RECRO net
We know IT

HROUG

Otkrivanje internih prijevara analizom obrazaca ponašanja korisnika IT sustava

Rovinj, 18.-22.10.2011.

Nevenko Bartolinčić

CISCO PARTNER Gold Certified

Microsoft GOLD CERTIFIED Partner

CISCO PARTNER Learning

Raspored

- Postavljanje scene
- Zaplet
- Vrhunac
- Rasplet
- Kava

Scena 1: Očigledno

SLUŽBENICA ZAGREBAČKE BANKE ANKICA LEPEJ OTKRILA RAČUN ANKICE TUĐMAN

20. listopada - **Ankica Lepej, dugogodišnja službenica Zagrebačke banke, predočila je javnosti stanje bankovnog računa Ankice Tuđman.** Ona se jučer sama prijavila Upravi banke.

Vesna Alaburić, odvjetnica Ankice Lepej, istaknula je kako su motivi gospođe Lepej da otkrije tu informaciju i da sada otkrije svoj identitet kao izvor informacije nevjerojatno časni. On
je to učinila kako bi zaštiti
Ankica Lepej objasnila je
preveliki šok. Držati takav
građanima biti primjer kak
informacija.
Njezina odvjetnica potvrdi
i na kojekakve daljnje istrage i motrenja ljudi, rekla je Alaburić.
e vidjela račune gospođe Tuđman, koji su za nju, kako je rekla, bili
gućim. Predsjednikova bi obitelj, barem mi se tako čini, trebala svim
od milijun kuna koju je Zagrebačka banka ponudila za otkrivanje izvora

Zagrebačka banka pokrenula je, prije otkrivanja identiteta
bankarske tajne te neovlaštenog i protuzakonitog priopćavanja

14. SIJEČNJA 2011. 14:24h

Obiteljska bankarica "očistila" račune šest klijenata za 355.000 kuna

Tekst

Like Send Be the first of your friends to like this.

Najmanje 355 tisuća kuna spremila je u džep 49-godišnja bankarska službenica iz Matulja, zaposlena kao obiteljski bankar u jednoj riječkoj banci. Kriminalističkim istraživanjem Odjela gospodarskog kriminaliteta PU Primorsko-goranske ustanovljeno je da je bankarica od prosinca 2008. do kolovoza 2010. godine oštetila šest klijenata.

Bez njihova znanja zatvorila je i otvorila više računa devizne štednje krivotvorivši dokumentaciju i ugovore o računima. Novac koji je zadržala za sebe šestorici oštećenih klijenata vratila je poslovnica banke i ostala oštećena za iznos kojim si je mjesečna primanja podebljavala njihova bivša službenica.

Bankarska službenica iz Matulja zbog tri kaznena djela zlouporabe položaja i ovlasti i tri kaznena djela krovotvorenja službene isprave Županijskom državnom odvjetništvu prijavljena je redovnim putem.

20. listopada - **MUP je objavio kako je otkriven još jed
Gajnicama, policija je podnošenje kaznene prijave najavila
Protiv njih će, stoji u priopćenju Ureda za odnose s javnoš
su počinile kazneno djelo neovlaštenog otkrivanja poslovne**

Pronevjera

Službenica banke ukrala 120.000 kuna

05.07.2010
Zadar

Dovršeno je kriminalističko istraživ
sumnja da je 36-godišnja šalterska
banke u Zadru u razdoblju od 10.
godine protupravno prisvojila nova
klijenata, izvijestila je PU zadarska

Sumnjiči se da je neovlašteno vršila isplate novca te ga zadržavala za sebe, dok je u rubrici ovjera nalogodavca lažno upisivala imena i prezimena klijenata, čime je banku oštetila za iznos od preko 120.000 kuna.

Protiv 36-godišnjakinje je podnesena kaznena prijava zbog pronevjere.

banke štedišama
e uzela 950.000 kuna

ru šalterska službenica (44) iz Bola oštetila je za nešto manje od
eno prijavila zbog neovlaštene uporabe, prijevare i krivotvorenja
o-dalmatinske Policijske uprave.

riminaliteta uhitili su 44-
govorna osoba u banci od 20.
2009. prekoračila ovlasti i
tvorila potpise na potvrdama o
čuna. Novac koji je podizala, a
za sebe te je tako više štediša

koji će ovo preporučiti.

ALATI
- Komentiraj članak
- Podijeli s drugima
- Pošalji članak
- Rss
- Ispiši članak
- Smanji slova
- Broj glasova: 0 | Prosjek: 0%

0%

KLJUČNE RIJEČI
- Gospodarski kriminalitet u RH
- ZABA (Zagrebačka banka d.d.)

Moje pretplate »

Scena 2: Malo manje očigledno

Index je jedini objavio njegovu policu osiguranja iz kojeg je vidljivo da je stajao više od četiri milijuna kuna.

MB 0000003276147

AUTOMOBILSKOG KASKA Br. 004620276406

Ugovaratelj: HRVATSKA DEMOKRATSKA ZAJEDNICA
(03469271-000)
TRG ŽRTAVA FAŠIZMA 4, 10000 ZAGREB

Osiguranik: HRVATSKA DEMOKRATSKA ZAJEDNICA
(03469271-000)
TRG ŽRTAVA FAŠIZMA 4, 10000 ZAGREB

HRVATSKA DEMOKRATSKA ZAJEDNICA

TRG ŽRTAVA FAŠIZMA 4
10000 ZAGREB

Trajanje: Početak: 16.01.2009. u 12:00. Istek: 16.01.2010. u 12:00.
JEDNOGODIŠNJE osiguranje dospijeva na obnovu svake godine na dan 16.01.

Predmet osiguranja: OSOBNO VOZILO BMW 760 LI Broj šasije WBAHP810X0DC73256, god. proizvodnje 2008, 327 kW	**Reg.ozn. ZG9636AP**
Osnovica za obračun premije i gornja granica obveze prema čl. 20. Uvjeta AK: **4.187.595,00 kn**	Bez franšize

Ukupno:				**160.318,10**
Plaćanje u gotovini	160.318,10	-	5,000 %	8.015,91
Porez na premiju kasko osiguranja 10% (osnovica 152.302,20 kn)				15.230,22
			Ukupno za naplatu:	**167.532,41**

Napomena: OSNOVICA ZA OBRAČUN PREMIJE SA PDV-OM
DODATNA OPREMA U PRILOGU

Scena 3: Veliki igrači

PCWorld

Search PC World | Search | Browse by Topic

Home | News | Hardware Reviews | Software Reviews | How-To | Videos | Downloads | Shop & Compare | Community

FIND A REVIEW

Select Category

- Audio & Video
- Business Center
- Cameras
- Cell Phones & PDAs
- Communications
- Components & Upgrading
- Desktop PCs
- DVD & Hard Drives
- Gaming Hardware & Software
- HDTV
- Laptops
- Macs & iPods
- Monitors
- Printers
- Spyware & Security
- The PCW Test Center
- Windows Vista & XP

Read More About: Online Security • Network Security • Cybercrime • Data Protection

Poor IT Security Blamed for Bank Fraud

Kerviel had previously worked in the bank's IT department, and so had in-depth knowledge of its systems and procedures.

Staff mostly followed those procedures, the investigating committee found, but the procedures were not in themselves sufficient to identify the fraud before Jan. 18, partly because of the effort Kerviel made to avoid detection, and partly because staff did not systematically conduct in-depth investigations when warnings flags were raised.

Among the tricks Kerviel used to hide his activities, the bank's General Inspection department highlighted the use of fake e-mail messages to justify missing trades, and the borrowing of colleagues log-in credentials to conduct trades in their name.

Investigators identified at least seven occasions on which Kerviel faked messages between April 2007 and Jan. 18, four of them referencing trades that never existed. The deception was eventually uncovered when they could find no trace of Kerviel receiving the purported messages in the bank's e-mail archival system, Zantaz.

Kako se to moglo primjetiti?

Detekcijom “posuđivanja” koleginog korisničkog računa

- **Isti User-ID istovremeno prijavljen s dvije različite IP adrese**
- **Nekoliko User-ID prijavljeno jedan za drugim s iste IP adrese**
- **Korisnik se prijavio u sustav, a nije se na ulazu u zgradu prijavio svojom identifikacijskom karticom da je ušao u zgradu**
- **Netipične aktivnosti poslije kraja radnog vremena**

Kako interni korisnici vrše zloupotrebu?

Preuzimaju tuđi račun

- Kradu korisnički identitet manipulirajući podatke o računu
- Otvaraju račune za posrednike prenos novca ili za skrivanje traga prenosa novca
- Otvaraju račune za nepostojeće ili neodgovarajuće korisnike kako bi ostvarili kvotu ili proviziju

Kradu novac

- Kradu novac od korisnika preko:
  - gotovine
  - čekova
  - kartica
  - transferom između računa
  - nalozima za plaćanje
- Kradu novac s internih računa preko:
  - gotovina
  - transferom između računa
  - nalozima za plaćanje

Ostali načini

- Osobni troškovi na teret korporacijskih kreditnih karica
- Obavljanje transakcija za sebe, obitelj, prijatelje
- Krađa korisničkih podata za prodaju ili zloupotrebu
- Obavljanje neovlaštenih potraživanja, popusta, povrata
- Iskorištavanje starijih i nemoćnih osoba
- Udruživanje više djelatnika
- Kršenje pravila / namjerne greške
- Pokušavanje izbjegavanje detekcije

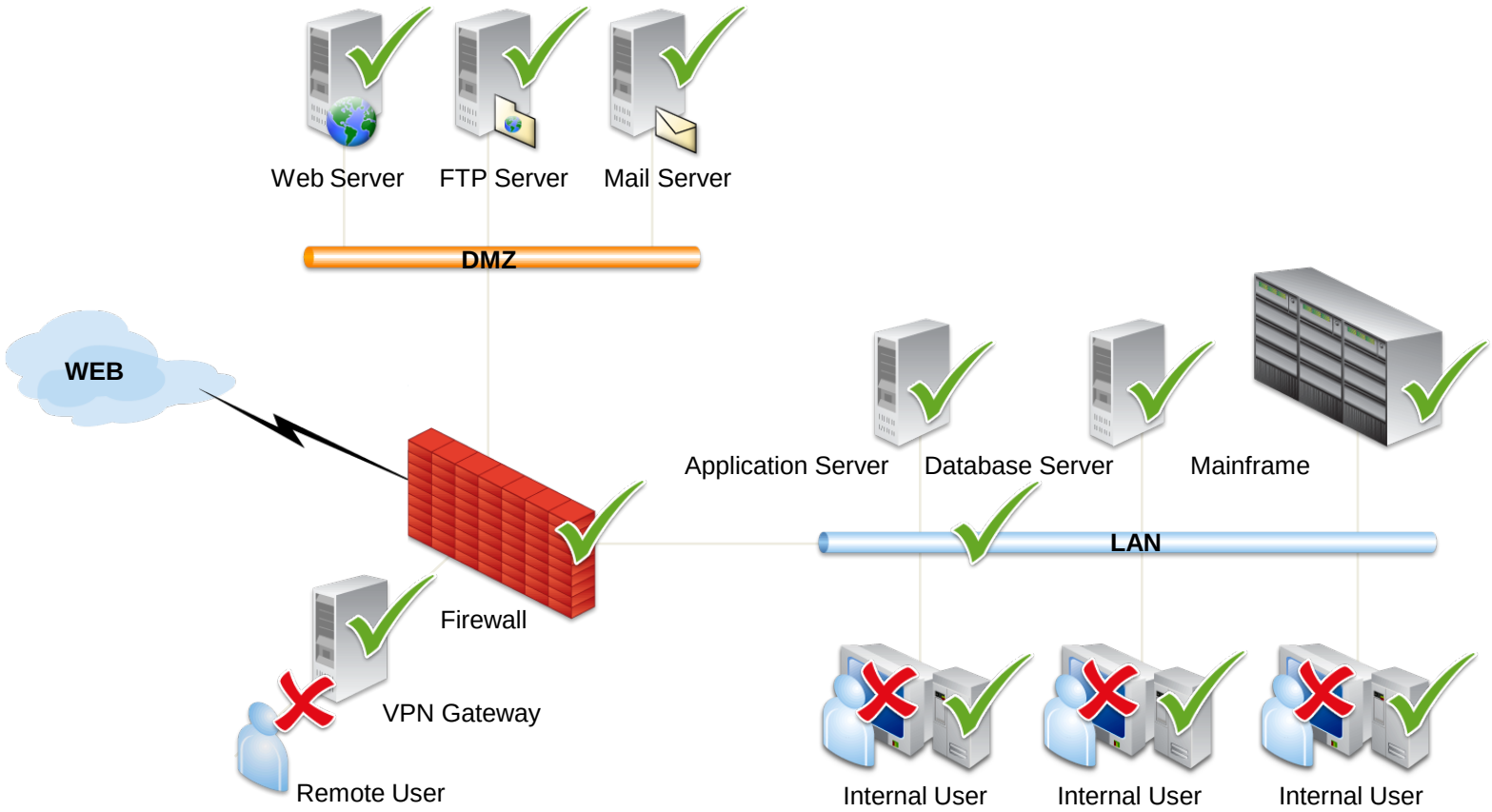
1. Ako su novci otišli možda je već prekasno
2. Vaši logovi ne sadrže cijelu priču
3. Koliko vaših pronevjera počinje s kršenjem kontrola?
4. Izbjegnuti gubitak vremena
5. Efikasno dobivanje konsolidiranih podataka

5 STVARI ZA RAZMISLITI

Postojeća sigurnosna rješenja

Svaki element je zaštičen…

…osim od pristupa ovlaštenih osoba



Ukratko o Intellinxu

- osnovan 2005. u Izraelu
- preko 100 korisnika širom svijeta
- 3 od 10 vodećih banaka u SAD koristi Intellinx
- Gartner report 2010 o Enterprise Fraud Managementu:
  - Intellinx pozicioniran kao #1 za Internal Fraud detection.
  - Intellinx pozicioniran kao #1 za Deployment and Support Simplicity

Korisnici Intellinxa

Banke i financijske ustanove

GE Money
US Bank
UnionBank
Comerica
Raiffeisen BANK
UniCredit Bank
EQUIFAX
TransUnion
TCF
FirstBank
中国农业银行 AGRICULTURAL BANK OF CHINA
bankinter
NEDBANK
לאומי leumi
SECSERVIZI
Inter-Európa Bank Rt.
VOLKSBANK Hungary A BIZALOM ÖSSZEKÖT.
BancaStato BANCA DELLO STATO DEL CANTONE TICINO
BANCO J. SAFRA
השלבנת ישראכרט
ISRAEL DISCOUNT BANK
K&H

Osiguravajuća društva

UNIQA
AVIVA
HAREL Insurance & Finance
מגדל
clal Insurance
Groupama

Državna uprava

POLICE DEPARTMENT CITY OF NEW YORK
Delaware Criminal Justice Information System
DELJIS
Serving Those Who Serve Others
Federal Bureau of Prisons
An agency of the U.S. Department of Justice
South African Department of Home Affairs
National Health Insurance Fund
Ekurhuleni METROPOLITAN MUNICIPALITY
Police Credit
Securing your future
חברת החשמל לישראל Israel Electric Corp.
המוסד לביטוח לאומי National Insurance Institute of Israel

Zdravstvo i Maloprodaja

HIGHMARK Blue Cross Blue Shield
Taipei Veterans General Hospital
MEUHEDET
שופרסל

Intellinx – prevencija internih zloupotreba

Data Capture & Collection

- Network sniffing: transactions, screens, intra-application messages, database access
- Log files and databases
- Reference Data

Forensic Visual Audit Trail

- Replay user activity screen by screen
- “Google like” search on captured data, e.g. Who accessed a specific customer account in a specific timeframe?
- Captured data is encrypted and digitally signed - potentially admissible in court when needed

Fraud Analytics

- Dynamic Profiling and scoring of various entities
- Customizable business rules
- Real-time alerts
- New rules may be applied after-the-fact

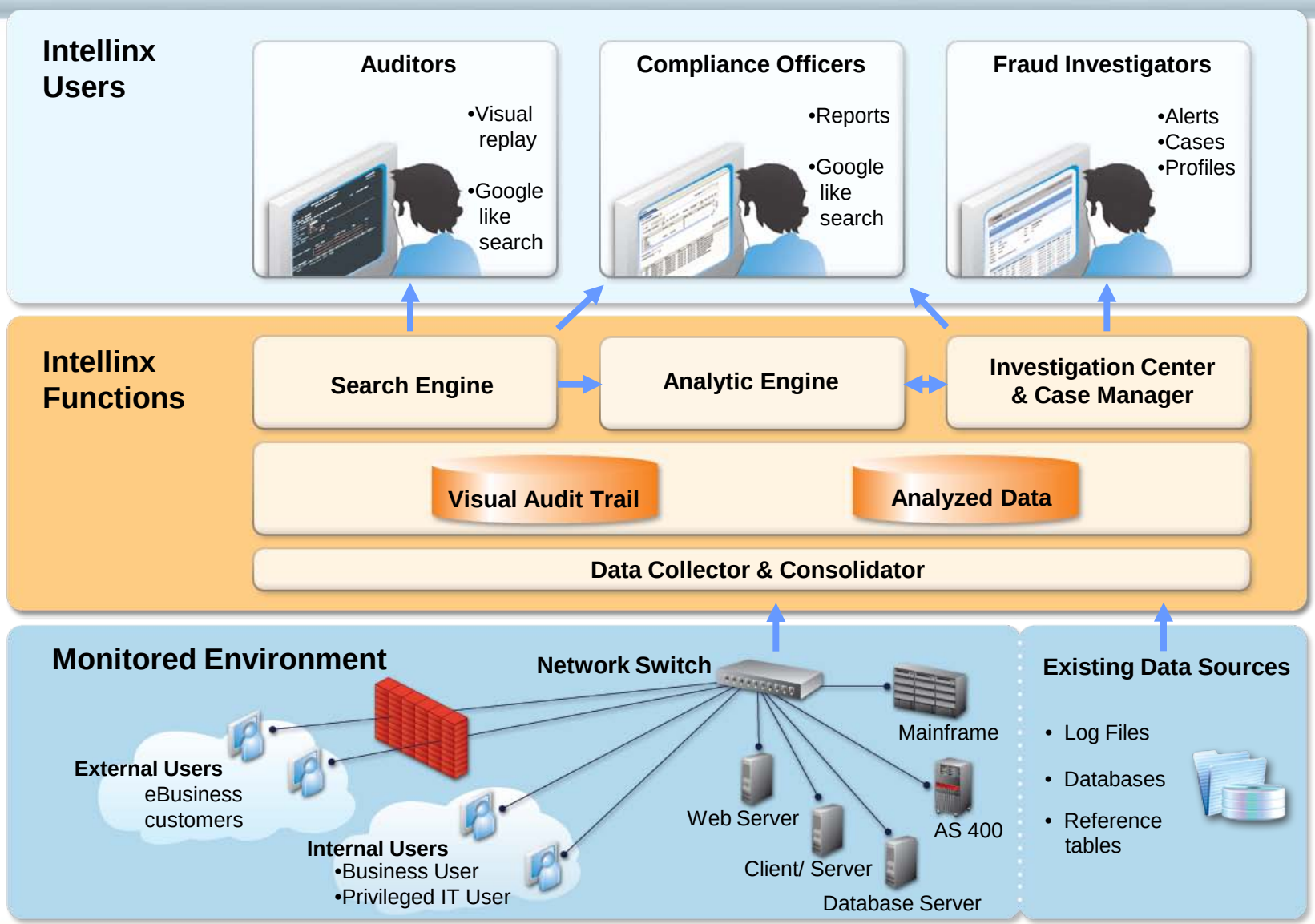
Investigation Workbench and Case Management

- Manage Cases, Alerts and Incidents
- Flexible Reporting
- Control parameters of rules, profiles and scoring

Intellinx – metode detekcije

- Različito ponašanja od sličnih korisnika
  - Homogene grupe korisnika sa sličnim poslovima
- Odstupanje od uobičajnog oblika ponašanja
  - Profiliranje korisnika, računa, klijenta i drugih
- Neubičajena povezanost korisnika i pojedinog klijenta / računa
  - U Call Centrima uočajeno je slučajni redosljed poziva
- Određeni sumnjivi scenariji
  - Promjena adrese nakon čega slijedi reizdavanje kartice
- Korelacija kadrovskih podataka s identitetom korisnika
  - Slična adresa korisnika i klijenta
- Korelacija aktivnosti korisnika s poznatim slučajevima vanjske zloupotrebe
  - Povećan broj aktivnosti korisnika prema vanjskim slučajevima zloupotrebe ili kreditnim karticama prije nego što je detektirana zloupotreba
- Aplikativni Honey Pot
  - Dostupne prividne prevelike ovlasti za sumnjive korisnike i praćenje njihove

Arhitektura



Patentirana tehnologija

- Agent-less network traffic sniffing
- No Impact on performance
- Highly scalable architecture
- Very short installation process (several hours), with no risk to normal IT operations
- Recordings stored in extremely condensed format
- Recording data is encrypted and digitally signed – potentially admissible in court when needed

Monitored Platforms:

- IBM Mainframe: 3270, MQ, LU0, LU6.2
- IBM System i: 5250, MPTN
- UNISYS T27
- Web: HTTP/ HTTPS
- Client/Server: TCP/IP, MQ Series, MSMQ, SMB
- Telnet, VT100, SSH
- Oracle (SQLNET), DB/2 (DRDA), MS SQL(TDS)
- SWIFT, FIX, ISO8583 (ATM), others

Dinamičko profiliranje

- Dynamic definition of profiles for any entity:
  - End-Users
  - Accounts
  - Customers
  - Any other Entity
- Time Dimension: Hour, Day, Week, Month
- Sample Behavior Attributes:
  - Working hours
  - Number of transactions per day
  - Total amounts of transfers per day
  - Total amounts of deposits per day
  - Number of dormant accounts accessed per day
  - Number of changes to dormant accounts per day
  - Number of account address changes per day
  - Number of beneficiary changes per day
  - Number of VIP queries per day
  - Number of changes to account statement mailing frequency per week
  - Number of credit limit changes per day

Primjeri pravila

- **What?**
  - Access of a specific account
  - Access an account included in a White list/ Black list
  - Access any account more than x times in an hour/day
- **How?**
  - Search for accounts according to customer name more than x times in an hour/ day
- **When?**
  - All the above – after hours
- **Where from?**
  - All the above from which department
- **Time correlation**
  - Same user-id login from different terminals in the same time
  - Access customer sensitive data without customer call in the call centre at the same time
- **Data correlation**
  - Add same address/ beneficiary to different accounts by the same user
- **Aggregation**
  - Sum of transfers of an account/ user exceeds x
- **Scenario**
  - Add beneficiary then transfer/withdraw money then delete beneficiary - all in 48 hours
  - Change address then transfer/withdraw money then delete address - all in 48 hours
  - Increase credit limit then transfer/withdraw money then decrease credit limit - all in 48 hours

Knjižnica gotovih pravila

- Više od 300 pravila za detekciju vazličitih vrsta zloupotreba
  - Bankarstvo
  - Osiguranje
  - Informacijska sigurnost
- Pravila izradili stručnjaci iz podrčja detekcije internih zloupotreba (bivši zaposlenici KPMG i službenici bankarskih anti Fraud odjela)
- Bazirana na prikupljenom iskustvu drugih Intellinx korisnika customers
- Nazirana na opčim poslovnim pravilima no može se modificirati za potrebe korisnika i njihovih specifičnih aplikacija ili poslovnog procesa
- Bankarstvo:

  zloupotrebe zaposlenika, curenje informacija, IT sabotaže, zloupotrebe transfera novca, zloupotrebe aplikacija, bankomata, kredinih kartica, čekova, e-bankinga Cards, Check Kiting, AML, eBanking
- Osiguranje:

  upravljanje korisnicima, uprvljanje policama, obrada zahtjeva, rad s agentima

Sva pravila korisnik može modificirati prema svojim potrebama

A few examples of common rule types:

- Count suspicious transactions
- Value of suspicious transactions
- Sudden increase in count or value (by % or standard deviation)
- Count or value different from peer group (by % or standard deviation)
- Decision table (e.g., if personal customer, 1x, if corporate customer, 2x)
- White lists (e.g., if customer on list, suppress alerts)
- Hot lists / black lists (e.g., if customer on list, immediately trigger alert)
- Any of the above over time (e.g., count over a week, increase over a month)

Zaštita privatnosti zaposlenika i korisnika

- Intellinx ne snima ni jednu aktivnost na korisničkom računalu već samo pristup do poslovnih aplikacija
- Samo ovlaštene osobe mogu pristupiti Intellinx sustavu
- Sustav se može podesiti da nadizre samo određenu aplikaciju ili određenog korisnika, ostale informacije se filtriraju i odbacuju
- Pojedina polja i ekrani koji sadrže vrlo osjetljive informacije se mogu zasjeniti tako da revizori koji koriste sustav ih ne mogu vidjeti
- Svaki pristup do sustava i svaka izvršena akcija se bilježe što omogućuje uvid koje aktivnosti je izvršio pojedini korisnik Intellinx sustava
- Polja koja omogućuju osobnu identifikaciju korisnika (npr. user-id or terminal-id) je moguće zasjeniti za vrijeme pregledavanje snimke sadržaja korisničkog ekrana

Studija slučaja: Credit Card Company X

Zaključak

Prednosti Intellinxa

- Osiguranje individualne odgovornosti korisnika:
  - Vizualni dokaz aktivnsoti korisnika uključujući read upite korisnika
- Osiguranje proaktivnosti u smanjenju internih zloupotreba pomoću:
  - Profiliranje korisnika na temelju analize stvarnog ponašanja korisnika
  - Alarmi u stvarnom vremenu
- Provođenje forenzičnih istraga:
  - Primjena novih pravila na već snimljenim podacima
- Osiguranje usklađenosti sa zahtjevima regulatora
- Out-of-box value
  - Potpuno snimanje i pretraživanje neovisno o korištenoj platformi

▸ No Agents ▸ No Overhead ▸ No Risk

Hvala!

Pitanja ???

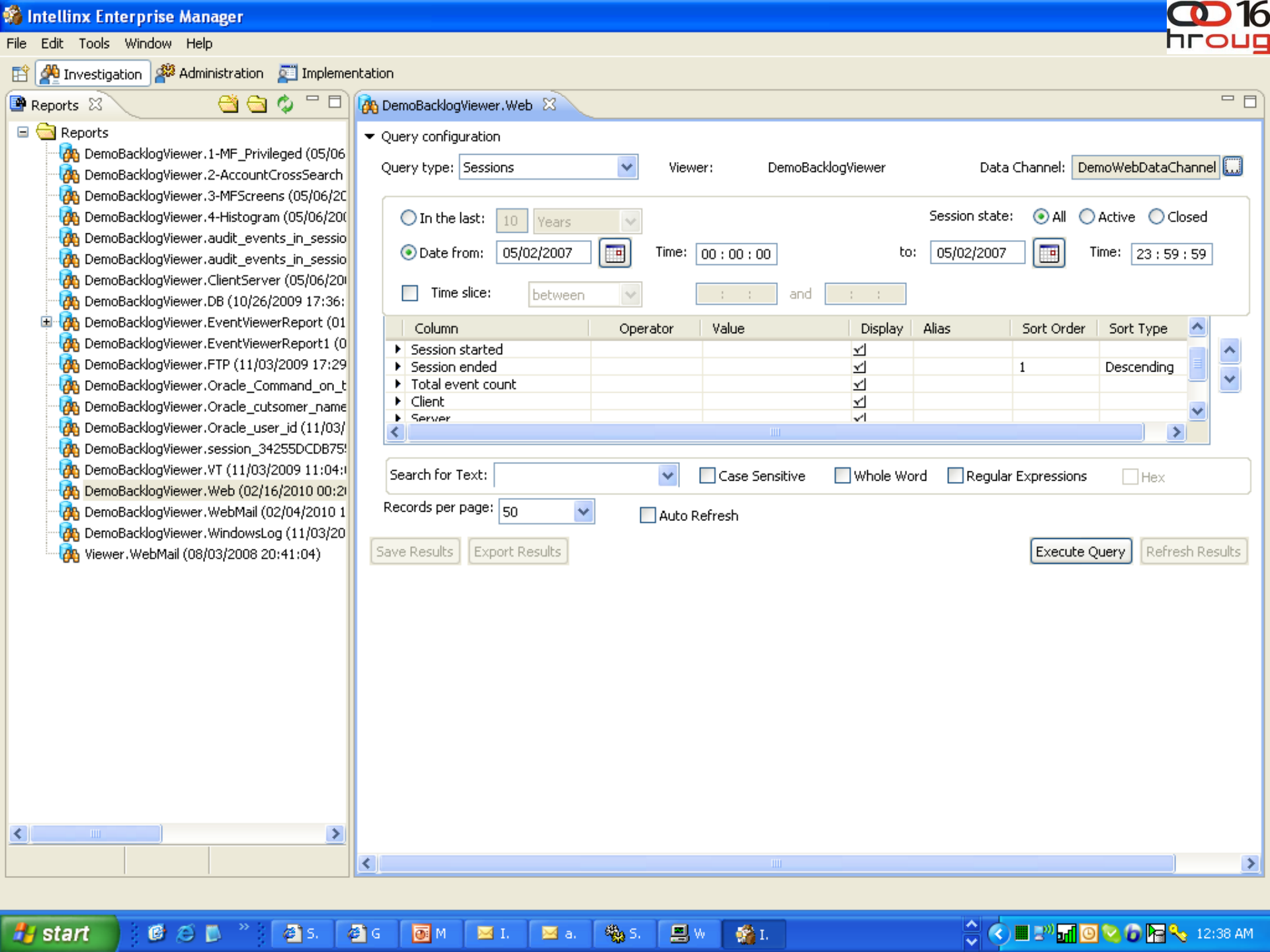
RECRO-NET d.o.o.	http://www.recro-net.hr
Av. V. Holjevca 40	Tel: +385 1 3030 600
10010 Zagreb	Fax: +385 1 6699 500
	info@recro-net.hr

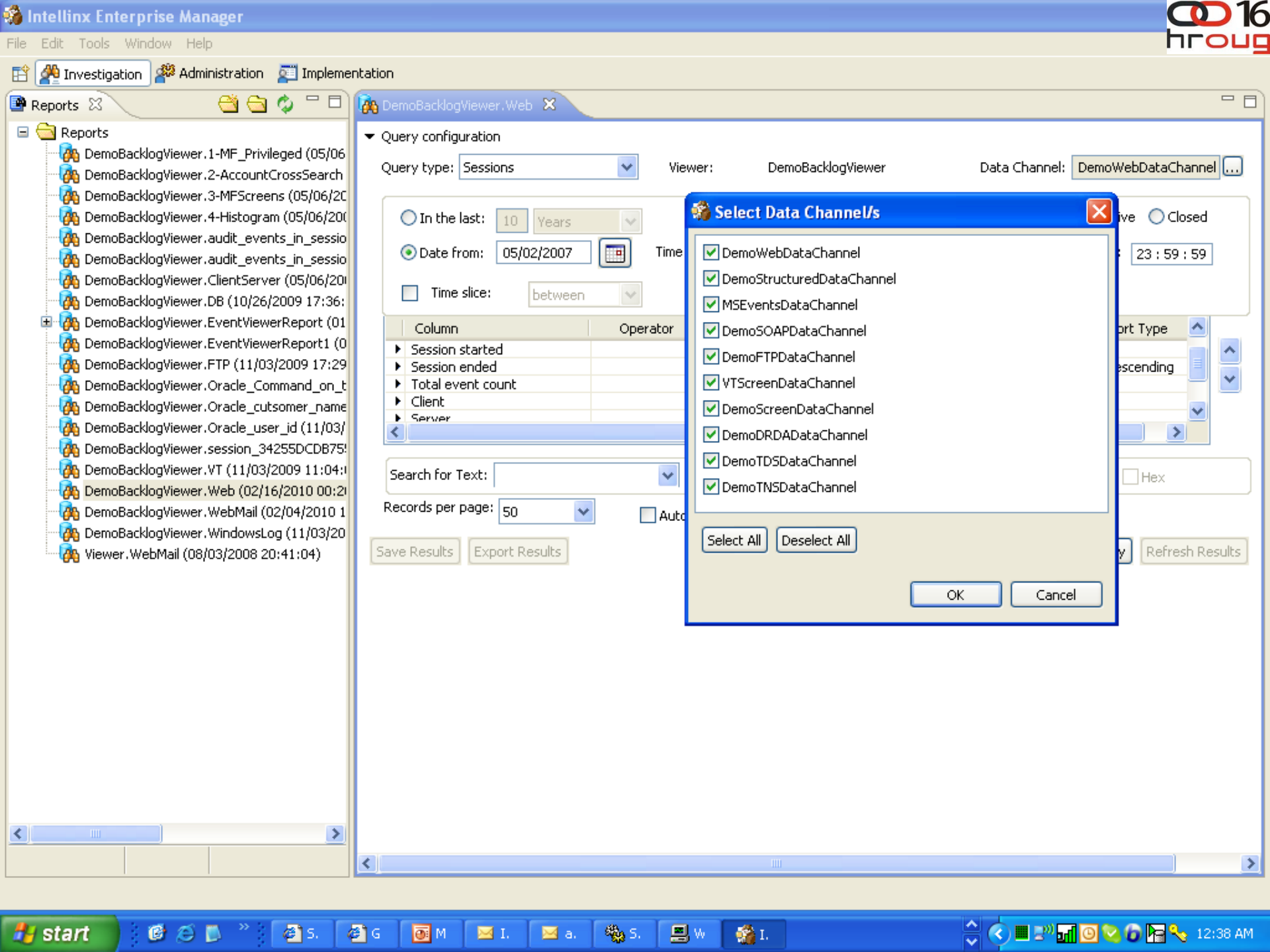
Dodatni slajdovi

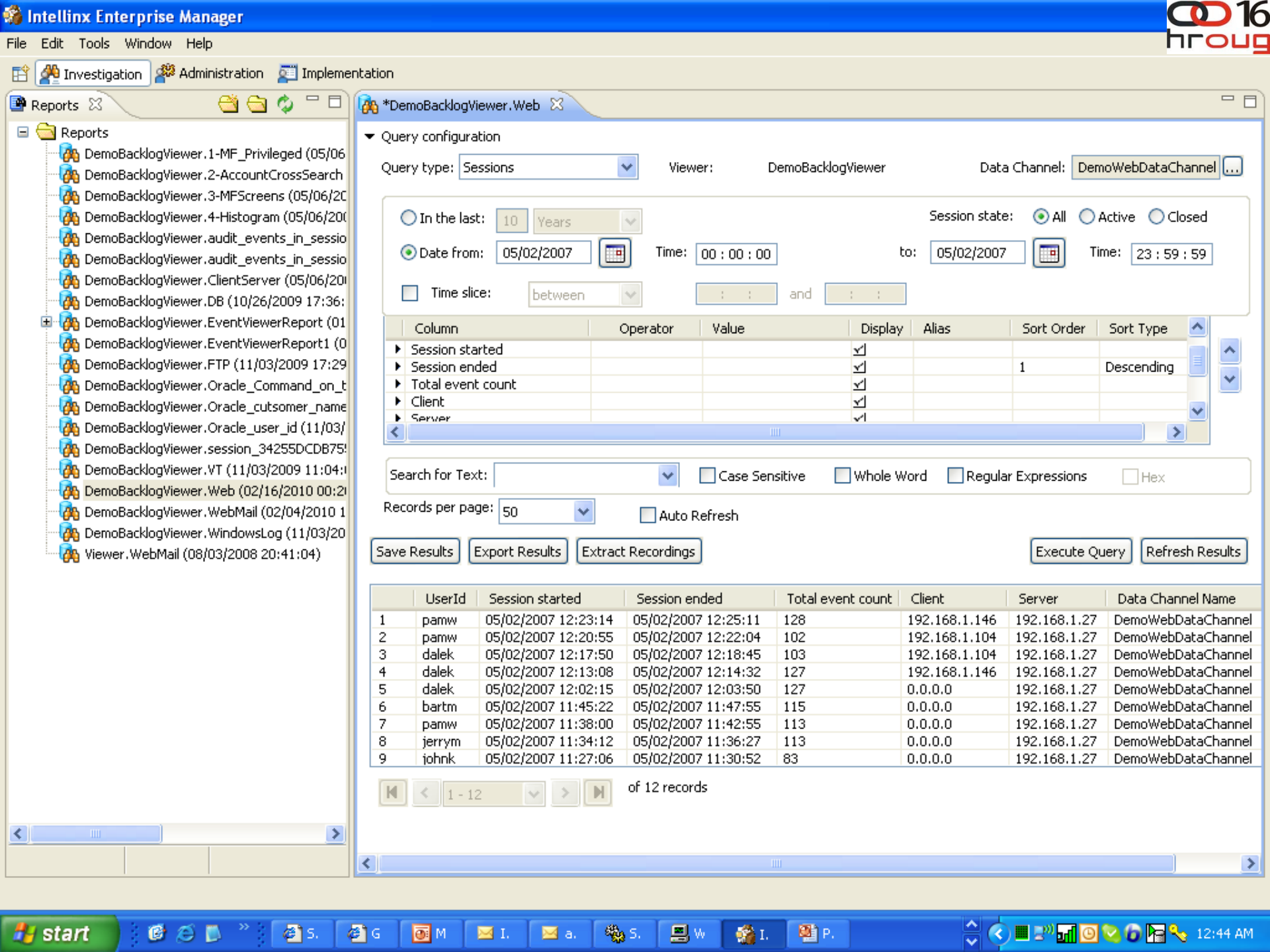
Vrste pravila – Real-Time / Batch

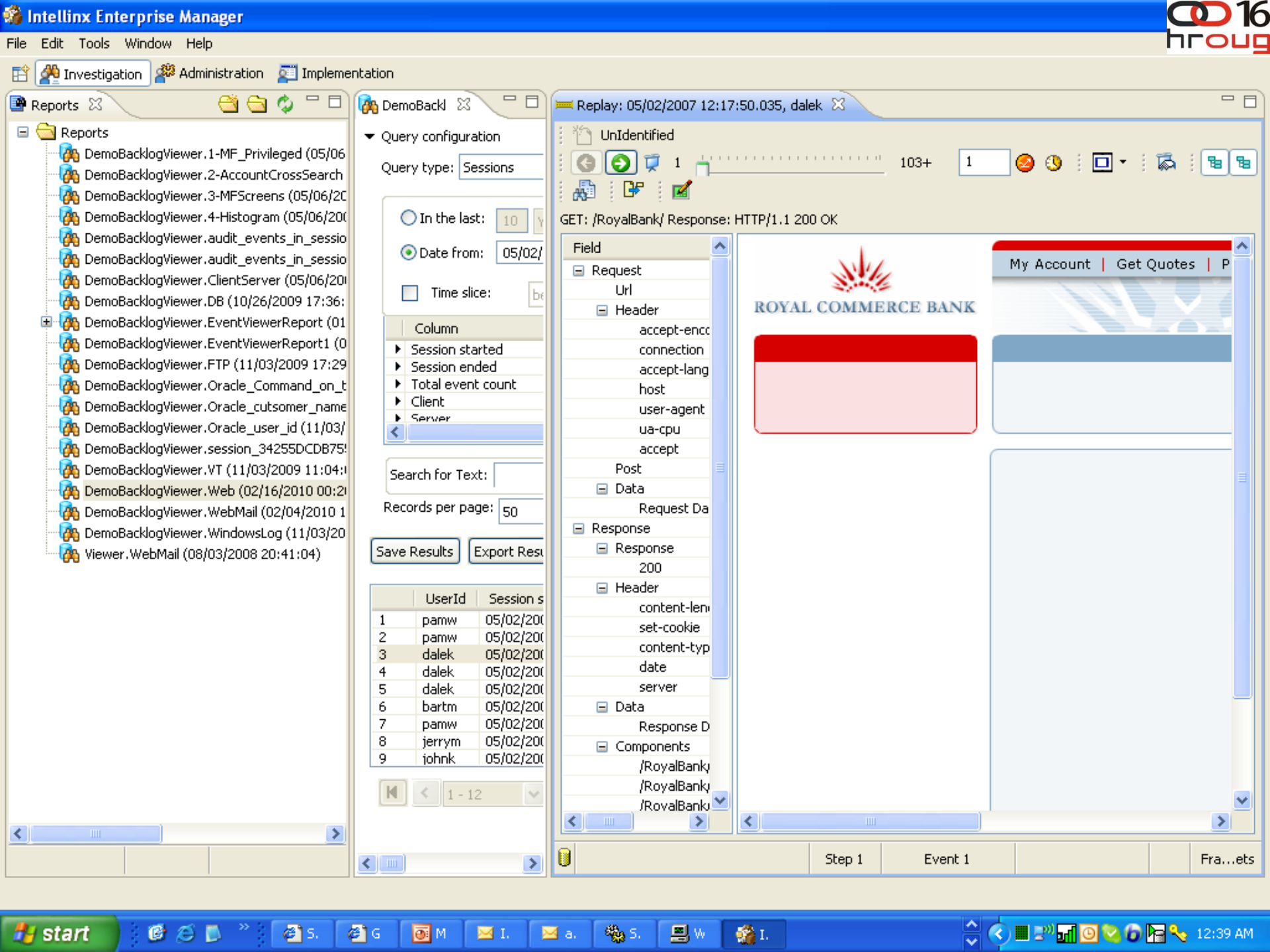
Type of Rule	Example
Peer group analysis	• Tellers inquiring on more accounts than other tellers • Employees accessing more dormant accounts than other tellers
Historical analysis	• Tellers that suddenly increase the number of inquiries they perform on out-of-state accounts
Transactional link analysis	• Call center agent servicing specific accounts repeatedly
Suspicious scenarios	• Real-time: suspicious callers in call center • Address change then card reissue then address change • Employees performing a high rate of transactions against general ledger accounts
Account link analysis	• Customer account with same address as employee
Case management link analysis	• Employee accessed accounts that led to fraud at a higher rate than other employees

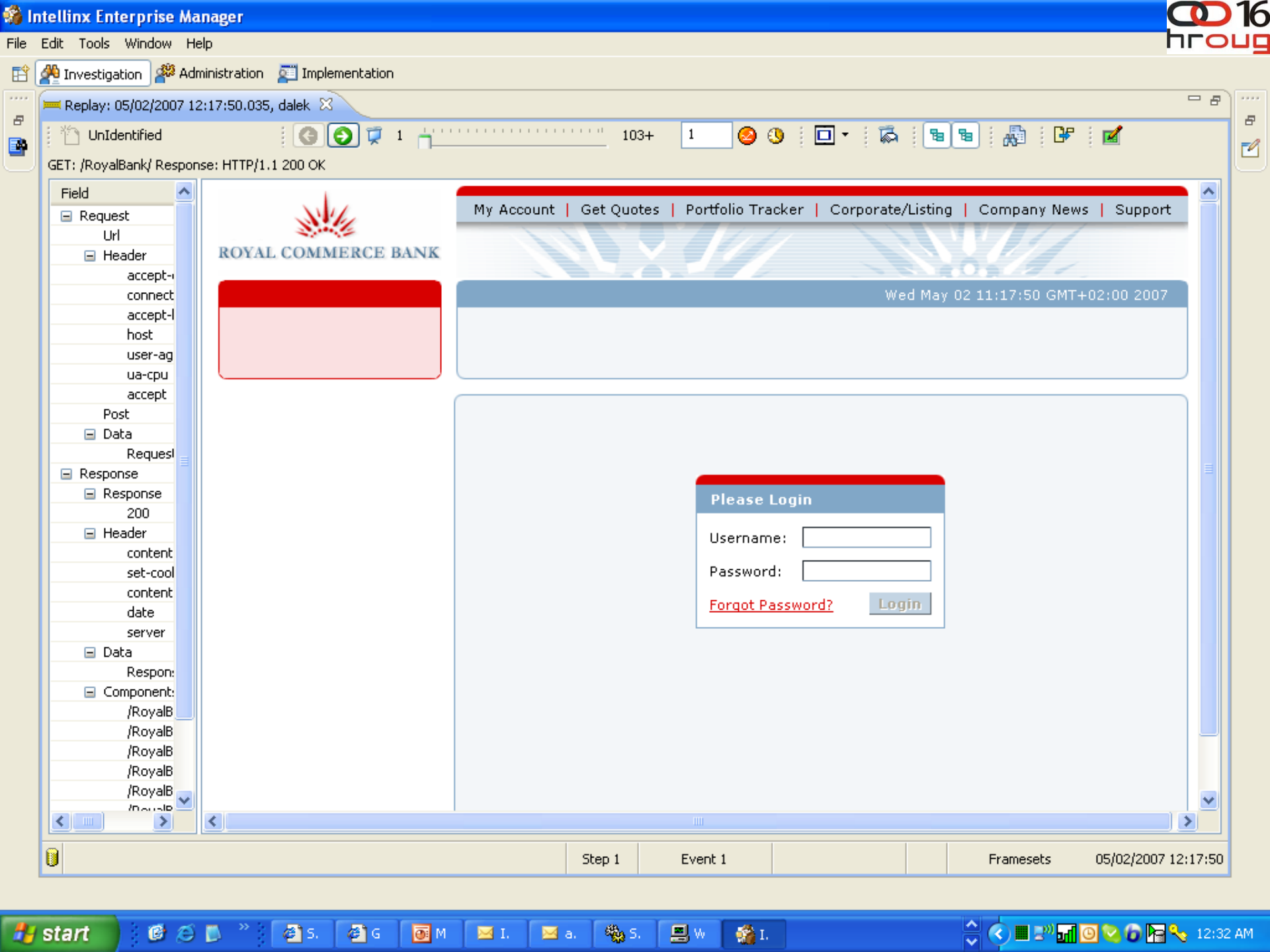

Solution Demonstration
Intellinx in Action

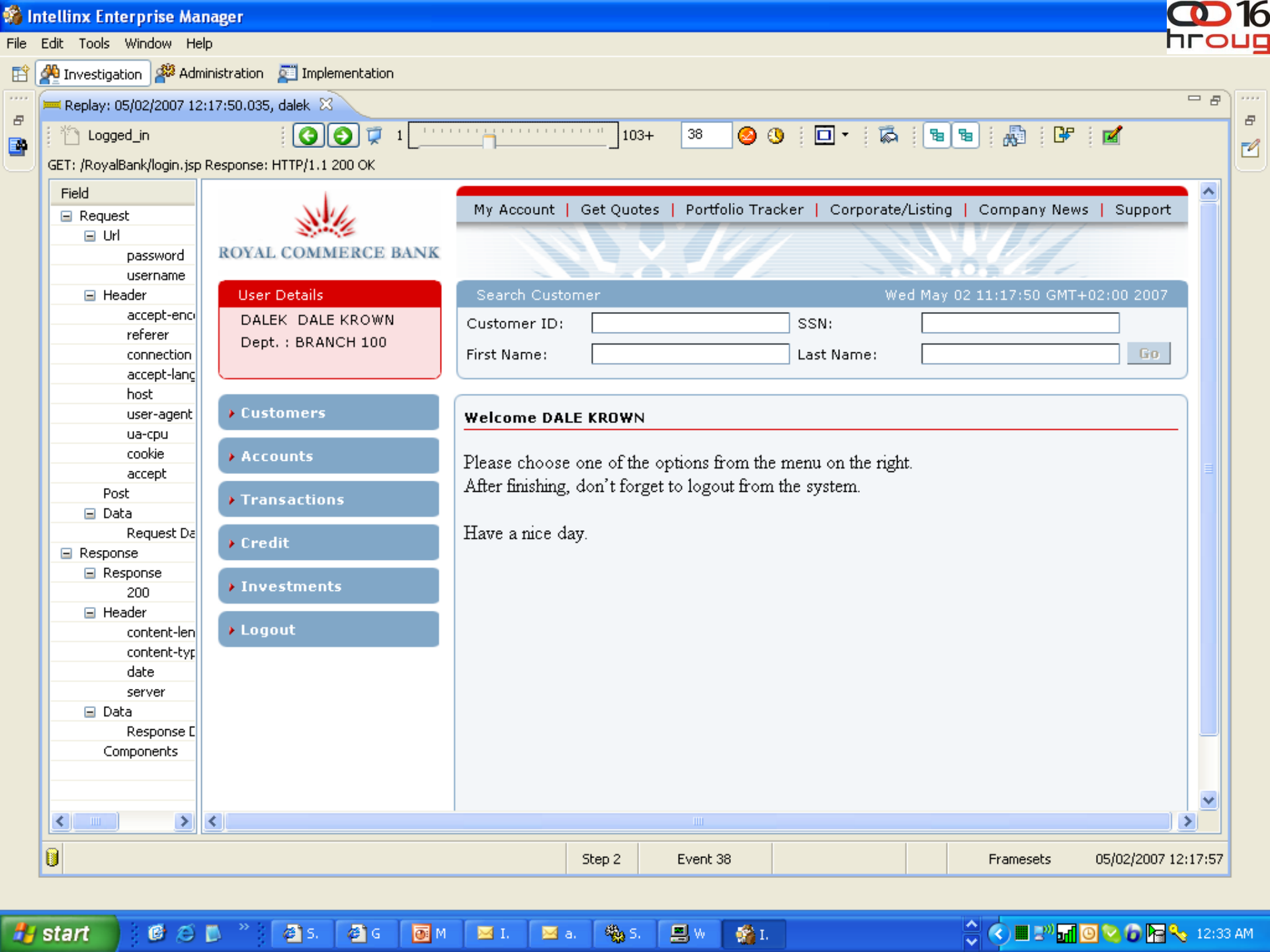

Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Reports
Reports
DemoBacklogViewer.1-MF_Privileged (05/06
DemoBacklogViewer.2-AccountCrossSearch
DemoBacklogViewer.3-MFScreens (05/06/2C
DemoBacklogViewer.4-Histogram (05/06/20(
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.ClientServer (05/06/20(
DemoBacklogViewer.DB (10/26/2009 17:36:
DemoBacklogViewer.EventViewerReport (01
DemoBacklogViewer.EventViewerReport1 (0
DemoBacklogViewer.FTP (11/03/2009 17:29
DemoBacklogViewer.Oracle_Command_on_t
DemoBacklogViewer.Oracle_cutsomer_name
DemoBacklogViewer.Oracle_user_id (11/03/
DemoBacklogViewer.session_34255DCDB75
DemoBacklogViewer.VT (11/03/2009 11:04:
DemoBacklogViewer.Web (02/16/2010 00:2
DemoBacklogViewer.WebMail (02/04/2010 1
DemoBacklogViewer.WindowsLog (11/03/20
Viewer.WebMail (08/03/2008 20:41:04)
DemoBacklogViewer.Web
Query configuration
Query type: Sessions
Viewer: DemoBacklogViewer
Data Channel: DemoWebDataChannel
In the last: 10 Years
Session state: All Active Closed
Date from: 05/02/2007
Time: 00 : 00 : 00
to: 05/02/2007
Time: 23 : 59 : 59
Time slice: between
and
Column Operator Value Display Alias Sort Order Sort Type
Session started
Session ended 1 Descending
Total event count
Client
Server
Search for Text:
Case Sensitive
Whole Word
Regular Expressions
Hex
Records per page: 50
Auto Refresh
Save Results
Export Results
Execute Query
Refresh Results
start
12:38 AM

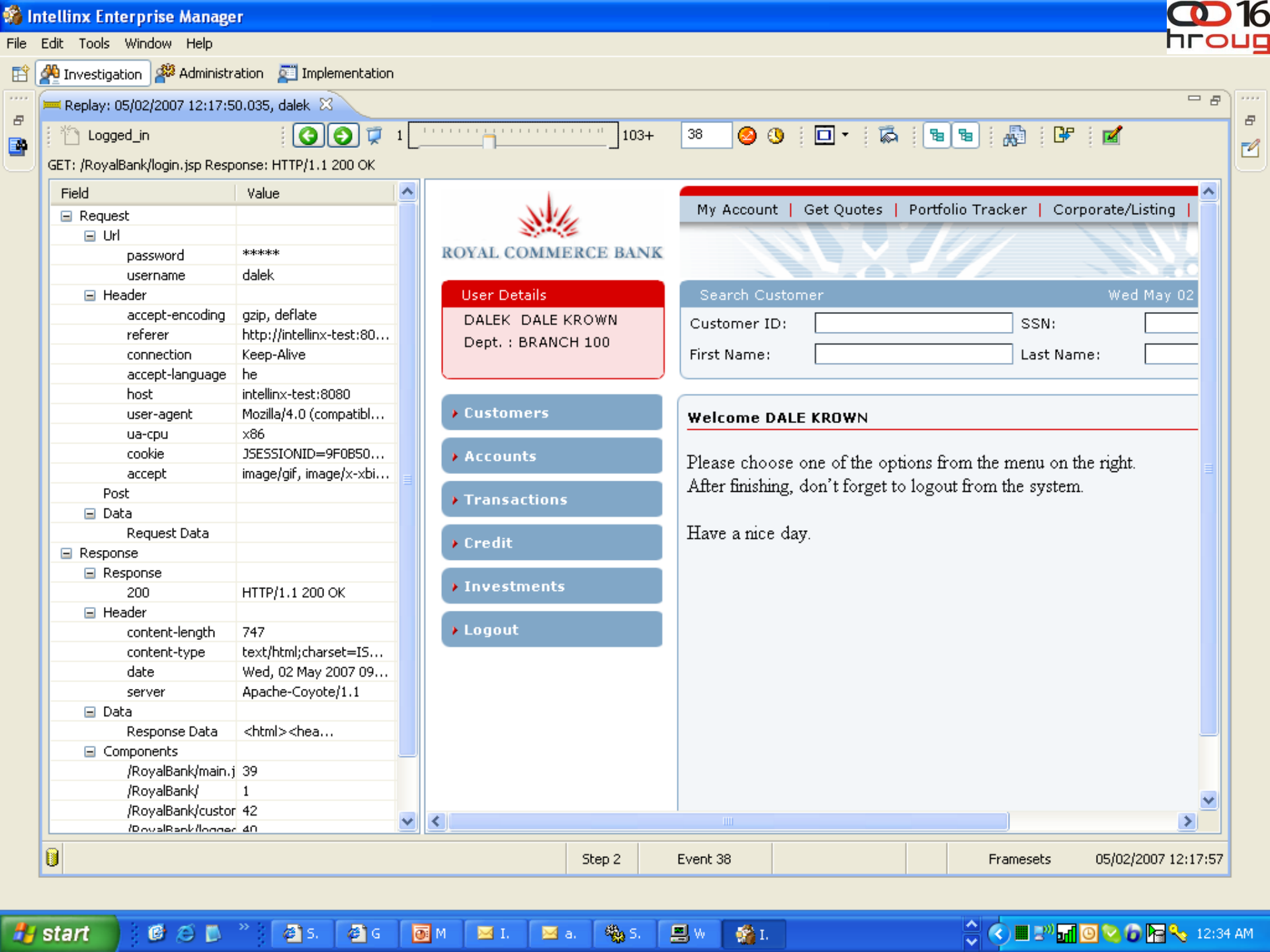

Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation
Administration
Implementation
Reports
Reports
DemoBacklogViewer.1-MF_Privileged (05/06
DemoBacklogViewer.2-AccountCrossSearch
DemoBacklogViewer.3-MFScreens (05/06/2C
DemoBacklogViewer.4-Histogram (05/06/20(
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.ClientServer (05/06/20(
DemoBacklogViewer.DB (10/26/2009 17:36:
DemoBacklogViewer.EventViewerReport (01
DemoBacklogViewer.EventViewerReport1 (0
DemoBacklogViewer.FTP (11/03/2009 17:29
DemoBacklogViewer.Oracle_Command_on_t
DemoBacklogViewer.Oracle_cutsomer_name
DemoBacklogViewer.Oracle_user_id (11/03/
DemoBacklogViewer.session_34255DCDB75
DemoBacklogViewer.VT (11/03/2009 11:04:
DemoBacklogViewer.Web (02/16/2010 00:2
DemoBacklogViewer.WebMail (02/04/2010 1
DemoBacklogViewer.WindowsLog (11/03/20
Viewer.WebMail (08/03/2008 20:41:04)
DemoBacklogViewer.Web
Query configuration
Query type: Sessions
Viewer: DemoBacklogViewer
Data Channel: DemoWebDataChannel
In the last: 10 Years
Date from: 05/02/2007
Time slice: between
Column
Operator
Session started
Session ended
Total event count
Client
Server
Search for Text:
Records per page: 50
Save Results
Export Results
Refresh Results
Hex
Closed
23 : 59 : 59
Select Data Channel/s
DemoWebDataChannel
DemoStructuredDataChannel
MSEventsDataChannel
DemoSOAPDataChannel
DemoFTPDataChannel
VTScreenDataChannel
DemoScreenDataChannel
DemoDRDADataChannel
DemoTDSDataChannel
DemoTNSDataChannel
Select All
Deselect All
OK
Cancel
start
12:38 AM

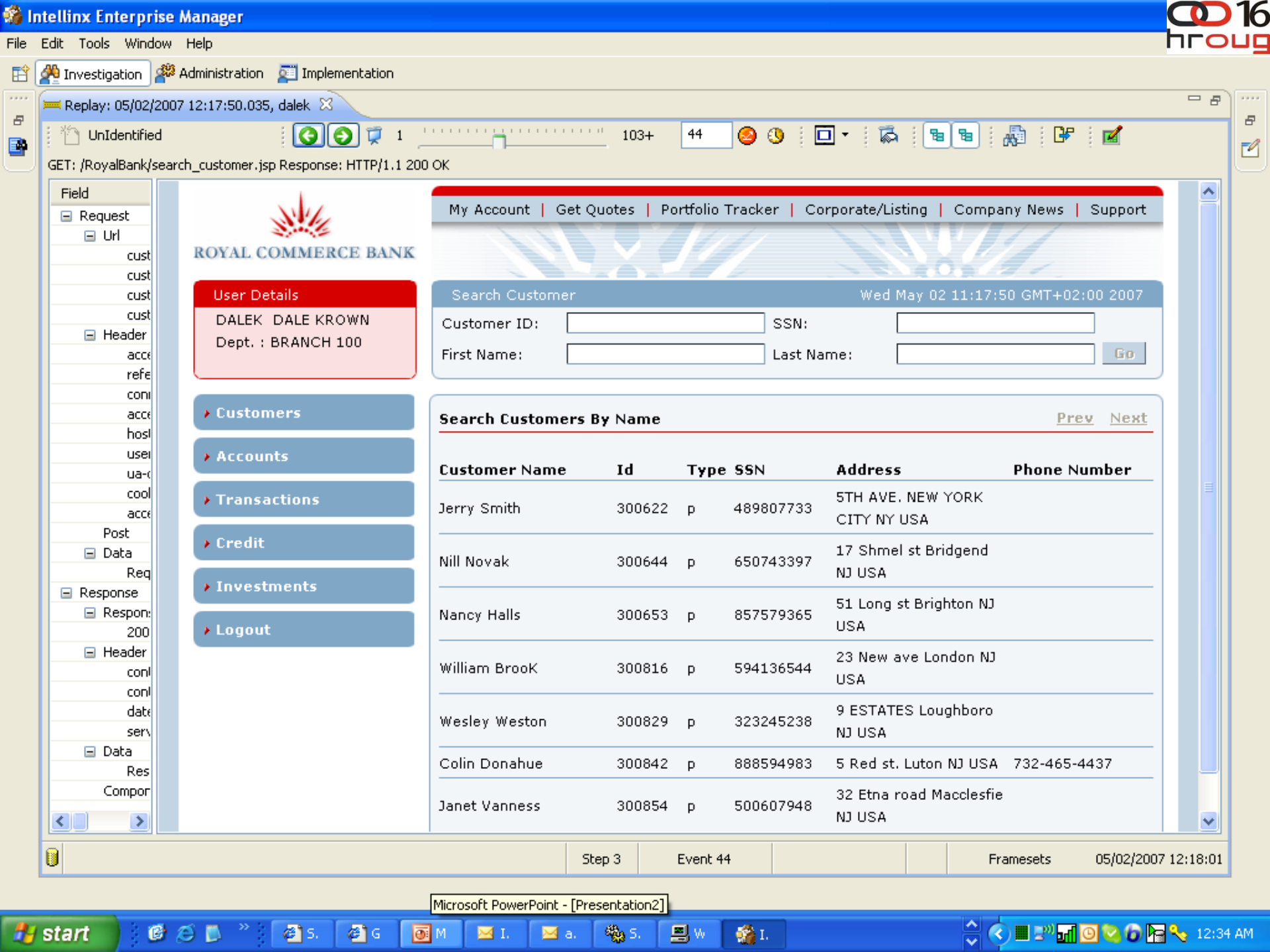

Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Reports
Reports
DemoBacklogViewer.1-MF_Privileged (05/06
DemoBacklogViewer.2-AccountCrossSearch
DemoBacklogViewer.3-MFScreens (05/06/2C
DemoBacklogViewer.4-Histogram (05/06/20(
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.ClientServer (05/06/20(
DemoBacklogViewer.DB (10/26/2009 17:36:
DemoBacklogViewer.EventViewerReport (01
DemoBacklogViewer.EventViewerReport1 (0
DemoBacklogViewer.FTP (11/03/2009 17:29
DemoBacklogViewer.Oracle_Command_on_t
DemoBacklogViewer.Oracle_cutsomer_name
DemoBacklogViewer.Oracle_user_id (11/03/
DemoBacklogViewer.session_34255DCDB75
DemoBacklogViewer.VT (11/03/2009 11:04:
DemoBacklogViewer.Web (02/16/2010 00:2
DemoBacklogViewer.WebMail (02/04/2010 1
DemoBacklogViewer.WindowsLog (11/03/20
Viewer.WebMail (08/03/2008 20:41:04)
*DemoBacklogViewer.Web
Query configuration
Query type: Sessions
Viewer: DemoBacklogViewer
Data Channel: DemoWebDataChannel
In the last: 10 Years
Session state: All Active Closed
Date from: 05/02/2007
Time: 00 : 00 : 00
to: 05/02/2007
Time: 23 : 59 : 59
Time slice: between
and
Column Operator Value Display Alias Sort Order Sort Type
Session started
Session ended 1 Descending
Total event count
Client
Server
Search for Text:
Case Sensitive
Whole Word
Regular Expressions
Hex
Records per page: 50
Auto Refresh
Save Results
Export Results
Extract Recordings
Execute Query
Refresh Results
UserId Session started Session ended Total event count Client Server Data Channel Name
1 pamw 05/02/2007 12:23:14 05/02/2007 12:25:11 128 192.168.1.146 192.168.1.27 DemoWebDataChannel
2 pamw 05/02/2007 12:20:55 05/02/2007 12:22:04 102 192.168.1.104 192.168.1.27 DemoWebDataChannel
3 dalek 05/02/2007 12:17:50 05/02/2007 12:18:45 103 192.168.1.104 192.168.1.27 DemoWebDataChannel
4 dalek 05/02/2007 12:13:08 05/02/2007 12:14:32 127 192.168.1.146 192.168.1.27 DemoWebDataChannel
5 dalek 05/02/2007 12:02:15 05/02/2007 12:03:50 127 0.0.0.0 192.168.1.27 DemoWebDataChannel
6 bartm 05/02/2007 11:45:22 05/02/2007 11:47:55 115 0.0.0.0 192.168.1.27 DemoWebDataChannel
7 pamw 05/02/2007 11:38:00 05/02/2007 11:42:55 113 0.0.0.0 192.168.1.27 DemoWebDataChannel
8 jerrym 05/02/2007 11:34:12 05/02/2007 11:36:27 113 0.0.0.0 192.168.1.27 DemoWebDataChannel
9 johnk 05/02/2007 11:27:06 05/02/2007 11:30:52 83 0.0.0.0 192.168.1.27 DemoWebDataChannel
1 - 12
of 12 records
start
12:44 AM

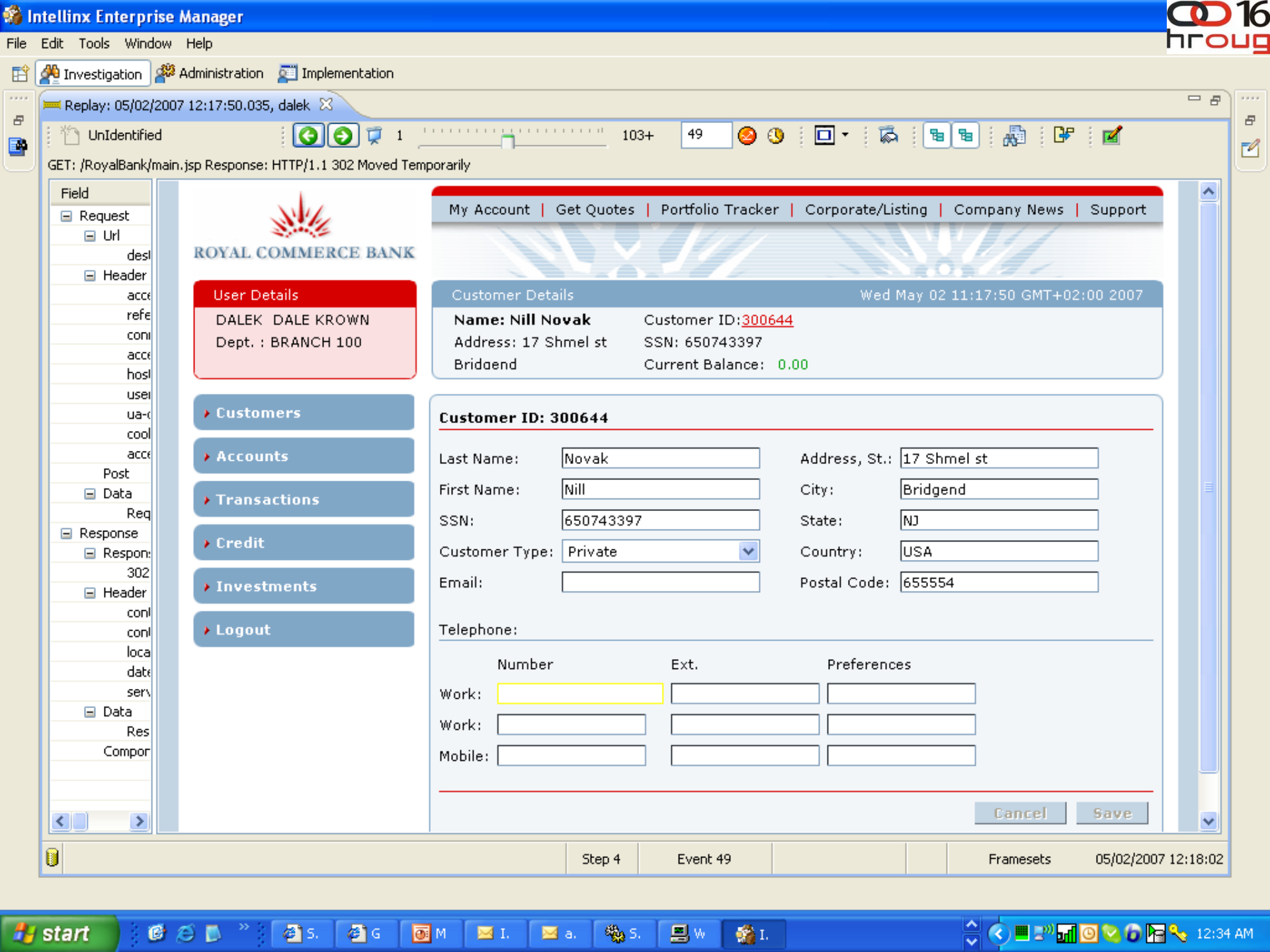

Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Reports
Reports
DemoBacklogViewer.1-MF_Privileged (05/06
DemoBacklogViewer.2-AccountCrossSearch
DemoBacklogViewer.3-MFScreens (05/06/2C
DemoBacklogViewer.4-Histogram (05/06/20(
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.audit_events_in_sessio
DemoBacklogViewer.ClientServer (05/06/20(
DemoBacklogViewer.DB (10/26/2009 17:36:
DemoBacklogViewer.EventViewerReport (01
DemoBacklogViewer.EventViewerReport1 (0
DemoBacklogViewer.FTP (11/03/2009 17:29
DemoBacklogViewer.Oracle_Command_on_t
DemoBacklogViewer.Oracle_cutsomer_name
DemoBacklogViewer.Oracle_user_id (11/03/
DemoBacklogViewer.session_34255DCDB75
DemoBacklogViewer.VT (11/03/2009 11:04:
DemoBacklogViewer.Web (02/16/2010 00:2
DemoBacklogViewer.WebMail (02/04/2010 1
DemoBacklogViewer.WindowsLog (11/03/20
Viewer.WebMail (08/03/2008 20:41:04)
DemoBackl
Query configuration
Query type: Sessions
In the last: 10
Date from: 05/02/
Time slice:
Column
Session started
Session ended
Total event count
Client
Server
Search for Text:
Records per page: 50
Save Results
Export Resu
UserId Session s
1 pamw 05/02/20(
2 pamw 05/02/20(
3 dalek 05/02/20(
4 dalek 05/02/20(
5 dalek 05/02/20(
6 bartm 05/02/20(
7 pamw 05/02/20(
8 jerrym 05/02/20(
9 johnk 05/02/20(
1 - 12
Replay: 05/02/2007 12:17:50.035, dalek
UnIdentified
1
103+
1
GET: /RoyalBank/ Response: HTTP/1.1 200 OK
Field
Request
Url
Header
accept-encc
connection
accept-lang
host
user-agent
ua-cpu
accept
Post
Data
Request Da
Response
Response
200
Header
content-len
set-cookie
content-typ
date
server
Data
Response D
Components
/RoyalBank
/RoyalBank
/RoyalBank
ROYAL COMMERCE BANK
My Account | Get Quotes | P
Step 1
Event 1
Fra...ets
start
12:39 AM


Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Replay: 05/02/2007 12:17:50.035, dalek
UnIdentified
GET: /RoyalBank/ Response: HTTP/1.1 200 OK
Field
Request
Url
Header
Post
Data
Response
Response
200
Header
Data
Component
ROYAL COMMERCE BANK
My Account | Get Quotes | Portfolio Tracker | Corporate/Listing | Company News | Support
Wed May 02 11:17:50 GMT+02:00 2007
Please Login
Username:
Password:
Forgot Password?
Login
Step 1
Event 1
Framesets
05/02/2007 12:17:50
start
12:32 AM


Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Replay: 05/02/2007 12:17:50.035, dalek
Logged_in
GET: /RoyalBank/login.jsp Response: HTTP/1.1 200 OK
Field
Request
Url
password
username
Header
referer
connection
host
user-agent
cookie
accept
Post
Data
Response
Response
200
Header
date
server
Data
Components
ROYAL COMMERCE BANK
My Account | Get Quotes | Portfolio Tracker | Corporate/Listing | Company News | Support
User Details
DALEK DALE KROWN
Dept. : BRANCH 100
Search Customer
Wed May 02 11:17:50 GMT+02:00 2007
Customer ID:
SSN:
First Name:
Last Name:
Go
Customers
Accounts
Transactions
Credit
Investments
Logout
Welcome DALE KROWN
Please choose one of the options from the menu on the right.
After finishing, don't forget to logout from the system.
Have a nice day.
Step 2
Event 38
Framesets
05/02/2007 12:17:57
start
12:33 AM


Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Replay: 05/02/2007 12:17:50.035, dalek
Logged_in
GET: /RoyalBank/login.jsp Response: HTTP/1.1 200 OK
Field Value
Request
Url
password *****
username dalek
Header
accept-encoding gzip, deflate
referer http://intellinx-test:80...
connection Keep-Alive
accept-language he
host intellinx-test:8080
user-agent Mozilla/4.0 (compatibl...
ua-cpu x86
cookie JSESSIONID=9F0B50...
accept image/gif, image/x-xbi...
Post
Data
Request Data
Response
Response
200 HTTP/1.1 200 OK
Header
content-length 747
content-type text/html;charset=IS...
date Wed, 02 May 2007 09...
server Apache-Coyote/1.1
Data
Response Data <html><hea...
Components
/RoyalBank/main.j 39
/RoyalBank/ 1
/RoyalBank/custor 42
ROYAL COMMERCE BANK
My Account | Get Quotes | Portfolio Tracker | Corporate/Listing |
User Details
DALEK DALE KROWN
Dept. : BRANCH 100
Search Customer
Wed May 02
Customer ID:
SSN:
First Name:
Last Name:
Customers
Accounts
Transactions
Credit
Investments
Logout
Welcome DALE KROWN
Please choose one of the options from the menu on the right.
After finishing, don't forget to logout from the system.
Have a nice day.
Step 2
Event 38
Framesets
05/02/2007 12:17:57
start
12:34 AM


Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Replay: 05/02/2007 12:17:50.035, dalek
UnIdentified
GET: /RoyalBank/search_customer.jsp Response: HTTP/1.1 200 OK
Field
Request
Url
Header
Post
Data
Response
Header
Data
ROYAL COMMERCE BANK
My Account | Get Quotes | Portfolio Tracker | Corporate/Listing | Company News | Support
User Details
DALEK DALE KROWN
Dept. : BRANCH 100
Search Customer
Wed May 02 11:17:50 GMT+02:00 2007
Customer ID:
SSN:
First Name:
Last Name:
Go
Customers
Accounts
Transactions
Credit
Investments
Logout
Search Customers By Name
Prev Next
Customer Name Id Type SSN Address Phone Number
Jerry Smith 300622 p 489807733 5TH AVE. NEW YORK CITY NY USA
Nill Novak 300644 p 650743397 17 Shmel st Bridgend NJ USA
Nancy Halls 300653 p 857579365 51 Long st Brighton NJ USA
William BrooK 300816 p 594136544 23 New ave London NJ USA
Wesley Weston 300829 p 323245238 9 ESTATES Loughboro NJ USA
Colin Donahue 300842 p 888594983 5 Red st. Luton NJ USA 732-465-4437
Janet Vanness 300854 p 500607948 32 Etna road Macclesfie NJ USA
Step 3
Event 44
Framesets
05/02/2007 12:18:01
Microsoft PowerPoint - [Presentation2]
start
12:34 AM


Intellinx Enterprise Manager
File Edit Tools Window Help
Investigation Administration Implementation
Replay: 05/02/2007 12:17:50.035, dalek
UnIdentified
GET: /RoyalBank/main.jsp Response: HTTP/1.1 302 Moved Temporarily
Field
Request
Response
ROYAL COMMERCE BANK
My Account | Get Quotes | Portfolio Tracker | Corporate/Listing | Company News | Support
User Details
DALEK DALE KROWN
Dept. : BRANCH 100
Customer Details
Wed May 02 11:17:50 GMT+02:00 2007
Name: Nill Novak
Customer ID:300644
Address: 17 Shmel st
SSN: 650743397
Bridgend
Current Balance: 0.00
Customers
Accounts
Transactions
Credit
Investments
Logout
Customer ID: 300644
Last Name: Novak
First Name: Nill
SSN: 650743397
Customer Type: Private
Email:
Address, St.: 17 Shmel st
City: Bridgend
State: NJ
Country: USA
Postal Code: 655554
Telephone:
Number
Ext.
Preferences
Work:
Work:
Mobile:
Cancel
Save
Step 4
Event 49
Framesets
05/02/2007 12:18:02
start
12:34 AM

Case #1 Demo:
Stealing from Dormant Accounts

How can we Automatically detect the Red Flags and avoid false alerts?

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/Inves

Intellinx Inves

Cases Alerts Repo

Alerts

Alert 00016

Alert

Alert #:	00016
Type:	User High Sc
Source:	Rule Engine
Employee:	jerrym
Account:	
Description:	Dormant Acc

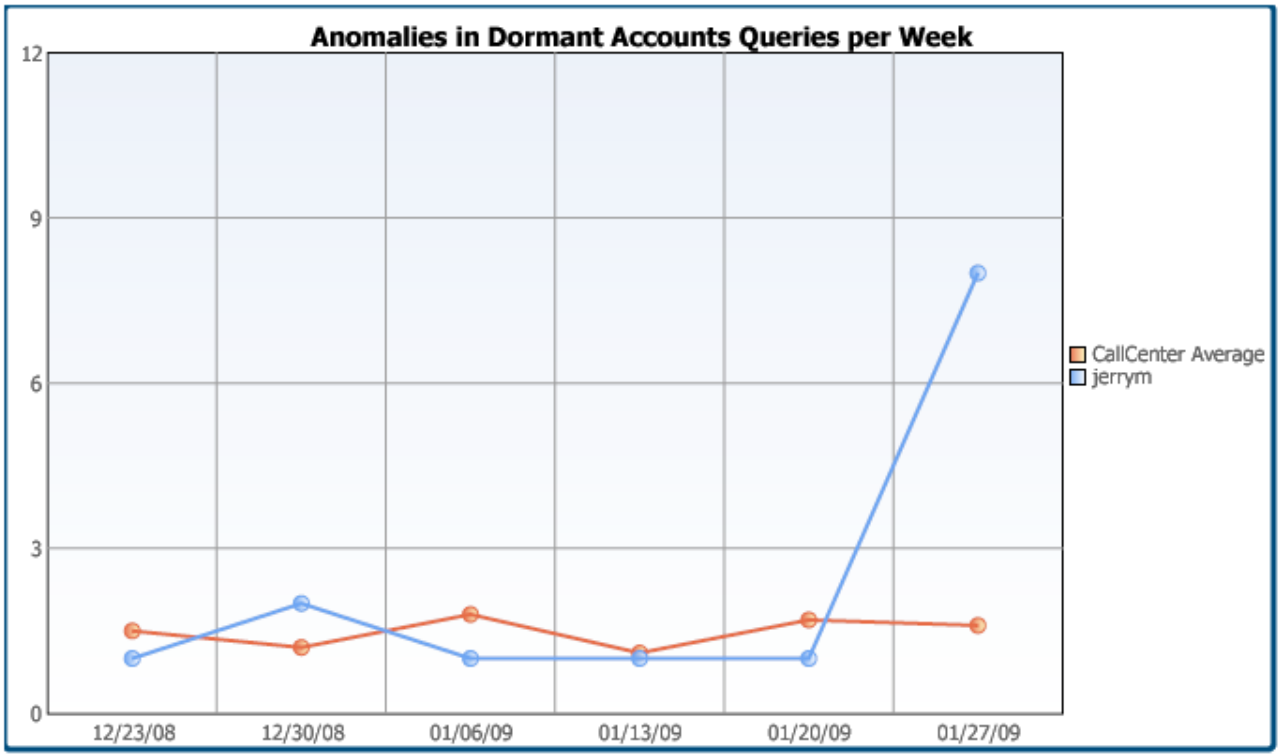
Related Issues

	id	Account Id								
Details	00001	5180495								
Details	00002	5180505								
Details	00003	5180564	00016	300560	Dormant Account Query	23/01/09 13:22	RULE01.2	10	23/01/09 13:18	jerrym
Details	00004	5180524	00016	300520	Dormant Account Query	24/01/09 11:13	RULE01.2	10	24/01/09 11:10	jerrym
Details	00005	5180535	00016	300531	Dormant Account Query	25/01/09 10:02	RULE01.2	10	25/01/09 10:00	jerrym

Trusted sites

Viewer - Microsoft Internet Explorer

Intellinx Investigation Center



Done

Trusted sites

start

I. M V.

2:20 AM

Intellinx Investigation Center

Alert 00016

Alert Details

Alert #:	00016	**Owner:**	Insider Fraud Team
Type:	User High Score	**Date:**	01/27/09 08:33
Origin:	Rule Engine	**Score:**	112
Employee:	jerrym		
Account:		**Customer:**	
Description:	Dormant Account Handling by User		

jerrym
- Link Analysis: Dormant Account Access
- Link Analysis: Employees-Accounts

Notes

Total 1 records

Note type	Text	Private
General	The employee has disciplinary issues	☐

Related Issues

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleList.jsf?conversationContext=e

Go Links

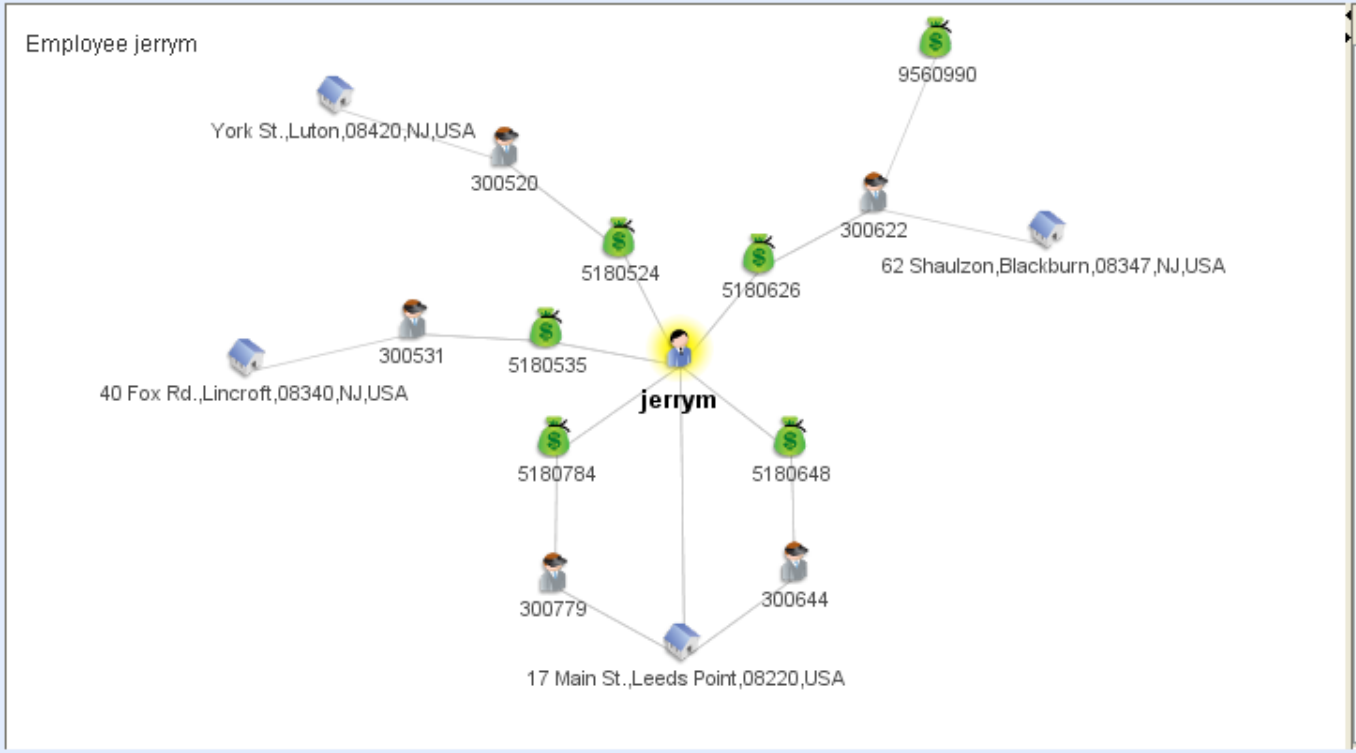
Intellinx Investigation Center

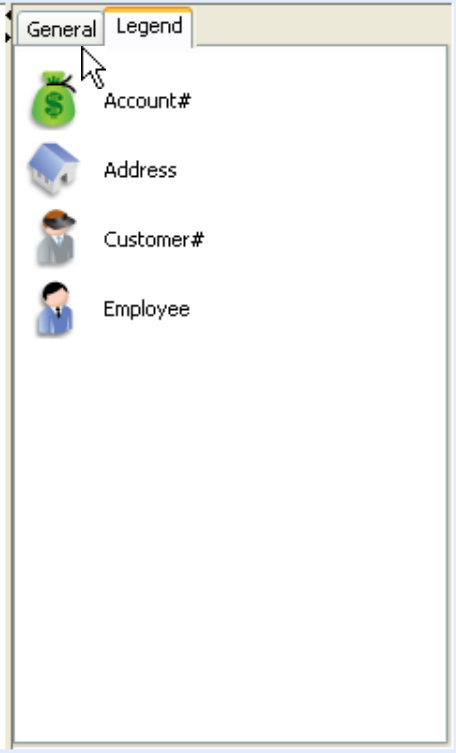
Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access





Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Trusted sites

start

7:27 PM

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleList.jsf?conversationContext=e

Go Links

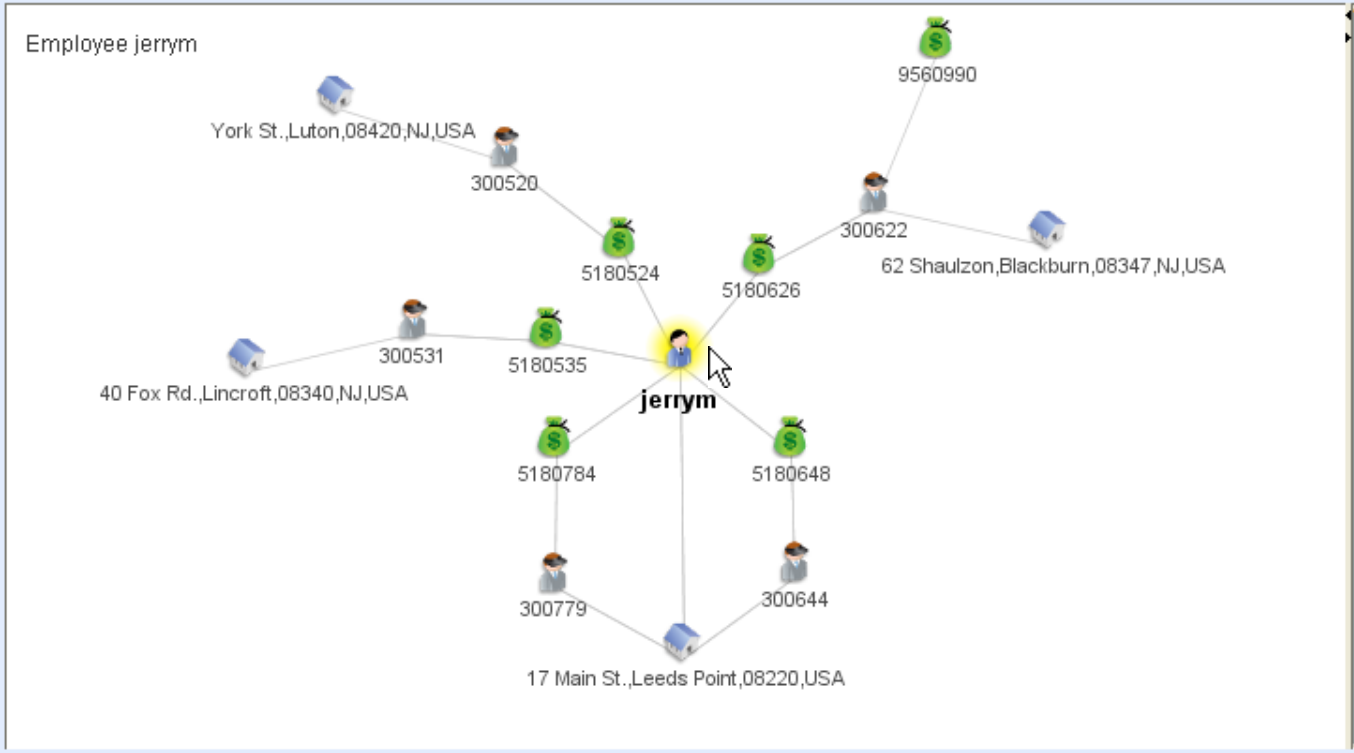
Intellinx Investigation Center

Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access



General | Legend

Start date: 01/24/2009

End date: 01/30/2009

Depth: 3

Show Risk Coloring:

- From Low to High
- Medium and High
- High only
- None

Auto Fit | 1:1

Refresh

Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Trusted sites

start 7:27 PM

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleList.jsf?conversationContext=e

Go Links

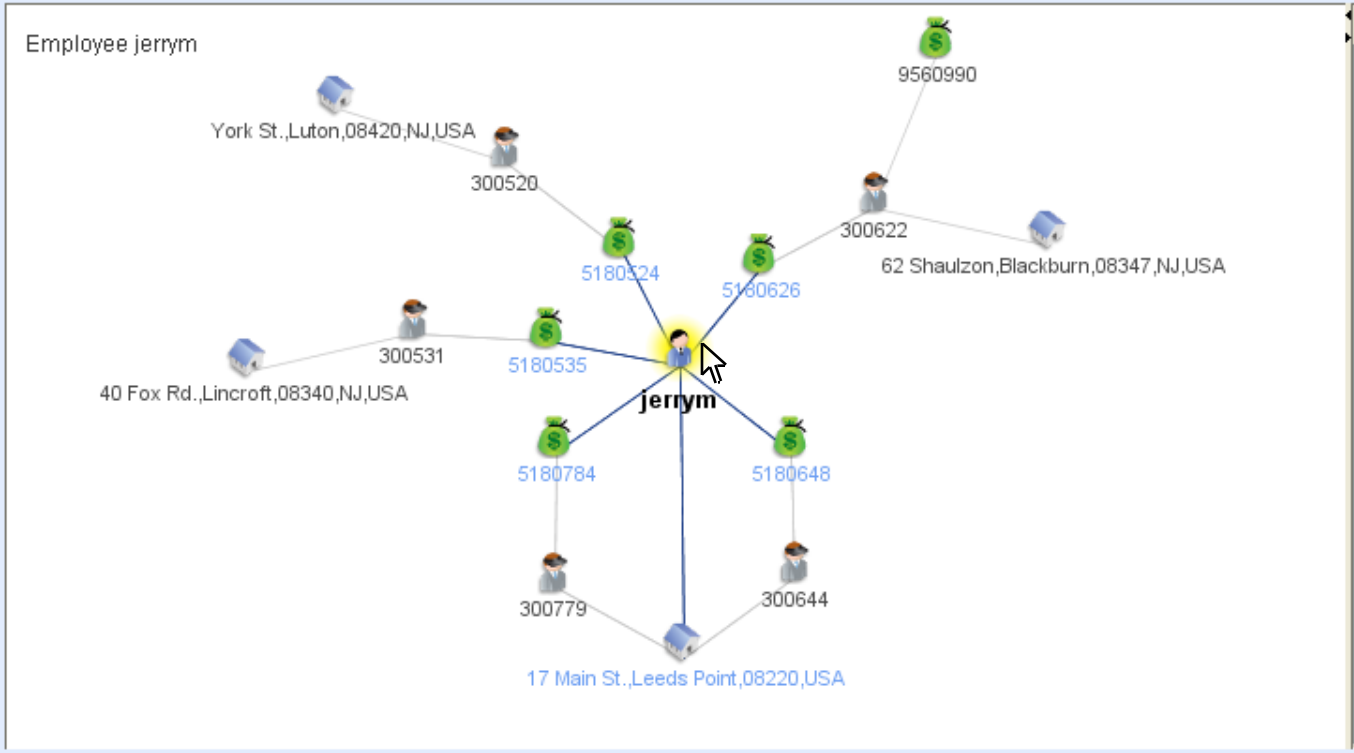
Intellinx Investigation Center

Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access



General | Legend

Account#

Address

Customer#

Employee

Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Trusted sites

start

7:28 PM

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleList.jsf?conversationContext=e

Go Links

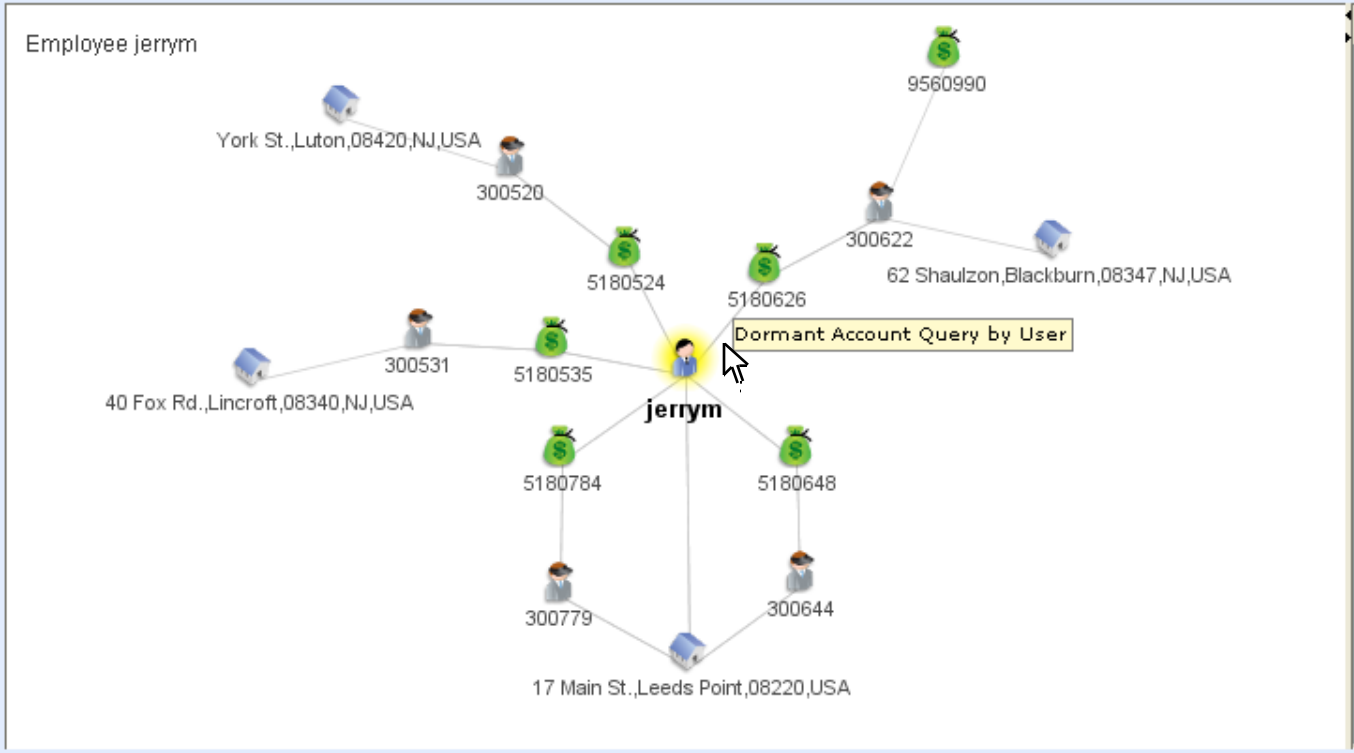
Intellinx Investigation Center

Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access



Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Trusted sites

start

7:44 PM

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleList.jsf?conversationContext=e

Go Links

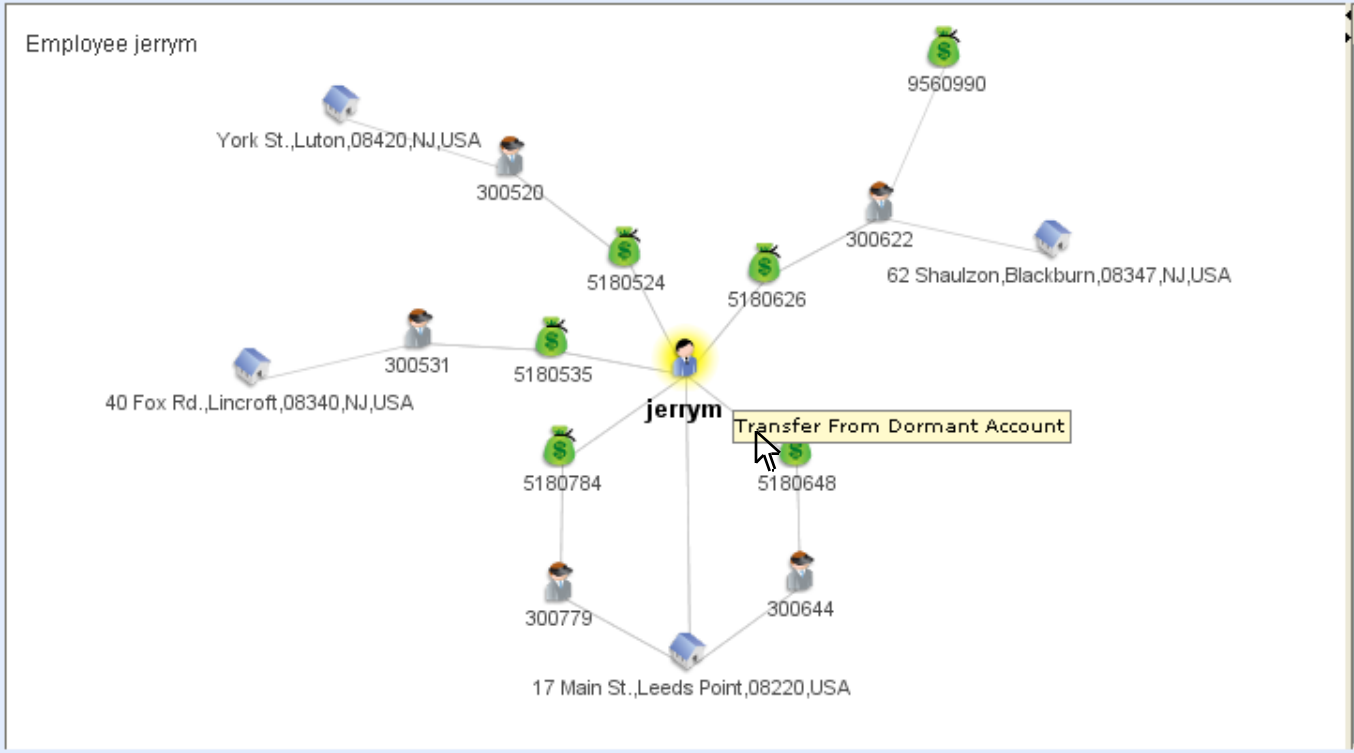
Intellinx Investigation Center

Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access



General | Legend

Account#

Address

Customer#

Employee

Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Trusted sites

start

7:44 PM

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleList.jsf?conversationContext=e

Go Links

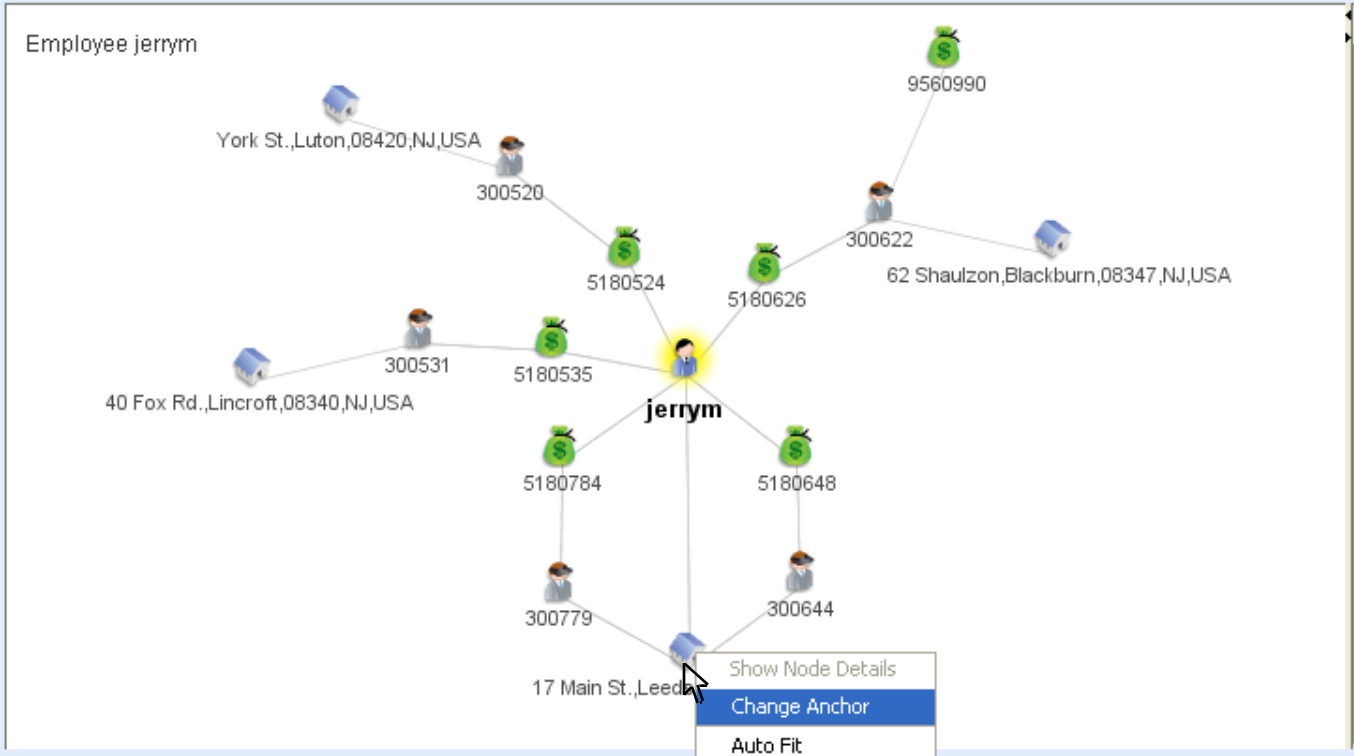
Intellinx Investigation Center

Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access



Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Java Applet Window

Trusted sites

start

7:45 PM

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleDetails.jsf?conversationContext=o

Go Links

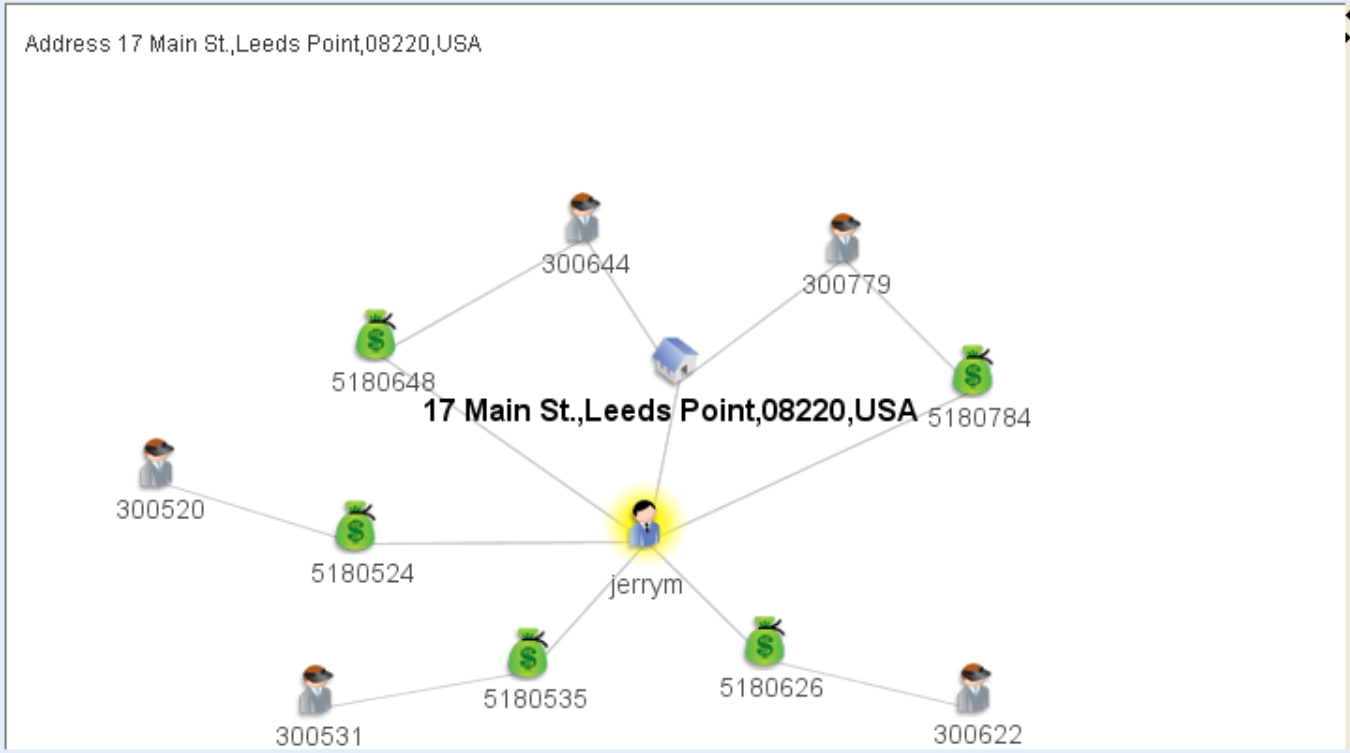
Intellinx Investigation Center

Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access



Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Trusted sites

start

8:27 PM

Investigation Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://localhost:7780/InvestigationCenter/pages/module/ModuleDetails.jsf?conversationContext=o

Go Links

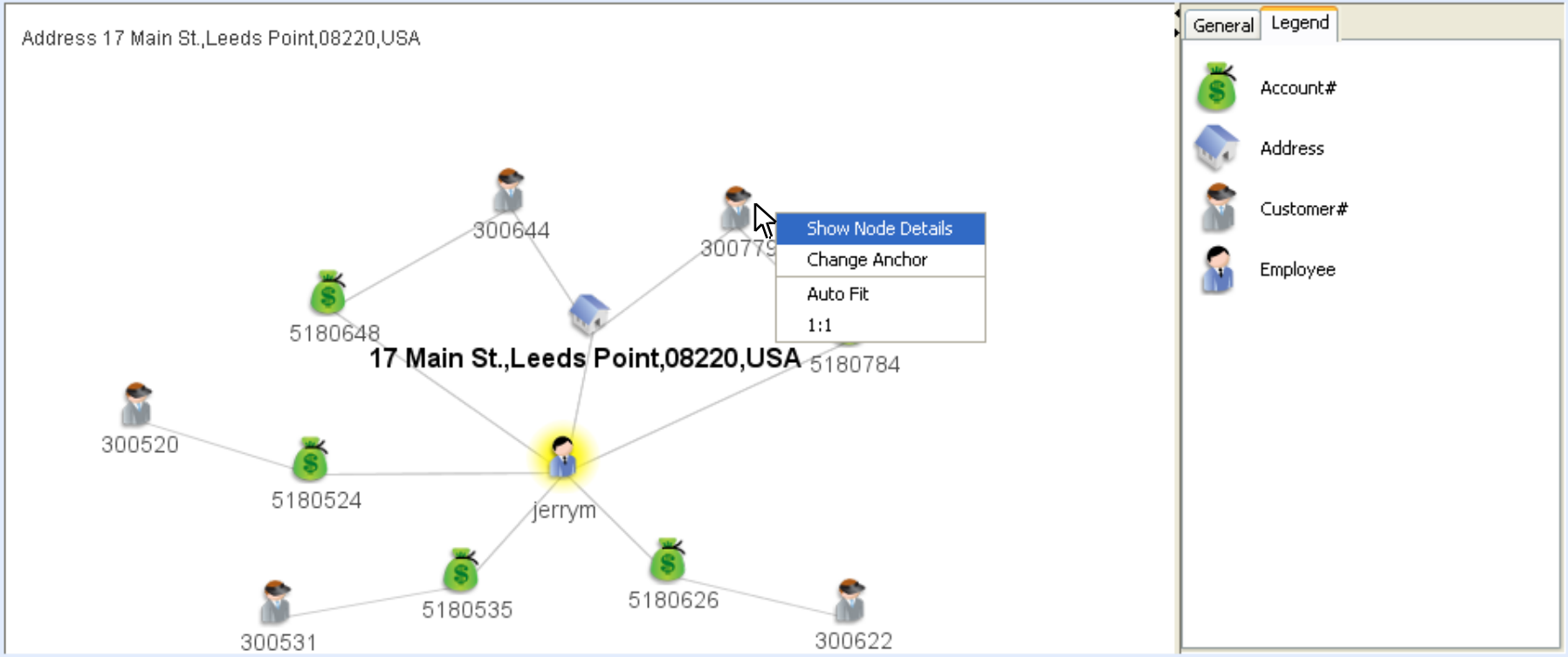
Intellinx Investigation Center

Administration | About | Logoff (Administrator Administrator)

Home | Cases | Alerts | Reports | Dashboards | Search | Rules

Alerts

Link Analysis: Dormant Account Access



Applet com.intellinx.ic.linkanalysis.applet.LinkAnalysisGraphApplet started

Trusted sites

start

8:31 PM

Customer# 300779

Link Analysis: Dormant Account Access

Customer #:	300779
Full Name:	Harris Beth
SSN:	191-22-4465
Address:	17 Main St.,Leeds Point,08220,USA

Accessing Customer Account

Changing Customer Address

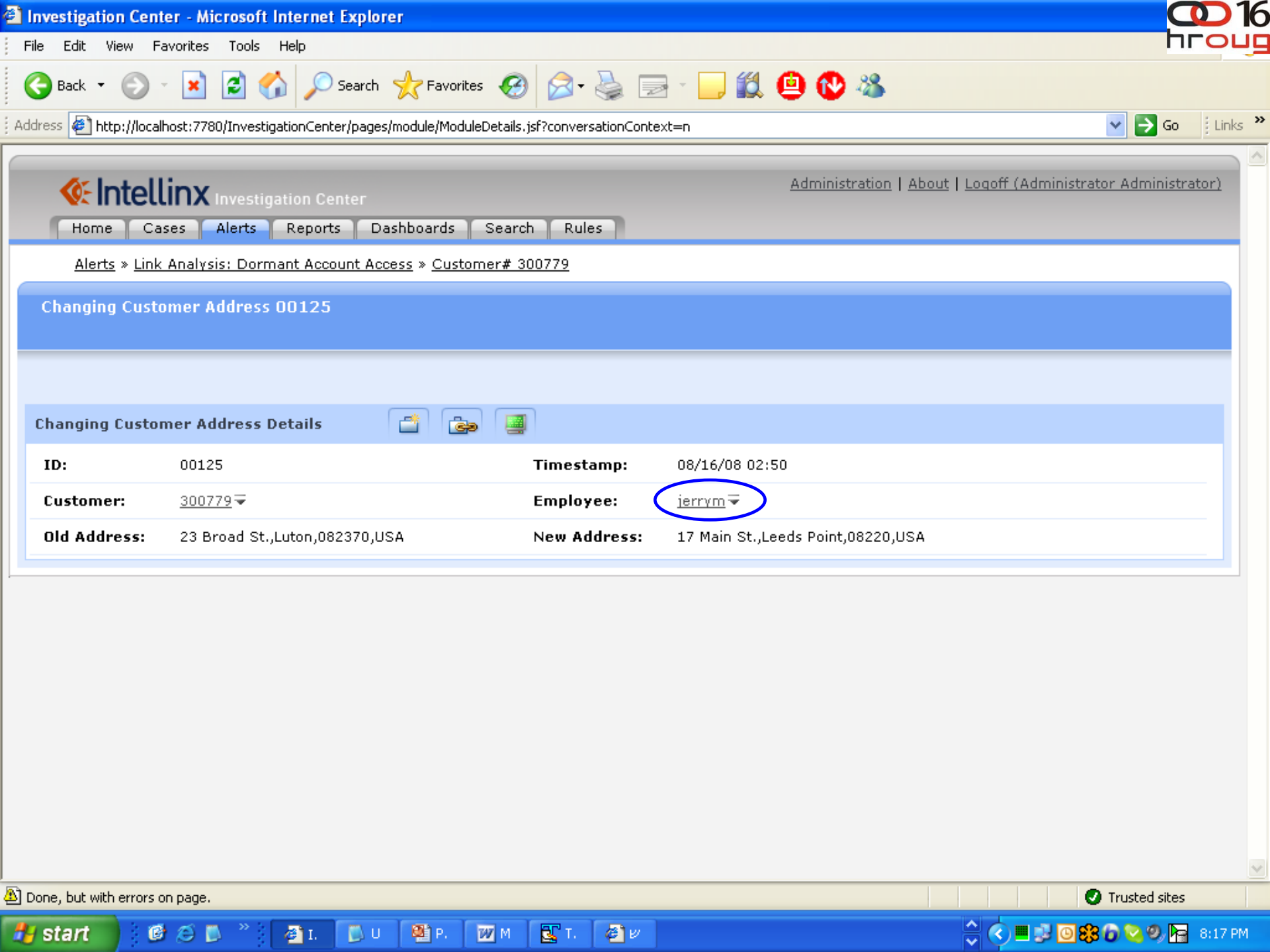
Total 1 records

Timestamp	Customer	Old Address	New Address
08/16/08 02:50	300779	23 Broad St.,Luton,082370,USA	17 Main St.,Leeds Point,08220,USA

Related Issues

Total 1 records

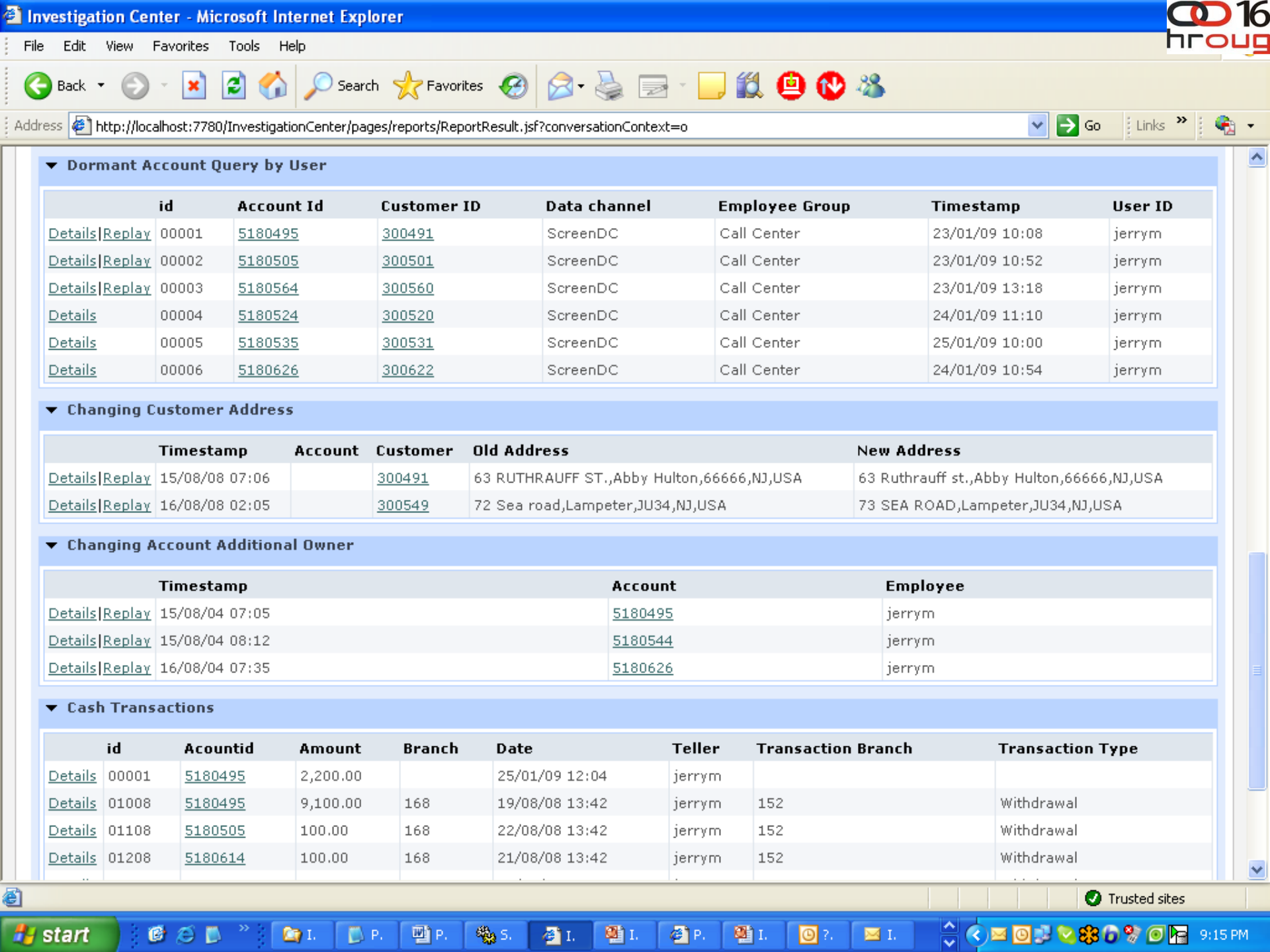
id	Rule ID	Description	Score	Detected At	Customer ID	Account Id	User ID


Investigation Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:7780/InvestigationCenter/pages/module/ModuleDetails.jsf?conversationContext=n
Go Links
Intellinx Investigation Center
Administration | About | Logoff (Administrator Administrator)
Home Cases Alerts Reports Dashboards Search Rules
Alerts » Link Analysis: Dormant Account Access » Customer# 300779
Changing Customer Address 00125
Changing Customer Address Details
ID: 00125
Timestamp: 08/16/08 02:50
Customer: 300779
Employee: jerrym
Old Address: 23 Broad St.,Luton,082370,USA
New Address: 17 Main St.,Leeds Point,08220,USA
Done, but with errors on page.
Trusted sites
start
8:17 PM

Case: Profiling of Call Centre Agents

Normal Behavior: Call-Centre Representative receives customer call; accesses customer data on mainframe

Intellinx Detects Suspicious Behavior: Call-Centre Representative accesses customer data on mainframe without prior receipt of a call


Investigation Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:7780/InvestigationCenter/pages/reports/ReportResult.jsf?conversationContext=o
Go Links
Dormant Account Query by User
id Account Id Customer ID Data channel Employee Group Timestamp User ID
Details|Replay 00001 5180495 300491 ScreenDC Call Center 23/01/09 10:08 jerrym
Details|Replay 00002 5180505 300501 ScreenDC Call Center 23/01/09 10:52 jerrym
Details|Replay 00003 5180564 300560 ScreenDC Call Center 23/01/09 13:18 jerrym
Details 00004 5180524 300520 ScreenDC Call Center 24/01/09 11:10 jerrym
Details 00005 5180535 300531 ScreenDC Call Center 25/01/09 10:00 jerrym
Details 00006 5180626 300622 ScreenDC Call Center 24/01/09 10:54 jerrym
Changing Customer Address
Timestamp Account Customer Old Address New Address
Details|Replay 15/08/08 07:06 300491 63 RUTHRAUFF ST.,Abby Hulton,66666,NJ,USA 63 Ruthrauff st.,Abby Hulton,66666,NJ,USA
Details|Replay 16/08/08 02:05 300549 72 Sea road,Lampeter,JU34,NJ,USA 73 SEA ROAD,Lampeter,JU34,NJ,USA
Changing Account Additional Owner
Timestamp Account Employee
Details|Replay 15/08/04 07:05 5180495 jerrym
Details|Replay 15/08/04 08:12 5180544 jerrym
Details|Replay 16/08/04 07:35 5180626 jerrym
Cash Transactions
id Acountid Amount Branch Date Teller Transaction Branch Transaction Type
Details 00001 5180495 2,200.00 25/01/09 12:04 jerrym
Details 01008 5180495 9,100.00 168 19/08/08 13:42 jerrym 152 Withdrawal
Details 01108 5180505 100.00 168 22/08/08 13:42 jerrym 152 Withdrawal
Details 01208 5180614 100.00 168 21/08/08 13:42 jerrym 152 Withdrawal
Trusted sites
start
9:15 PM