Developing a platform of organisational security reporting using existing tool sets

Adrian Heald

ITSM Reporting Services

ITSM Reporting Services

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

Or

The importance of validating your systems and assumptions!

ITSM Reporting Services

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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!

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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)

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

The reporting architecture

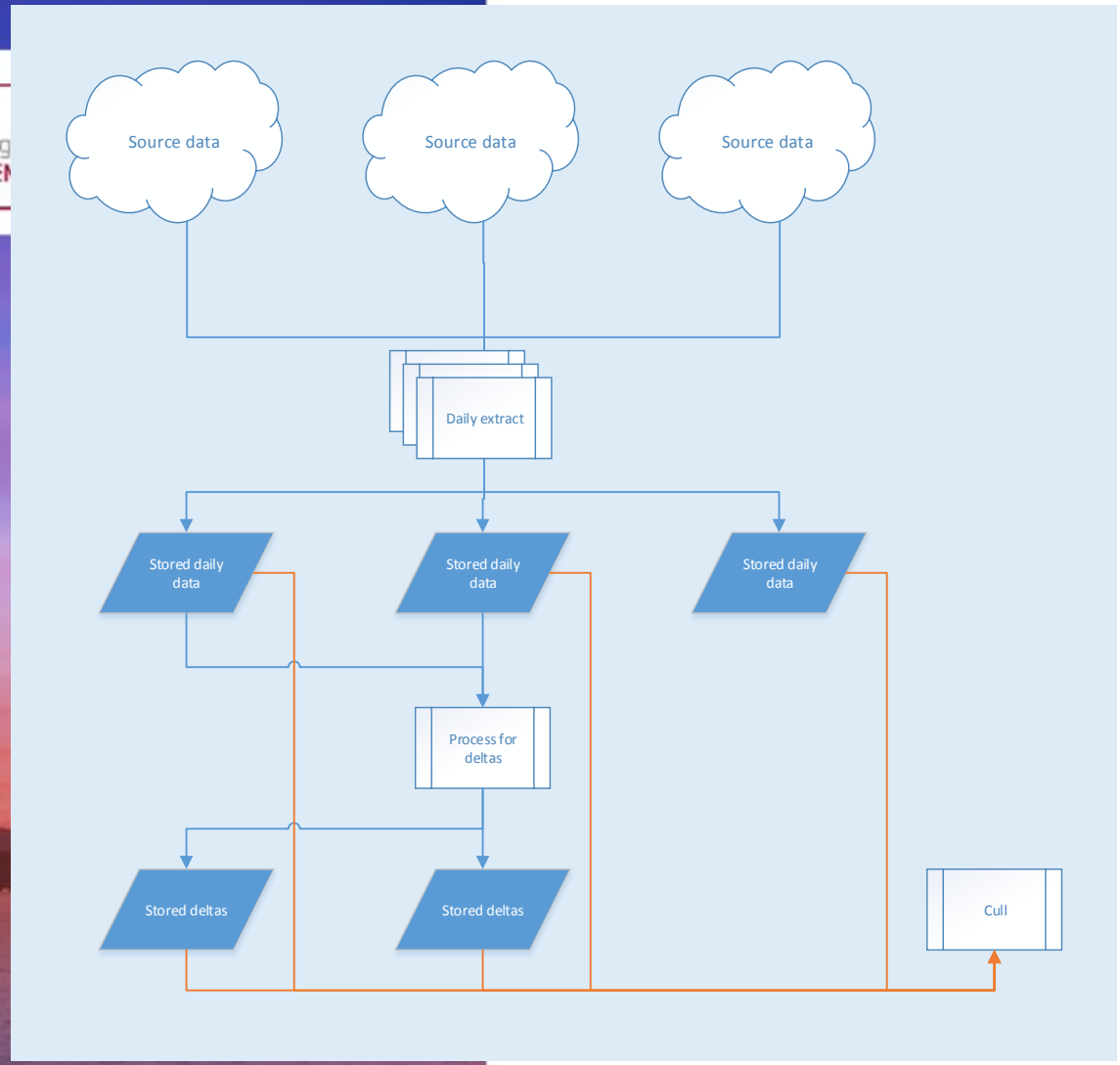
- Use the existing reporting framework
  - SQL Server 2008 R2
  - Captell for data extraction and loading
  - SQL Server Reporting Services (SSRS) for reporting
  - Quad core windows 2008 R2 server 8GB ram
  - 50GB database
- Utilise data from the tool sets used to manage the various security and other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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

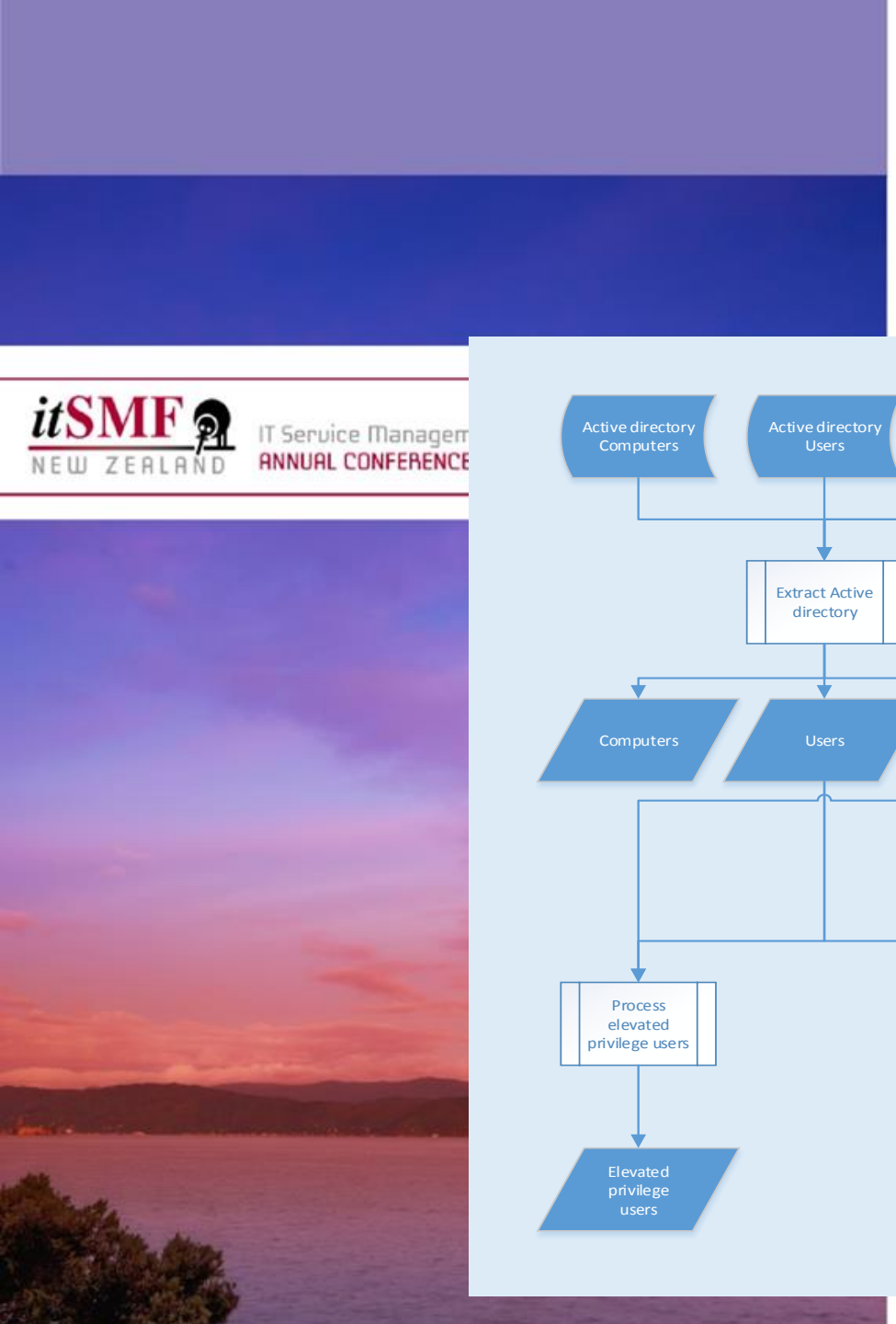
Basic reporting principals

- 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

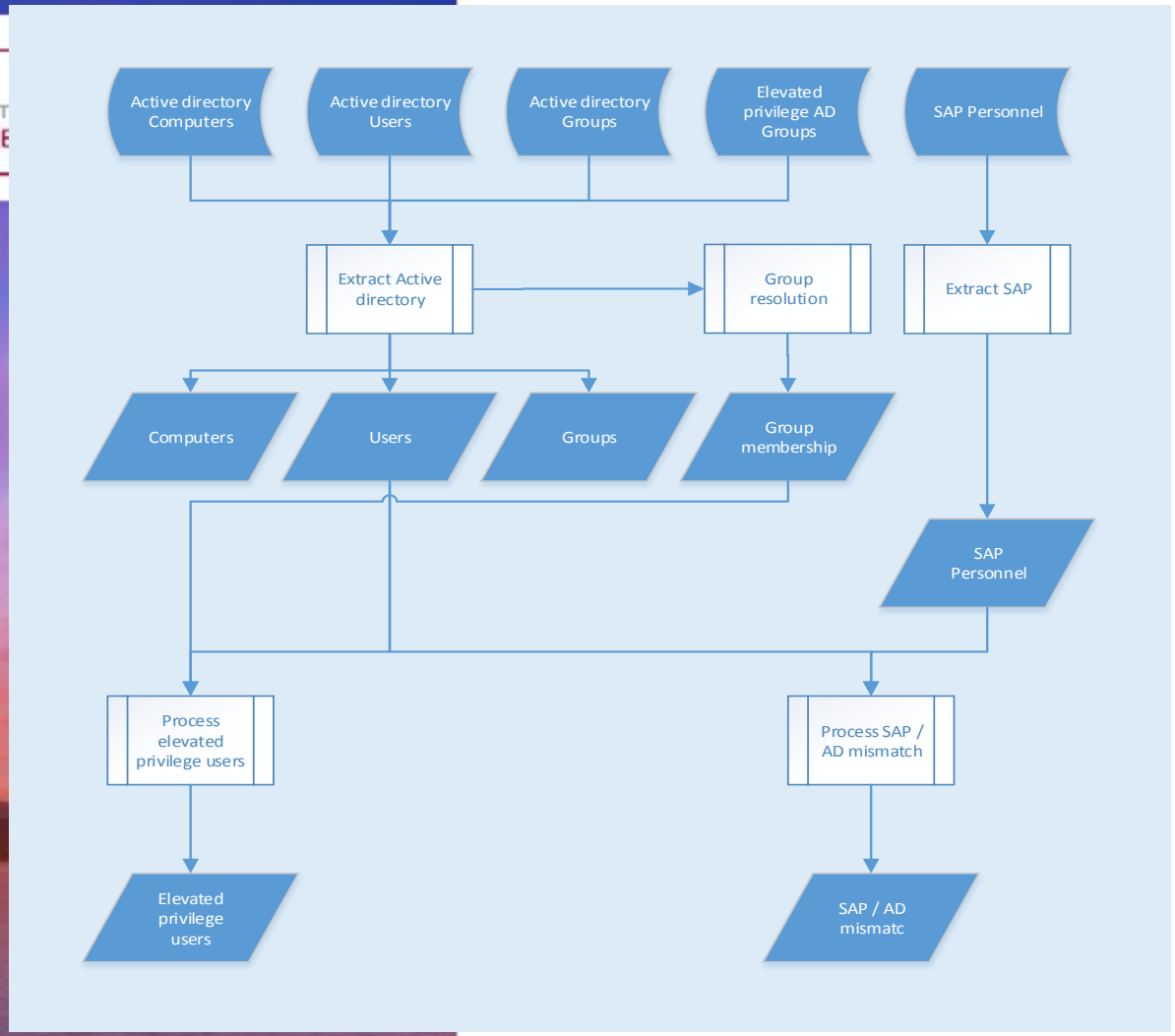
General data management processing



- 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

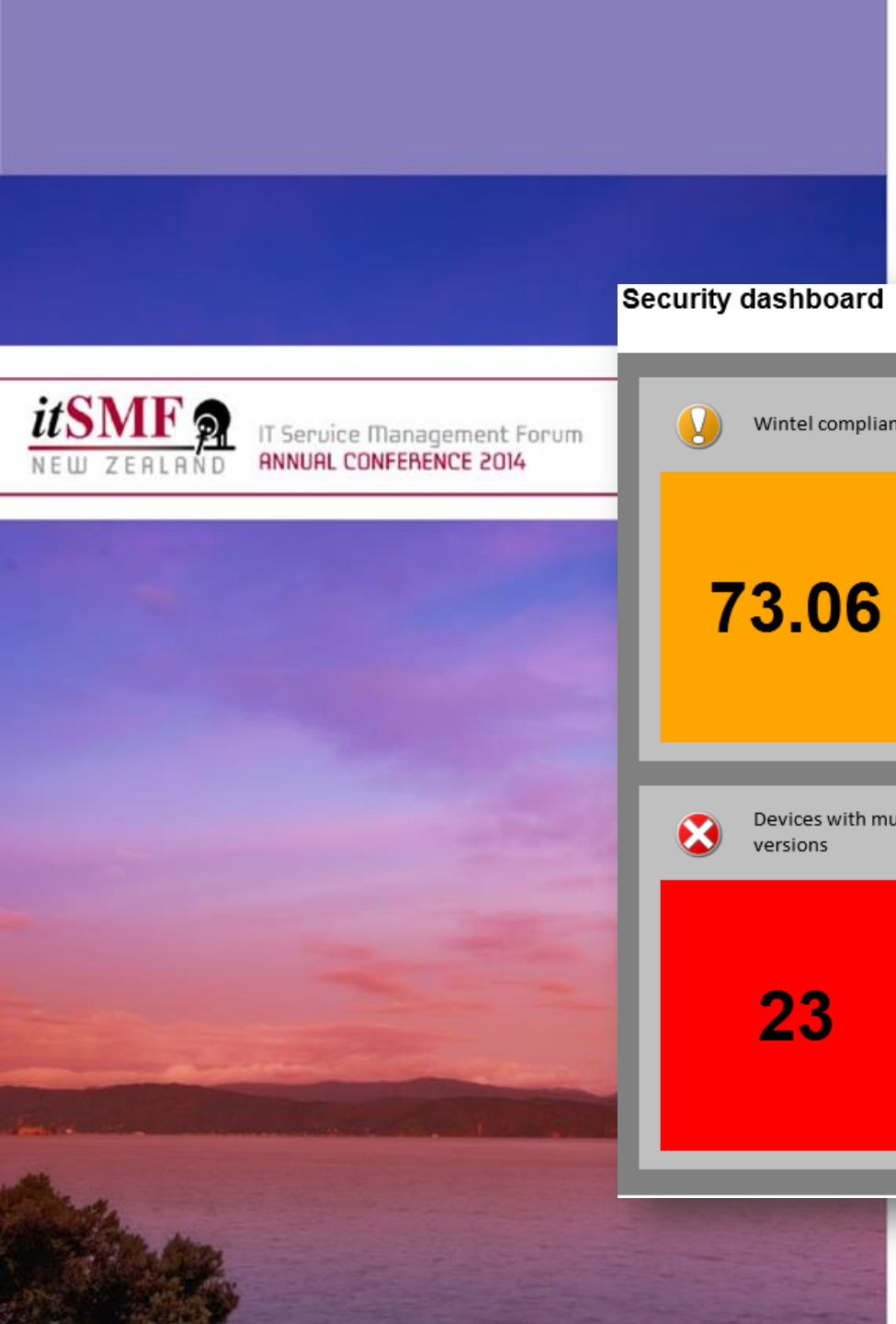


- Extract from AD and SAP
  - Computers
  - Users
  - Groups
  - Group membership
    - Needs separate process to resolve groups
  - SAP Personnel
- Determine AD users no longer in SAP
- Determine individual users with elevated privileges

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

3 levels of reporting

Level 1: The security dashboard



Click to jump to the Level 2 report

Security dashboard

Wintel compliance (%)	Virus signature compliance (%)	Accounts not requirin… Password
73.06	79.53	18
Patching compliance	Virus detection	Identity management
Devices with multiple OS versions	Firewall rules used in past 365 days	SAP - AD mismatches
23	76	158
Network device OS	Perimiter security	

Related reports

- 300 - Identity Management Dashboard
- 301 - Identity Management Account Details
- 302 - AD accounts without matching SAP record
- 303 - AD accounts with elevated privileges
- 304 - AD EPO device match mismatch
- 305 - Patching Dashboard
- 306 - Security Dashboard
- 307 - Patching nonCompliant Devices
- 308 - Devices missing a patch
- 309 - Virus Threat Dashboard
- 310 - Virus Threats at a device
- 311 - Network Device OS Dashboard
- 312 - Network Devices
- 313 - Perimiter Security
- 314 - Missing patches
- 315 - Security reports
- 316 - Firewall Rule Usage
- 317 - Members of an AD Group
- 318 - AD accounts
- [illegible] - AppSense Usage Data
- 399 - Security Dashboard test

Click to jump to other reports

Level 2: Identity management

Click to jump to the Level 3 report

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

Level 3:

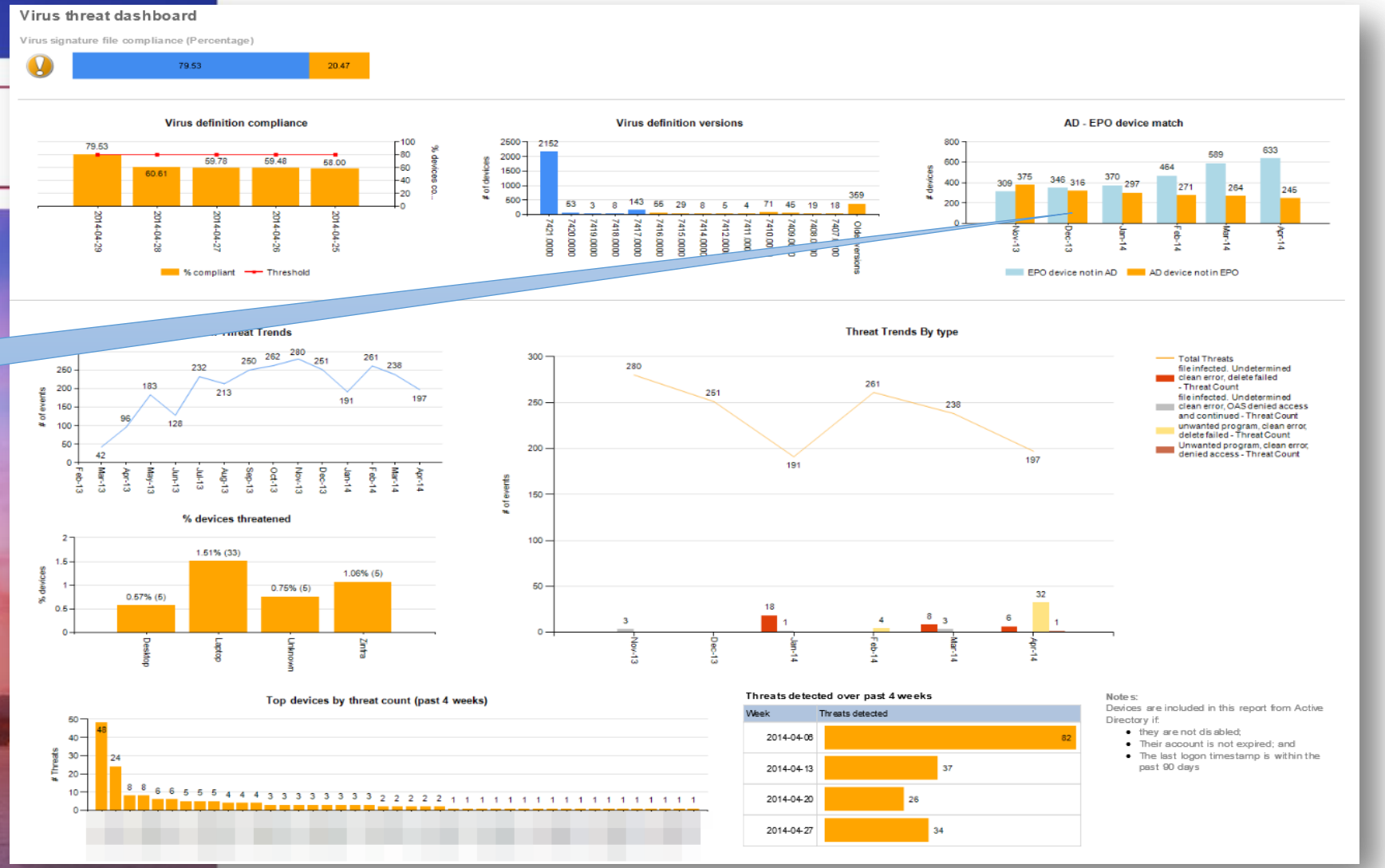
- In this case the level 3 report identified the AD user records that don't have a matching SAP record or a SAP record that is no longer current

AD Name	AD Given Name	AD Sur Name	Display Name	Distinguished Name	Mail	Manager

Level 2: Virus threat dashboard

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

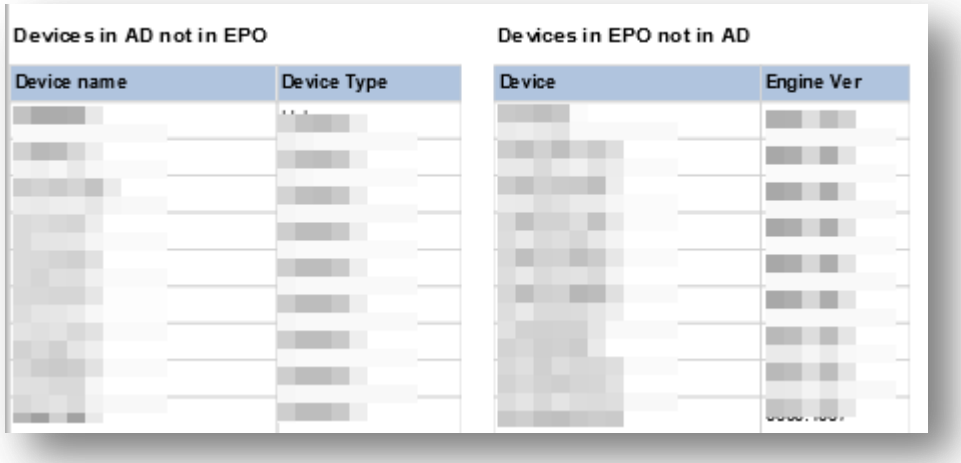
Click to jump to the Level 3 report



itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

Level 3

- This level 3 report identifies AD devices not in EPO and visa-versa



Devices in AD not in EPO

Device name	Device Type

Devices in EPO not in AD

Device	Engine Ver

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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)

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

itSMF NEW ZEALAND IT Service Management Forum ANNUAL CONFERENCE 2014

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

Web: www.reportingservices.com