



# Developing a platform of organisational security reporting using existing tool sets

Adrian Heald

ITSM Reporting Services



Or

The importance of validating your  
systems and assumptions!

# Introduction



- We all need to be alert to the possibility of violation of our IT security
  - Viruses
  - Unauthorised access to sensitive data
  - Malicious or unintentional deletion or corruption of data
  - Physical access control
- We implement various security features
  - Anti virus
  - Access control (physical and logical)
  - Software patching
  - Backup and DR
  - etc. etc.
- Typically these are strictly controlled within the individual process but is that enough?

**Our experience has shown that it is not!**

# The client



- Enterprise Business Services (EBS)
  - Part of Singapore Power
  - Responsible for providing IT support services to SP\_Ausnet (SPA) and Jemena (JEM) power companies
  - 250 staff
- Seeking to improve overall IT service management
- Recently announced that they will be no more as of July 2014
  - Moving back into SPA and JEM

# What we set out to do



- Develop some reporting capability around various aspects of IT security, specifically:
  - Patching compliance;
  - Virus detection;
  - Identity management;
  - Perimeter security; and
  - Network device OS;
- Simplify the management of these areas and thus improve overall organisational security
- Report using high level dashboards for management down to low level operational reports
  - all using the same data source
- Gain some benefits from the various sources of data available
  - Connect different data sources for improved intelligence



# Why

- The current state was unknown
- A desire for continual improvement
  - through a reporting feedback mechanism
- Improve and simplify management and operational control
- Reduce the manual reporting effort at all levels
- Through these efforts, reduce the likelihood of a security breach



# A holistic view

- Like ALL IT Service Management operations security needs a more holistic view of the world
- Link data from different sources for validation and gained intelligence
  - SAP and AD – Expired accounts
  - AD and EPO - anti virus
  - Etc.
- Provide information to more people for added insights
- Track changes to see improvements (or degradation)



# How

- Utilise existing tools and data sources, i.e. no additional operational tools
- Integrate data into a single security reporting database
  - Extract data daily
  - Automate
  - Collate weekly
  - Report monthly
- Self service reporting where possible





# The process



- We had a brief spec, unfortunately with very little detail
- Good handle on the data sources from the SME
- Reports went through several review iterations and changed quite a lot
- We spent a lot of time at the end of the project revalidating all the data as the changes that occurred during the reviews broke several of the early assumptions

# The reporting architecture



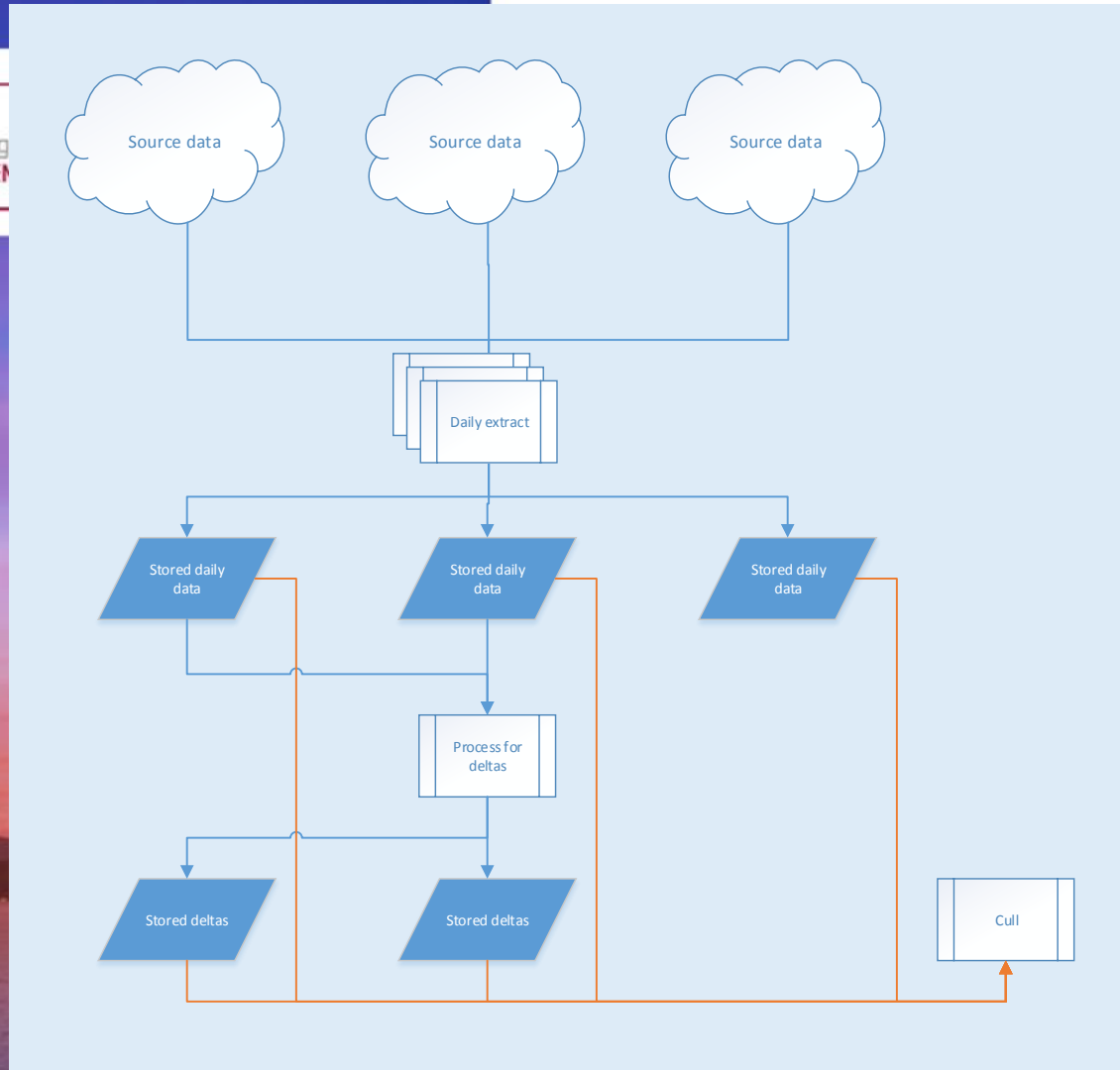
- Use the existing reporting framework
  - SQL Server 2008 R2
  - Captell for data extraction and loading
  - SQL Server Reporting Services (SSRS) for reporting
  - Quad core windows 2008 R2 server 8GB ram
  - 50GB database
- Utilise data from the tool sets used to manage the various security and other processes

# Basic reporting principals



- Independent
  - Don't rely on individual tools, processes or services, cross validate
- Centralised
  - Allows joining of different data sources for validation and added intelligence
- Timely
  - Allows timely response to reported information
- Consistent
  - All reports at all levels telling the same story, on the same page
- Accurate
  - All reports from the same place in the same format for improved management at all levels
- Cost effective
  - Reuse reporting infrastructure, tools, techniques and data

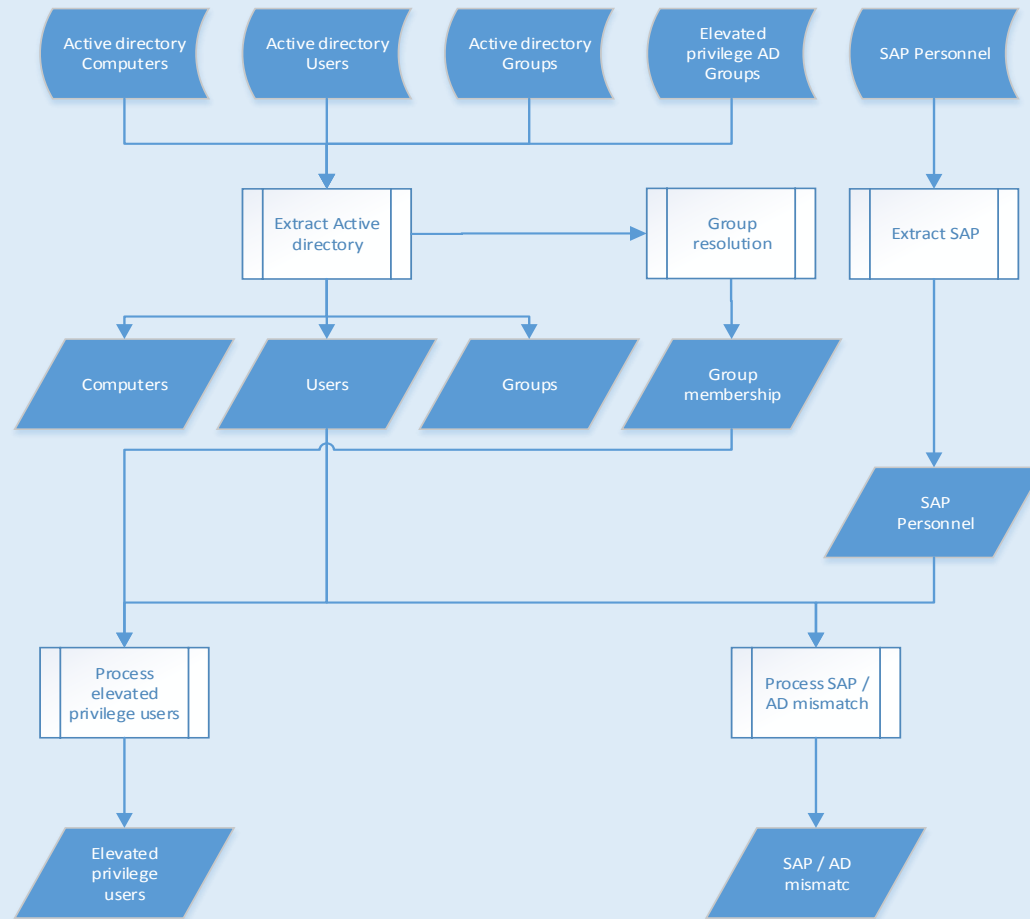
# General data management processing



- Extract process for each source
- Store data daily
  - Allows for early detection of data extract failures
- Calculate differences and store
  - Most tool sets only retain current values
  - To track improvement (or degradation) need to see differences
- Cull older unwanted data

# Typical data source processing

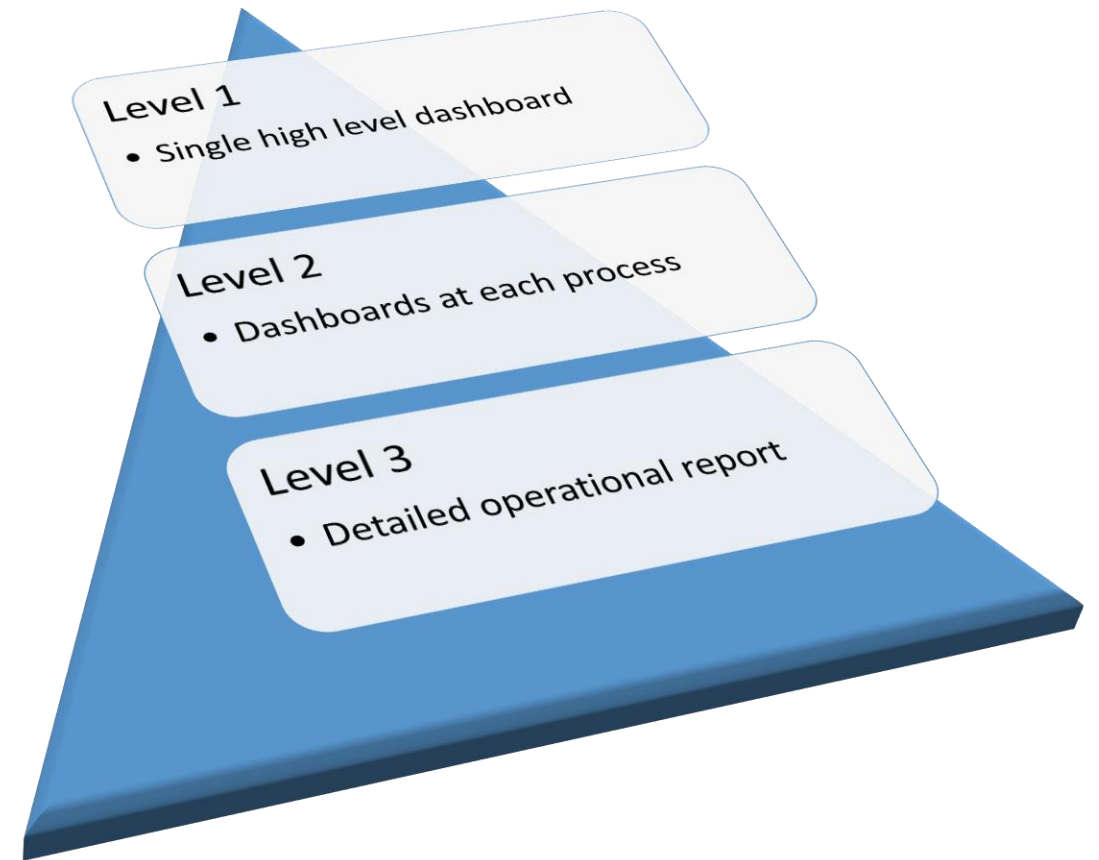
## Active directory / SAP data processing



- Extract from AD and SAP
  - Computers
  - Users
  - Groups
  - Group membership
    - Needs separate process to resolve groups
  - SAP Personnel
- Determine AD users no longer in SAP
- Determine individual users with elevated privileges



# 3 levels of reporting



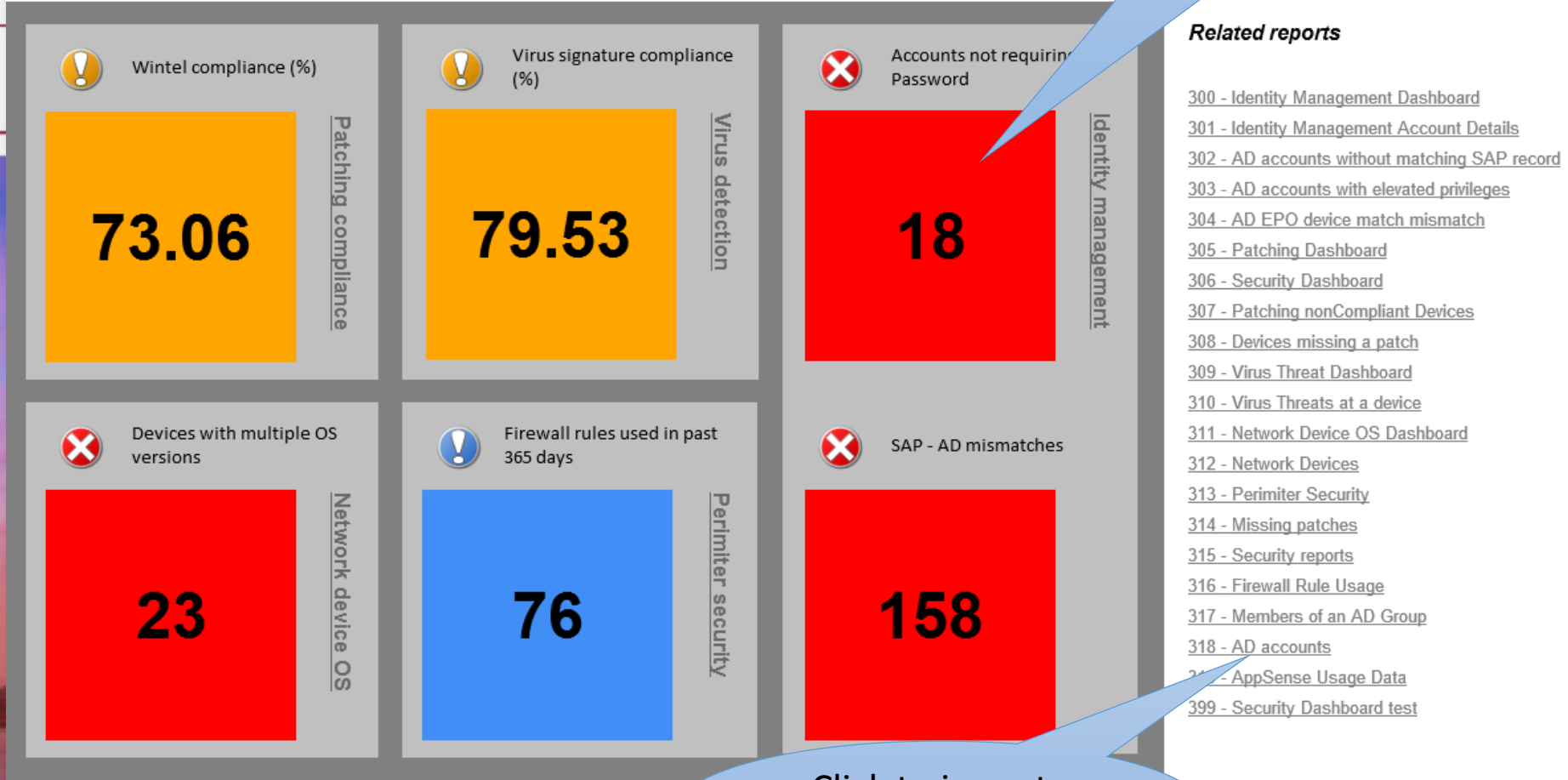
# Level 1: The security dashboard

Click to jump to the Level 2 report

## Security dashboard



IT Service Management Forum  
ANNUAL CONFERENCE 2014



Click to jump to other reports

# Level 2: Identity management

## Identity management

Accounts not requiring a password

18

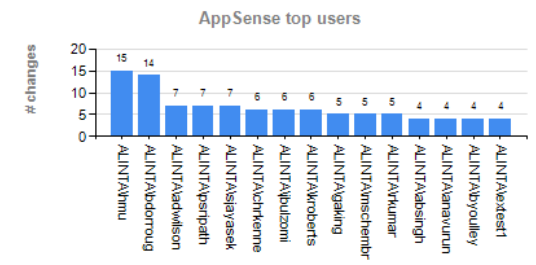
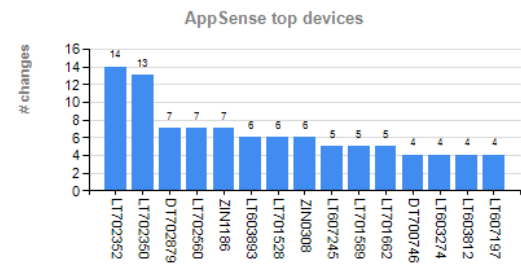
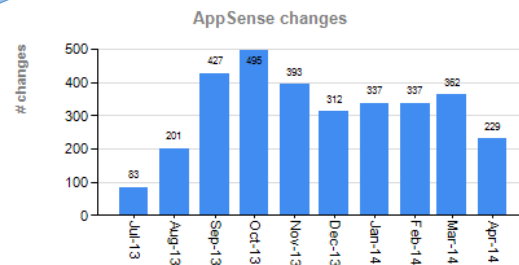
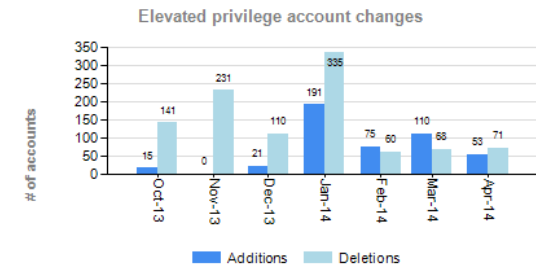
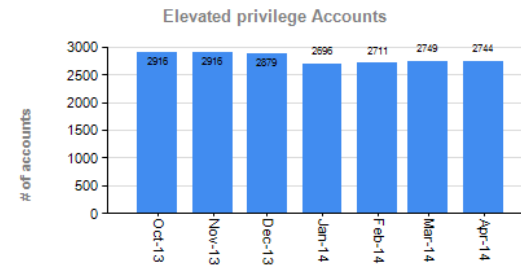
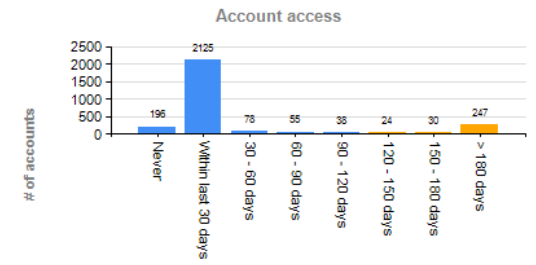
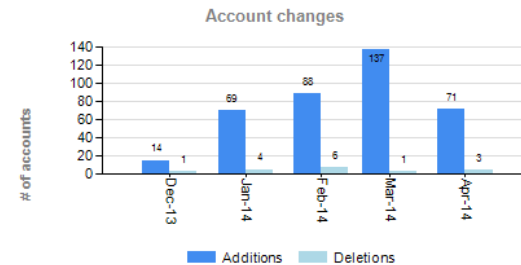
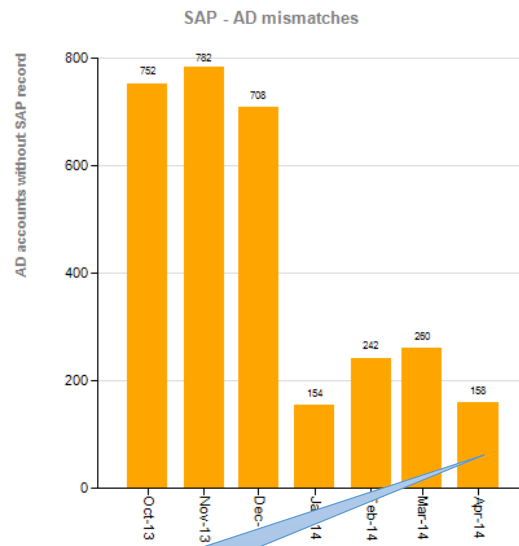


SAP - AD mismatches

158



Total accounts:	11120
Enabled accounts:	4826
Disabled accounts:	6294
Enabled and expired accounts:	108
Enabled and Not expired accounts:	4718
Locked out accounts:	0
Password not required accounts:	✗ 18
Password cant change accounts:	✔ 0
Dont expire password accounts:	✗ 1170
Password expired accounts:	108
Service accounts:	401
Generic accounts:	76
Mailbox accounts:	566
Active accounts not used in 90 days:	✗ 703
Elevated privilege accounts:	2746
AD-SAP mismatches:	✗ 158



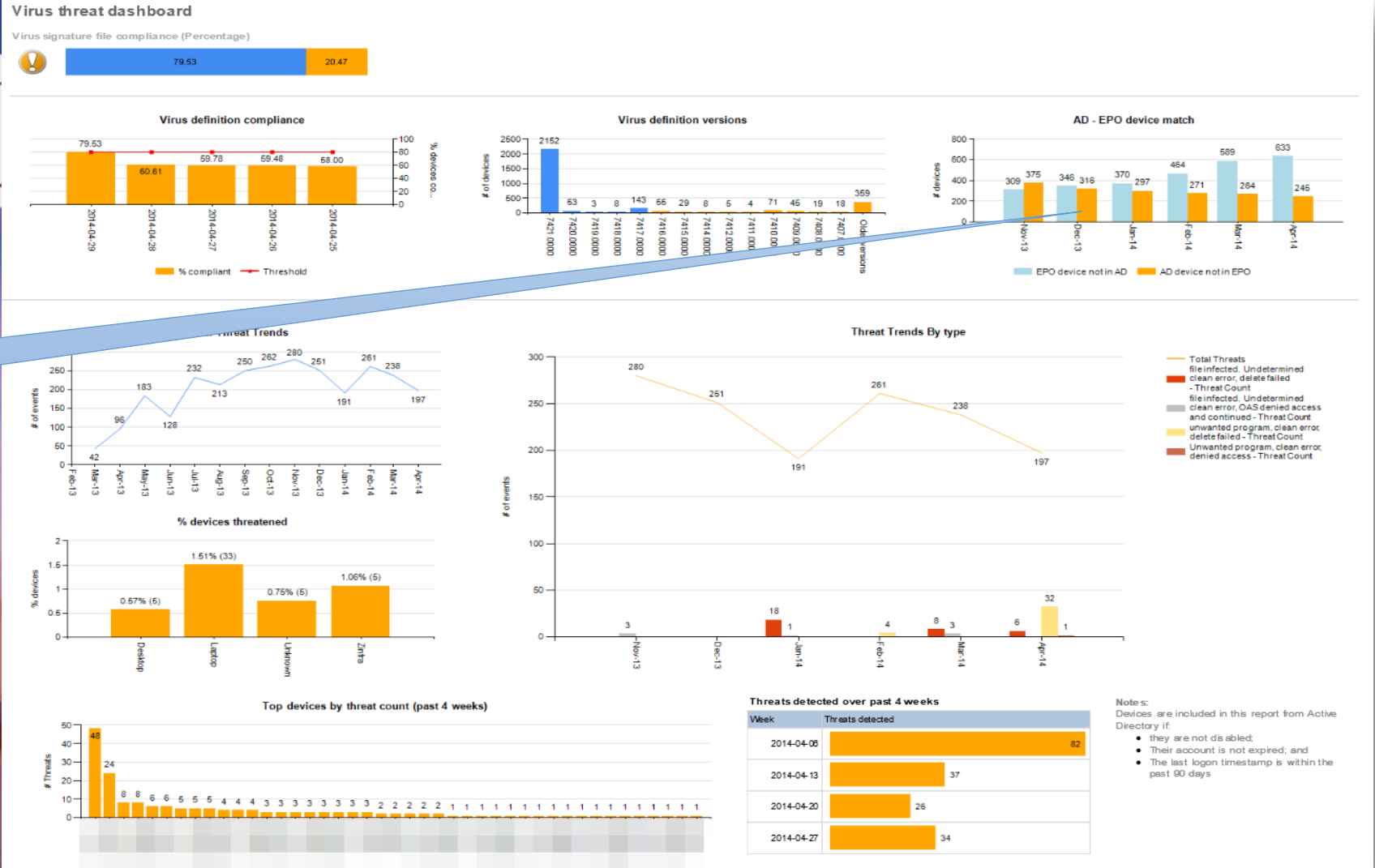
Click to jump to the Level 3 report

# Level 3:

- In this case the level 3 report identified the AD user records that don't have a matching SAP record or a SAP record that is no longer current

AD Name ↕	AD Given Name ↕	AD Sur Name ↕	Display Name ↕	Distinguished Name ↕	Mail ↕	Manager ↕
[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]		[REDACTED]
[REDACTED]			[REDACTED]	[REDACTED]	[REDACTED]	

# Level 2: Virus threat dashboard



Click to jump to the Level 3 report





# Difficulties



- There are no processes which included the reports
  - While they recognised the need for reporting they didn't have a process that utilised the reported output
  - Its important that any report is part of an overall process. Otherwise why produce the report in the first place?
- Some data sources were impossible to process
  - Encrypted, proprietary data

# What we learnt about the report development process



- Its very difficult to develop a reporting system without a clear picture of what the reports are to be used for
  - Without a process to utilise the reports it's uncertain what should be reported on
- Validation, Validation, Validation
  - After every set of review changes we revalidated, this always resulted in more changes as earlier assumptions changed
- The iterative approach works ok but it wastes time and money
  - Some changes were simply moving back to an earlier version

# What the client learnt



- The benefits of cross validation
  - Antivirus claimed 100% of devices were up to date with anti virus definition files
  - However they didn't have all devices in their database
  - Cross data validation identified the missing devices (AD – EPO)

# Outcomes



- Improvement to several aspects of security
  - Patching compliance
    - More responsive to new patch releases
  - Clean up of Active Directory
    - Ensuring user accounts have active SAP record
    - Rationalisation of AD groups
  - Anti virus protection
    - Inclusion of all devices into EPO management
- A recognition that improvements can be made
- A recognition of the importance of cross data validation



# Take home message

- Develop processes for security management that include a report feedback loop
- Establish cross process reporting from all the sources of security related data such that they feed the processes
- Validate your results



# Questions?

Adrian Heald

Director

ITSM Reporting Services

Ph: +61 (0)411 238 755

Email: [adrian@reportingservices.com](mailto:adrian@reportingservices.com)

Web: [www.reportingservices.com](http://www.reportingservices.com)

