observe it
people audit

# ObserveIT:
# User Activity Monitoring

## “You don’t know what you don’t know!”

besecure
Managed E-Business Security™

www.observeit.com

# Quick Overview of BESECURE

besecure
Managed E-Business Security™

- **Established :** 2006 **Regional Offices :** Athens, Greece & Nicosia, Cyprus
- **Client base :** Large & Enterprise Government, Financial, Insurance, Telecom, Utilities and Business Services companies throughout Southeastern Europe and Middle East.
- **Products and Services Portfolio**
  - Governance, Risk, and Compliance Services
  - Enterprise Security Solutions
  - Cloud Security Services
  - Training & Awareness Programs

- **Why us**
  - Trusted Security Services & Solutions Provider
  - Commitment to Quality
  - Customer-Focused Approach
  - Experience and Expertise
  - Innovation

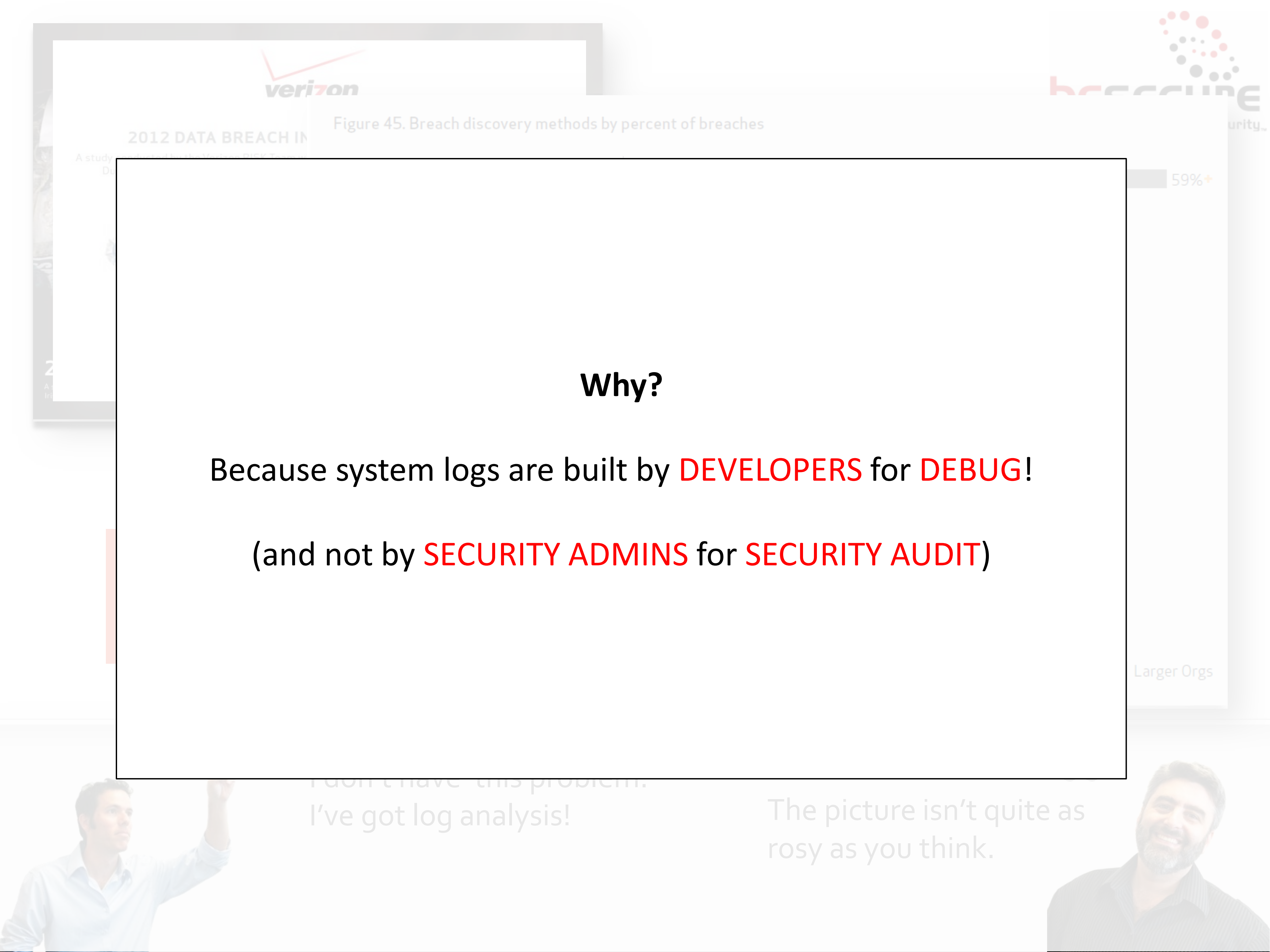
TÜV AUSTRIA HELLAS EN ISO 27001:2005

CERTIFIED IQNet MANAGEMENT SYSTEM

Quality Management DQS ISO 9001:2008

Companies invest in access control
but once users gain access,
there is **little knowledge** of
**who they are** and **what they do**!

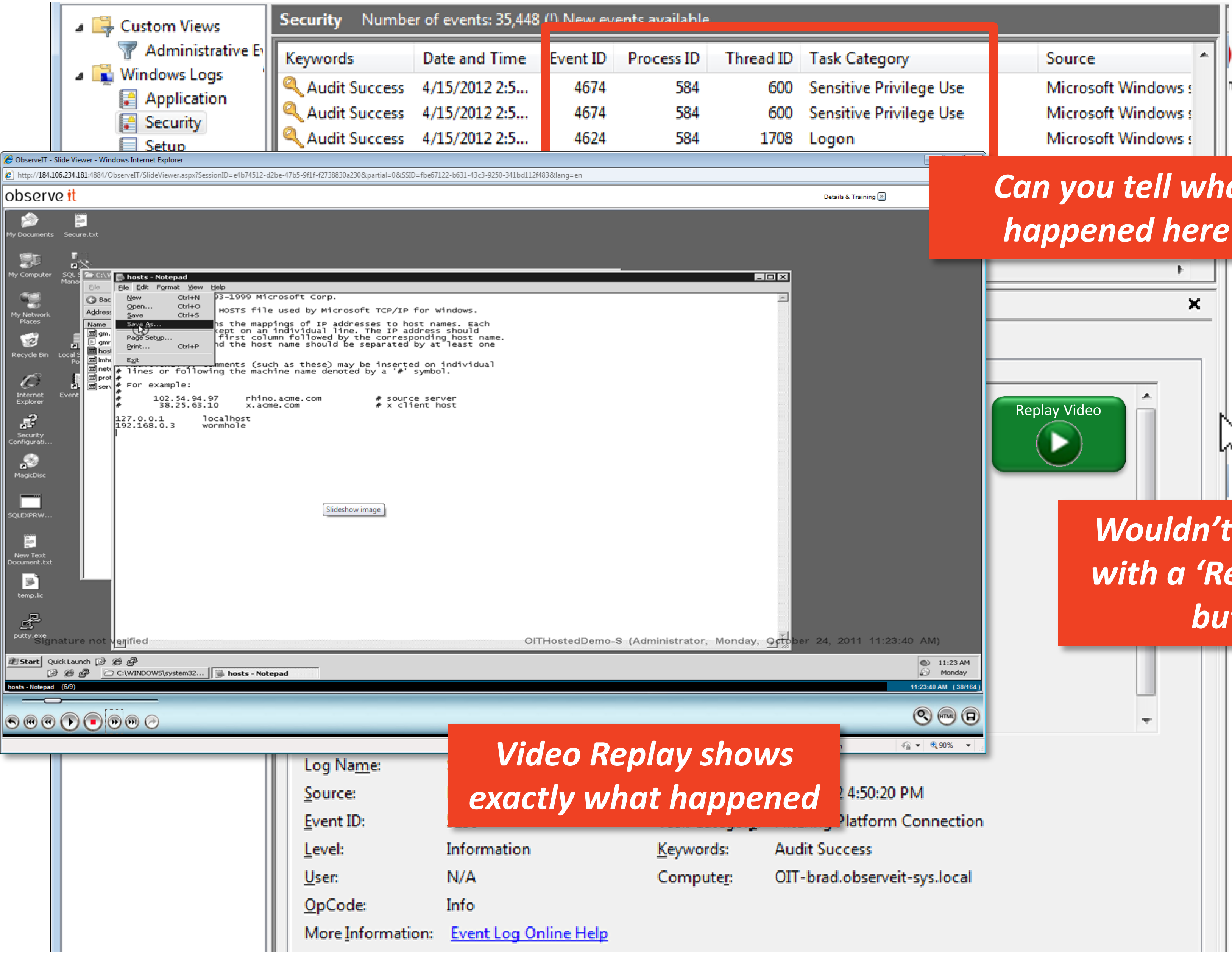
*(Even though 71% of data breaches
involve privileged user credentials)*


verizon
2012 DATA BREACH IN
Figure 45. Breach discovery methods by percent of breaches
59%
Larger Orgs
I don't have "this problem."
I've got log analysis!
The picture isn't quite as rosy as you think.

**Why?**

Because system logs are built by DEVELOPERS for DEBUG!

(and not by SECURITY ADMINS for SECURITY AUDIT)



Security   Number of events: 35,448 (!) New events available

| Keywords | Date and Time | Event ID | Process ID | Thread ID | Task Category | Source |
|---|---|---|---|---|---|---|
| Audit Success | 4/15/2012 2:5... | 4674 | 584 | 600 | Sensitive Privilege Use | Microsoft Windows s |
| Audit Success | 4/15/2012 2:5... | 4674 | 584 | 600 | Sensitive Privilege Use | Microsoft Windows s |
| Audit Success | 4/15/2012 2:5... | 4624 | 584 | 1708 | Logon | Microsoft Windows s |

```
93-1999 Microsoft Corp.

 HOSTS file used by Microsoft TCP/IP for Windows.

ns the mappings of IP addresses to host names. Each
kept on an individual line. The IP address should
 first column followed by the corresponding host name.
nd the host name should be separated by at least one

mments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
192.168.0.3     wormhole
```

Log Name:

Source: 4:50:20 PM

Event ID: Platform Connection

Level: Information Keywords: Audit Success

User: N/A Computer: OIT-brad.observeit-sys.local

OpCode: Info

More Information: Event Log Online Help

*Can you tell what happened here?*

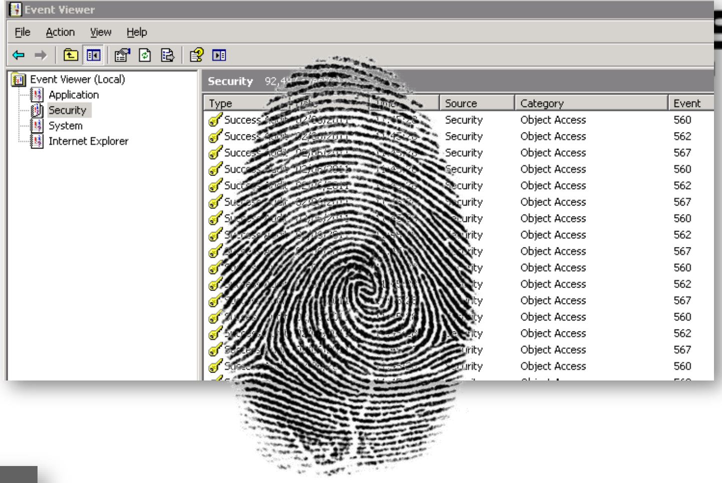
*Wouldn't it be easier with a 'Replay Video' button?*

*Video Replay shows exactly what happened*

secure
E-Business Security

## System Logs are like Fingerprints

*They show the **results/outcome** of what took place*



| Type | Date | Time | Source | Category | Event |
|---|---|---|---|---|---|
| Success [illegible] | [illegible] | [illegible] | Security | Object Access | 560 |
| Success [illegible] | [illegible] | [illegible] | Security | Object Access | 562 |
| Success [illegible] | [illegible] | [illegible] | Security | Object Access | 567 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 560 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 562 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 567 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 560 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 562 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 567 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 560 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 562 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 567 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 560 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 562 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 567 |
| [illegible] | [illegible] | [illegible] | Security | Object Access | 560 |

## User Audit Logs are like Surveillance Recordings

*They show **exactly what** took place!*

“Both are valid…
…But the video log goes right to the point!”

# And many commonly used apps don't even have their own logs!

## DESKTOP APPS

- Firefox / Chrome / IE
- MS Excel / Word
- Outlook
- Skype

## ADMIN TOOLS

- Registry Editor
- SQL Manager
- Toad
- Network Config

## REMOTE & VIRTUAL

- Remote Desktop
- VMware vSphere

## TEXT EDITORS

- vi
- Notepad

# Challenges with Log Analysis

- Too many logs
- Logs are too technical
- Logs are designed for IT purposes, not Security
- Not all applications/activities generate logs
- Investigation with Log Analysis is resource intensive

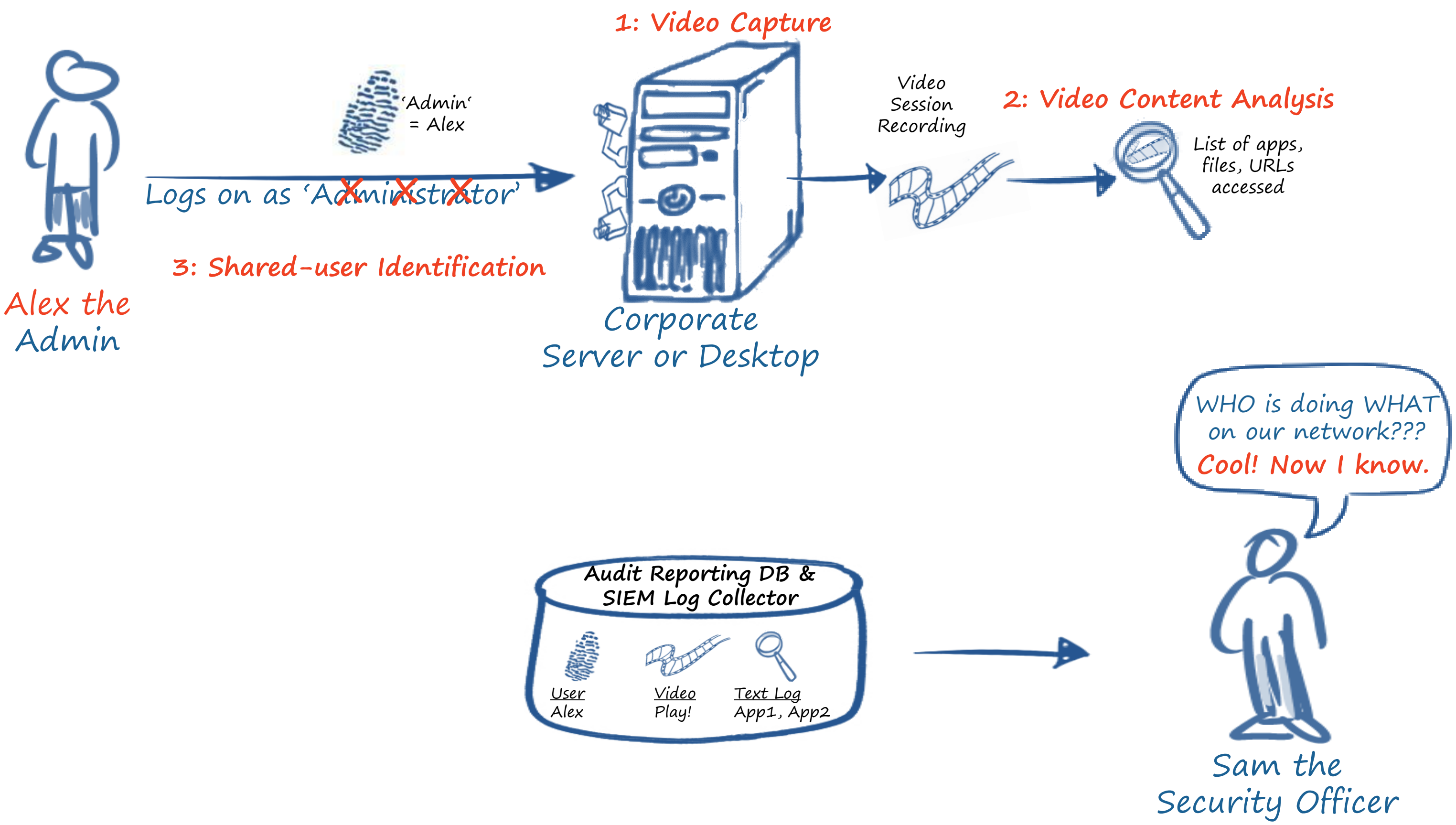
“ No wonder only 1% of data breaches are discovered via log analysis! “

# ObserveIT - Software that acts like a security camera on your servers!

- **Video camera:** Recordings of all user activity
- **Summary of key actions:** Alerts for problematic activity

# Our Solution

TO~~D~~AY with ObserveIT's 3 key features



1: Video Capture

Alex the Admin

'Admin' = Alex

Logs on as 'Administrator'

3: Shared-user Identification

Corporate Server or Desktop

Video Session Recording

2: Video Content Analysis

List of apps, files, URLs accessed

WHO is doing WHAT on our network???

Cool! Now I know.

Audit Reporting DB & SIEM Log Collector

User Alex

Video Play!

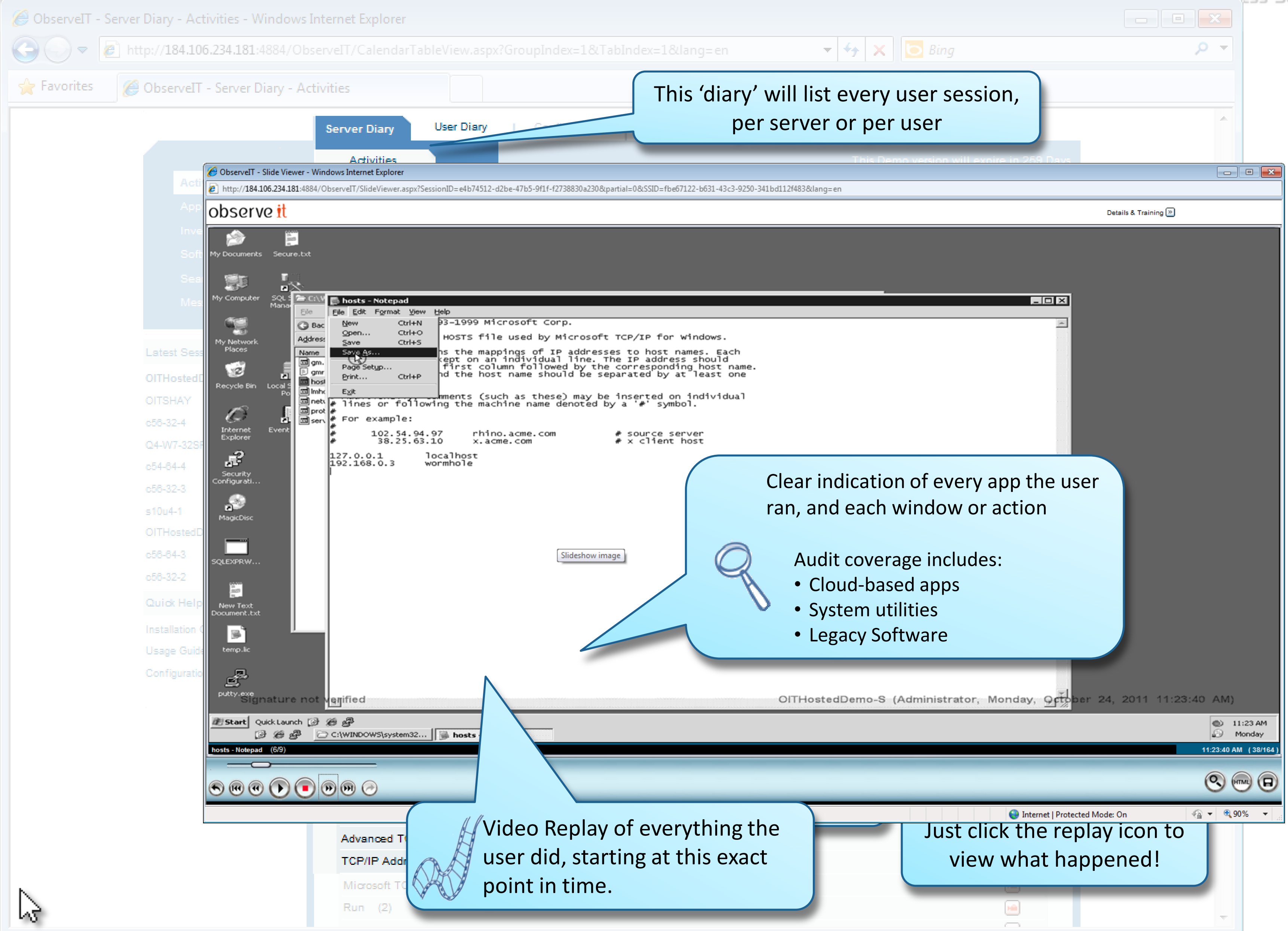
Text Log App1, App2

Sam the Security Officer

# User Activity Monitoring: In Windows

observe it people audit

besecure Managed & Business Security



ObserveIT - Server Diary - Activities - Windows Internet Explorer

http://184.106.234.181:4884/ObserveIT/CalendarTableView.aspx?GroupIndex=1&TabIndex=1&lang=en

ObserveIT - Slide Viewer - Windows Internet Explorer

http://184.106.234.181:4884/ObserveIT/SlideViewer.aspx?SessionID=e4b74512-d2be-47b5-9f1f-f2738830a230&partial=0&SSID=fbe67122-b631-43c3-9250-341bd112f483&lang=en

```
93-1999 Microsoft Corp.

 HOSTS file used by Microsoft TCP/IP for Windows.

ns the mappings of IP addresses to host names. Each
kept on an individual line. The IP address should
 first column followed by the corresponding host name.
nd the host name should be separated by at least one

        mments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
192.168.0.3     wormhole
```

Signature not verified

OITHostedDemo-S (Administrator, Monday, October 24, 2011 11:23:40 AM)

This 'diary' will list every user session, per server or per user

Clear indication of every app the user ran, and each window or action

Audit coverage includes:

- Cloud-based apps
- System utilities
- Legacy Software

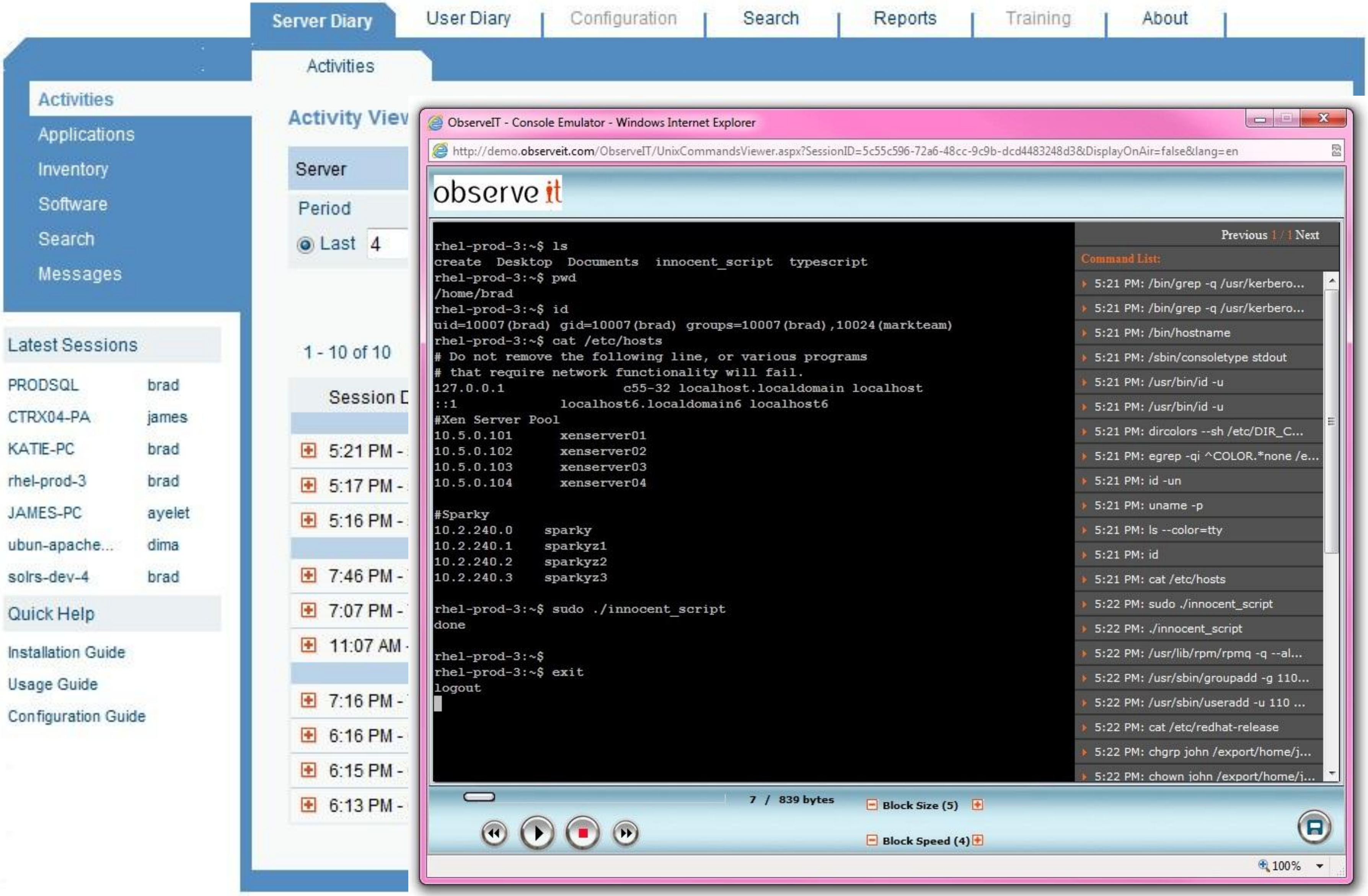
Video Replay of everything the user did, starting at this exact point in time.

Just click the replay icon to view what happened!

# User Activity Monitoring in Linux

observe it people audit

besecure Managed E-Business Security



Latest Sessions

| | |
|---|---|
| PRODSQL | brad |
| CTRX04-PA | james |
| KATIE-PC | brad |
| rhel-prod-3 | brad |
| JAMES-PC | ayelet |
| ubun-apache... | dima |
| solrs-dev-4 | brad |

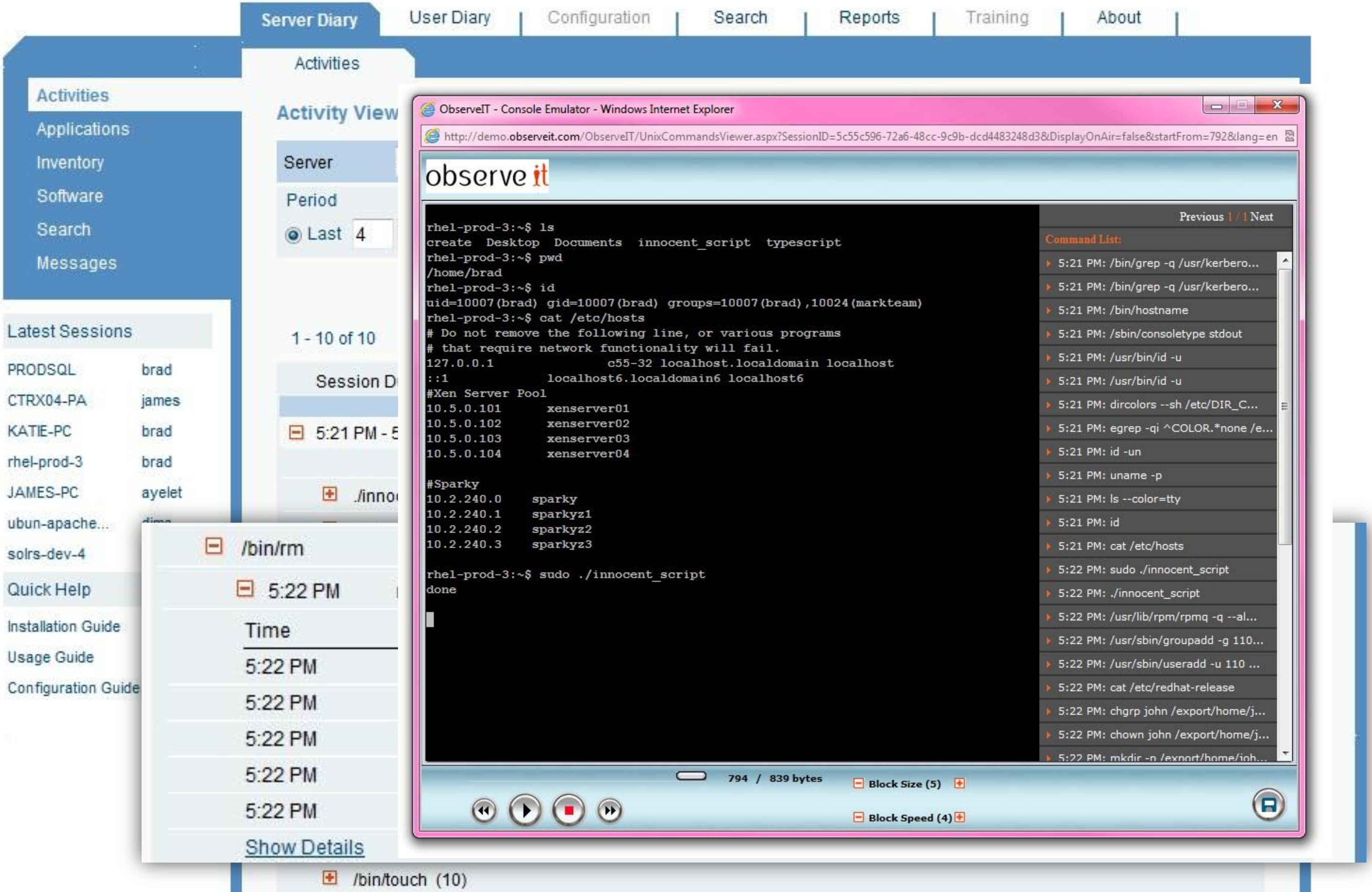
http://demo.observeit.com/ObserveIT/UnixCommandsViewer.aspx?SessionID=5c55c596-72a6-48cc-9c9b-dcd4483248d3&DisplayOnAir=false&lang=en

```
rhel-prod-3:~$ ls
create  Desktop  Documents  innocent_script  typescript
rhel-prod-3:~$ pwd
/home/brad
rhel-prod-3:~$ id
uid=10007(brad) gid=10007(brad) groups=10007(brad),10024(markteam)
rhel-prod-3:~$ cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               c55-32 localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
#Xen Server Pool
10.5.0.101      xenserver01
10.5.0.102      xenserver02
10.5.0.103      xenserver03
10.5.0.104      xenserver04

#Sparky
10.2.240.0     sparky
10.2.240.1     sparkyz1
10.2.240.2     sparkyz2
10.2.240.3     sparkyz3

rhel-prod-3:~$ sudo ./innocent_script
done

rhel-prod-3:~$
rhel-prod-3:~$ exit
logout
```

Command List:

```
5:21 PM: /bin/grep -q /usr/kerbero...
5:21 PM: /bin/grep -q /usr/kerbero...
5:21 PM: /bin/hostname
5:21 PM: /sbin/consoletype stdout
5:21 PM: /usr/bin/id -u
5:21 PM: /usr/bin/id -u
5:21 PM: dircolors --sh /etc/DIR_C...
5:21 PM: egrep -qi ^COLOR.*none /e...
5:21 PM: id -un
5:21 PM: uname -p
5:21 PM: ls --color=tty
5:21 PM: id
5:21 PM: cat /etc/hosts
5:22 PM: sudo ./innocent_script
5:22 PM: ./innocent_script
5:22 PM: /usr/lib/rpm/rpmq -q --al...
5:22 PM: /usr/sbin/groupadd -g 110...
5:22 PM: /usr/sbin/useradd -u 110 ...
5:22 PM: cat /etc/redhat-release
5:22 PM: chgrp john /export/home/j...
5:22 PM: chown john /export/home/j...
```

# User Activity Monitoring in Linux



Latest Sessions

| | |
|---|---|
| PRODSQL | brad |
| CTRX04-PA | james |
| KATIE-PC | brad |
| rhel-prod-3 | brad |
| JAMES-PC | ayelet |
| ubun-apache... | dima |
| solrs-dev-4 | |

ObserveIT - Console Emulator - Windows Internet Explorer

http://demo.observeit.com/ObserveIT/UnixCommandsViewer.aspx?SessionID=5c55c596-72a6-48cc-9c9b-dcd4483248d3&DisplayOnAir=false&startFrom=792&lang=en

```
rhel-prod-3:~$ ls
create  Desktop  Documents  innocent_script  typescript
rhel-prod-3:~$ pwd
/home/brad
rhel-prod-3:~$ id
uid=10007(brad) gid=10007(brad) groups=10007(brad),10024(markteam)
rhel-prod-3:~$ cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               c55-32 localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
#Xen Server Pool
10.5.0.101      xenserver01
10.5.0.102      xenserver02
10.5.0.103      xenserver03
10.5.0.104      xenserver04

#Sparky
10.2.240.0    sparky
10.2.240.1    sparkyz1
10.2.240.2    sparkyz2
10.2.240.3    sparkyz3

rhel-prod-3:~$ sudo ./innocent_script
done
```

Previous 1 / 1 Next

Command List:

- 5:21 PM: /bin/grep -q /usr/kerbero...
- 5:21 PM: /bin/grep -q /usr/kerbero...
- 5:21 PM: /bin/hostname
- 5:21 PM: /sbin/consoletype stdout
- 5:21 PM: /usr/bin/id -u
- 5:21 PM: /usr/bin/id -u
- 5:21 PM: dircolors --sh /etc/DIR_C...
- 5:21 PM: egrep -qi ^COLOR.*none /e...
- 5:21 PM: id -un
- 5:21 PM: uname -p
- 5:21 PM: ls --color=tty
- 5:21 PM: id
- 5:21 PM: cat /etc/hosts
- 5:22 PM: sudo ./innocent_script
- 5:22 PM: ./innocent_script
- 5:22 PM: /usr/lib/rpm/rpmq -q --al...
- 5:22 PM: /usr/sbin/groupadd -g 110...
- 5:22 PM: /usr/sbin/useradd -u 110 ...
- 5:22 PM: cat /etc/redhat-release
- 5:22 PM: chgrp john /export/home/j...
- 5:22 PM: chown john /export/home/j...
- 5:22 PM: mkdir -p /export/home/joh...

794 / 839 bytes

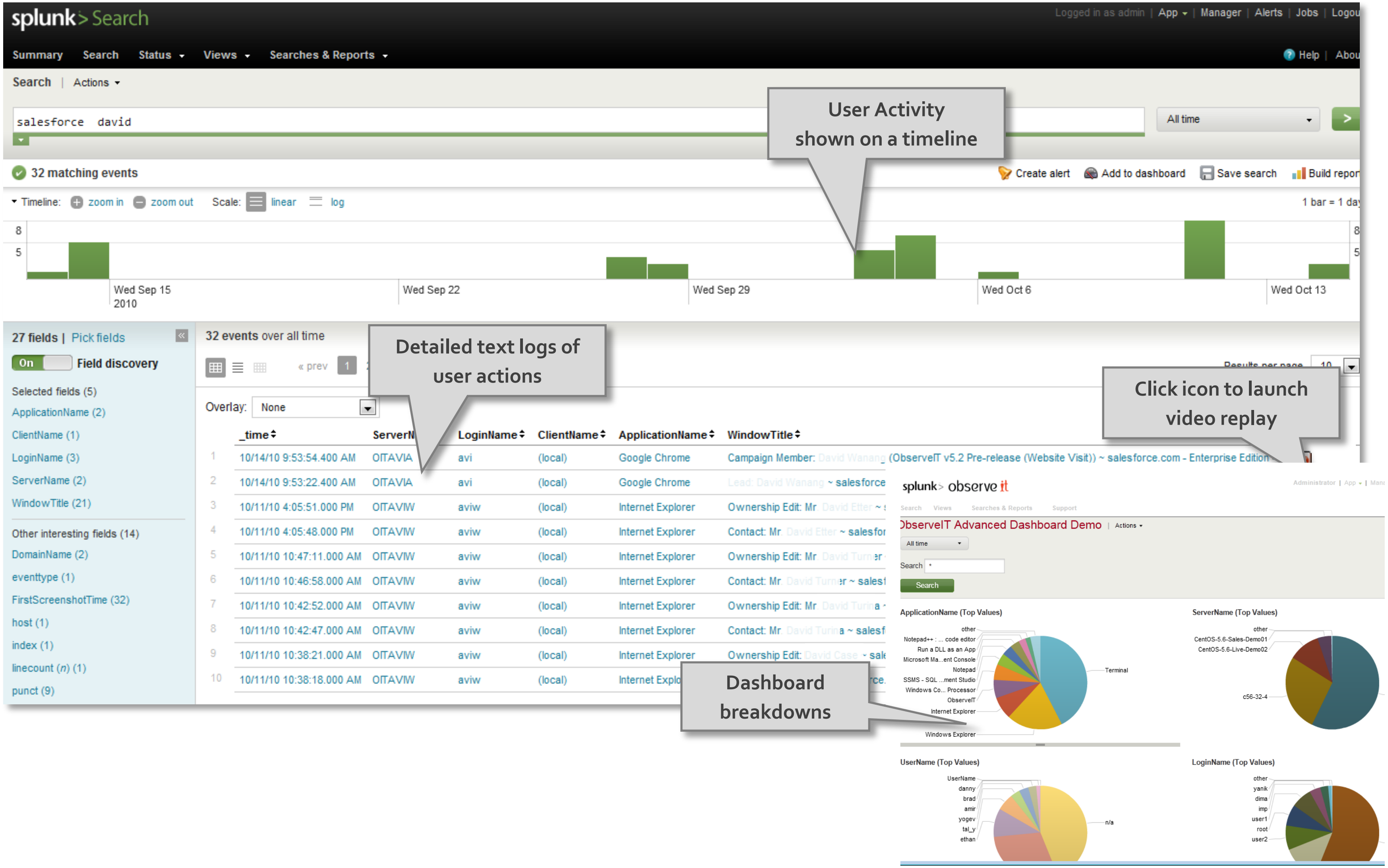
Block Size (5)

Block Speed (4)

# ObserveIT Video and Logs in Splunk

observe it people audit

besecure Managed E-Business Security™



User Activity shown on a timeline

Detailed text logs of user actions

Click icon to launch video replay

Dashboard breakdowns

salesforce david

32 matching events

27 fields | Pick fields

On Field discovery

Selected fields (5)
ApplicationName (2)
ClientName (1)
LoginName (3)
ServerName (2)
WindowTitle (21)

Other interesting fields (14)
DomainName (2)
eventtype (1)
FirstScreenshotTime (32)
host (1)
index (1)
linecount (n) (1)
punct (9)

32 events over all time

Overlay: None

| | _time | ServerN | LoginName | ClientName | ApplicationName | WindowTitle |
|---|---|---|---|---|---|---|
| 1 | 10/14/10 9:53:54.400 AM | OITAVIA | avi | (local) | Google Chrome | Campaign Member: David Wanang (ObserveIT v5.2 Pre-release (Website Visit)) ~ salesforce.com - Enterprise Edition |
| 2 | 10/14/10 9:53:22.400 AM | OITAVIA | avi | (local) | Google Chrome | Lead: David Wanang ~ salesforce |
| 3 | 10/11/10 4:05:51.000 PM | OITAVIW | aviw | (local) | Internet Explorer | Ownership Edit: Mr. David Etter ~ s |
| 4 | 10/11/10 4:05:48.000 PM | OITAVIW | aviw | (local) | Internet Explorer | Contact: Mr. David Etter ~ salesfor |
| 5 | 10/11/10 10:47:11.000 AM | OITAVIW | aviw | (local) | Internet Explorer | Ownership Edit: Mr. David Turner |
| 6 | 10/11/10 10:46:58.000 AM | OITAVIW | aviw | (local) | Internet Explorer | Contact: Mr. David Turner ~ salesf |
| 7 | 10/11/10 10:42:52.000 AM | OITAVIW | aviw | (local) | Internet Explorer | Ownership Edit: Mr. David Turina |
| 8 | 10/11/10 10:42:47.000 AM | OITAVIW | aviw | (local) | Internet Explorer | Contact: Mr. David Turina ~ salesf |
| 9 | 10/11/10 10:38:21.000 AM | OITAVIW | aviw | (local) | Internet Explorer | Ownership Edit: David Case ~ sale |
| 10 | 10/11/10 10:38:18.000 AM | OITAVIW | aviw | (local) | Internet Explo | rce. |

splunk> observe it

ObserveIT Advanced Dashboard Demo | Actions

All time

Search *

# Business challenges that ObserveIT addresses

observe it
people audit

besecure
Managed E-Business Security™

## Remote Vendor Monitoring

- *Impact human behavior*
- *Transparent SLA and billing*
- *Eliminate 'Finger pointing'*

## Compliance & Security Accountability

- *Reduce compliance costs for GETTING compliant and STAYING compliant*
- *Satisfy PCI, HIPAA, SOX, ISO*

## Root Cause Analysis & Documentation

- *Immediate root-cause answers*
- *Document best-practices*

# 700+ Enterprise Customers

observe it
people audit

besecure
Managed E-Business Security

## Healthcare / Pharma

BlueCross BlueShield Association
ECOLAB
Boehringer Ingelheim
sanofi aventis
University Health Systems of Eastern Carolina
Fresenius health care worldwide
SUNY Downstate Medical Center
St. Jude Medical
Western Governors University
Yonsei University Health System
Washington University in St.Louis
University of California 1868

## Financial

BNP PARIBAS
SOCIETE GENERALE
GE Money
ING
DEUTSCHE BÖRSE GROUP
Bank of Cyprus
Allianz
BLACKROCK
VOCALINK safer payments, smarter partner
Scotiabank
CAJA MADRID
HELLENIC BANK
MFS INVESTMENT MANAGEMENT
momentum
中国建设银行 China Construction Bank
VONTOBEL
LASER
LGT
American Century Investments

## Telco & Media

vodafone
tigo
中国移动通信 CHINA MOBILE
orange
TalkTalk
T Deutsche Telekom
BELLSOUTH
T··Mobile·
swisscom
TELECOM
MEGAFON
Telecom NEW ZEALAND
Taiwan Mobile
MultiChoice
BBC
sky
AASTRA

## Manufacturing

Coca-Cola
NISSAN
TOSHIBA
SAMSUNG
SIEMENS
xerox

## Retail / Service

CDW
TESCO
Domino's Pizza
COST PLUS WORLD MARKET
CLICKS

## Utilities & Logistics

ups
DHL
New Zealand Post
Petrotrin
bp
PGE
交通部臺灣鐵路管理局 Taiwan Railways Administration,MOTC
woodside
GS Caltex
SBB
toronto hydro electric system
elektrotim

## IT Services

IBM
Cisco webex
BT
Microsoft
LOGICALIS
dimension data
COMVERSE
HCL
QinetiQ
WIPRO
T··Systems·

## Government

UNITED NATIONS
Statistics South Africa
Ministry of Foreign Affairs
Central Bureau of Statistics
National Statistics Republic of China(Taiwan)

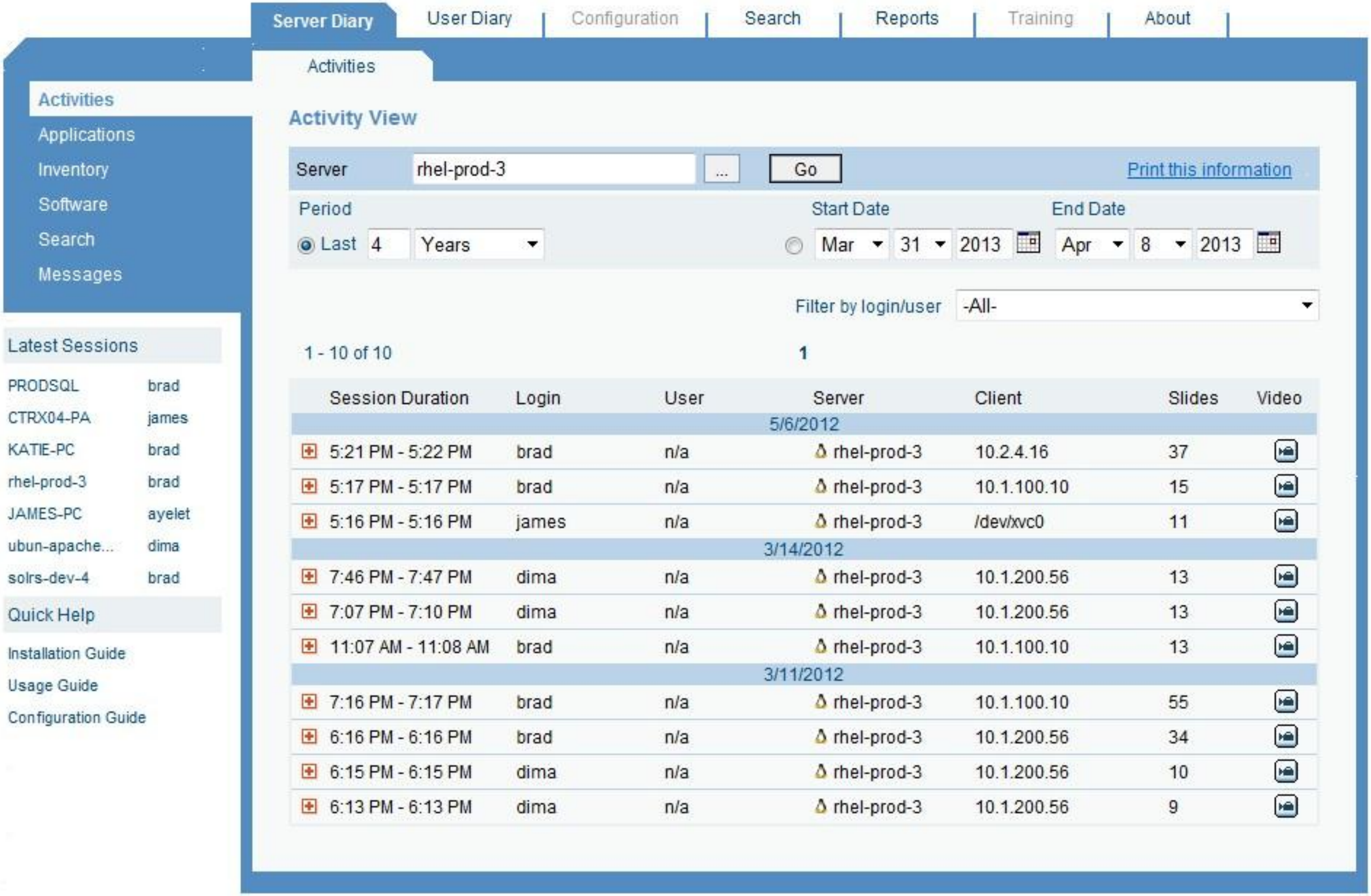
## Gaming

Fort McDowell Casino
LOTO QUÉBEC
CASINO ARIZONA
香港賽馬會 The Hong Kong Jockey Club

# User Activity Monitoring in Linux

observe it
people audit

besecure
Managed E-Business Security



Activity View

Server: rhel-prod-3

Period: ● Last 4 Years

○ Start Date: Mar 31 2013 End Date: Apr 8 2013

Filter by login/user: -All-

1 - 10 of 10 1

| Session Duration | Login | User | Server | Client | Slides | Video |
|---|---|---|---|---|---|---|
| 5/6/2012 | | | | | | |
| 5:21 PM - 5:22 PM | brad | n/a | rhel-prod-3 | 10.2.4.16 | 37 | |
| 5:17 PM - 5:17 PM | brad | n/a | rhel-prod-3 | 10.1.100.10 | 15 | |
| 5:16 PM - 5:16 PM | james | n/a | rhel-prod-3 | /dev/xvc0 | 11 | |
| 3/14/2012 | | | | | | |
| 7:46 PM - 7:47 PM | dima | n/a | rhel-prod-3 | 10.1.200.56 | 13 | |
| 7:07 PM - 7:10 PM | dima | n/a | rhel-prod-3 | 10.1.200.56 | 13 | |
| 11:07 AM - 11:08 AM | brad | n/a | rhel-prod-3 | 10.1.100.10 | 13 | |
| 3/11/2012 | | | | | | |
| 7:16 PM - 7:17 PM | brad | n/a | rhel-prod-3 | 10.1.100.10 | 55 | |
| 6:16 PM - 6:16 PM | brad | n/a | rhel-prod-3 | 10.1.200.56 | 34 | |
| 6:15 PM - 6:15 PM | dima | n/a | rhel-prod-3 | 10.1.200.56 | 10 | |
| 6:13 PM - 6:13 PM | dima | n/a | rhel-prod-3 | 10.1.200.56 | 9 | |

Latest Sessions

| | |
|---|---|
| PRODSQL | brad |
| CTRX04-PA | james |
| KATIE-PC | brad |
| rhel-prod-3 | brad |
| JAMES-PC | ayelet |
| ubun-apache... | dima |
| solrs-dev-4 | brad |

Quick Help

Installation Guide
Usage Guide
Configuration Guide

# Interested to learn more ?

- Contact our regional partner BESECURE : www.besecuregroup.com

- Register to attend a webinar

- Feel free to ask for a free trial of ObserveIT : sales@besecure.gr

- Visit us during conference at BESECURE's booth for a live demonstration and discuss with us

Thank you for your time