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

Ce este?

- Un instrument de investigatii pentru securitatea IT
- Primul produs 100% Romanesc de securitate
- Ofera 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
- Ofera:
  - 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

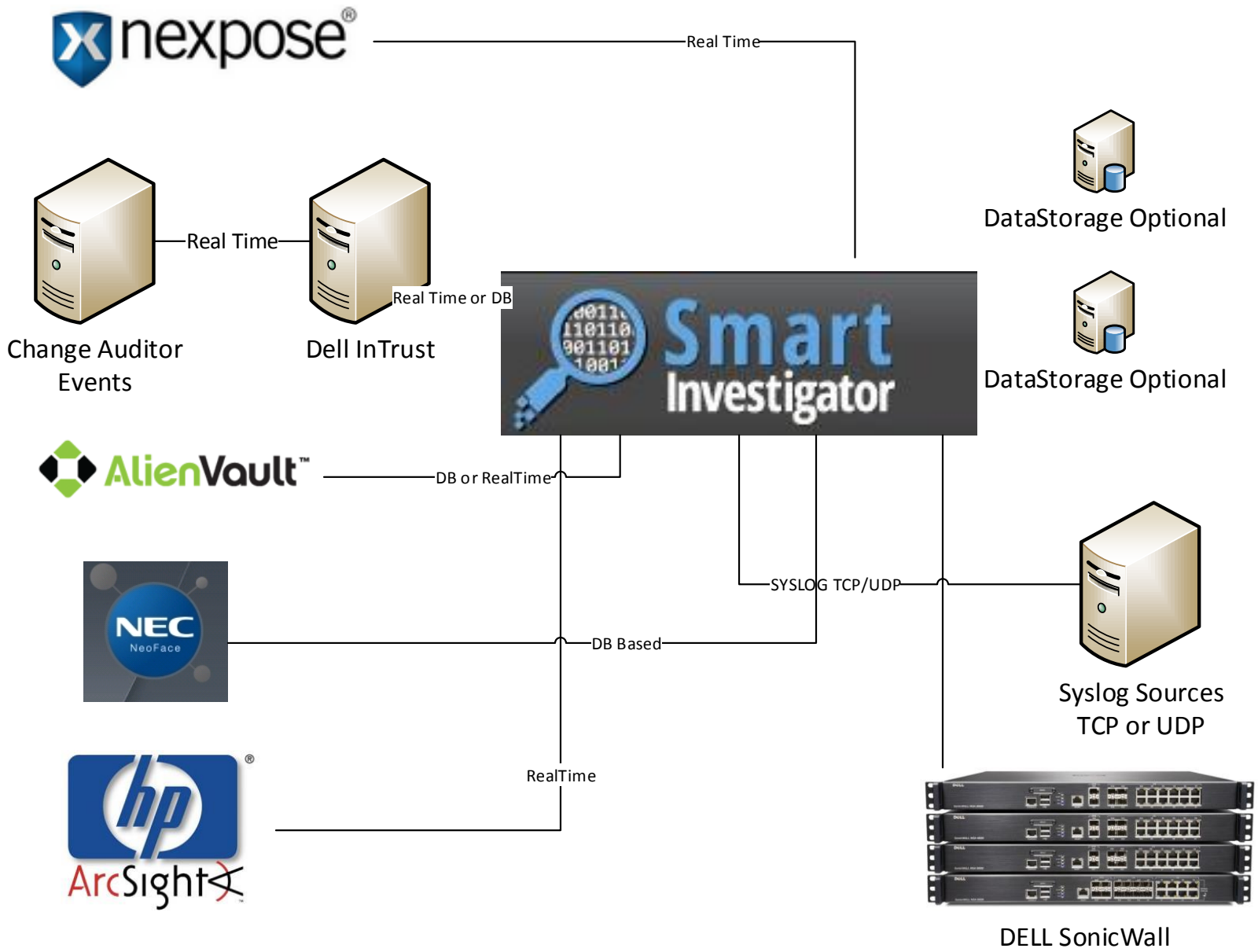
Beneficii

- 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

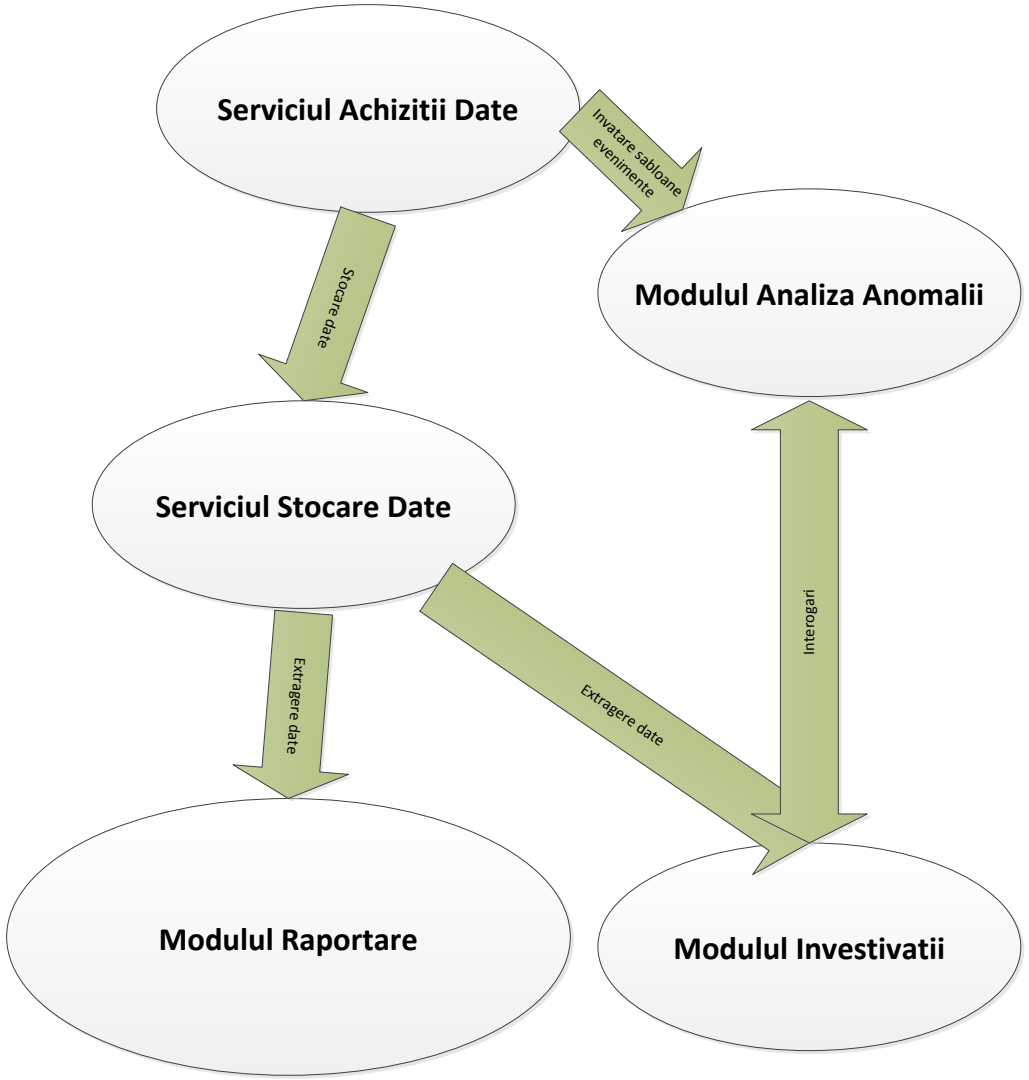
Cum ?

- 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

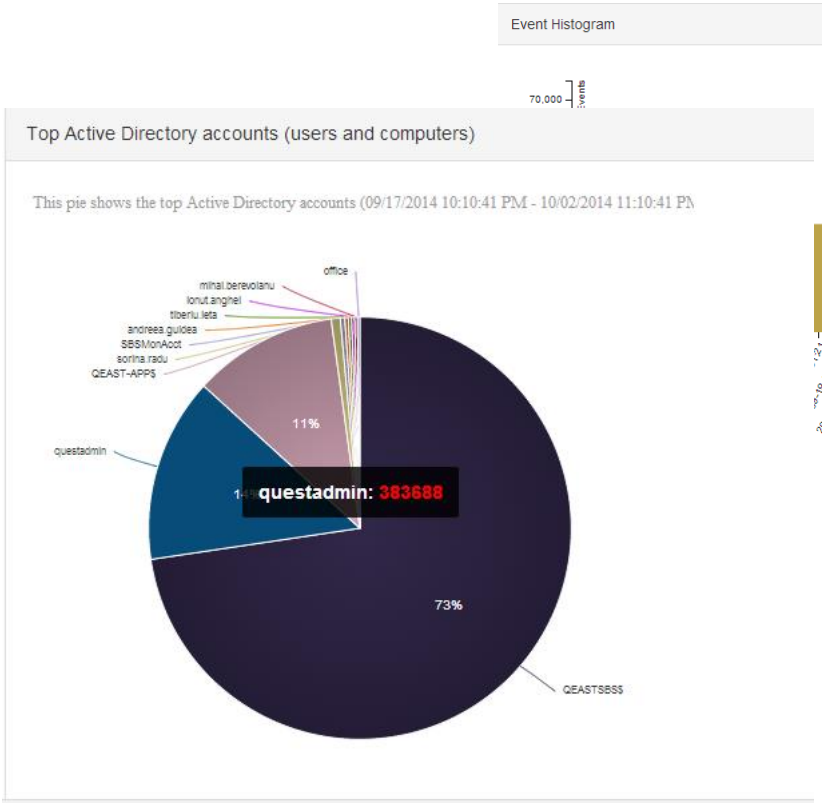


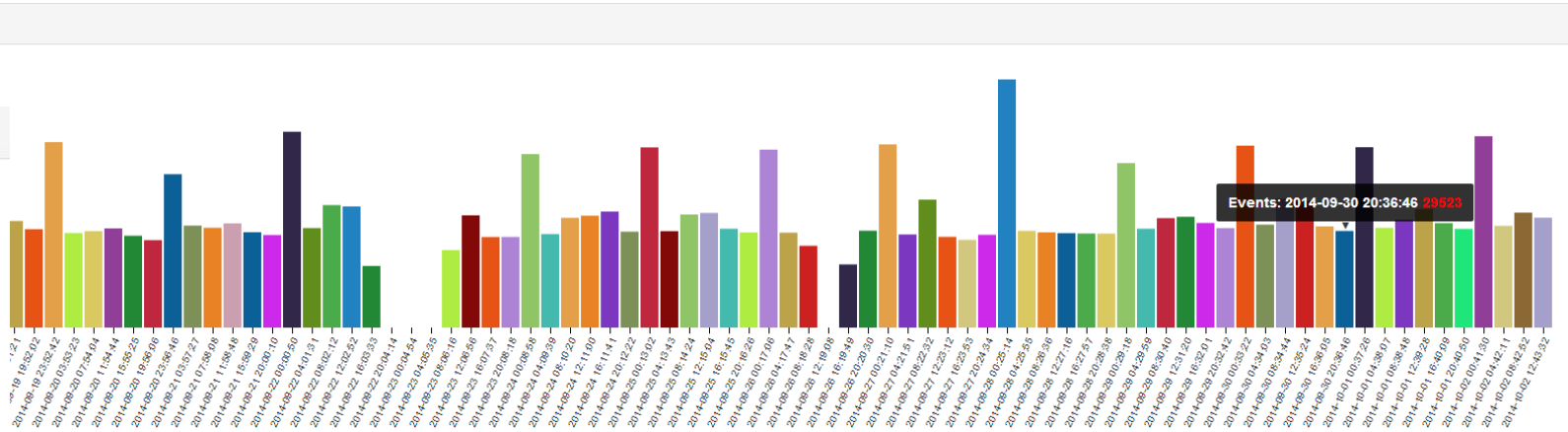
Arhitectura interna – Schema generala



Q-East Smart Investigator

Dashboard-uri Q-East SmartInvestigator

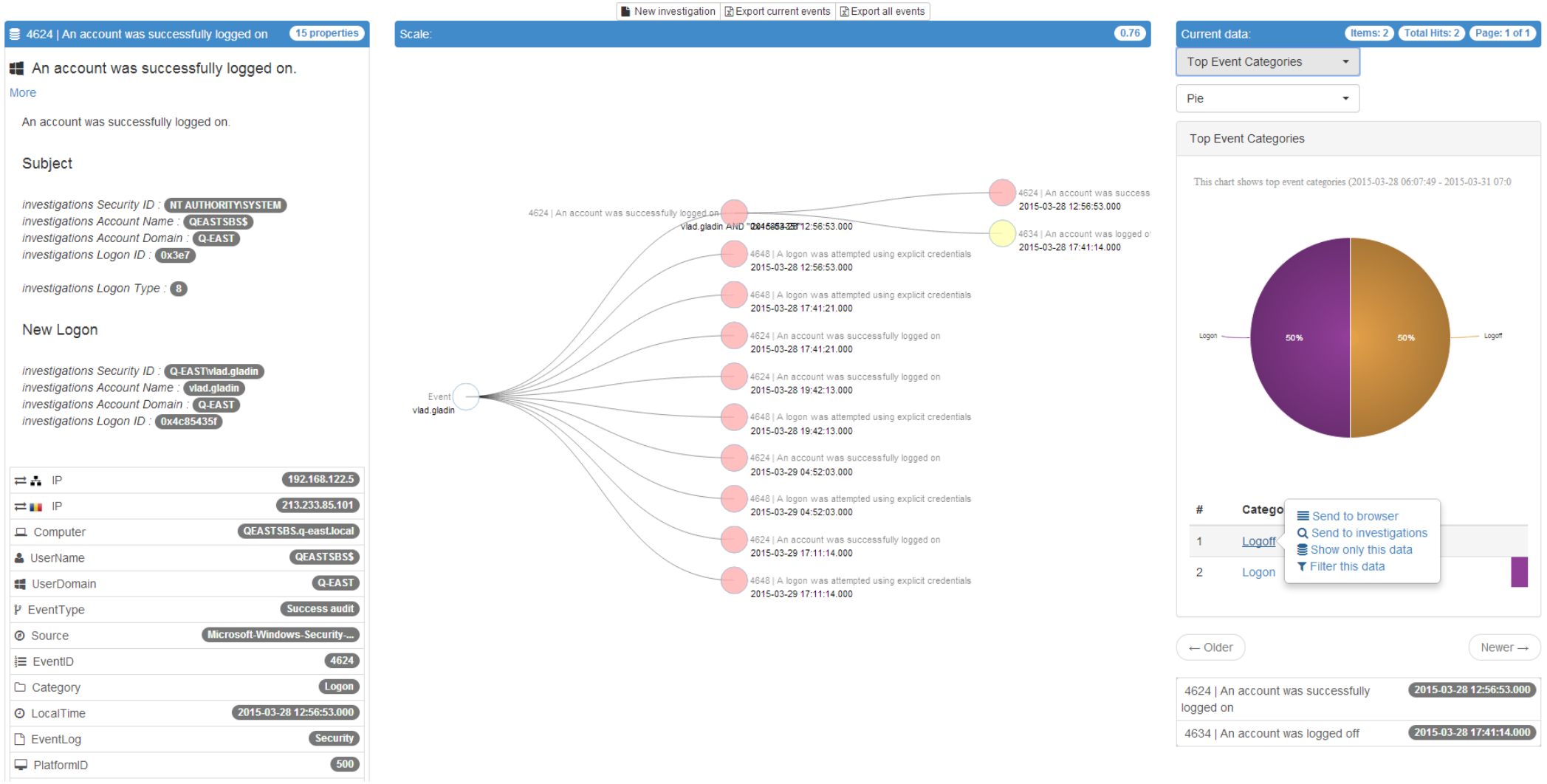




Software

Q-EAST SOFTWARE
Smart Systems Management

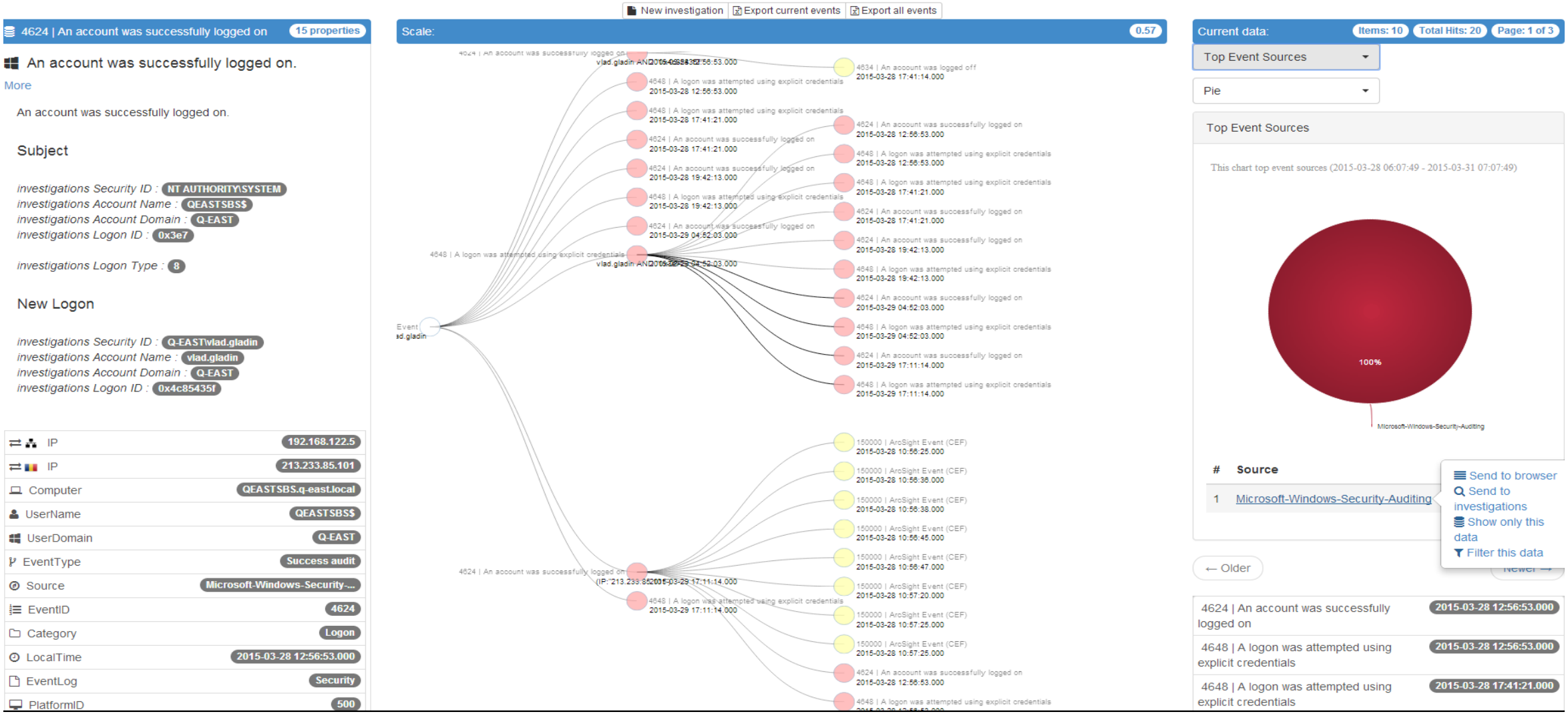
Modul Investigatii



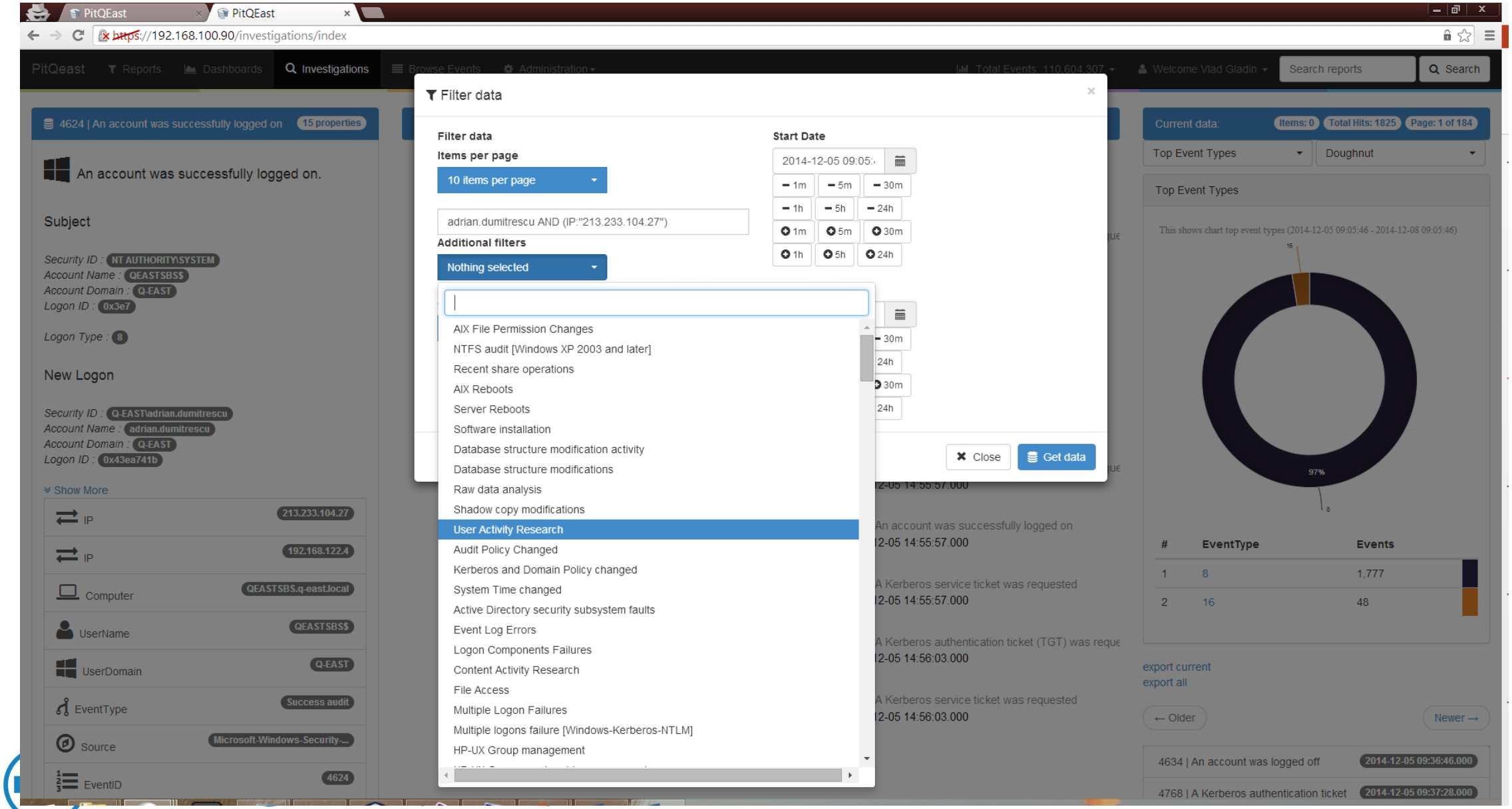
DELL Software

Q-EAST SOFTWARE
Smart Systems Management

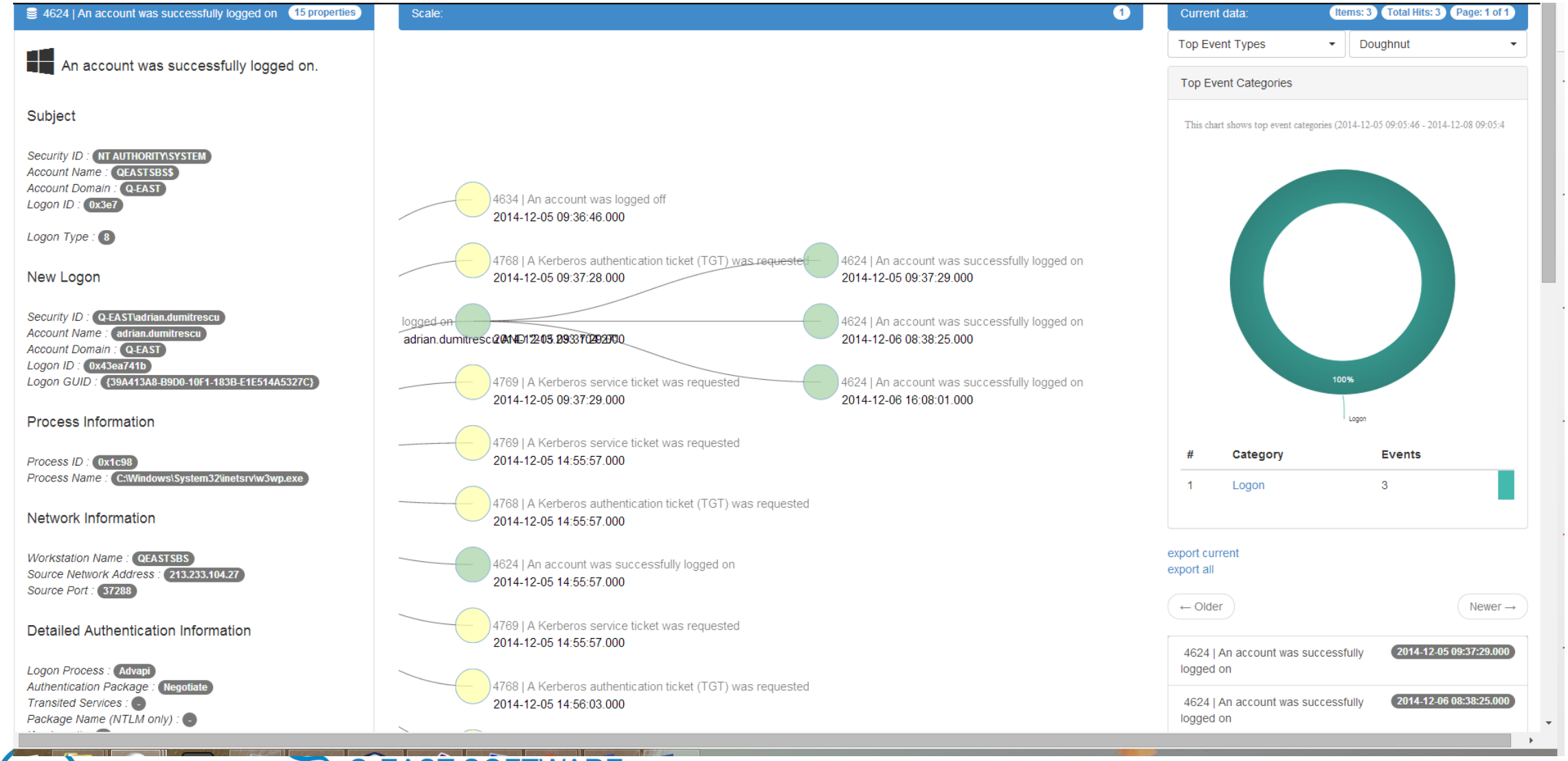
Investigatii in mod grafic pas cu pas (din nod in nod)



Filtre inteligente simple sau/si compuse



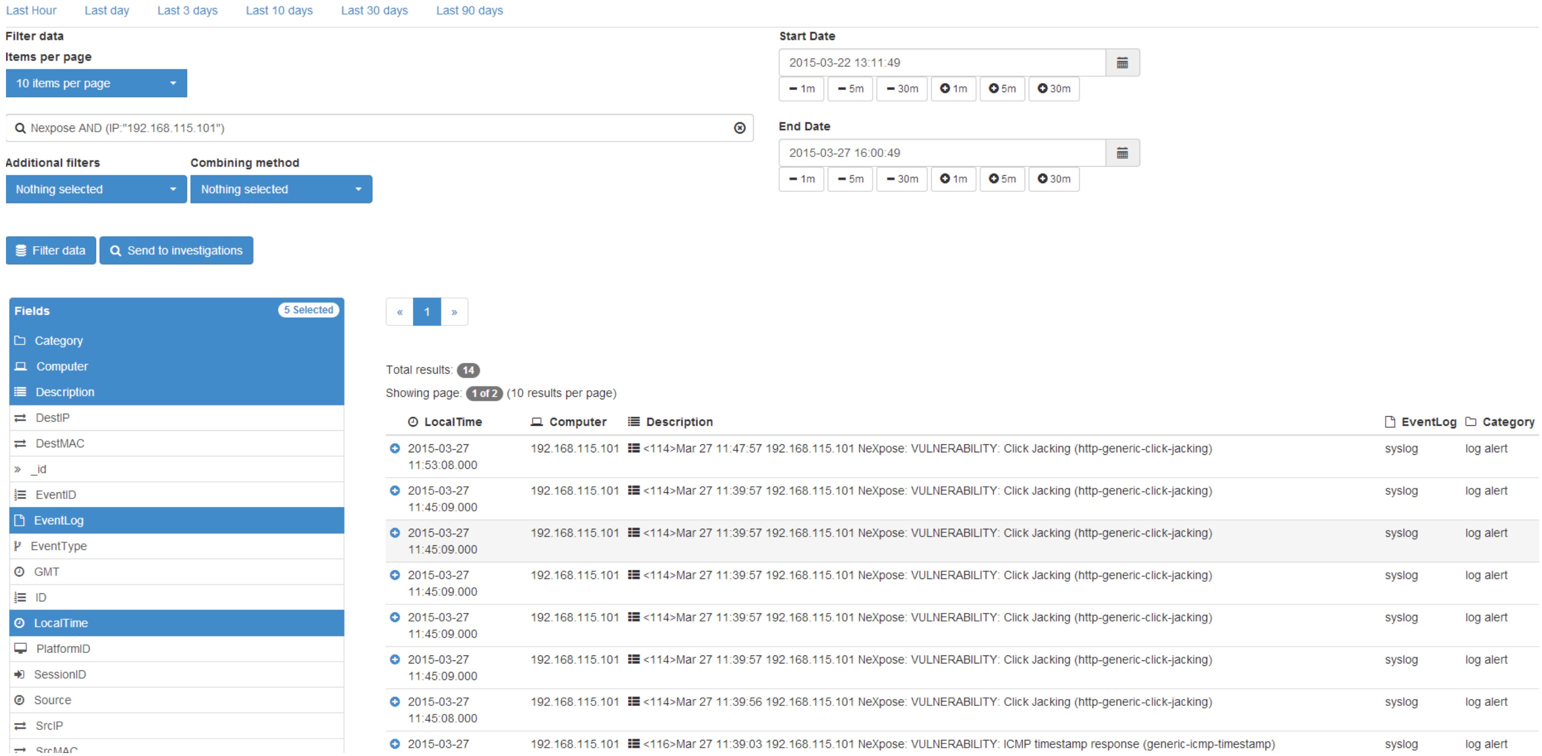
Filtre inteligente simple sau/si compuse



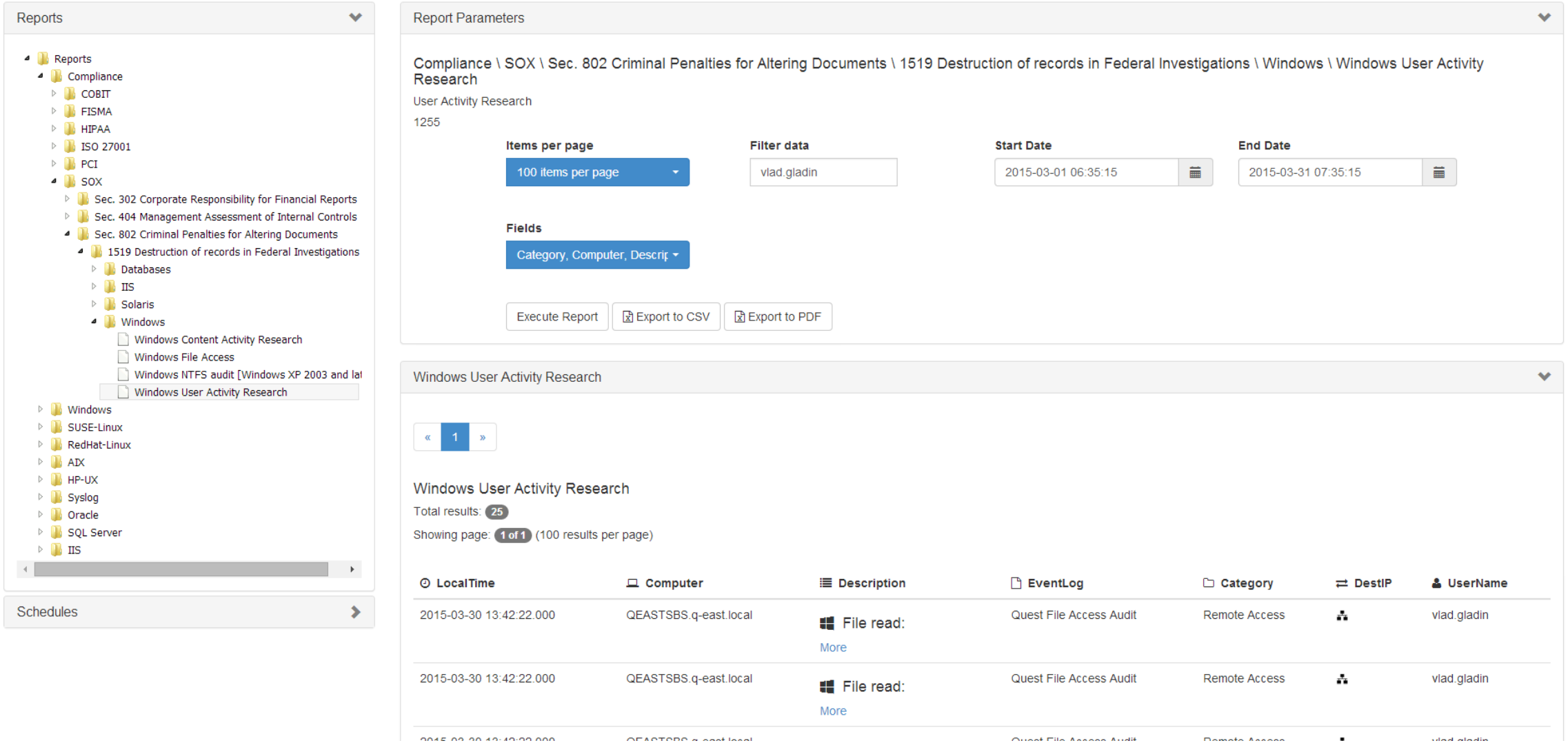
Event Browser; filtre simple sau si/compuse

- Search as string: “vlad.gladin”
- Search with column filter (“UserName:”vlad.gladin”)
- Multiple conditions:

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



Modul raportare. Rapoarte bazate pe standard si tehnologii



DELL Software

Q-EAST SOFTWARE
Smart Systems Management

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

Multumesc!

Vlad Gladin
Vlad.Gladin@QEast.ro

DELL Software
Q-EAST SOFTWARE
Smart Systems Management