



Software



Q-EAST SOFTWARE
Smart Systems Management

Q-East Smart Investigator

Vlad Gladin - Senior Technical Consultant - Q-East Software

Provocarile de securitate actuale

Lipsa informatiilor relevante venite la timpul oportun



Resurse putine, suprautilizate



Software



Q-EAST SOFTWARE
Smart Systems Management

Resurse putine, suprautilizate



Software



Q-EAST SOFTWARE
Smart Systems Management

Ce este?



- › Un instrument de investigatii pentru securitatea IT
- › Primul produs 100% Romanesc de securitate
- › Oferă capabilitati avansate de cautare incidente de Securitate de orice natura

Ce este ?

- › Un appliance Software-hardware ce se instaleaza langa sistemele traditionale de SIEM

SAU

- › Virtual machine appliance ce se poate deploy-a pe sistemele de vSphere sau Hyper-V

Cui se adreseaza ?

- › Departamentelor de securitate ale companiilor medii si mari
- › Investigatorilor de Securitate
- › Oferă:
 - Investigatii rapide in evenimente de securitate
 - Rapoarte de conformitate cu standarde de Securitate
 - SOX
 - ISO 27001
 - PCI-DSS

Facilitati

› Raportare

- Rapoarte pentru standard de Securitate
- COBIT, FISMA, HIPPA, ISO 27001, PCP/DSS, SOX
- Report pack-uri pe tehnologii (Windows, Unix)

› Dashboard-uri interactive, contextuale

- Generale
- Active Directory
- Active Directory

Facilitati

› Investigatii avansate

- Filtre predefinite (din rapoarte)
- Seturi de obiecte dinamice

› Event browser avansat

› Tehnologie de detectie anomalii

- Detectie automata de evenimente suspicioase de logon
 - La nivel de zi
 - La nivel de saptamna
 - La nivel de luna



Software



Q-EAST SOFTWARE
Smart Systems Management

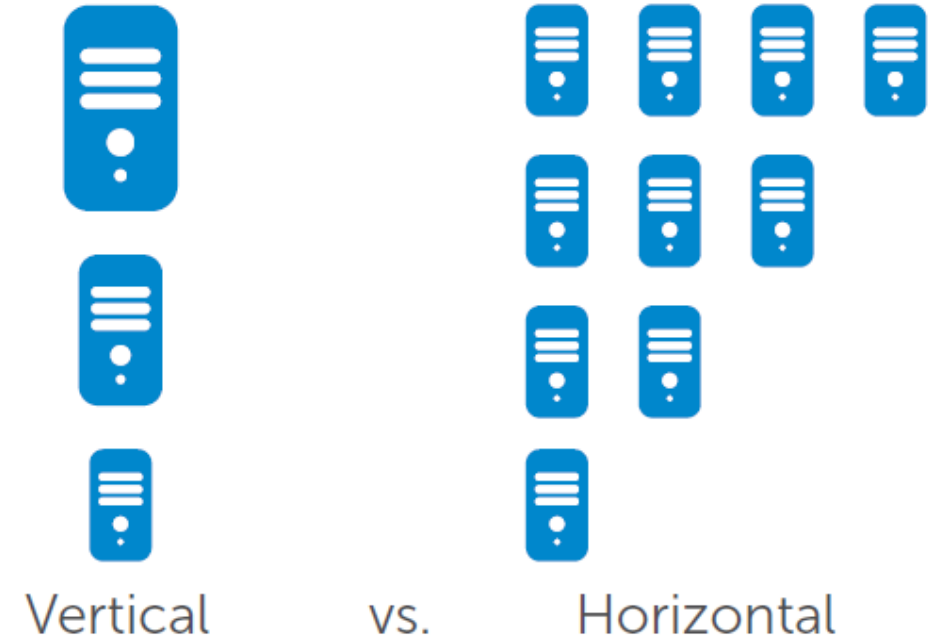
Beneficii

- Rapiditate pentru cautari
 - Timp de raspuns la query-uri extrem de mic
- Normalizare pentru toate solutiile
- MultiSolution
- Investigatii IT corelate cu sistem de detective anomalii
- Multi-SIEM
 - Suporta Alienvault, Dell Intrust , Arcsight
- Integreaza securitatea fizica cu securitatea IT

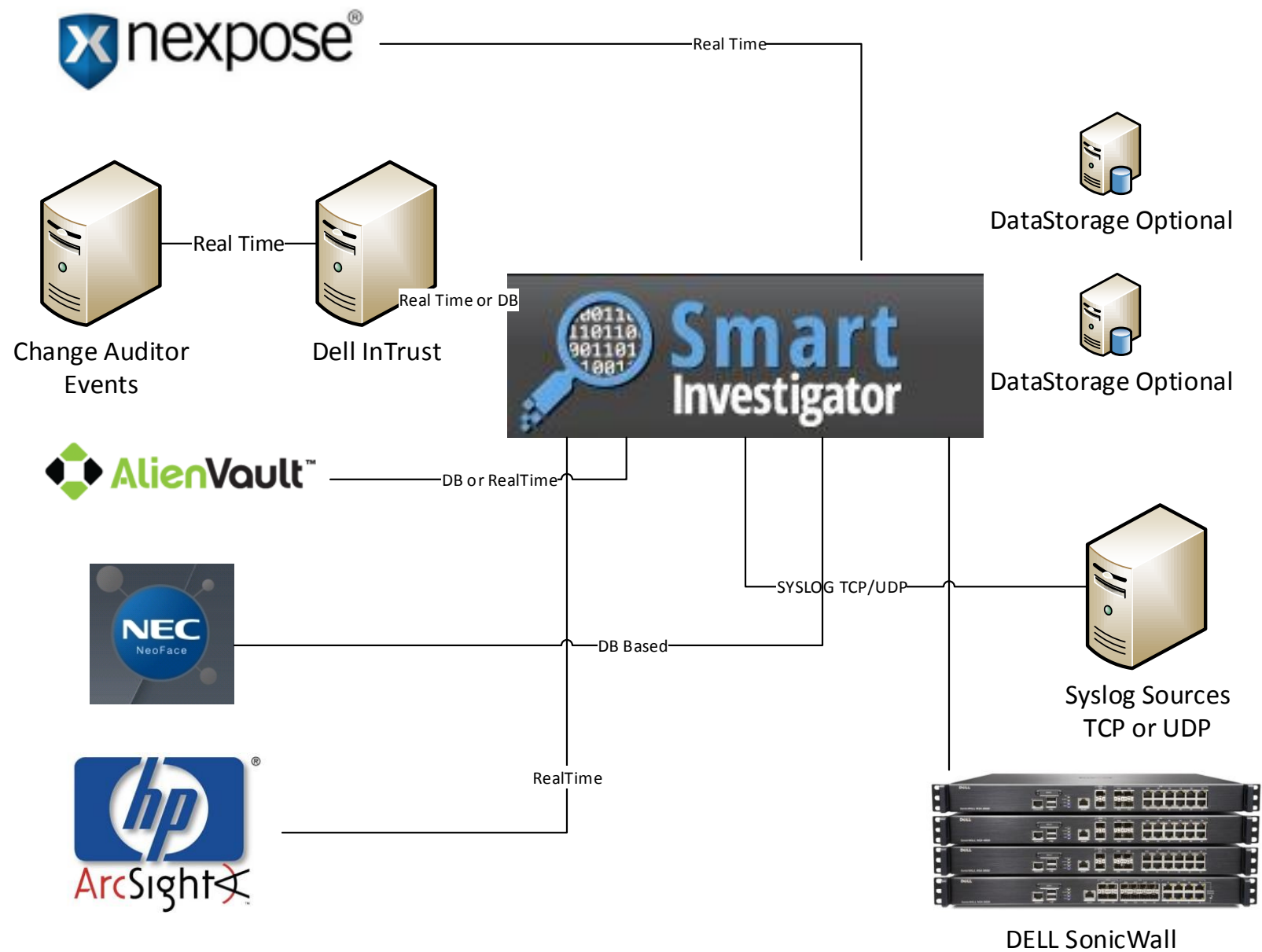
Cum ?

› Tehnologie revolutionara:

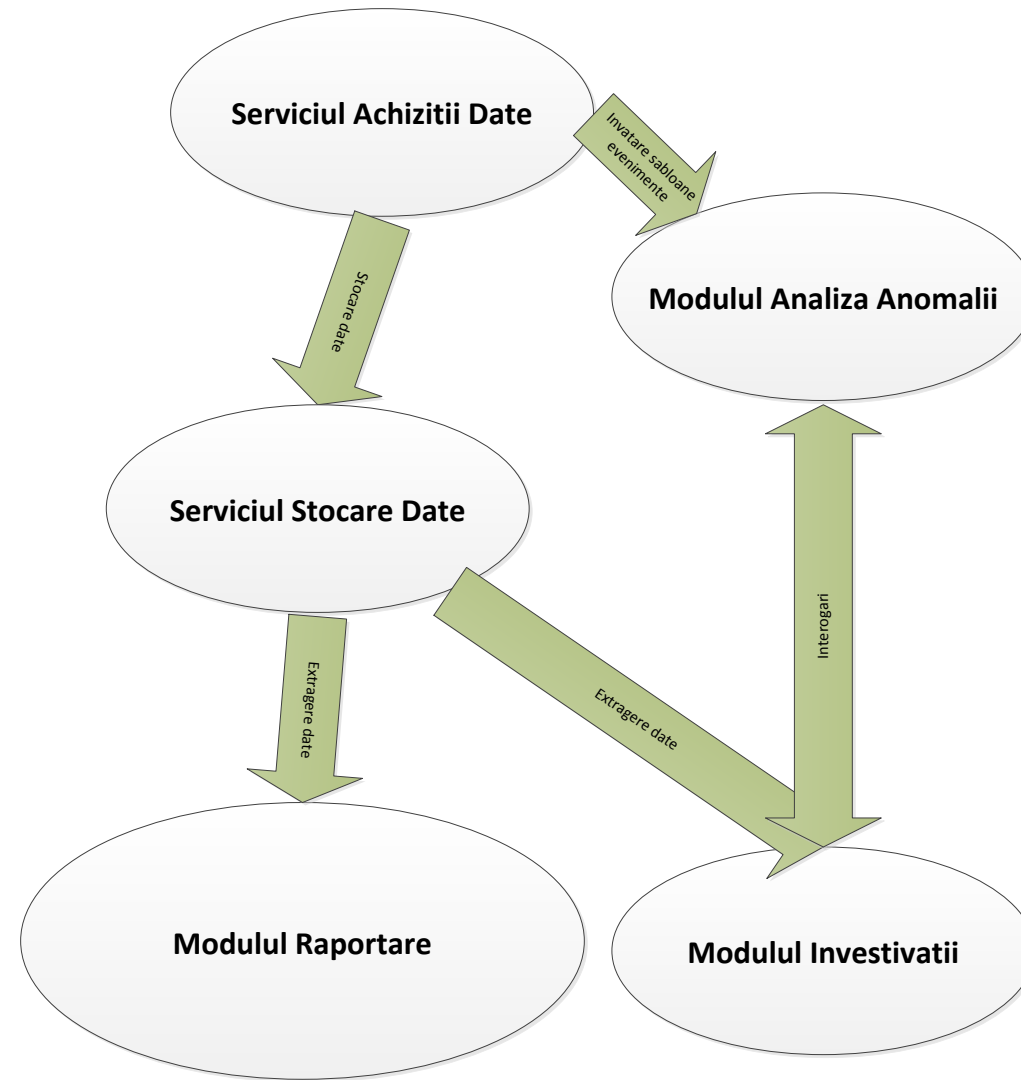
- NoSQL Database Storage
- Timp de raspuns minim (in general sub 5 secunde pe orice query)
- Scalabilitate orizontala nelimitata built-in fara costuri suplimentare pentru baze de date
- Detectie de evenimente anormale (Logon-uri, acces la resurse)
- Autotraining pe modulul de detectie anomalii
- Appliance software/hardware



Surse de date



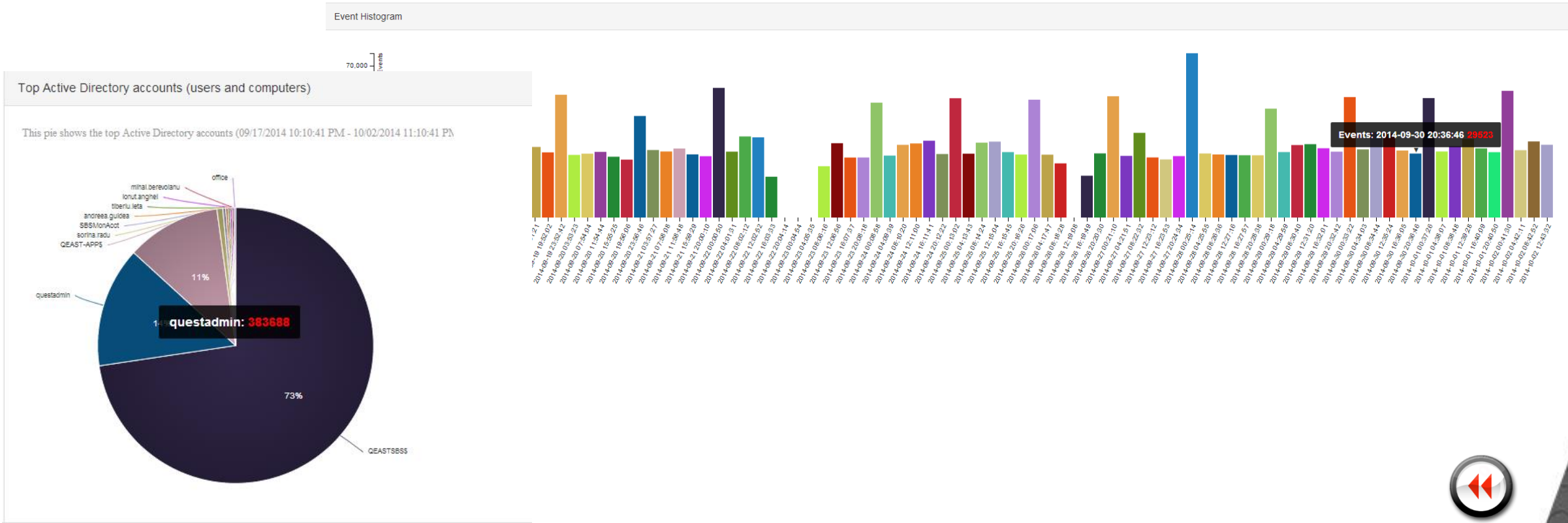
Arhitectura interna - Schema generala



Q-East Smart Investigator



Dashboard-uri Q-East SmartInvestigator



Modul Investigatii

4624 | An account was successfully logged on 15 properties

An account was successfully logged on.

More

An account was successfully logged on.

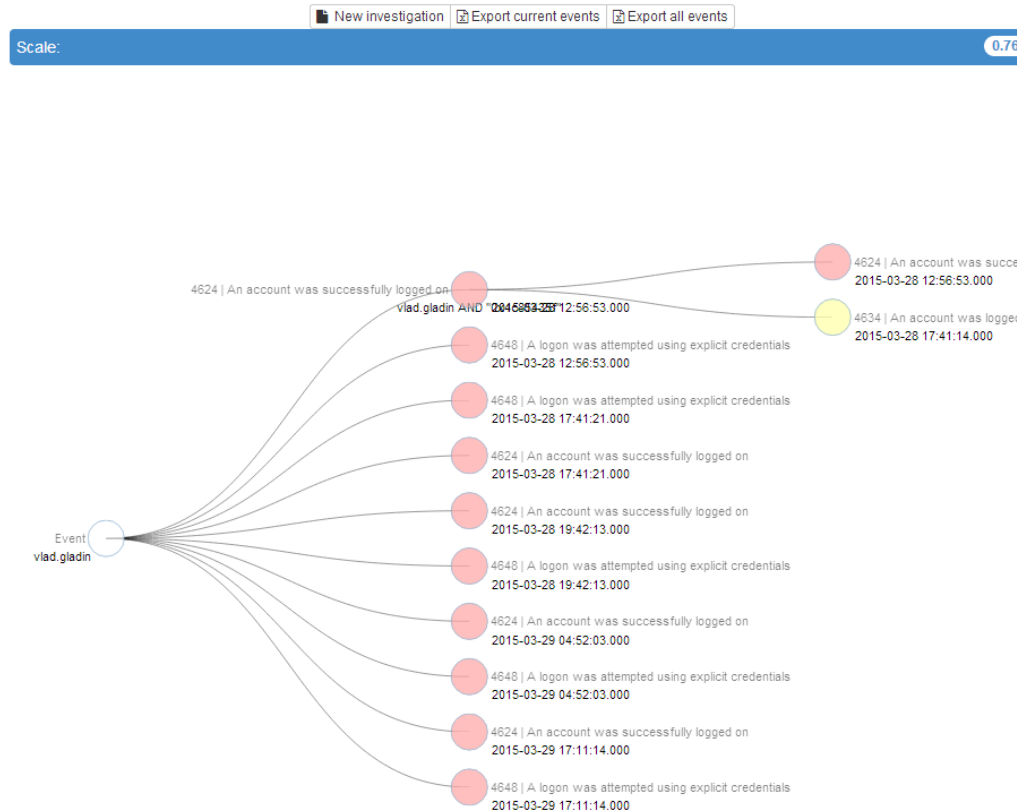
Subject

Investigations Security ID : NT AUTHORITY\SYSTEM
 Investigations Account Name : QEASTSBS\$
 Investigations Account Domain : Q-EAST
 Investigations Logon ID : 0x3e7
 Investigations Logon Type : 8

New Logon

Investigations Security ID : Q-EAST\vlad.gladin
 Investigations Account Name : vlad.gladin
 Investigations Account Domain : Q-EAST
 Investigations Logon ID : 0x4c85435f

IP	192.168.122.5
IP	213.233.85.101
Computer	QEASTSBS.q-east.local
UserName	QEASTSBS\$
UserDomain	Q-EAST
EventType	Success audit
Source	Microsoft-Windows-Security...
EventID	4624
Category	Logon
LocalTime	2015-03-28 12:56:53.000
EventLog	Security
PlatformID	500



Current data: Items: 2 Total Hits: 2 Page: 1 of 1

Top Event Categories

Pie

Top Event Categories

This chart shows top event categories (2015-03-28 06:07:49 - 2015-03-31 07:0)

#	Category
1	Logoff
2	Logon

Send to browser
 Send to investigations
 Show only this data
 Filter this data

← Older Newer →

4624 An account was successfully logged on	2015-03-28 12:56:53.000
4634 An account was logged off	2015-03-28 17:41:14.000

Investigatii in mod grafic pas cu pas (din nod in nod)

An account was successfully logged on. 15 properties

More

An account was successfully logged on.

Subject

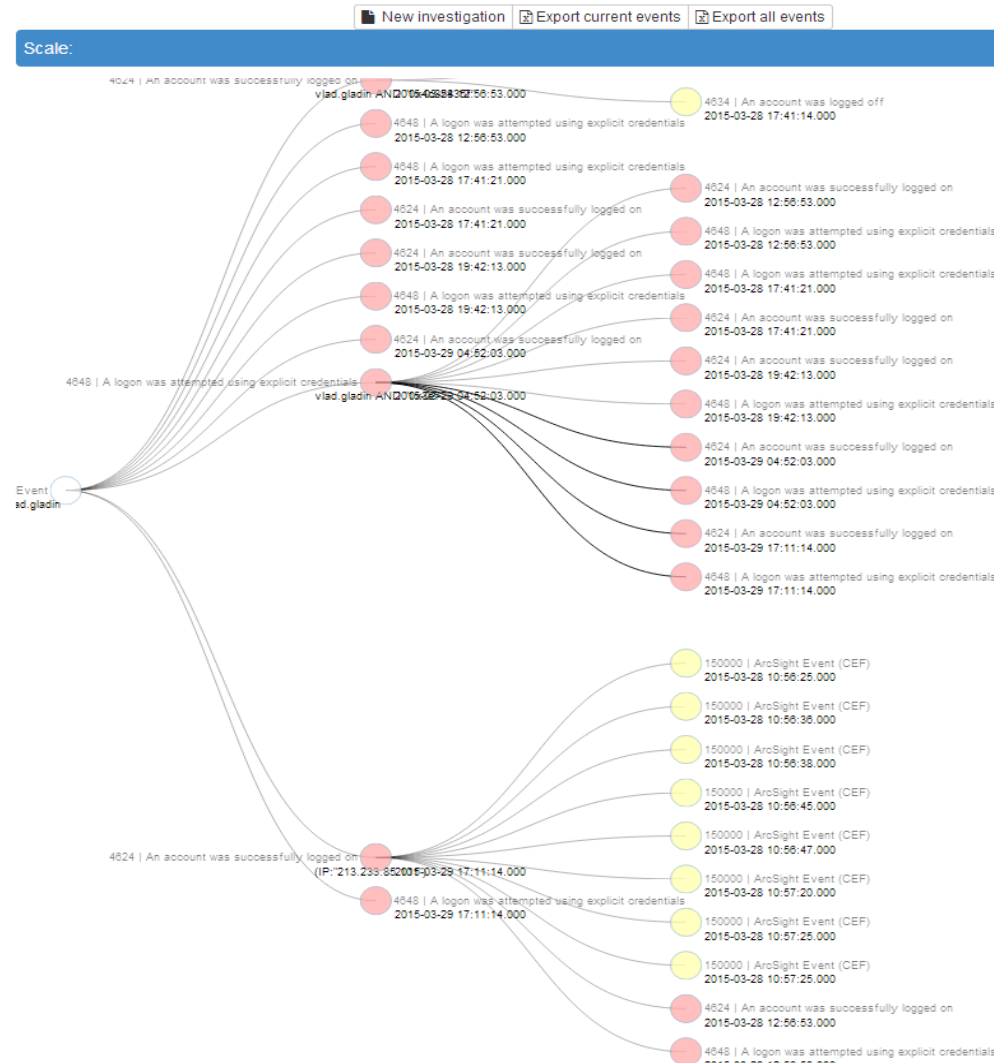
investigations Security ID : NT AUTHORITY\SYSTEM
 investigations Account Name : QEASTSBSS\$
 investigations Account Domain : Q-EAST
 investigations Logon ID : 0x3e7

investigations Logon Type : 8

New Logon

investigations Security ID : Q-EAST\vlad.gladin
 investigations Account Name : vlad.gladin
 investigations Account Domain : Q-EAST
 investigations Logon ID : 0x4c85435f

	IP	192.168.122.5
	IP	213.233.85.101
	Computer	QEASTSBS.q-east.local
	UserName	QEASTSBSS\$
	UserDomain	Q-EAST
	EventType	Success audit
	Source	Microsoft-Windows-Security...
	EventID	4624
	Category	Login
	LocalTime	2015-03-28 12:56:53.000
	EventLog	Security
	PlatformID	500



Current data:

Items: 10

Total Hits: 20

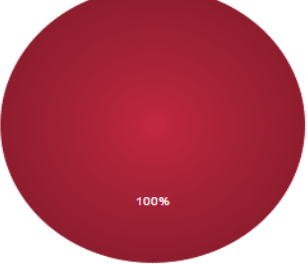
Page: 1 of 3

Top Event Sources

Pie

Top Event Sources

This chart top event sources (2015-03-28 06:07:49 - 2015-03-31 07:07:49)



100%

Microsoft-Windows-Security-Auditing

Source

1 [Microsoft-Windows-Security-Auditing](#)

Send to browser

Send to investigations

Show only this data

Filter this data

← Older

NEWER →

4624 An account was successfully logged on	2015-03-28 12:56:53.000
4648 A logon was attempted using explicit credentials	2015-03-28 12:56:53.000
4648 A logon was attempted using explicit credentials	2015-03-28 17:41:21.000

Filtre inteligente simple sau/si compuse

Filter data

Filter data

Items per page

10 items per page

Start Date

2014-12-05 09:05

1m 5m 30m

1h 5h 24h

1m 5m 30m

1h 5h 24h

Additional filters

Nothing selected

AIX File Permission Changes

NTFS audit [Windows XP 2003 and later]

Recent share operations

AIX Reboots

Server Reboots

Software Installation

Database structure modification activity

Database structure modifications

Raw data analysis

Shadow copy modifications

User Activity Research

Audit Policy Changed

Kerberos and Domain Policy changed

System Time changed

Active Directory security subsystem faults

Event Log Errors

Logon Components Failures

Content Activity Research

File Access

Multiple Logon Failures

Multiple logons failure [Windows-Kerberos-NTLM]

HP-UX Group management

Close **Get data**

Current data: Items: 0 Total Hits: 1825 Page: 1 of 184

Top Event Types

Doughnut

Top Event Types

This shows chart top event types (2014-12-05 09:05:46 - 2014-12-08 09:05:46)

97%

#	EventType	Events
1	8	1,777
2	16	48

export current

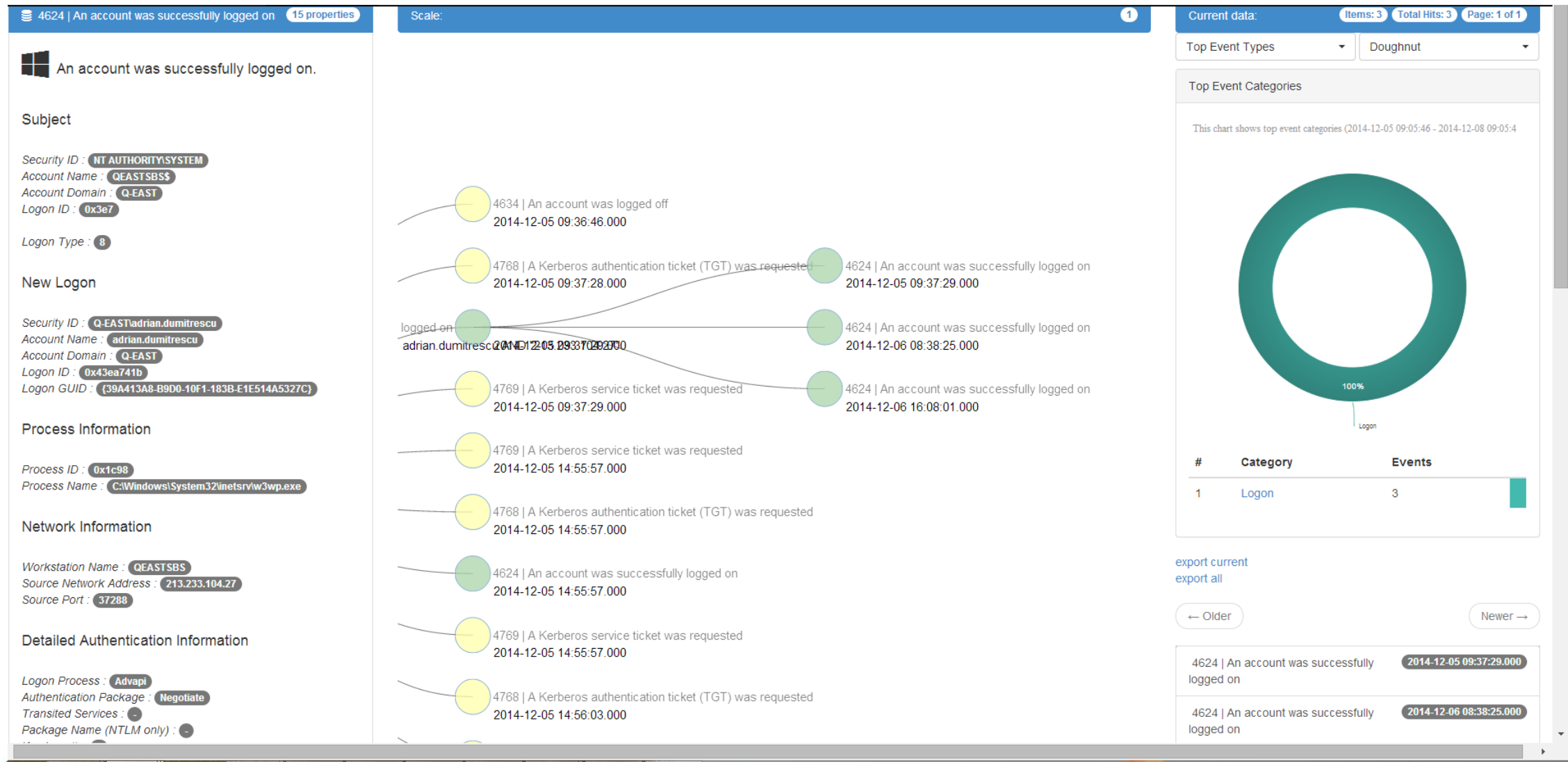
export all

Older **Newer**

4634 | An account was logged off 2014-12-05 09:36:46.000

4768 | A Kerberos authentication ticket 2014-12-05 09:37:28.000

Filtre inteligente simple sau/si compuse



Software



Q-EAST SOFTWARE
Smart Systems Management

Event Browser; filtre simple sau si/compose

➤ Search as string: “vlad.gladin”

➤ Search with column filter
(“UserName:”vlad.gladin”)

➤ Multiple conditions:

(UserName:"vlad.gladin") AND
(IP:"192.168.122.55")

The screenshot displays the Event Browser interface with the following components:

- Time Range:** Last Hour, Last day, Last 3 days, Last 10 days, Last 30 days, Last 90 days.
- Filter data:** Items per page (10 items per page).
- Search:** Nexpose AND (IP:"192.168.115.101")
- Additional filters:** Nothing selected
- Combining method:** Nothing selected
- Filter data:** Filter data, Send to investigations
- Fields:** 5 Selected
 - Category
 - Computer
 - Description
 - DestIP
 - DestMAC
 - _id
 - EventID
 - EventLog
 - EventType
 - GMT
 - ID
 - LocalTime
 - PlatformID
 - SessionID
 - Source
 - SrcIP
 - SrcMAC
- Start Date:** 2015-03-22 13:11:49
- End Date:** 2015-03-27 16:00:49
- Total results:** 14
- Showing page:** 1 of 2 (10 results per page)
- Table:**

LocalTime	Computer	Description	EventLog	Category
2015-03-27 11:53:08.000	192.168.115.101	<114>Mar 27 11:47:57 192.168.115.101 Nexpose: VULNERABILITY: Click Jacking (http-generic-click-jacking)	syslog	log alert
2015-03-27 11:45:09.000	192.168.115.101	<114>Mar 27 11:39:57 192.168.115.101 Nexpose: VULNERABILITY: Click Jacking (http-generic-click-jacking)	syslog	log alert
2015-03-27 11:45:09.000	192.168.115.101	<114>Mar 27 11:39:57 192.168.115.101 Nexpose: VULNERABILITY: Click Jacking (http-generic-click-jacking)	syslog	log alert
2015-03-27 11:45:09.000	192.168.115.101	<114>Mar 27 11:39:57 192.168.115.101 Nexpose: VULNERABILITY: Click Jacking (http-generic-click-jacking)	syslog	log alert
2015-03-27 11:45:09.000	192.168.115.101	<114>Mar 27 11:39:57 192.168.115.101 Nexpose: VULNERABILITY: Click Jacking (http-generic-click-jacking)	syslog	log alert
2015-03-27 11:45:09.000	192.168.115.101	<114>Mar 27 11:39:57 192.168.115.101 Nexpose: VULNERABILITY: Click Jacking (http-generic-click-jacking)	syslog	log alert
2015-03-27 11:45:08.000	192.168.115.101	<114>Mar 27 11:39:56 192.168.115.101 Nexpose: VULNERABILITY: Click Jacking (http-generic-click-jacking)	syslog	log alert
2015-03-27	192.168.115.101	<116>Mar 27 11:39:03 192.168.115.101 Nexpose: VULNERABILITY: ICMP timestamp response (generic-icmp-timestamp)	syslog	log alert

Modul raportare. Rapoarte bazate pe standard si tehnologii

Reports

- Reports
 - Compliance
 - COBIT
 - FISMA
 - HIPAA
 - ISO 27001
 - PCI
 - SOX
 - Sec. 302 Corporate Responsibility for Financial Reports
 - Sec. 404 Management Assessment of Internal Controls
 - Sec. 802 Criminal Penalties for Altering Documents
 - 1519 Destruction of records in Federal Investigations
 - Databases
 - IIS
 - Solaris
 - Windows
 - Windows Content Activity Research
 - Windows File Access
 - Windows NTFS audit [Windows XP 2003 and later]
 - Windows User Activity Research
 - Windows
 - SUSE-Linux
 - RedHat-Linux
 - ADX
 - HP-UX
 - Syslog
 - Oracle
 - SQL Server
 - IIS

Schedules

Report Parameters

Compliance \ SOX \ Sec. 802 Criminal Penalties for Altering Documents \ 1519 Destruction of records in Federal Investigations \ Windows \ Windows User Activity Research

User Activity Research

1255

Items per page

100 items per page

Filter data

vlad.gladin

Start Date

2015-03-01 06:35:15

End Date

2015-03-31 07:35:15

Fields

Category, Computer, Descr

Execute Report

Export to CSV

Export to PDF

Windows User Activity Research

« 1 »

Windows User Activity Research

Total results: 25

Showing page: 1 of 1 (100 results per page)

LocalTime	Computer	Description	EventLog	Category	DestIP	UserName
2015-03-30 13:42:22.000	QEASTSBS.q-east.local	File read: More	Quest File Access Audit	Remote Access		vlad.gladin
2015-03-30 13:42:22.000	QEASTSBS.q-east.local	File read: More	Quest File Access Audit	Remote Access		vlad.gladin
2015-03-30 13:42:22.000	QEASTSBS.q-east.local	File read: More	Quest File Access Audit	Remote Access		vlad.gladin

 Software

 **Q-EAST SOFTWARE**
Smart Systems Management

21

Viziunea Q-East Software

abordare holista a provocarilor de securitate

Detectie si protectie (networking)	Dell SonicWall	NextGen Firewall, Inspectie Malware, Antivirus de gateway, IDS/IPS
Detectie si protectie (layer 7)	Dell Intrust, Change Auditor for AD, Exchange, File Servers, VMWare	Ofera protectii la nivel de aplicatii, sisteme de operare
Colectare si stocare evenimente de audit	Dell Intrust, ArcSight, AlienVault	Colecteaza si stocheaza toate evenimentele de log generate de politicile interne de securitate
Detectie si validare de vulnerabilitati	Rapid 7 Nexpose si MetaSploit	Detecteaza vulnerabilitatile din sisteme de operare/aplicatii etc si ofera validarea acestora
Analiza si investigatii	Q-East SmartInvestigator	Culege toate informatiile pentru o vedere de ansamblu



Software



Q-EAST SOFTWARE
Smart Systems Management



Software



Q-EAST SOFTWARE
Smart Systems Management

Multumesc!

Vlad Gladin

Vlad.Gladin@QEast.ro



Software



Q-EAST SOFTWARE
Smart Systems Management