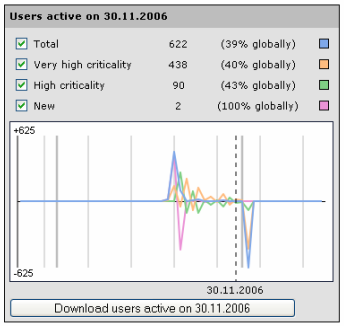
Statistics from 18.11.2006 to 24.11.2006

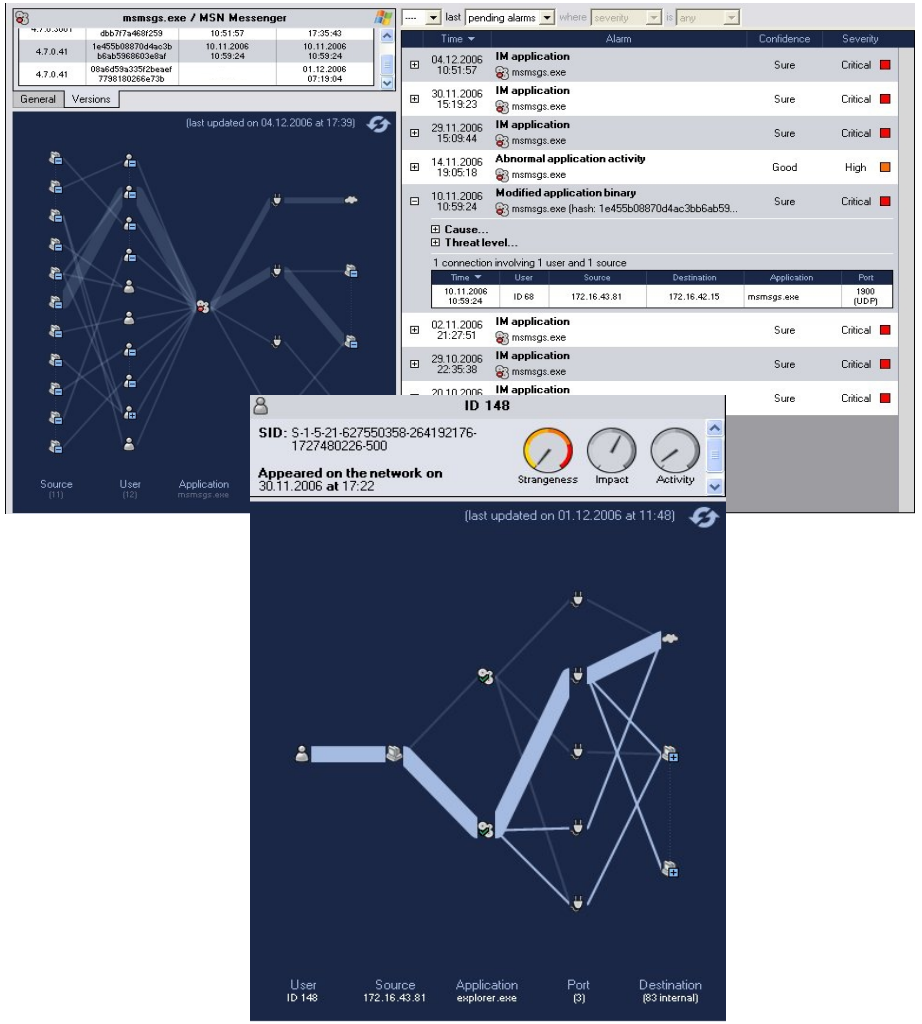
Active applications			
Total	332	100%	+332
Very high criticality	173	52%	+173
High criticality	0	0%	0
Denied	108	32%	+108

Active users			
Total	1563	100%	+1563
Very high criticality	1052	34%	+1052
High criticality	713	23%	+713
New	1563	100%	+1563

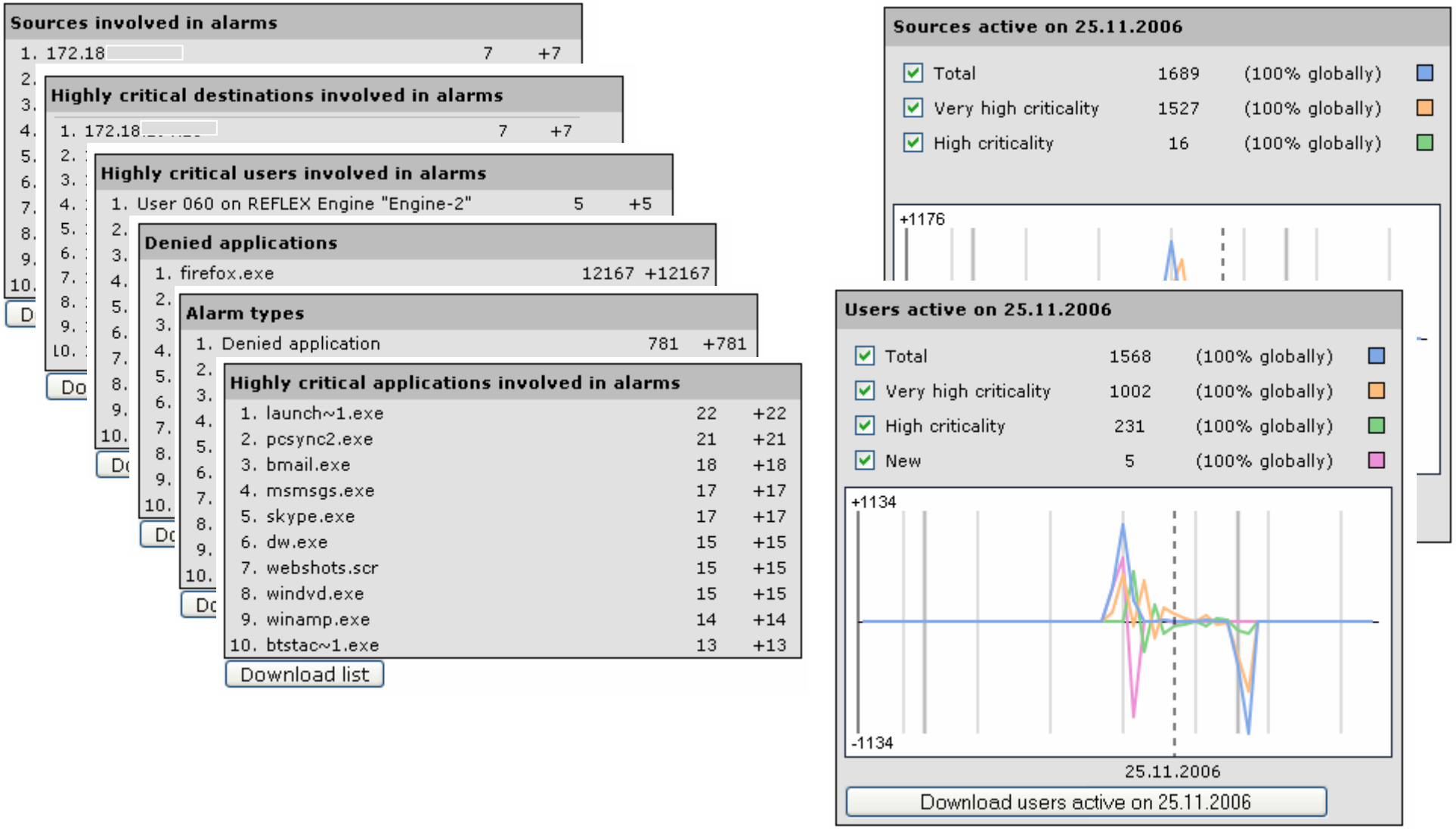
Active sources			
Total	1675	100%	+1675
Very high criticality	1503	81%	+1503
High criticality	47	81%	+47

Active internal destinations			
Total	832	100%	+832
Very high criticality	48	5%	+48
High criticality	0	0%	0

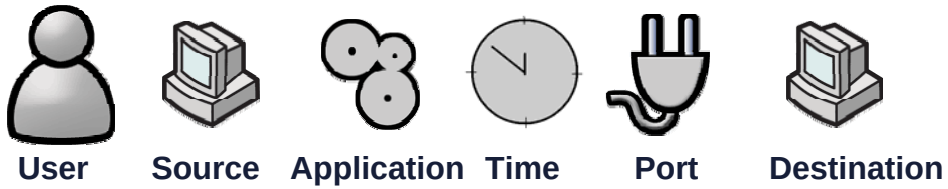




REFLEX ™ has various risk reporting data



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



Behavioral Influencers

REFLEX by NEXThink

RISK Metrics and Diagnostics

NEXThink Smart Technology

New Hard Data and Risk Analysis by NEXThink

Audit

Policy

Awareness

Key Information Security Activities

Behavioral Audit Management **EBA™**

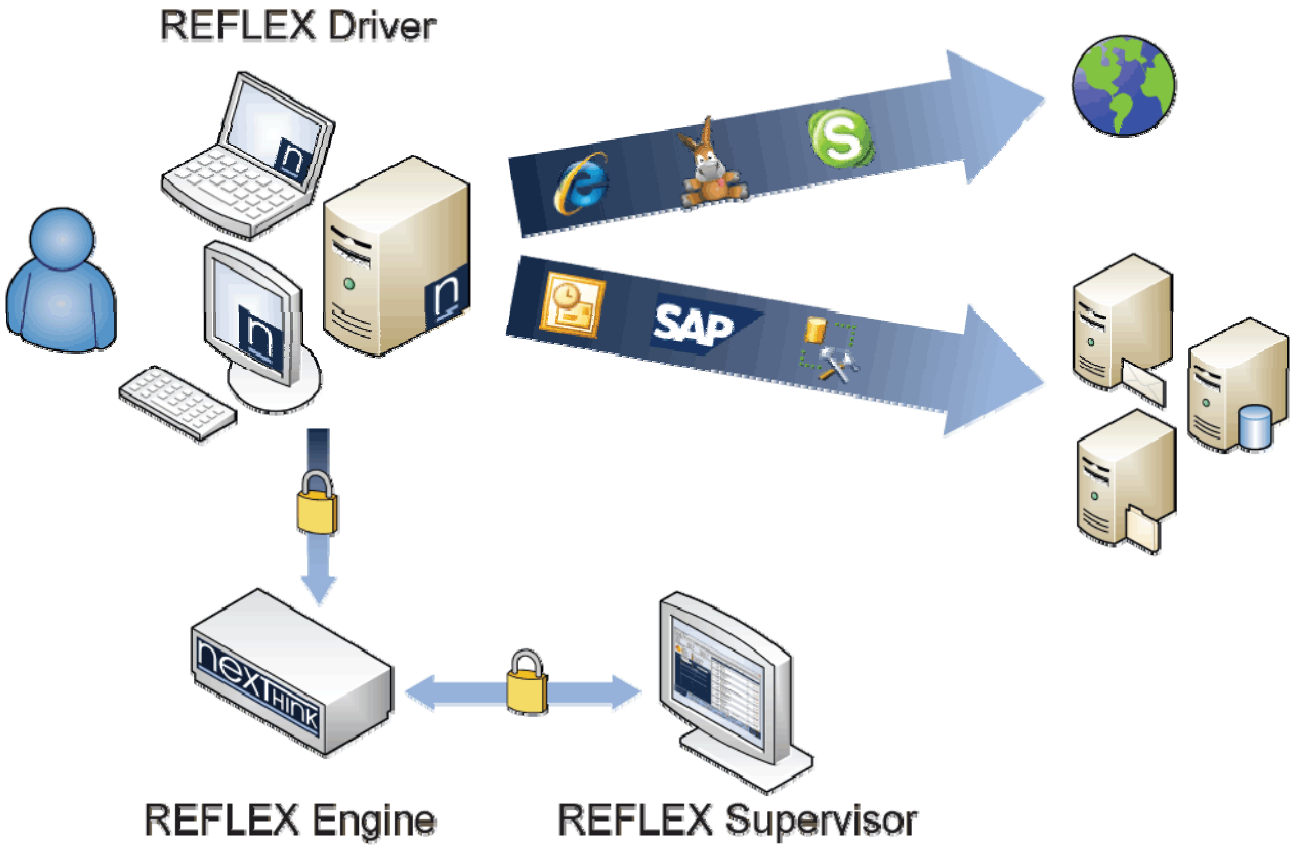
Security Policy Review **SPA™**

Management of Awareness Program **MAP™**

NEXThink Methodologies

REFLEX Technology

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



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

nexThink

REFLEX components and innovations

REFLEX Driver

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

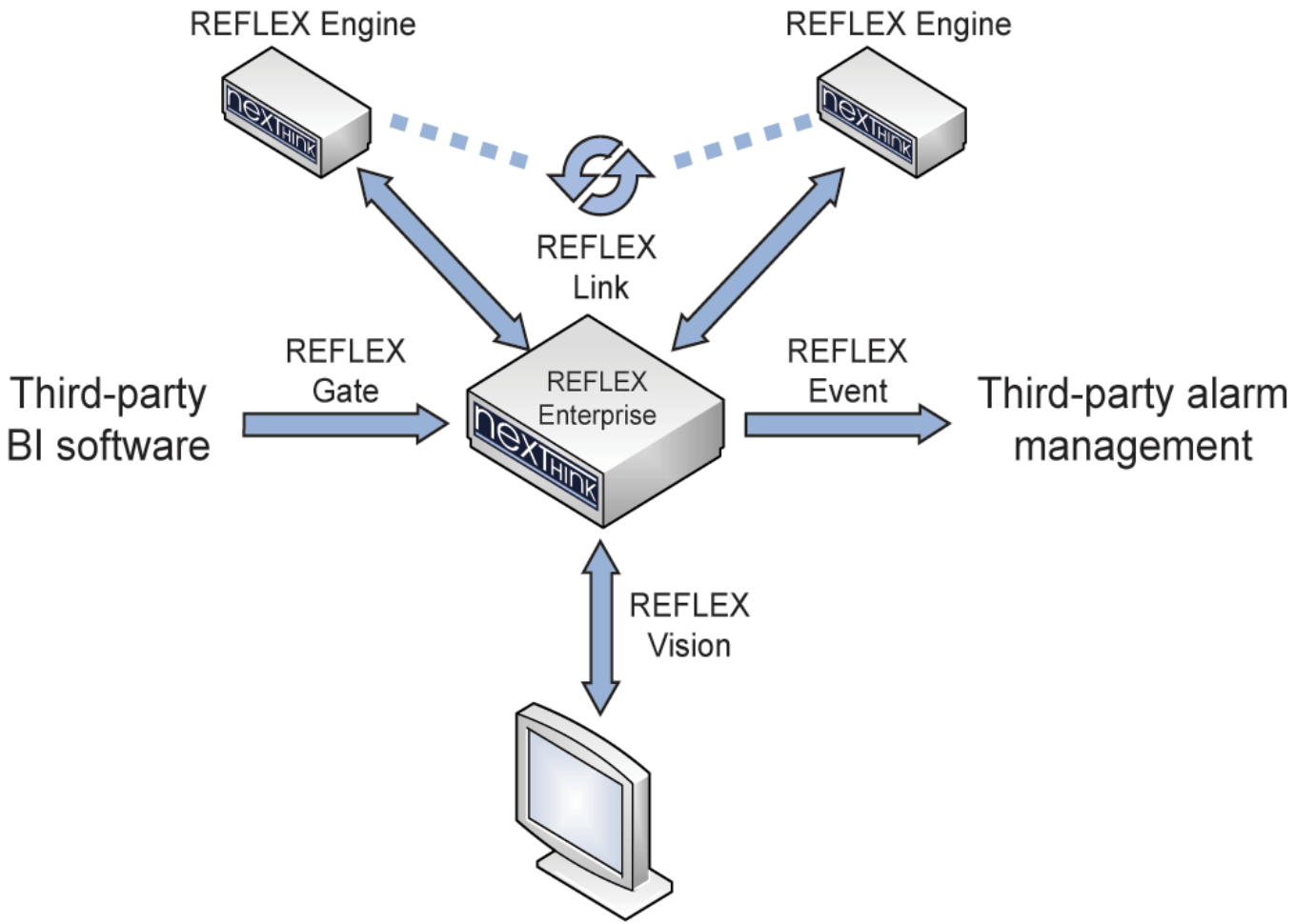
REFLEX Engine

- 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

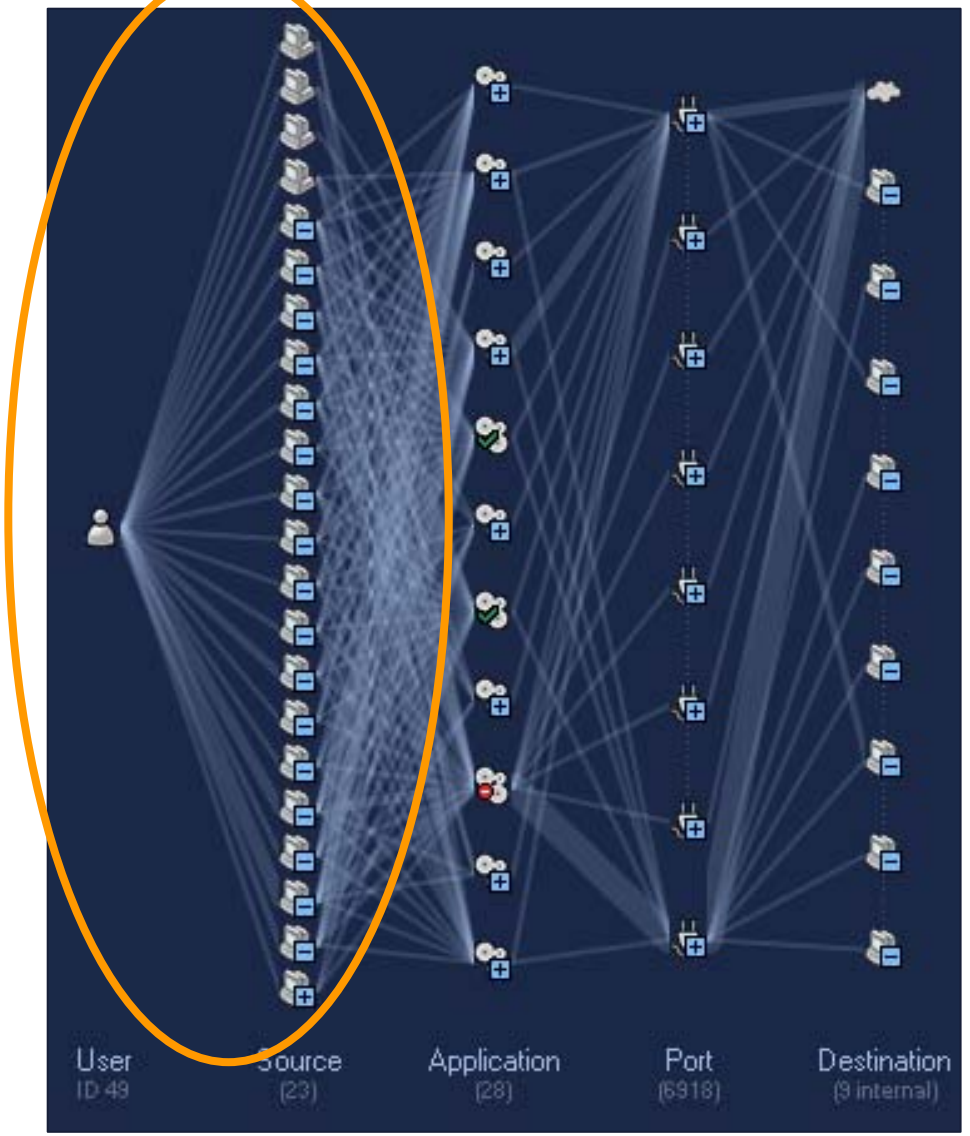
REFLEX extended architecture for multi-Engine deployments



REFLEX Behavioral Vulnerabilities Examples

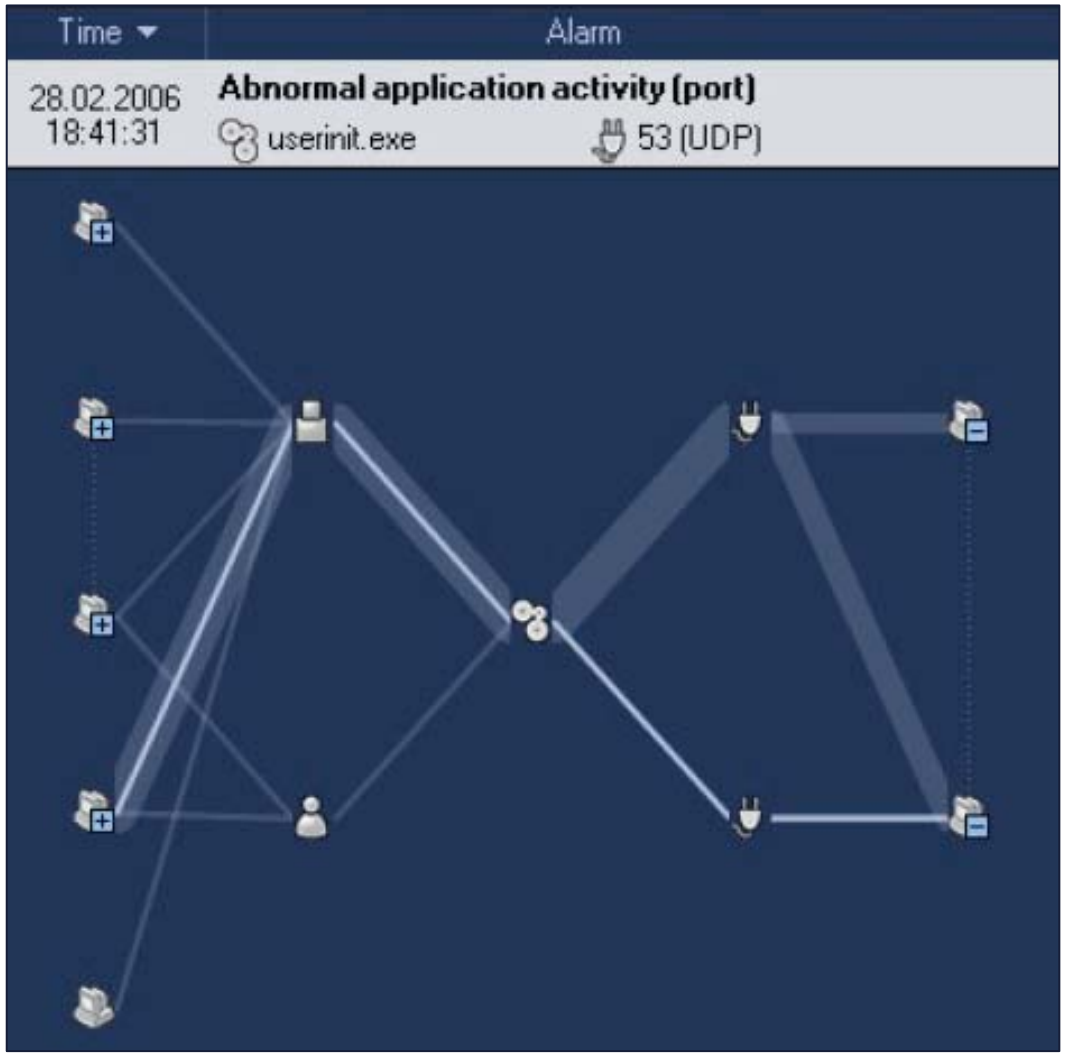
Example of behavioral vulnerabilities (user)

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



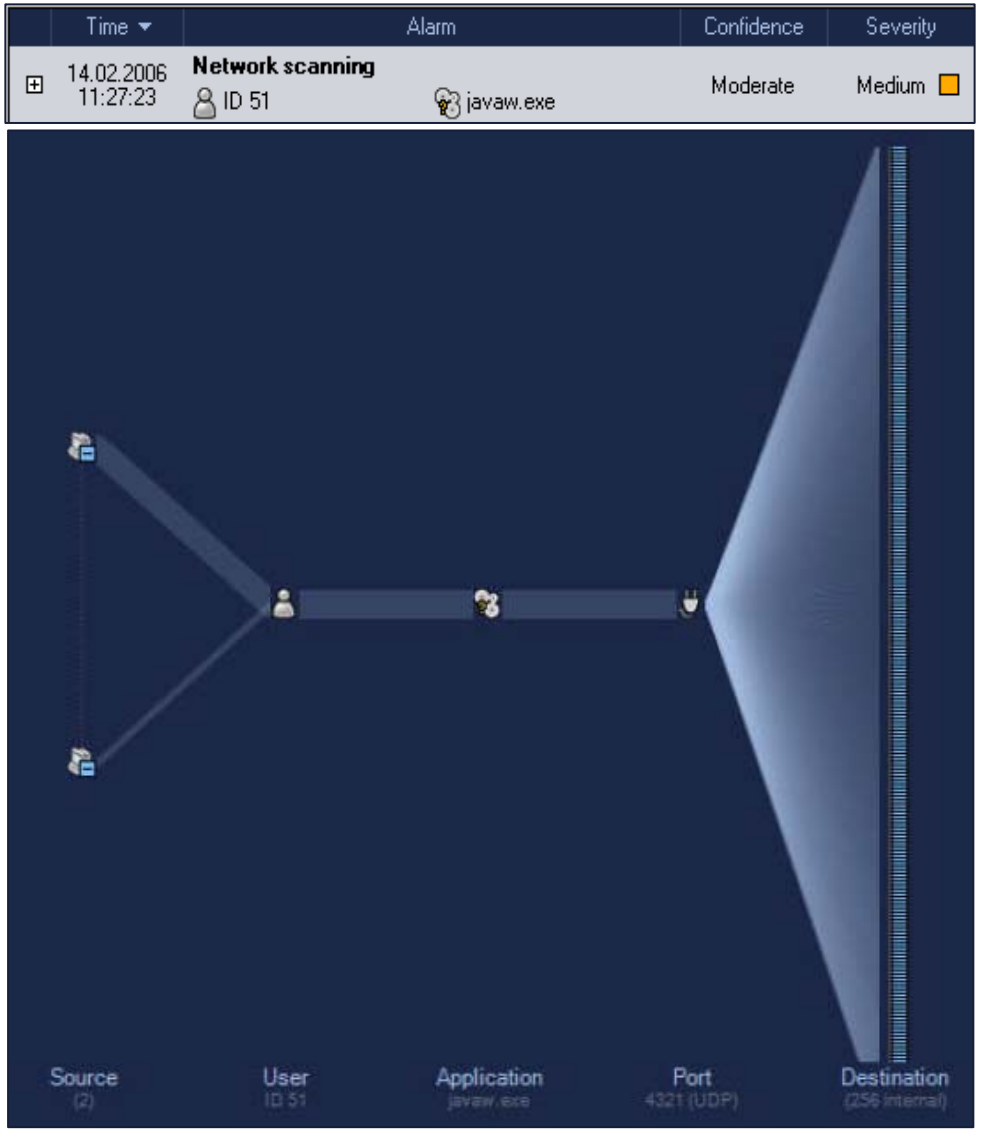
Example of behavioral vulnerabilities (application/network)

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



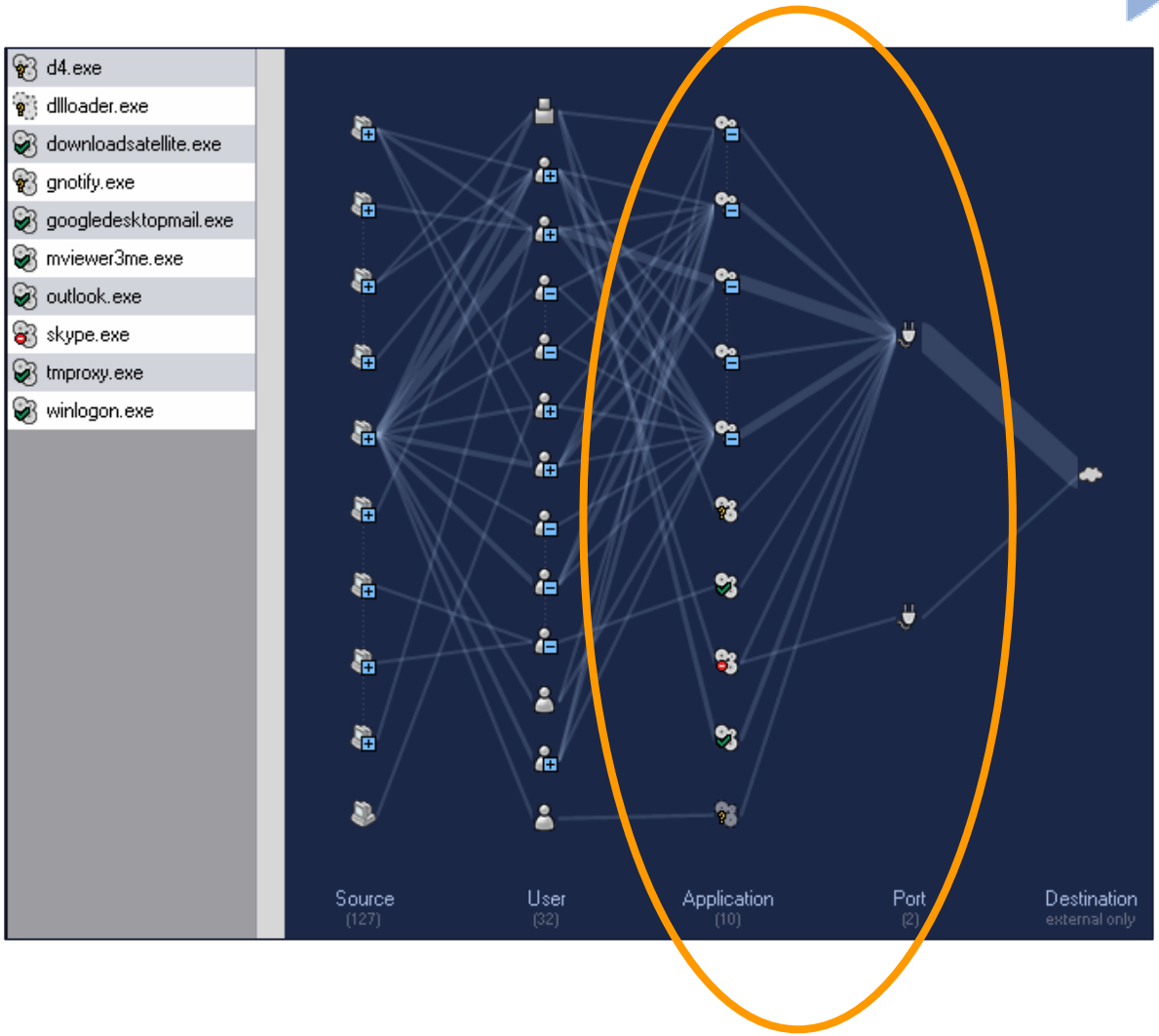
Example of behavioral vulnerabilities (internal scanning)

- Application (and user?) scanning the network



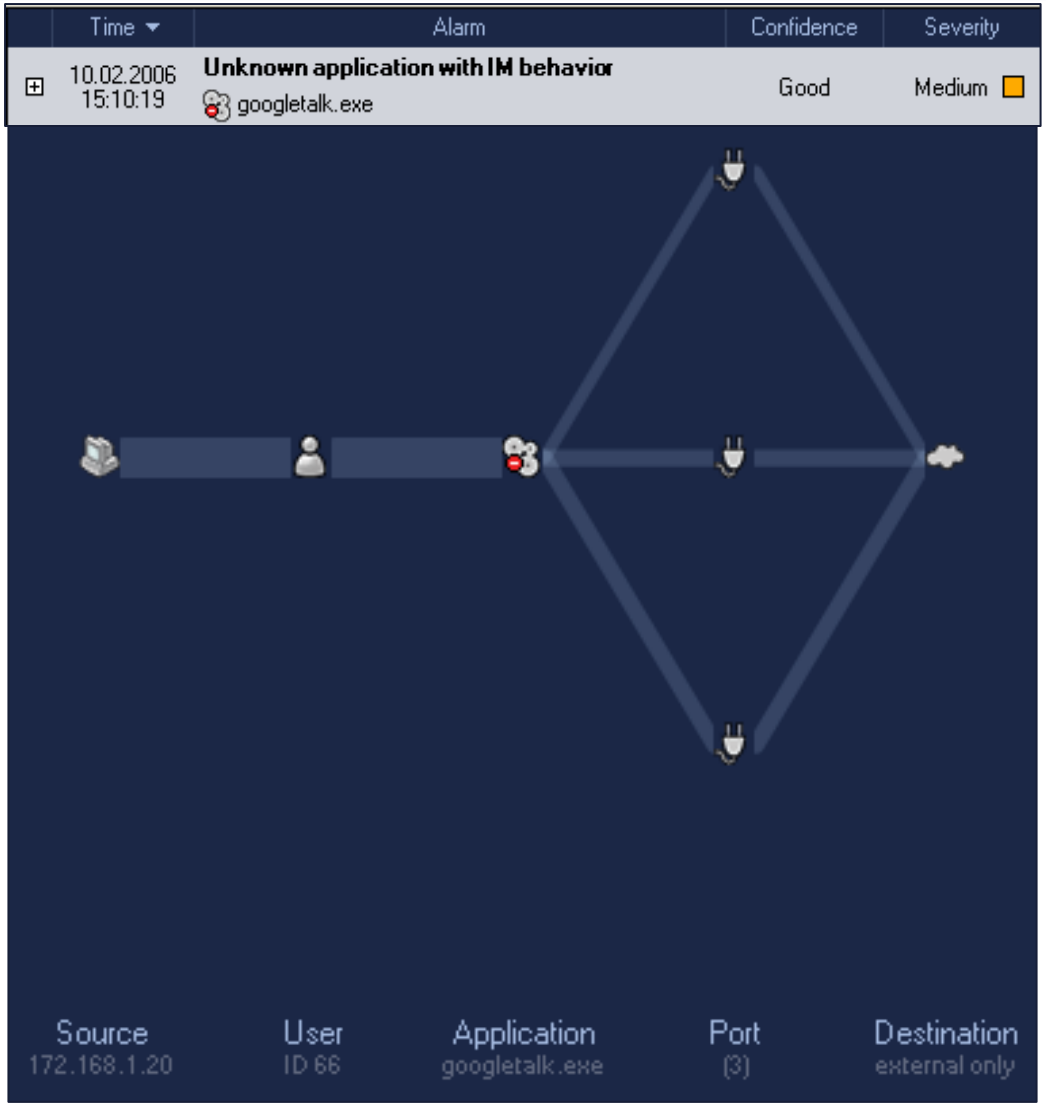
Example of behavioral vulnerabilities (port/network)

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



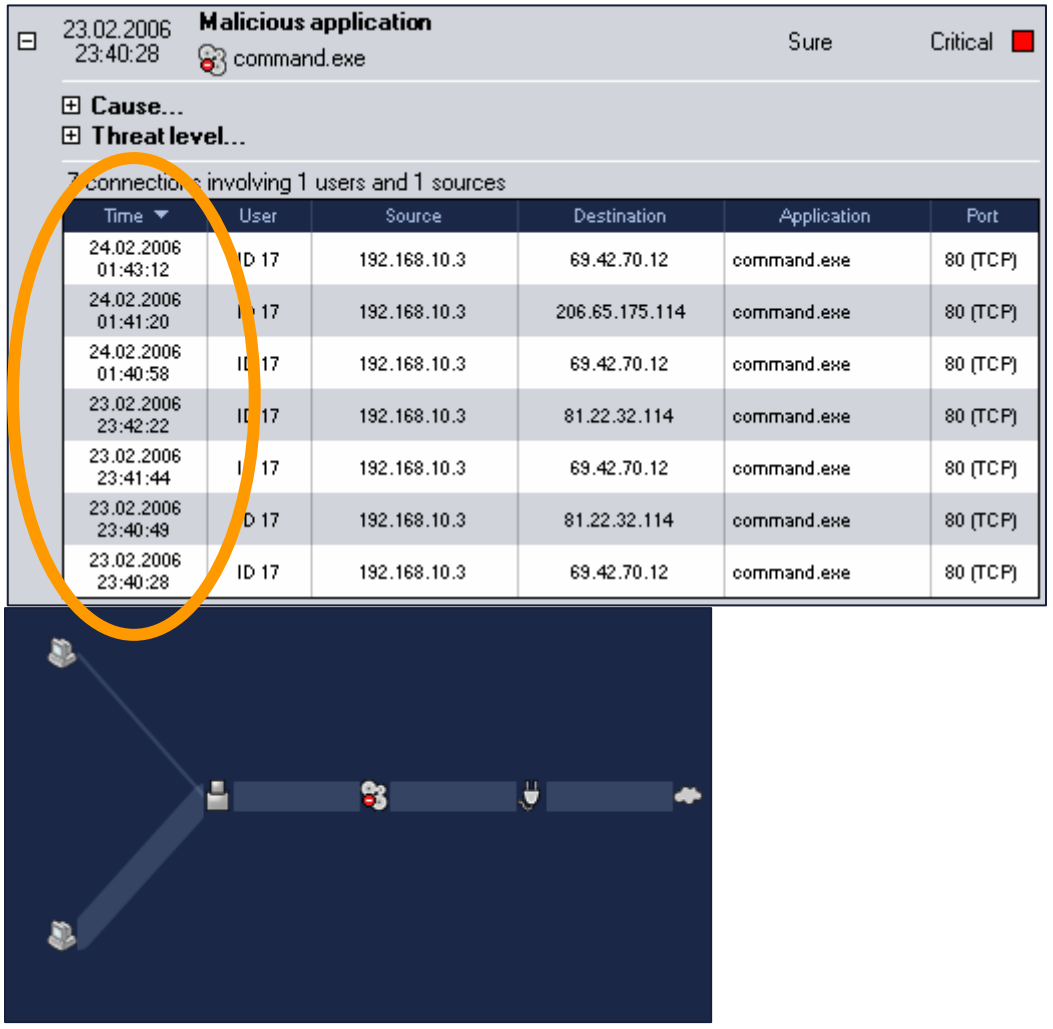
Example of behavioral vulnerabilities (application)

- Instant messaging application usage

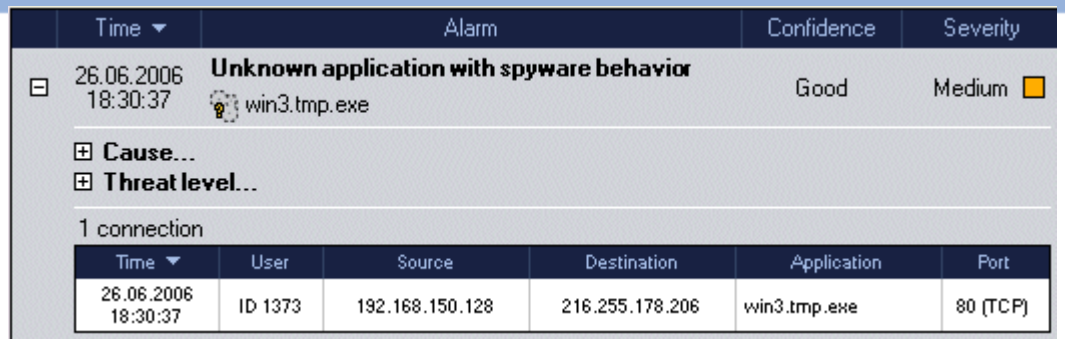


Example of behavioral vulnerabilities (malware)

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



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)

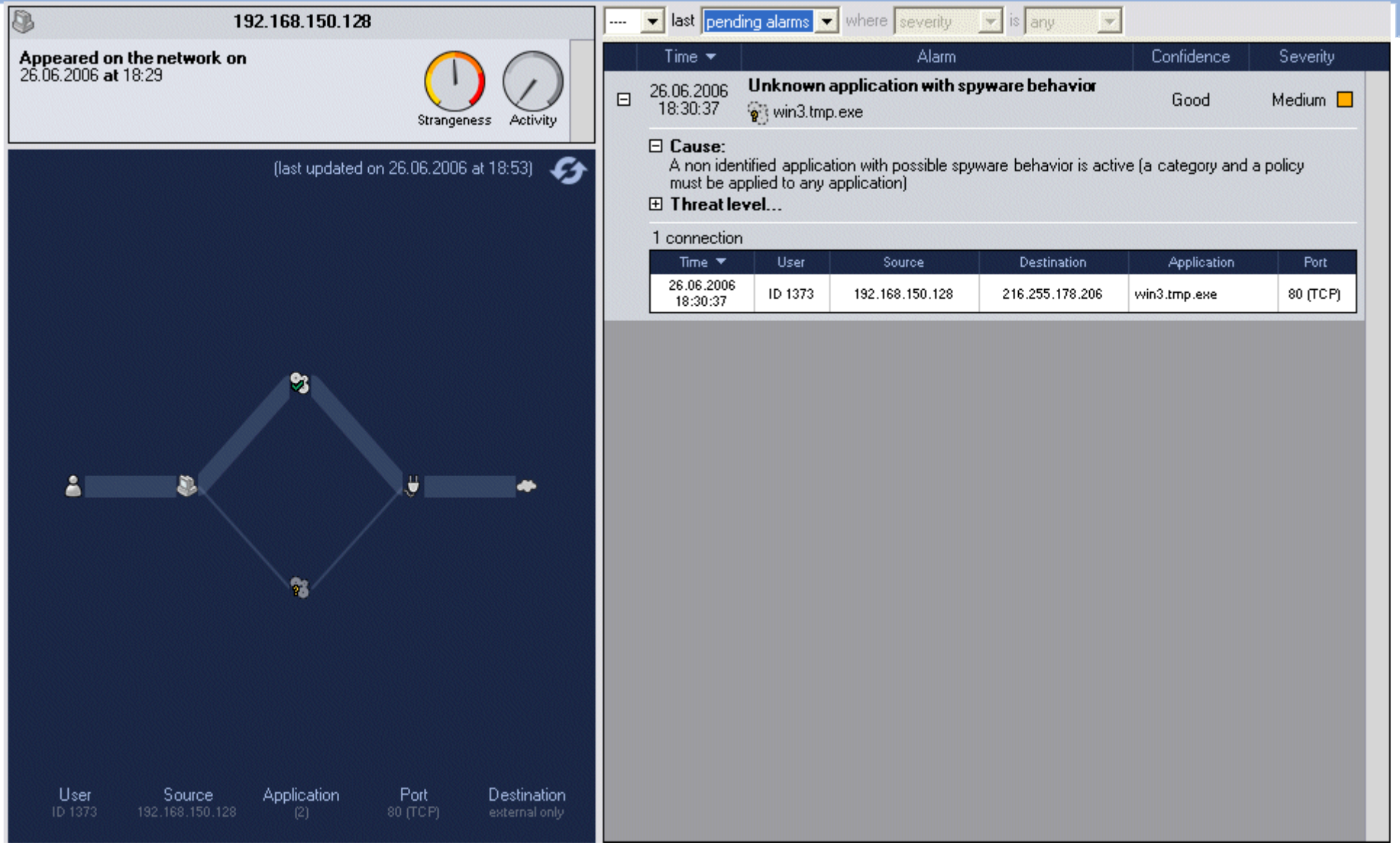
Complete scanning result of "windows_server_2003_enterprise_ed", received in VirusTotal at 06.26.2006, 12:11:47 (CET).

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.aqg
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.aqg
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

nexThink

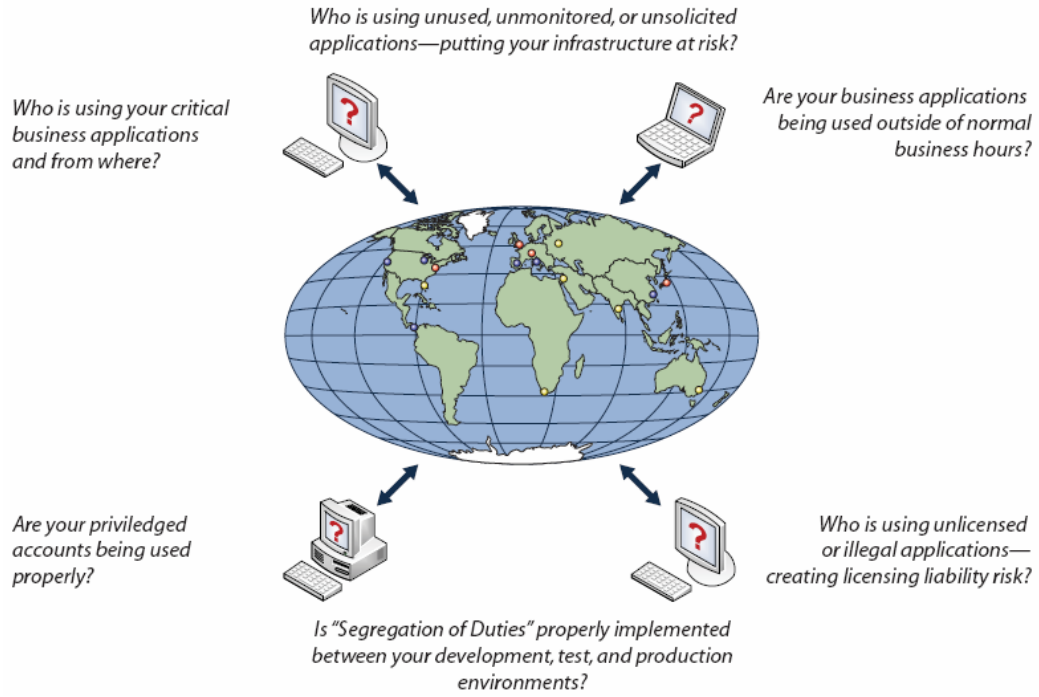
Example of behavioral vulnerabilities (unknown application) 2/2

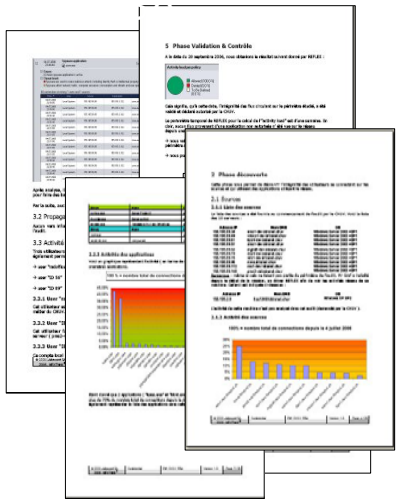


Audit EBA – Case Study

Audit EBA™ -- Endpoint Behavior Analysis

discover, evaluate and measure risk

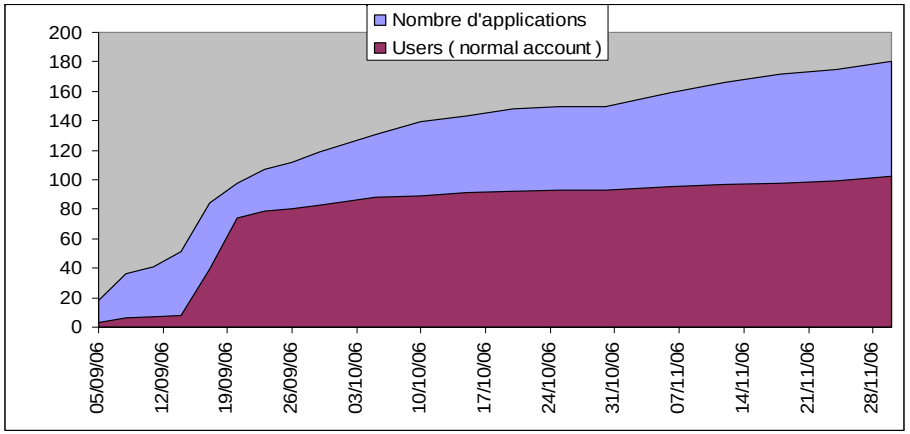


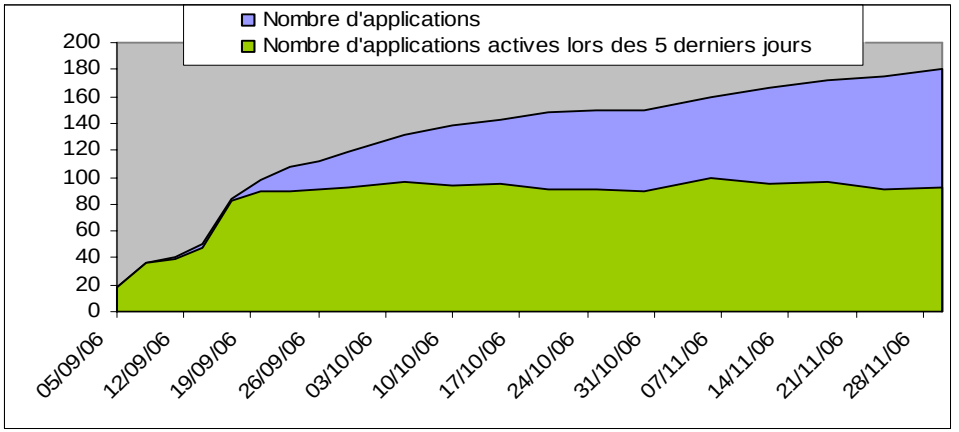


	Preparation	Installation	Self-learning phase	EBA™ service	EBA™ report
Activity	Pre-configuration questionnaire and interview	Installation of REFLEX™	REFLEX Engine self-learning phase Performance tuning	EBA™ phases 1. Discover 2. React 3. Analyze 4. Create	Report presentation

Initial inventory of activity

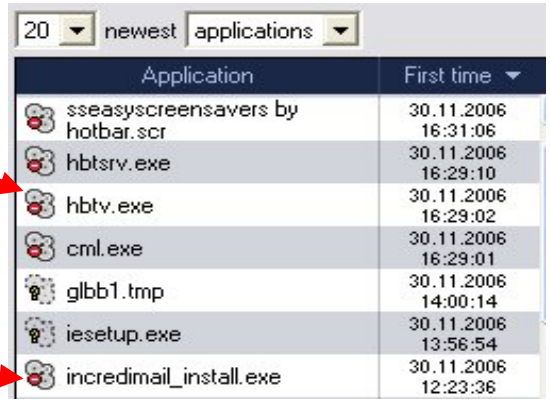
- **Installation :** **September 15th, 2006**
- **Users :** **110**
- **Applications :** **180**
- **Sources :** **160**

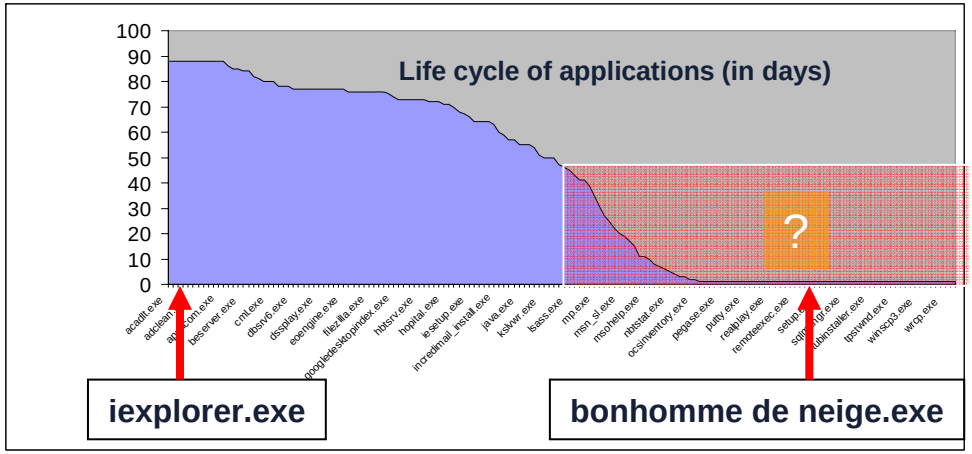




HotBar

Incredimail

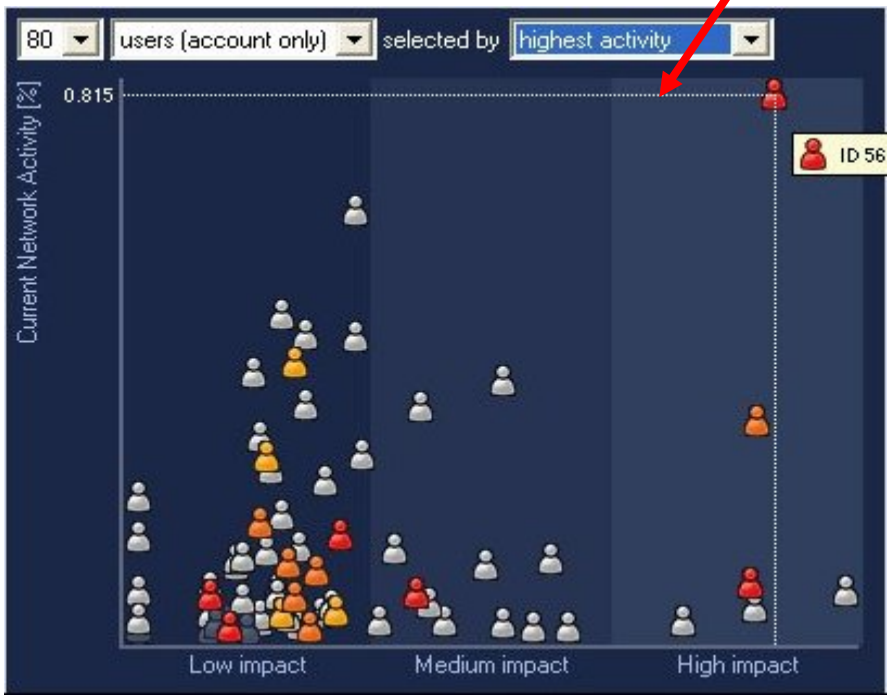




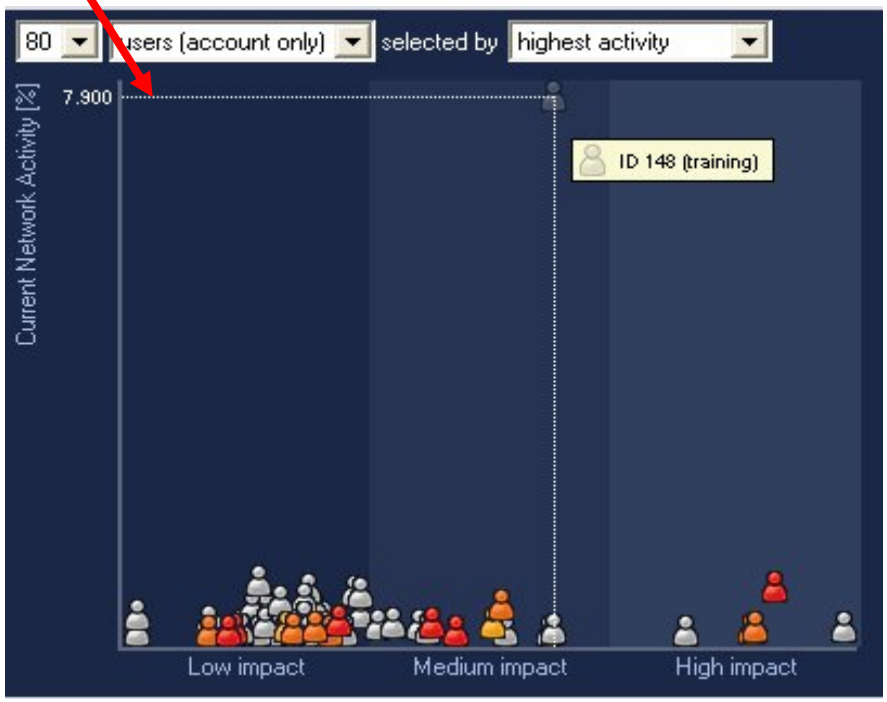
Reactivity based on intuitive visualizations

Network Activity (last 3 days)

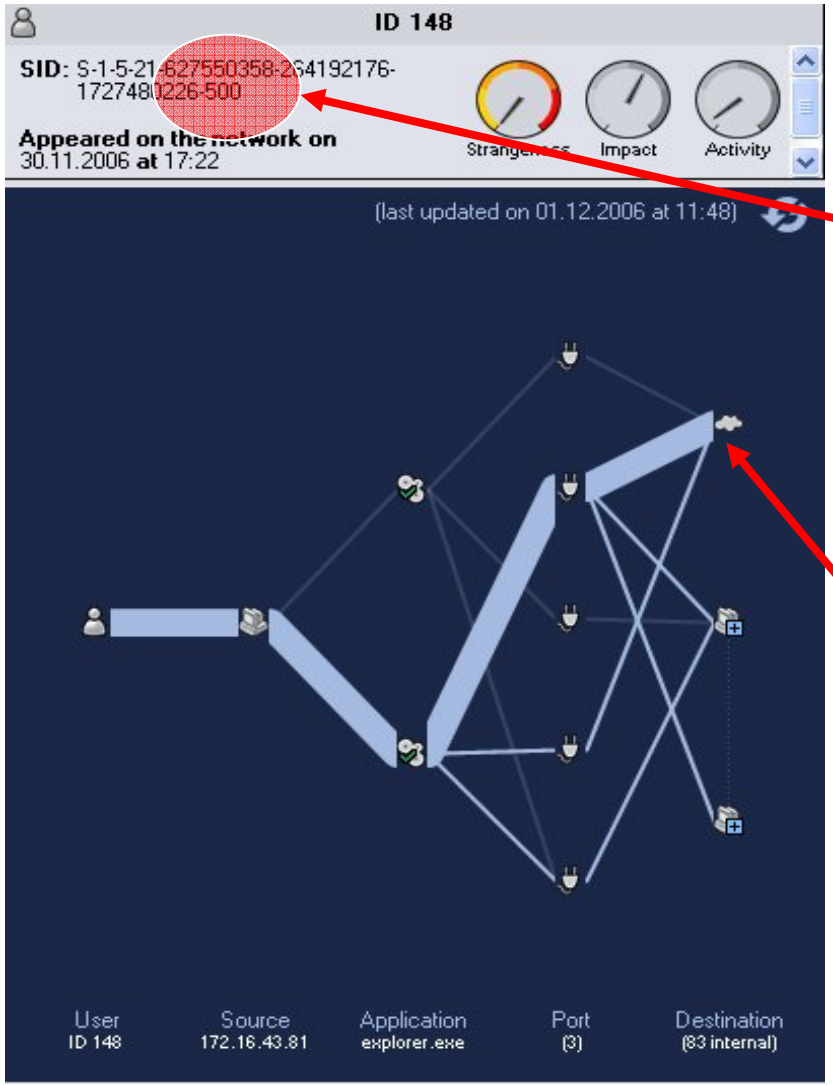
Thursday November 30th



Friday December 1st (next day)



Immediate qualification of the potential problem



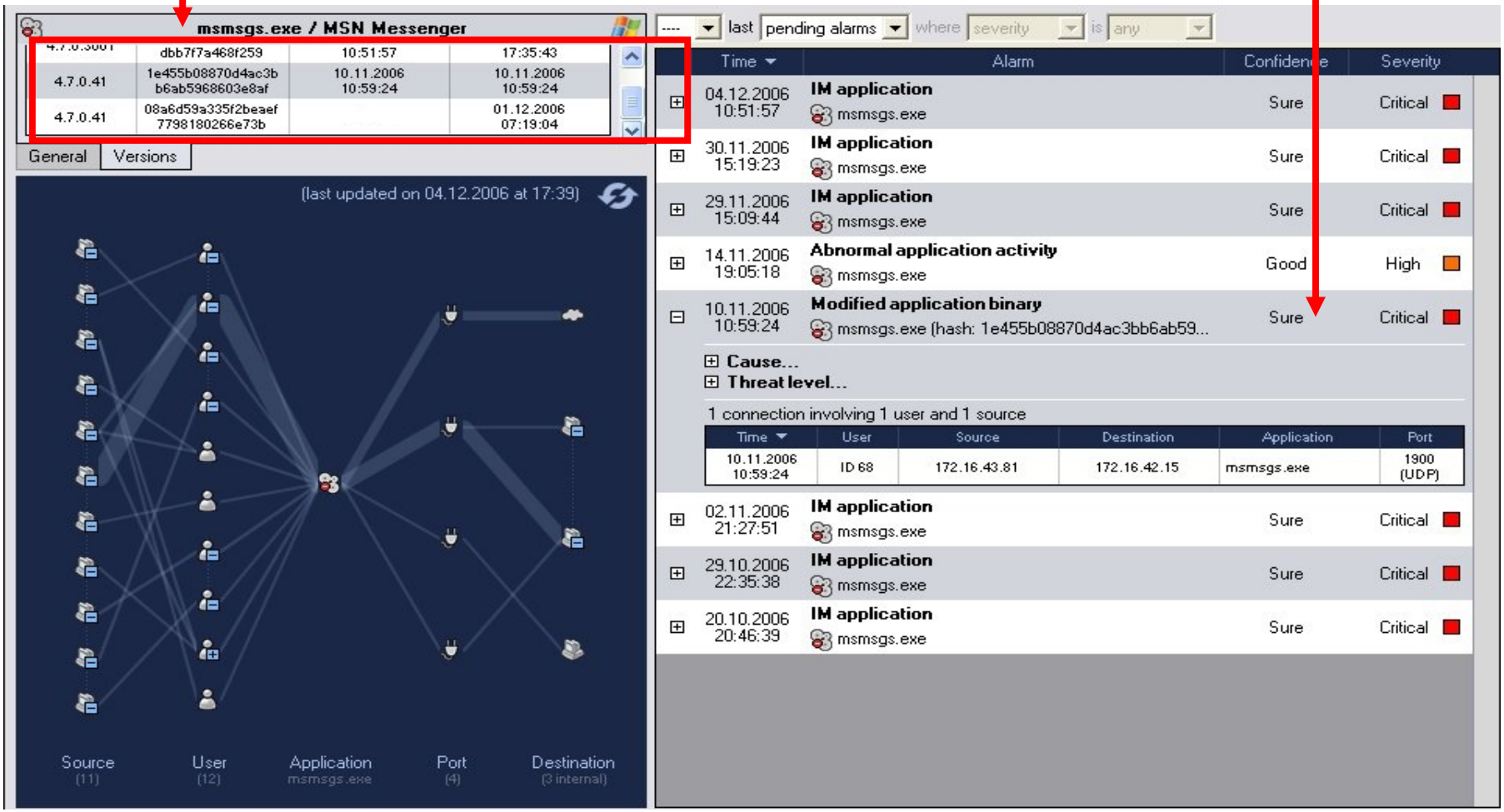
Event on Thursday Nov 30th 17:22

New Local Admin User

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

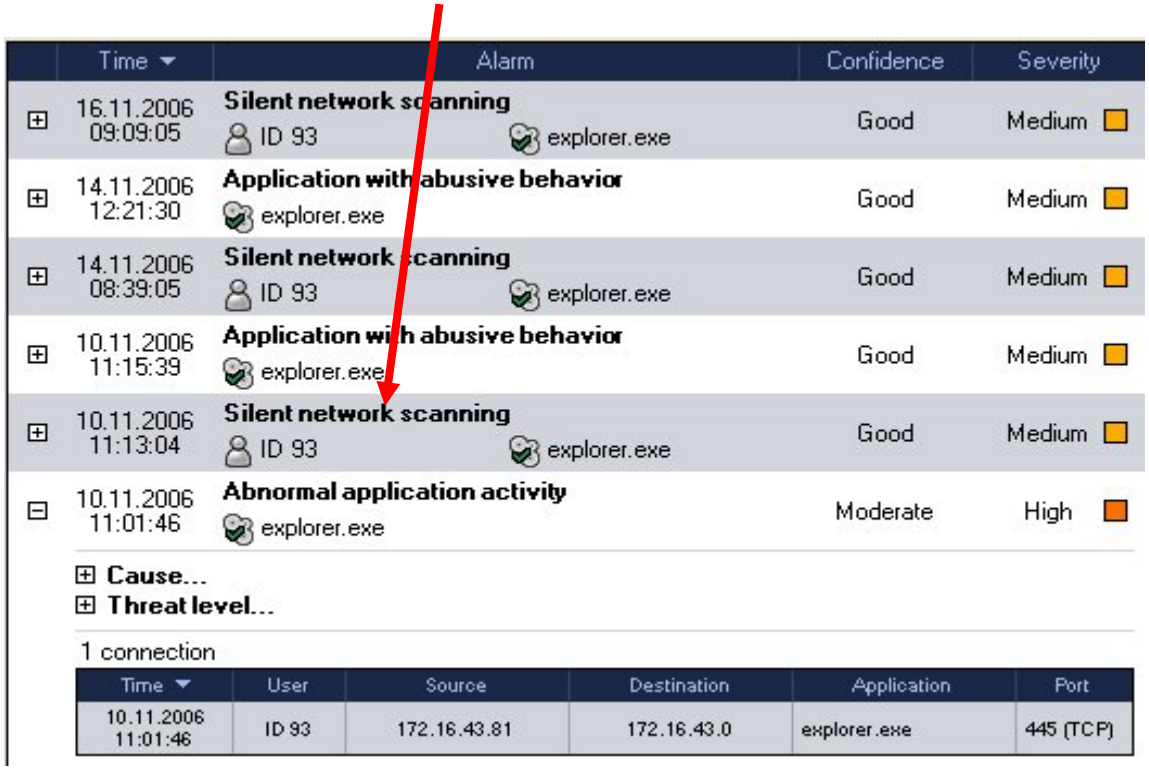
Causal analysis based on time, user, application and source

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

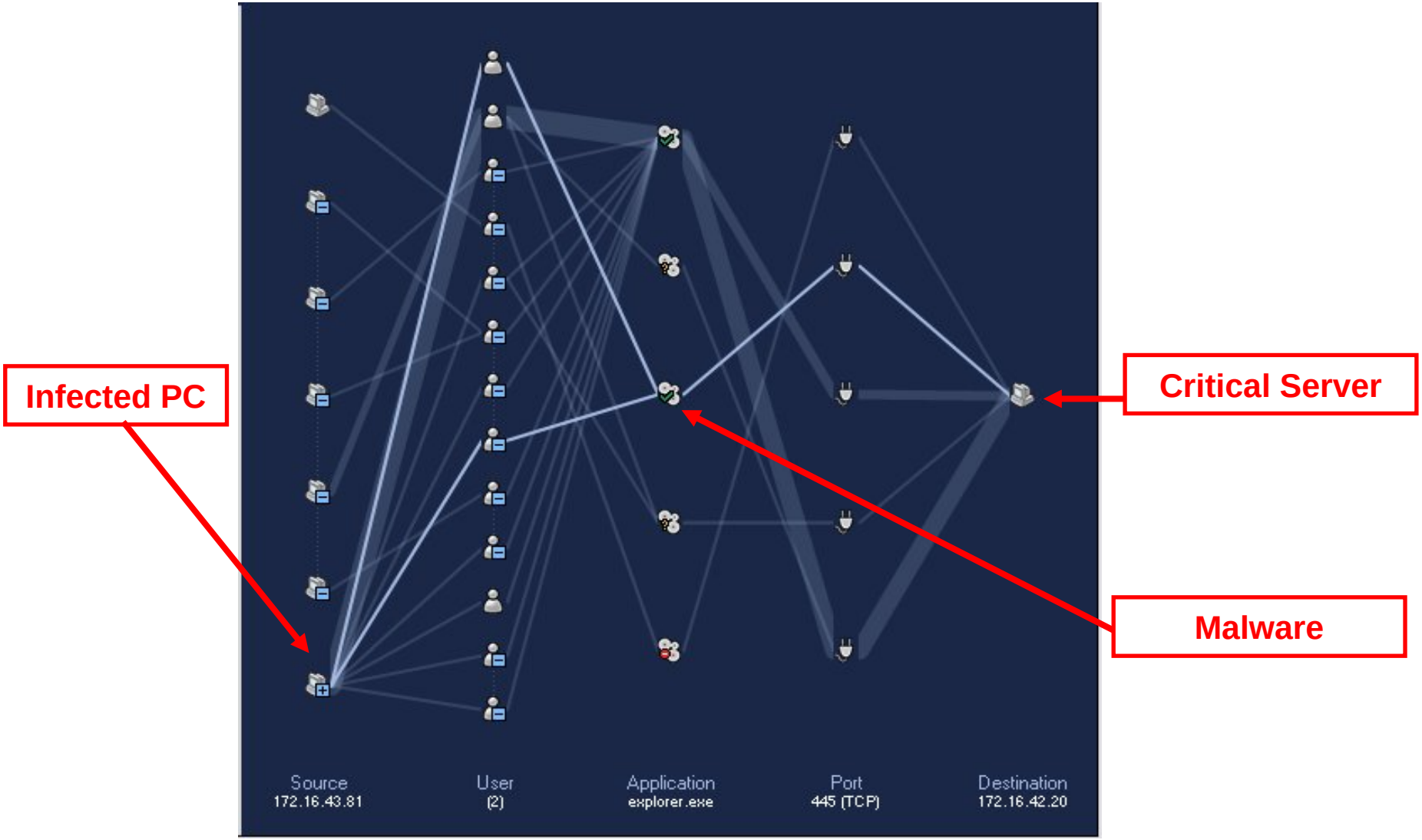


Impact alerting and full scope of the problem

- 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)

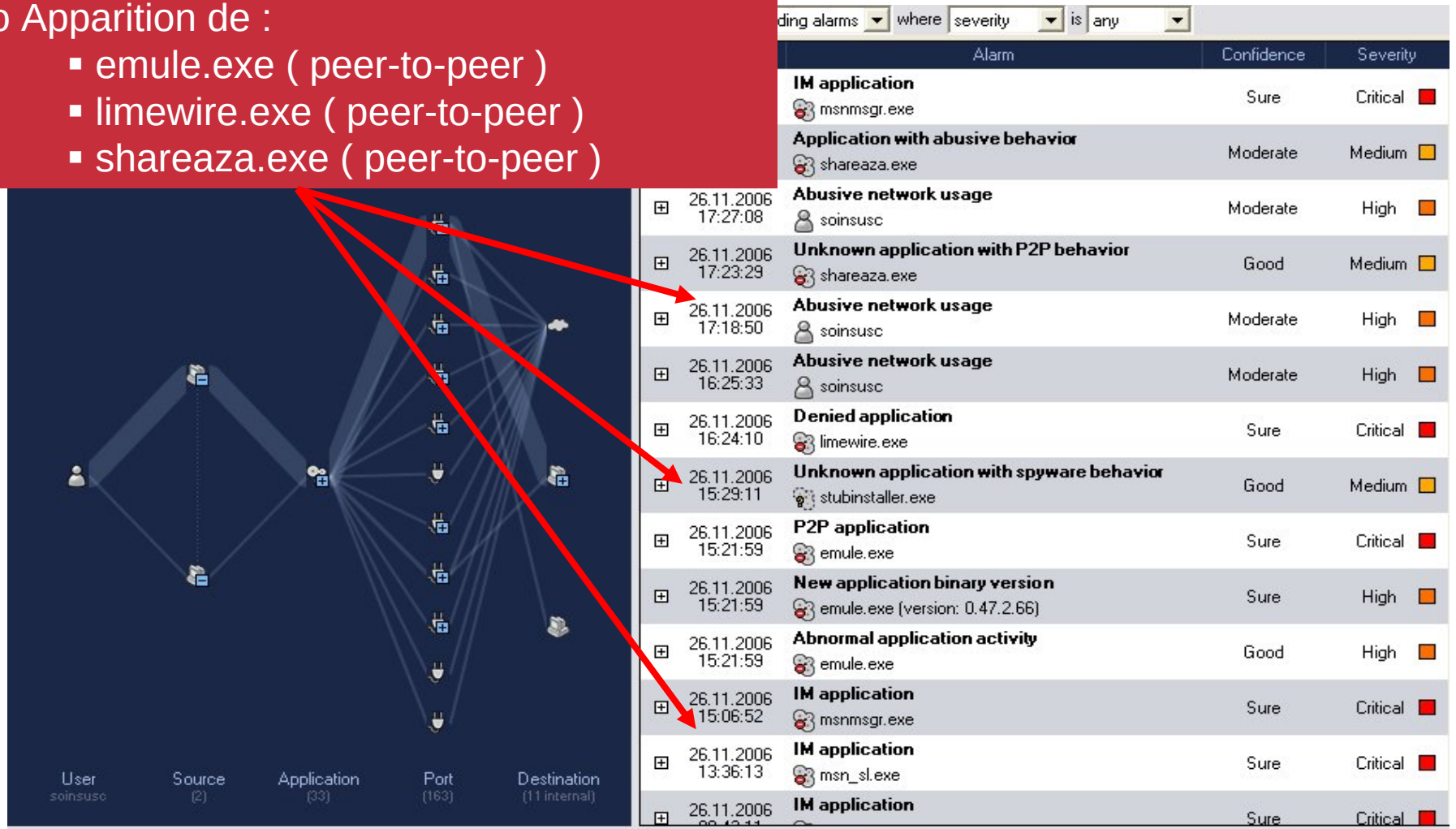


Risk analysis of a highly critical destination



Risk analysis of a shared computer

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



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®