Security Analytics Driving Better Metrics

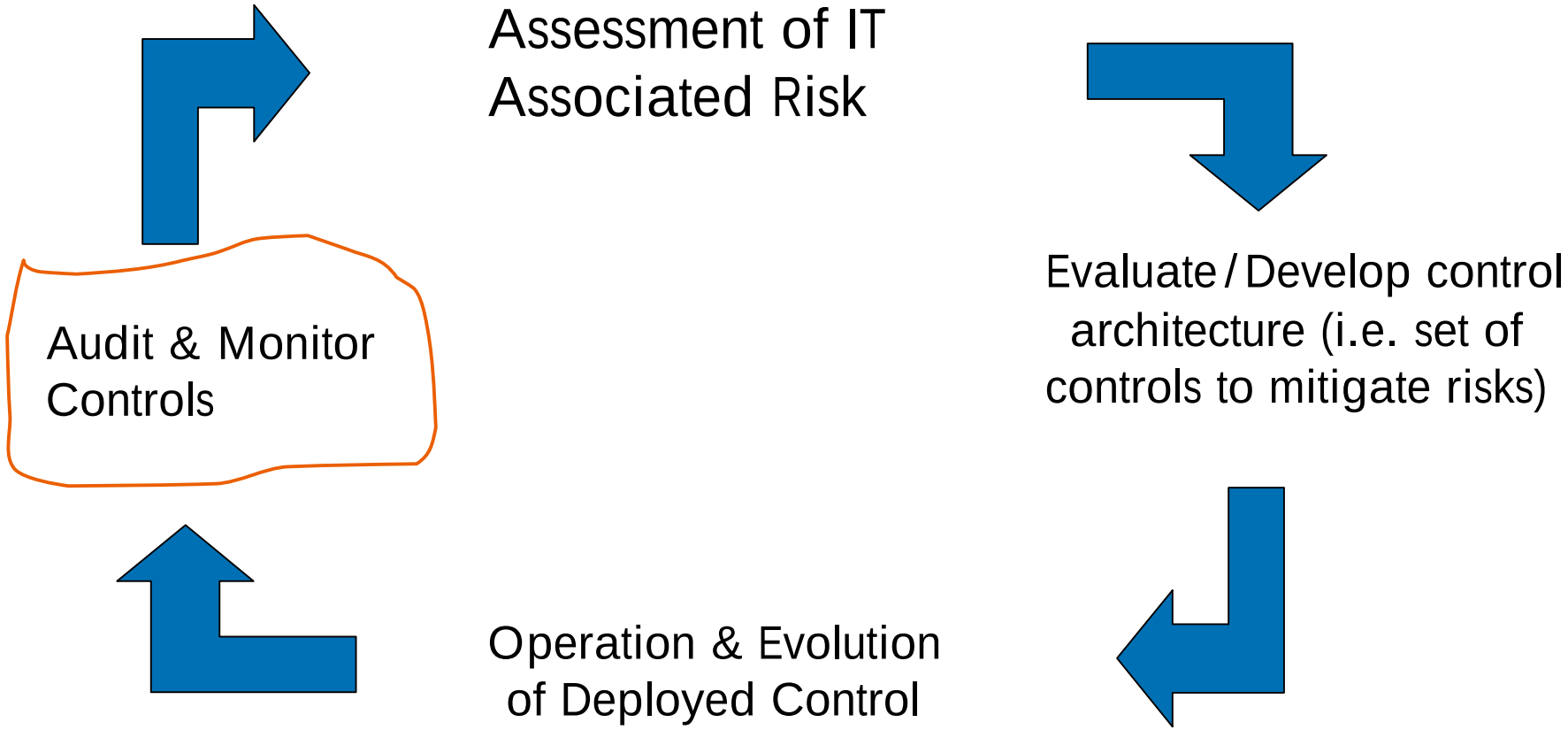
Yolanta Beres

HP Labs, UK

Agenda

- Risk Management Lifecycle
- Historical data based metrics
- Predictive Simulations: selecting better metrics
- Example: vulnerability and patch management
- Conclusions

Security Risk Analysis & Risk Measurement Lifecycle



Changing Assurance Requirements

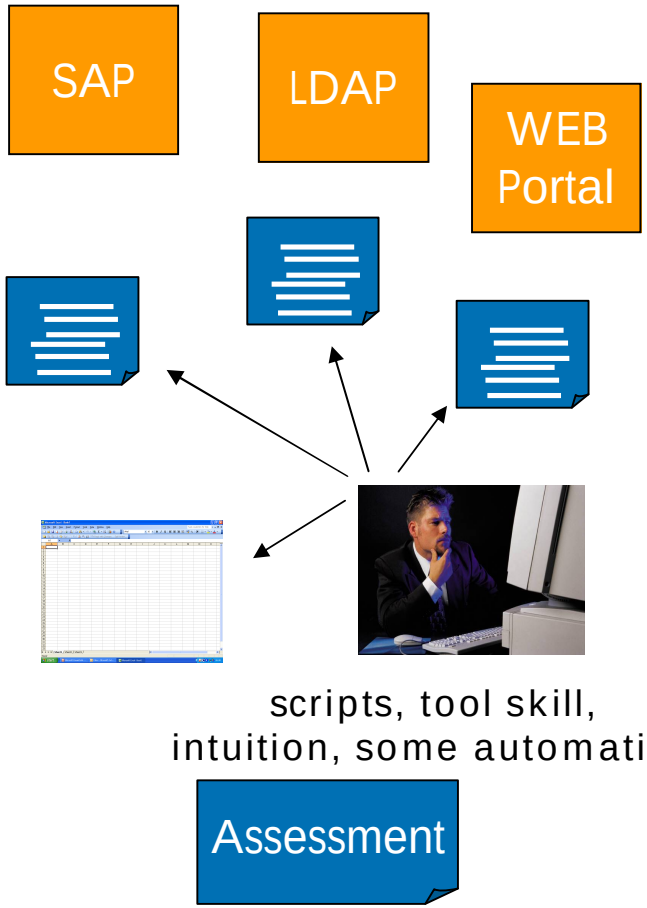
Traditional Assurance

- Cyclical reviews
- Historical-based
- Intrusive
- Point-in-time retrospective
- Unexpected fluctuations in the control environment
- Adherence to rules

New Requirements

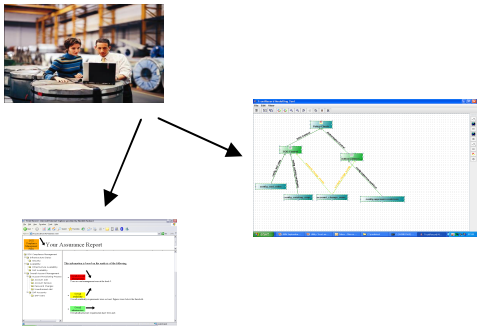
- Ongoing assurance
- Real-time & predictive
- Non-intrusive & remote
- Risk-based
- Analytical decision data
- Sustainable governance model

Security Metrics: Today and Tomorrow



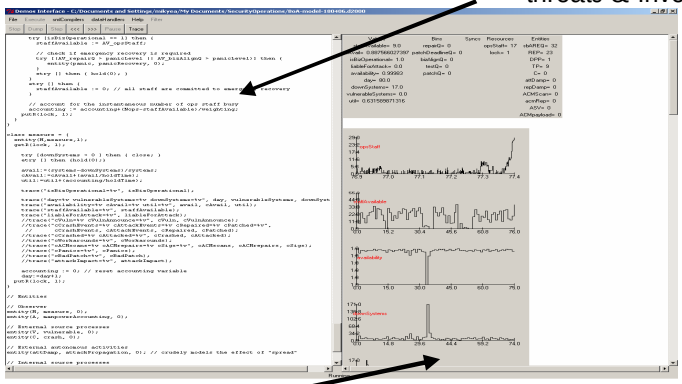
scripts, tool skill,
intuition, some automation

1. Models Driving continuous metrics gathering based on historical data



2. Simulation based security analysis and metrics identification

Systems Models
to vary assumptions on
threats & investments



Predictive Outcomes

Historical data based security metrics

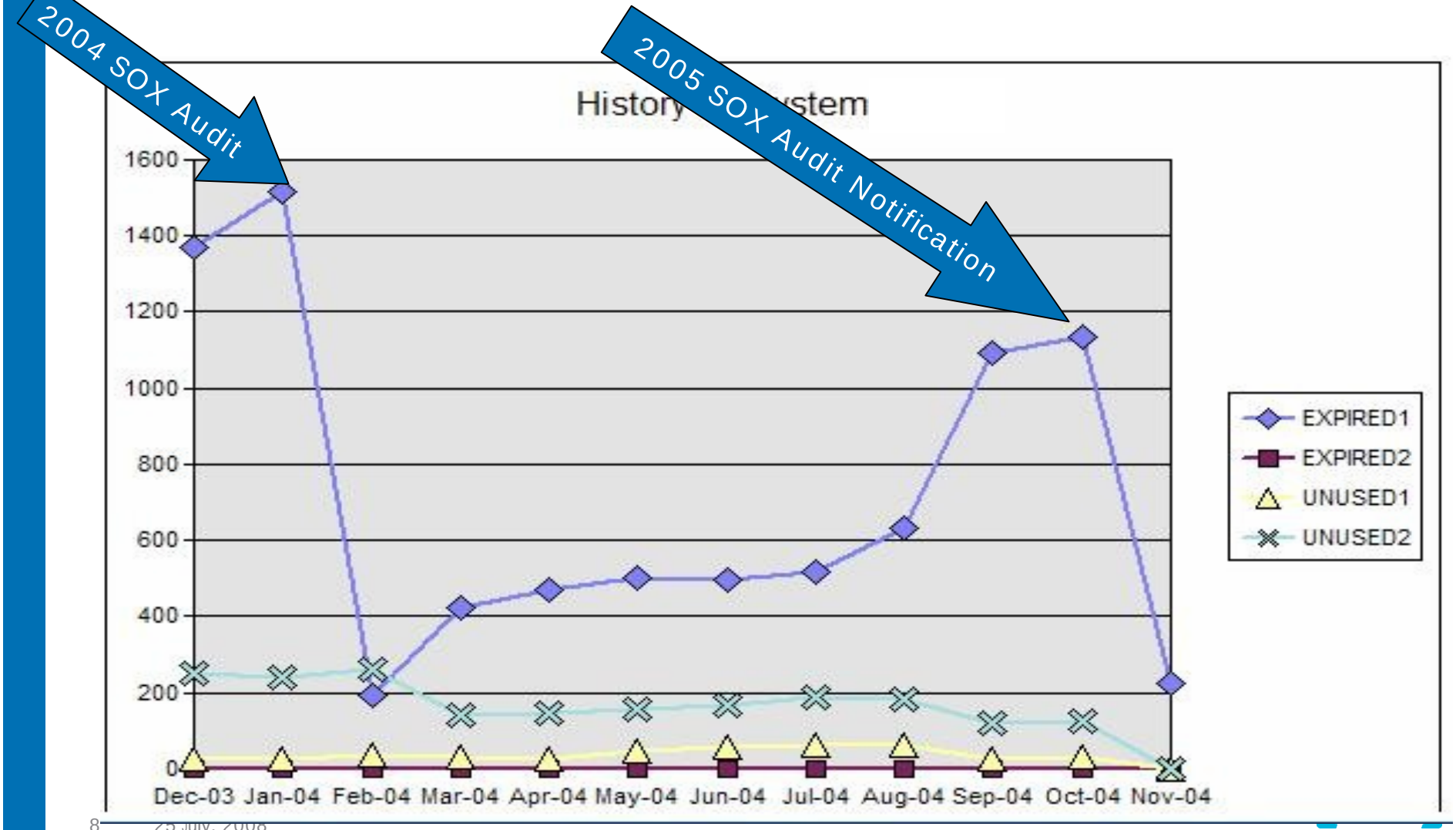
- Often gathered because of audit / compliance requirements
- Allow administrators to measure performance against baseline
- Are meaningful measures to show
  - if security controls are working (not)effectively
  - where risk is emerging (sometimes)

System and security risk modelling

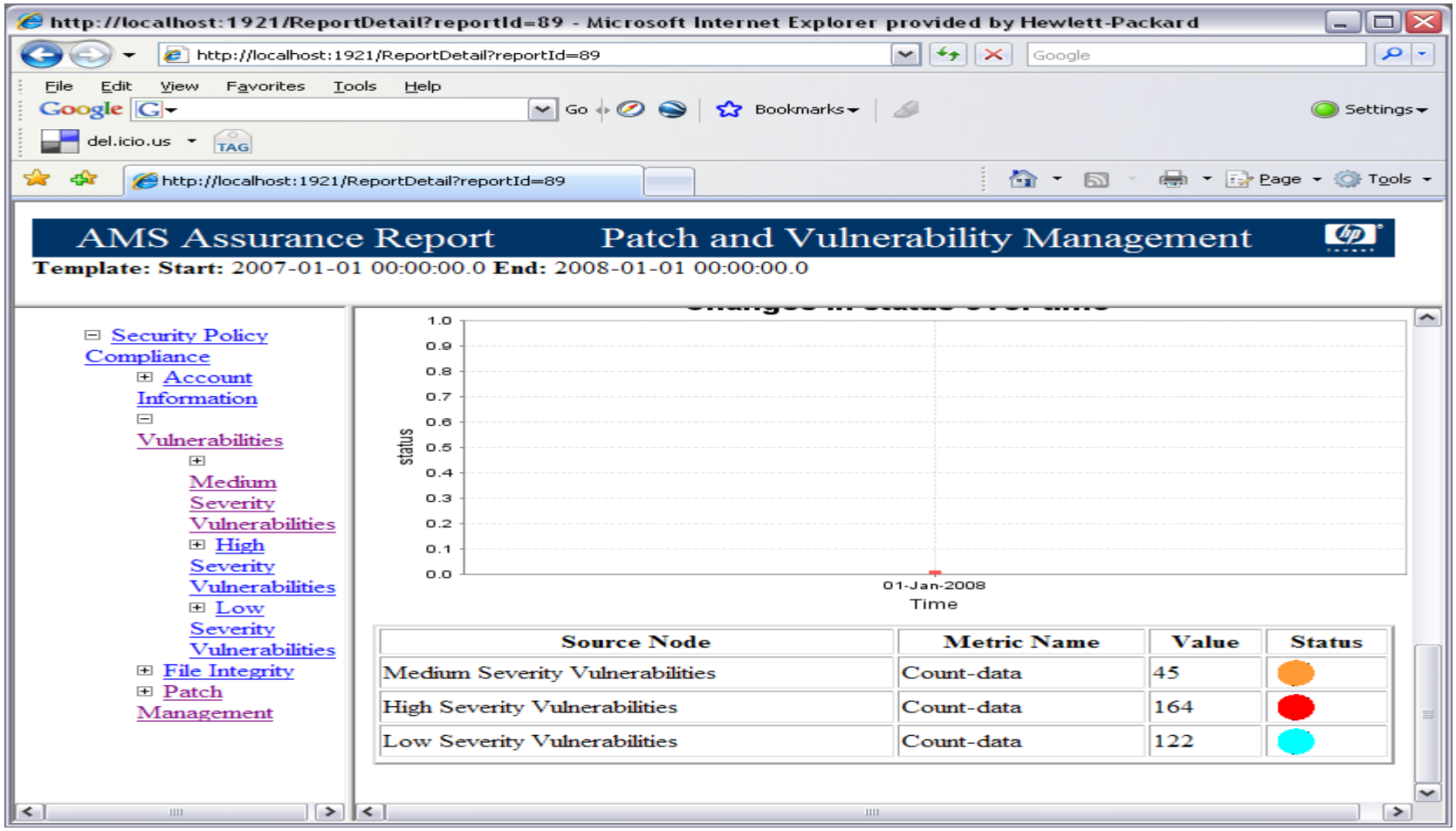
- Explore the effect of various unknown or difficult to obtain inputs, e.g. threat environment
- Enable the prediction of the outcome of investment decisions or changes in security policies
- Identify better RISK metrics
- Identify metrics that are relevant to an organisation

Audit selected key indicators

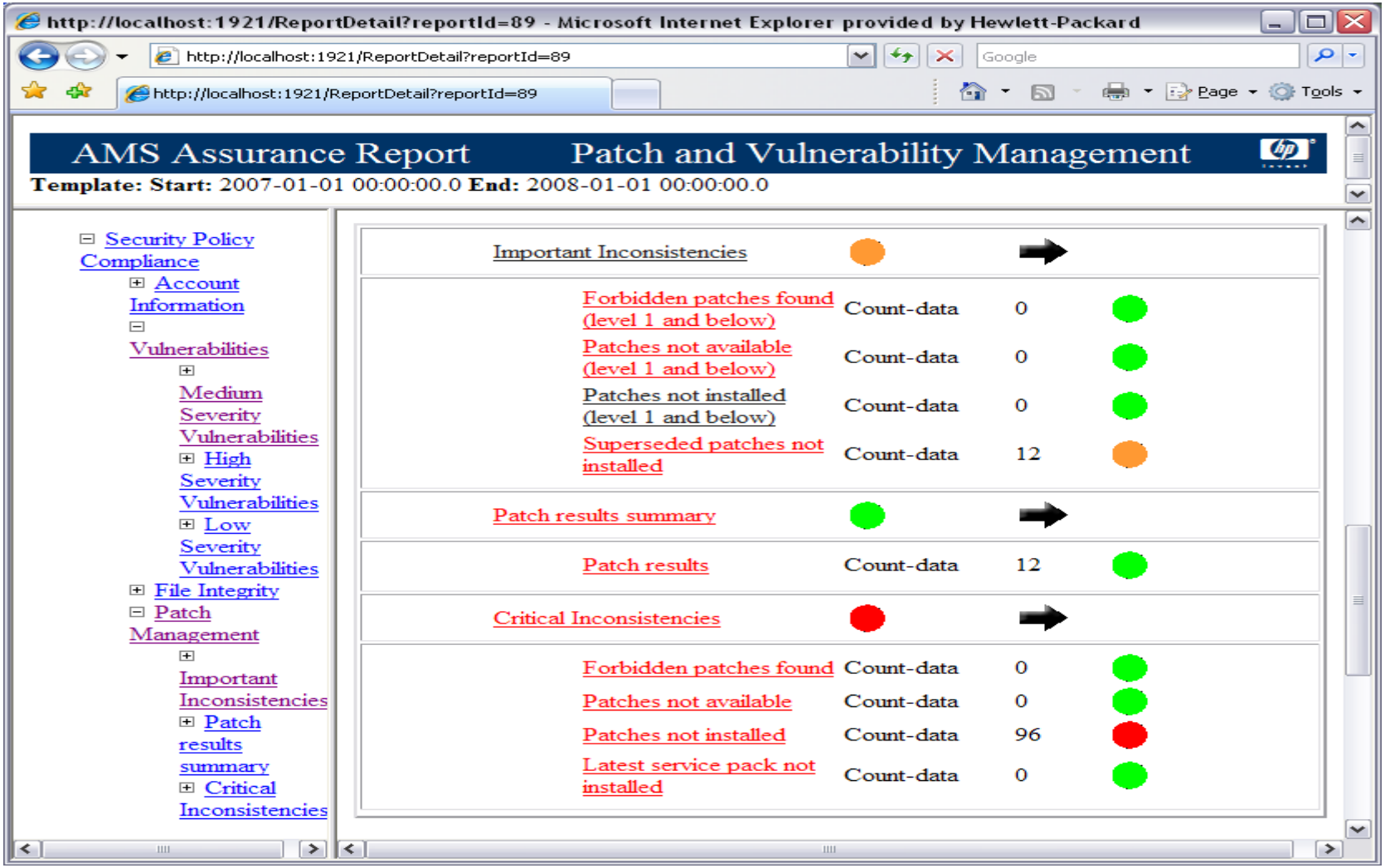
Measuring Inactive Users as a Leading Indicator of Security Effectiveness



Traditional security metrics for vulnerability reporting



Traditional security metrics for patch management



Better metrics needed

Example: threat mitigation by patch management

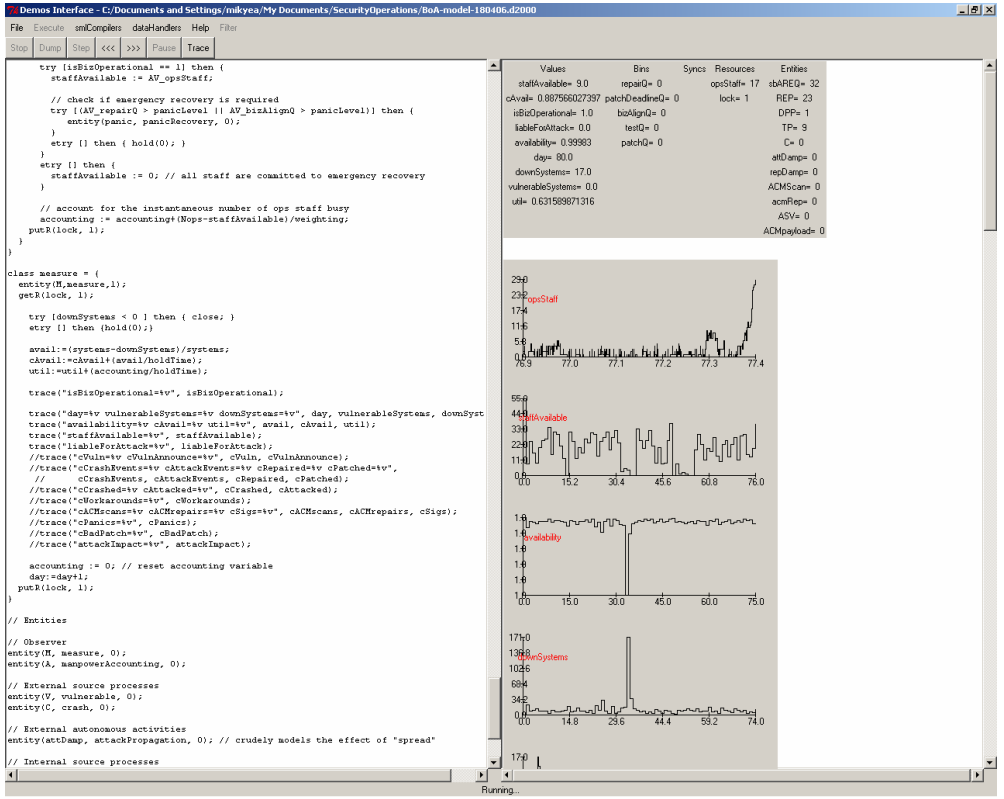
- Historical metrics
  - Indicate performance of patch management process
  - Show what happened

But:

- Do not explain why or implications
  - Is it high risk if a couple of patches are not installed?
  - How much an organization will be exposed when malware hits?

Stochastic Simulations: what are they?

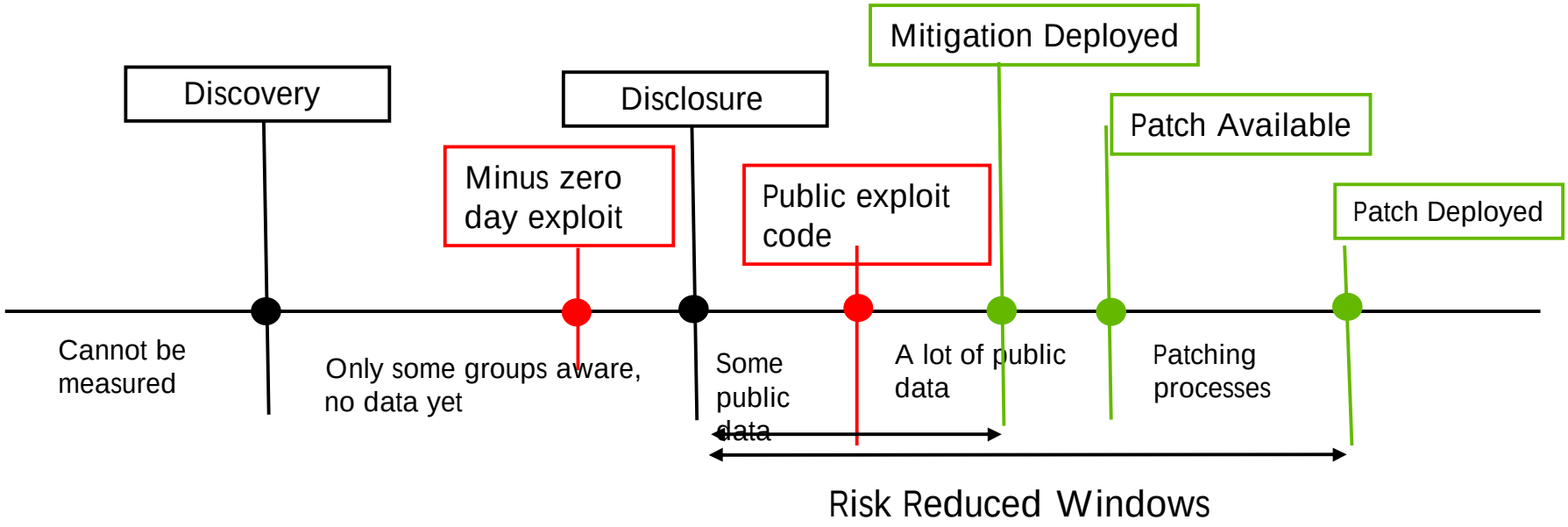
- A large number of discrete event simulations which reflect the random variation in the input events as observed in historical data
- Capture / model the system, its usage and processes
- Sample the known distributions for input events: exploit after disclosure and for patch after disclosure
- Monte-Carlo approach to gather statistically significant information, via repeated experimental runs.
- Measure potential outcomes as probability distributions



Vulnerability Management Example

- Select the metric: exposure window
  - Time from vulnerability disclosure to risk reduced
- Model the patch management processes, and processes to deploy early, often signature-based mitigations and workarounds
- Analysis
  - Current state: assessing robustness against threat environment assumptions
  - Potential improvements

Selecting metrics based on vulnerability timeline

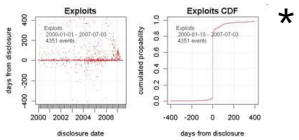


Showing time to risk reduced as probability distribution function across thousands of vulnerability instance

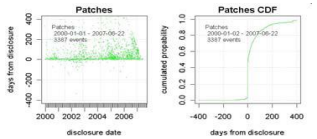
Select metrics

- Mean time to risk reduced
- Early mitigation: within the first days of disclosure
- The tail: after the set policy deadline

Modelling the security processes



*



*

Malware

Exploit Available

Vulnerability Disclosed

Patch Available

Assess

Test Solution

Patch Preparation

Threat Assessment

Deploy

Standard Patching

Signature-based Early Mitigations

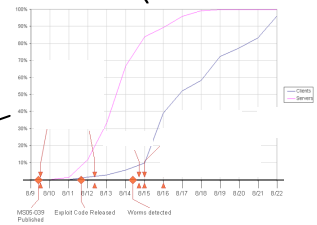
Accelerated Patching

Deploy twice quicker than Standard Patching

Work Around

Ermergency Patching

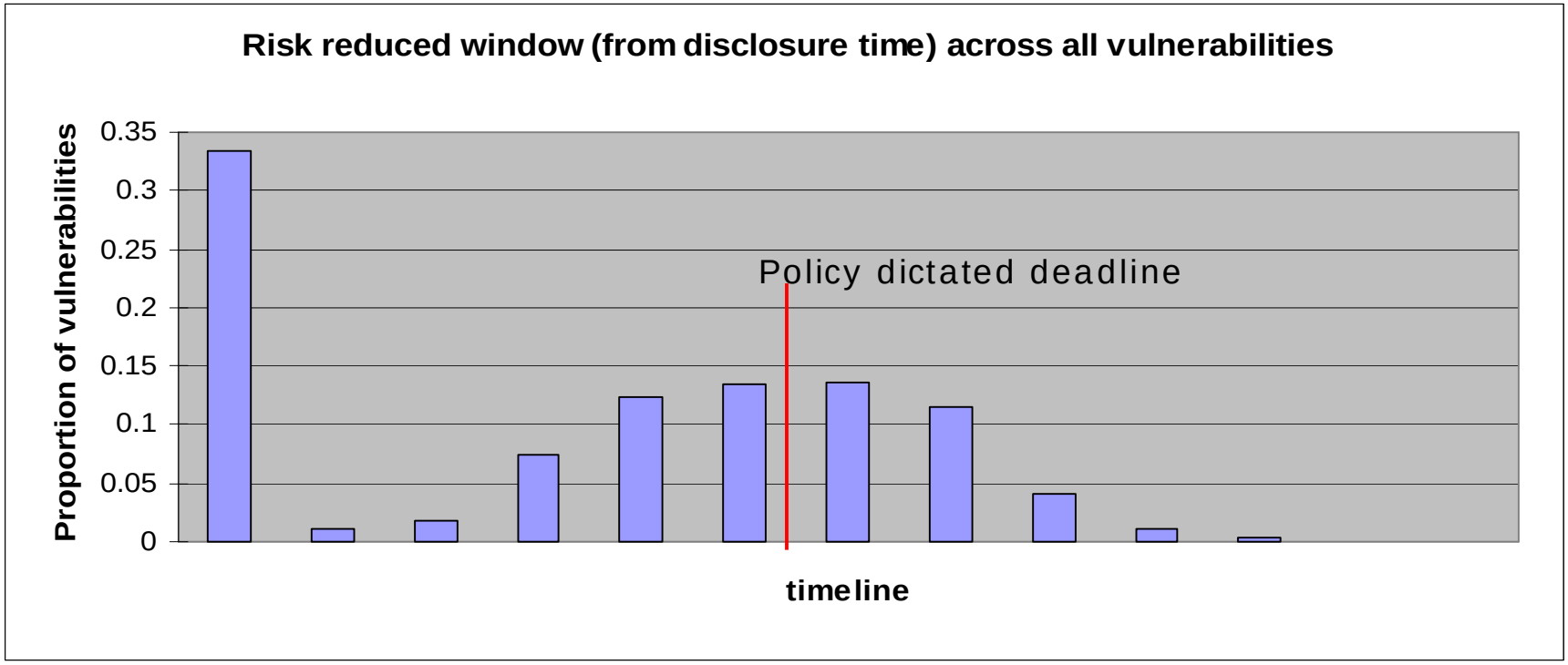
Deploy three times quicker than Standard Patching



Sample a uniform distribution of 3-5 days for signature deployment

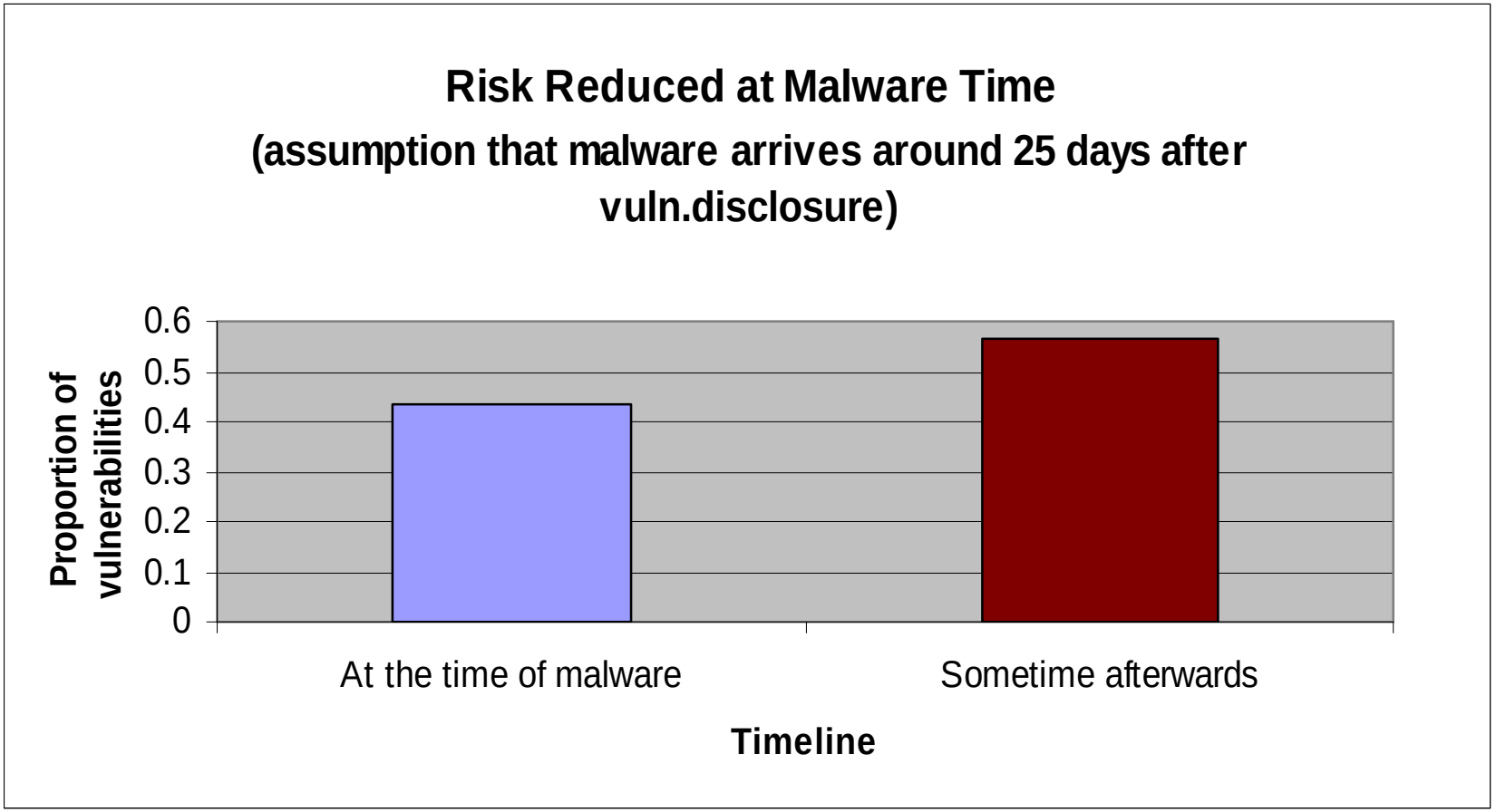
* Source: Stefan Frei, Martin May, Ulrich Fiedler, Bernhard Plattner. Large-Scale Vulnerability Analysis. Proc. of SIGCOMM'06 Workshops, September 2006

Risk reduced window overall



	Proportion mitigated in early days	Proportion not mitigated after the policy deadline
Current state	33%	31%

What is the state when malware arrives?



Better metrics for historical monitoring

- Previously:
  - #patches not installed
  - #open vulnerabilities
- After the modelling and simulations:
  - How long vulnerabilities have been opened
  - How many patches are behind policy dictated deadline
  - How many patches not installed that AV does not cover
  - Monitoring threat level for each case

Conclusions

- Historical data based metrics are good to show
  - Where controls are working effectively
  - Or where risk is emerging
- Predictive modelling allows
  - Helps select better metrics that are risk indicators of current and future security risks
  - Ensure robustness of selected metrics in changing conditions
  - Use metrics in simulations to understand trade-offs between different solutions


LABS hp