Everything you wanted to know about mainframe security, pen testing and vulnerability scanning .. But were too afraid to ask!

World Class, Full Spectrum, z Services

Agenda

- Introduction
- Objectives
- Skills
- Processes
- Tools
- Education
- Putting the tools to use
- Summary
- Questions

IBM Mainframe
Are they really secure?

Introduction

Introduction

- Mark Wilson
  - Technical Director at RSM Partners
  - I am a mainframe technician who's specialist subject is Mainframe Security
  - I have been doing this for over 30 years (35 to be precise ☺)
  - This is part seven of seven one hour long sessions on mainframe security…
  - Full details can be seen on the New Era Website:
    - http://www.newera-info.com/MF-SEC.html

My passions outside of work?

- One wife and three daughters…..enough said…..don't have anytime or money for anything else….or so they tell me ☺

- Motorbikes
  - www.wilson-mark.co.uk

- Football
  - www.wba.co.uk

- Scuba Diving
  - Way too many links to list here…..But I have been and dived here
  - http://en.wikipedia.org/wiki/Chuuk_Lagoon

OBJECTIVES

Objectives

- We have covered a fair amount of technical stuff over the last few months
- This is not so much of a technical session
- We will look at the skills needed to do mainframe security properly
- We will look at some of the processes we need
- Then we will take a look at the tools required today

Skills

Skills

- This is not just an IT security issue
- We know we have an IT skills issue and this is even more evident in the mainframe security space
- We need a wide array of skills:
  - Security Administration
  - Security Engineering
  - Auditing
  - Risk, Compliance, Assurance
  - A Translator…..er a what???

Process

Process

- I must admit being a mainframe techie / systems programmer I have never been a big fan of process…
- My how times have changed.....
- We need formal, well documented and well managed processes for:
  - Joiner, Mover & Leavers (JML)
  - Role Based Access Control (RBAC)
  - Re-Certification
  - Data Classification

JML

- This needs to be an Enterprise Wide process
- Its not just about your mainframe users
- One day we had a user called FRED
  - Who was a senior VP in the marketing team, who left to join a competitor….. What a tale that was!!

Role Based Access Control (RBAC)

- Something a lot of organisations believe they have actually implemented
- From a mainframe security perspective this is granting access in a logical and structured matter
- Implementing RBAC needs careful planning and analysis of the current access patterns of your user base
- You need a design and a detailed plan

Re-Certification

- This is so much easier if you have implemented RBAC as it allows the organisation to:
  - From a User perspective review which roles each user has on a fairly regular basis
  - From a role perspective look at what access rights a role has

- But….If we are going to ask the business to do this we need to couch the reports/data we give them to review in business terms and not just a list of RACF, ACF2 or TSS resources

Data Classification

- In my opinion this is one of the main building blocks for delivering a strong mainframe security implementation

- How can we expect…
  - Our adminsitarors to effectivley manage
  - Our business users to recertify access if they
  - Our securty engineers to implemenet the correct level of monitoring, alaerting and reporting if they

- The problem is this is a large project for most organisations as we tend to have a lot of data and resources on our mainframe systems

Tools

Tools

- The days of the techies writing bespoke tools/solutions for their own organisation are long over

- Mark the Systems Programmer writing Assembler, REXX, etc is a major risk to most organisations today

Tools

- What about when Mark…
  - Moves team/department
  - Leaves the organisation
  - Retires…..because trust me Mark wants to retire

- But also what happens when:
  - IBM/ISVs update their products and your tools stop working
  - You have a major issue with the tools and Mark is not available

- There are way too many risks for any large organisation to rely on a bit of code that Mark the Sysprog has written….

Tools

- Trust me I know my coding abilities ☺
- Therefore, we must look to the professional tool developers for solutions
- The tools are:
  - Designed by Security Professionals
  - Written by, in most cases experienced Software Developers
  - Supported by the vendor 24 x 7
  - They are tested with the latest releases of z/OS and other software products

Tools

- The Techies, Engineers or Security Engineers should be focused on integrating the tools you have acquired into your processes and procedures
- And not creating/writing tools with all of the risks previously mentioned
- So we need to look to the market for solutions and we do have some choices

What's out there?

- The majority are RACF focused, but some do support ACF/2 and TSS

- The key players are:
  - IBM with zSecure
    - https://www-01.ibm.com/software/security/products/zsecure/index.html
  - Vanguard
    - https://www.go2vanguard.com/

- Make sure the tools you choose can meet the majority if not all of your requirements

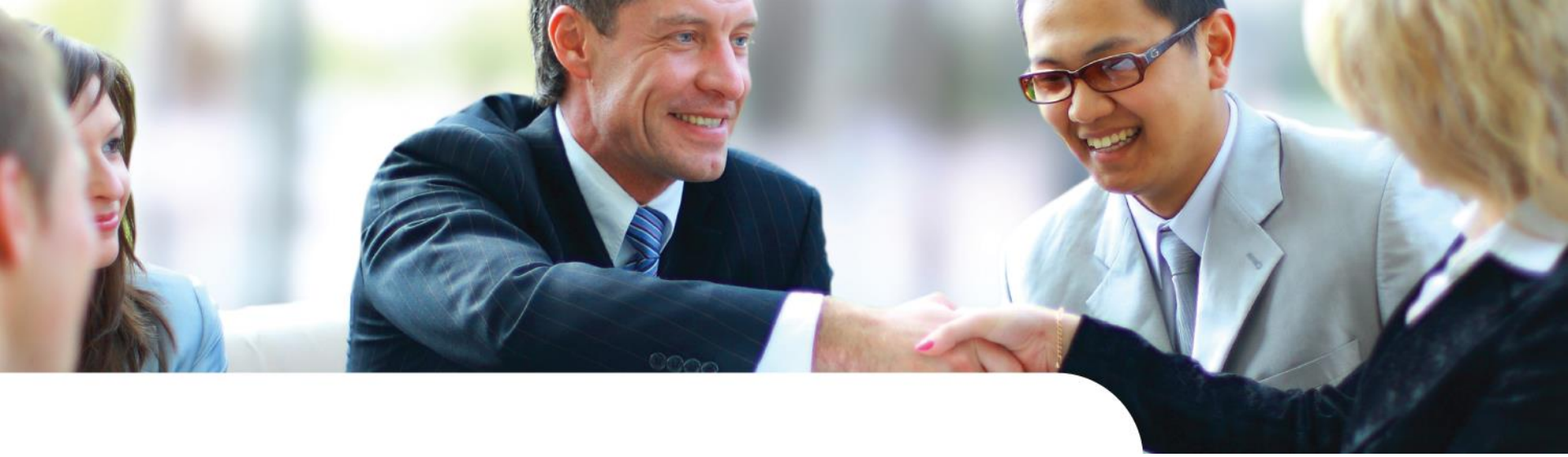
What's out there?

- Other RACF tools
  - ASPG with ERQ
  - Beta Systems with BETA88
  - SEA with RA/2, RA2002 and RA/7
  - RSM with RACF GUI
  - Etc……
- There are ACF2 and TSS tools available from:
  - EKC
  - INFOSEC
  - Etc…….

Tools

- Don’t rush in and buy the cheapest tools out there
- Gather ALL of your requirements
- Make sure their solutions can meet your requirements
- And remember…

Quality is remembered long after the price is forgotten



Education

Education

- Is a key component in any security strategy
- And this is not just about technical training for the security teams
- We need to educate our users and not just the users of our mainframe systems
- Security Awareness training is just as important as technical training for the engineers

Education

- However, as we are all techies lets focus on that..
- There are many organisations out there offering mainframe security training
- Just google RACF Administration training…

Education

- IBM
- Vanguard
- Stu Henderson
- RSM Technology
- RSH Consulting
- Then you have the conferences
  - Share
  - GSE UK and Europe
  - Vanguard

Putting the tools to use

The good old days!

The good old days

The good old days

- Believe it or not there are still organisations who do this today…
- OK, they may not print it all, but they review the previous 24 hours activity
- So, if you run your reports at 06:00hrs each day….How much time do I have to play with your system before you realise something is wrong?

Where are we getting it wrong?

Where are we getting it wrong?

- Processing data that is up to 24 hours old is just not a viable solution in **the world we live in today**

- Having to pore over thousands of lines of output is too time consuming and prone to error and not viable for **the world we live in today**…..

Where are we getting it wrong?

- What world do we live in today?
  - We live in a world where our IT Systems are under constant attack from inside and outside of the organisation
  - Many of the thinkers in this space believe the bad guys/gals are already in our organisations and wandering around our networks and servers doing something
  - We need to know what they are up to and we need to know as soon as they start doing something
  - IBM has stated that the average time to realise a breach has occurred is 205 days and it's usually a client or the FBI who notices it first

Where are we getting it wrong?

- Other challenges we see/face:
  - Reports are produced, but no one really looks at them
  - If the reports are created/reviewed there is quite often a lack of understanding
  - Lack of a dedicated monitoring team or SOC
    - And in some cases when they do exist, they see the mainframe as an environment too complex or too secure that does not require their attention
  - Lack of proper planning, we see clients just producing alerts and monitoring reports just to appease the auditors

Where are we getting it wrong?

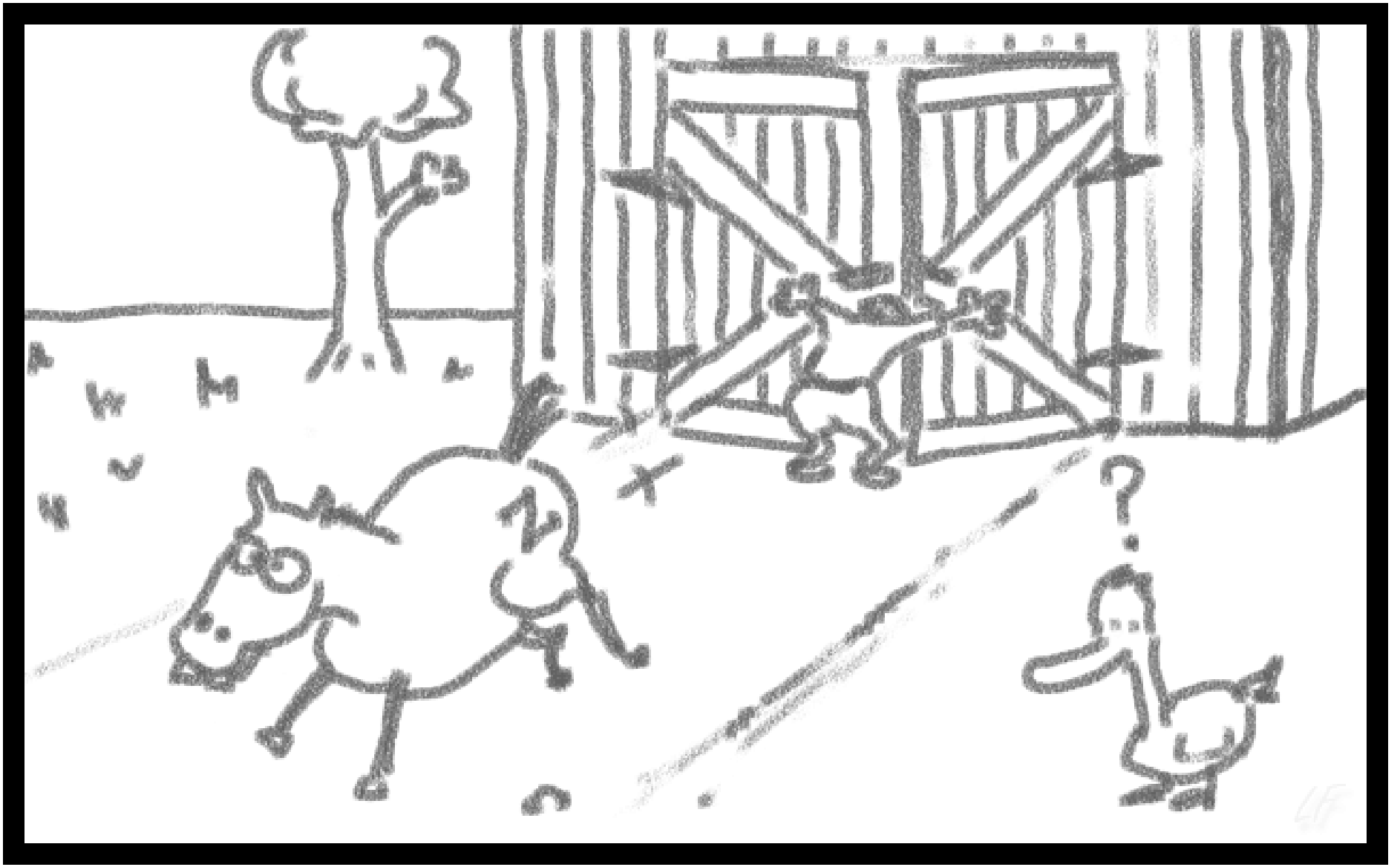
- Conversation that we were party to at a client..
  - What do you think audit may want to see?
  - Don’t really know…..but let’s create the following reports and alerts……..that will keep them happy……
- Result….
  - A solution that’s most likely not fit for purpose
  - With no real owner

Where are we getting it wrong?

- So, hopefully you can all see that processing our log data 24 hours after the event is just no longer fit for purpose
- Alerting needs to be Real Time and it needs a purpose
- We need to move to exception based reporting, so that we can see the wood for the trees!

Where are we getting it wrong?

- And its not just a mainframe issue!
- Ever heard of a SIEM?
- How many of you have a solution?
- How many of you are integrating your mainframe data into your SIEM?
- What's the old saying…. About the horse having already bolted!!



What's an SIEM?

SIEM – As far as Wikipedia is concerned

- What is SIEM?
  - Security information and event management
  - The acronyms SEM, SIM and SIEM have been sometimes used interchangeably
  - The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as security event management (SEM)
  - The second area provides long-term storage as well as analysis and reporting of log data, and is known as security information management (SIM)
  - As with many meanings and definitions of capabilities evolving requirements continually shape derivatives of SIEM product categories

Getting Mainframe Data into an SIEM

- Not as difficult as it might seem
- There are solutions out there to do this….
- But you have to be careful not all of our current SMF, SYSLOG and other log data needs to go to our SIEM
- You need to analyse what you produce, why you produce it and then decide if it should go to the SIEM

Why put mainframe data into an SIEM

- I would hope that you all have got this by now!!

- If you want to create that holistic view of what's going on in your enterprise from a security perspective then you have to populate your SIEM with the relevant mainframe data

Which SIEM?

- Well there are certainly plenty out there:
  - Splunk (Seems to be the most popular today)
  - Graylog2
  - Nxlog
  - Octopussy
  - Logscape,
  - ELSA
  - LOGanalyzer
  - Logalyzer,
  - Logwatcher
  - logHound
  - logReport
  - Logsurfer
  - PHP-Syslog-NG

The ELK Stack

- Elasticsearch:
  - Indexing, storage and retrieval engine
- Logstash:
  - Log input slicer and dicer and output writer
- Kibana:
  - Data displayer

- http://linuxfestnorthwest.org/sites/default/files/slides/Log%20Analysis%20with%20the%20ELK%20Stack.pdf

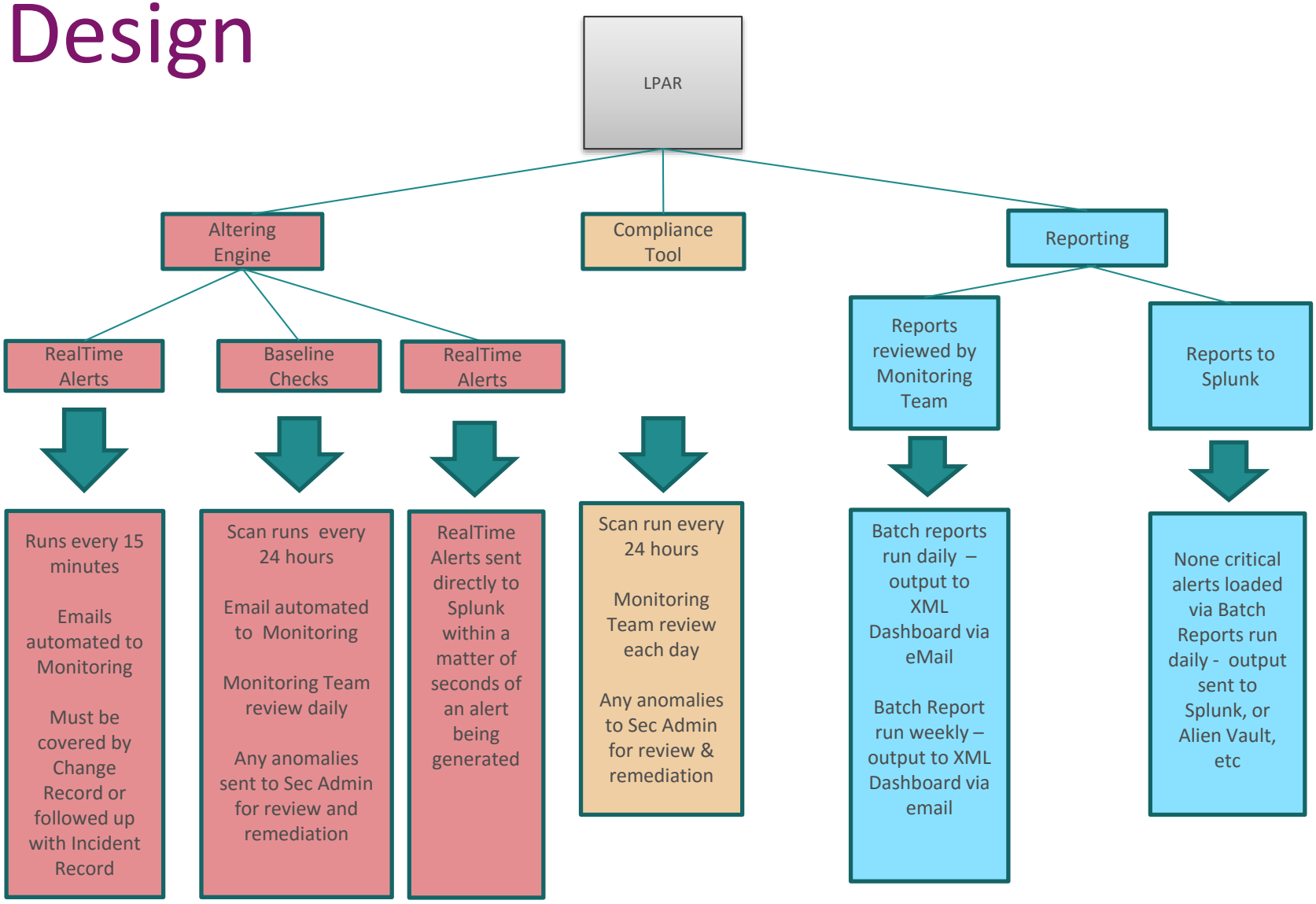
A Design and Plan

Design and Plan

- You must have a
  - Design
    - High level to start with
    - Detailed when you have collected all of your requirements
  - Plan

- How can you choose tools/solutions from vendors if you don't know what you want to achieve

A Design


LPAR
Altering Engine
Compliance Tool
Reporting
RealTime Alerts
Baseline Checks
RealTime Alerts
Reports reviewed by Monitoring Team
Reports to Splunk
Runs every 15 minutes
Emails automated to Monitoring
Must be covered by Change Record or followed up with Incident Record
Scan runs every 24 hours
Email automated to Monitoring
Monitoring Team review daily
Any anomalies sent to Sec Admin for review and remediation
RealTime Alerts sent directly to Splunk within a matter of seconds of an alert being generated
Scan run every 24 hours
Monitoring Team review each day
Any anomalies to Sec Admin for review & remediation
Batch reports run daily – output to XML Dashboard via eMail
Batch Report run weekly – output to XML Dashboard via email
None critical alerts loaded via Batch Reports run daily - output sent to Splunk, or Alien Vault, etc

Summary

Summary

- The rules of the road have changed
- The systems we look after need professionally developed tools to support all of YOUR security processes and procedures
- Its too risky to rely on an individual techie to create, manage and support the tools that underpin your mainframe security posture
- You must have a design and a plan
- Its much more than just your mainframe

Questions

Contact

Mark Wilson
RSM Partners

markw@rsmpartners.com

mobile: +44 (0) 7768 617006

www.rsmpartners.com