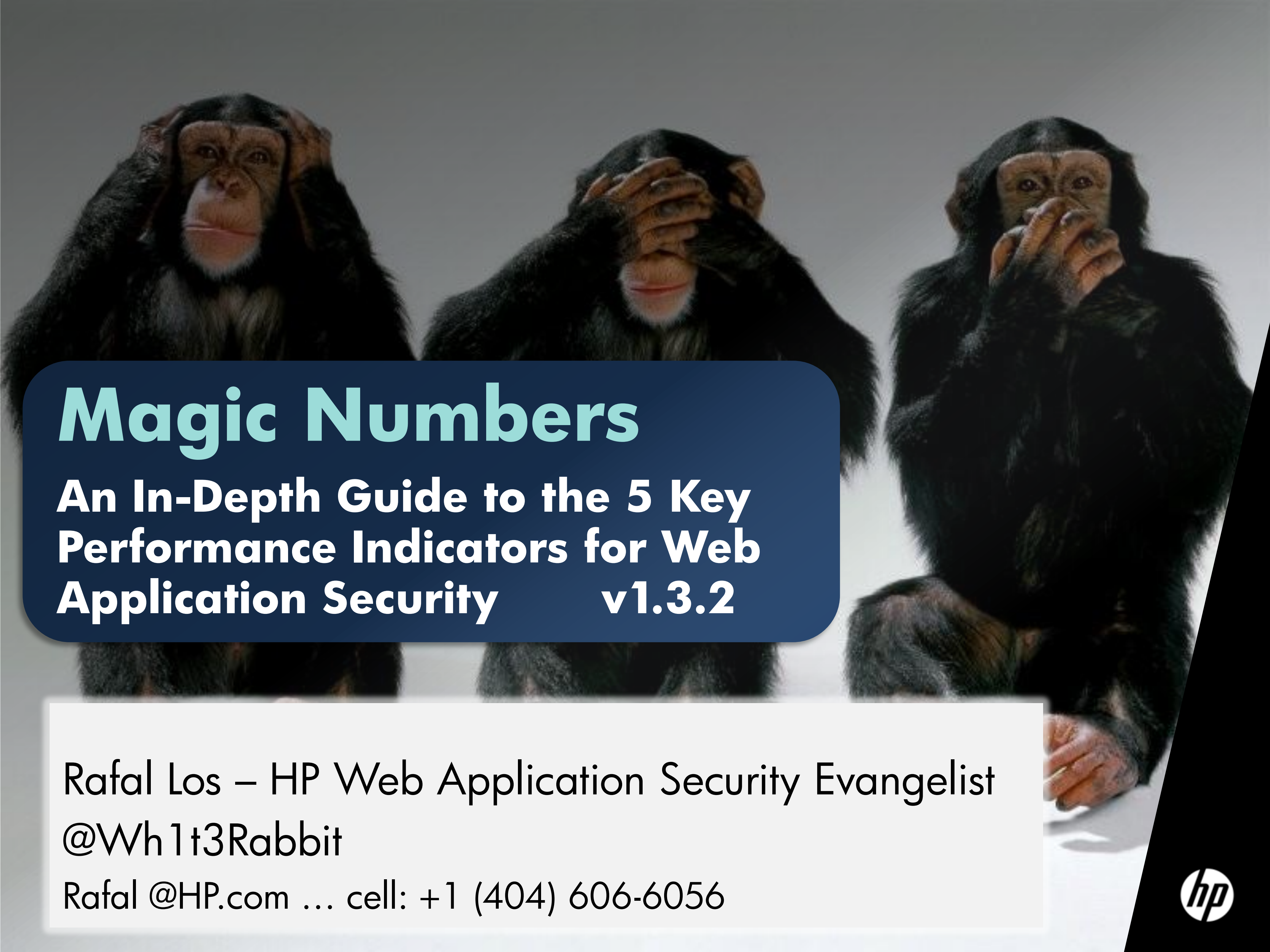


Magic Numbers

An In-Depth Guide to the 5 Key Performance Indicators for Web Application Security v1.3.2

Rafal Los – HP Web Application Security Evangelist
@Wh1t3Rabbit
Rafal @HP.com … cell: +1 (404) 606-6056

Proceedings

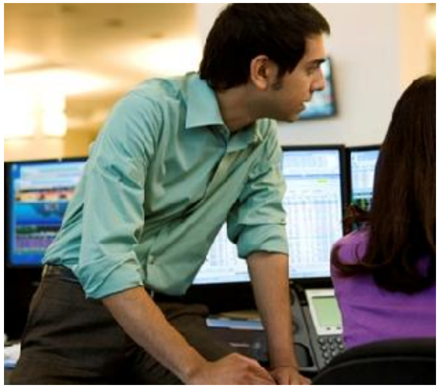
1 Background

Understand the need for business-level intelligence

2 Essential KPIs

Identify essential KPIs, their definitions, components

3 Applications



Applying the 5 Essential KPIs to Enterprise Programs

4 Practical

A practical example of real-life application of KPIs

Background

Metrics, KPIs, and Information Security

When I first came here, this was all swamp. Everyone said I was daft to build a castle on a swamp, but I built in all the same, just to show them.

It sank into the swamp.

So I built a second one. That sank into the swamp.

So I built a third. That burned down, fell over, then sank into the swamp.

But the fourth one stayed up. And that's what you're going to get, Lad, the strongest castle in all of England.

Monty Python & the Holy Grail (King of Swamp Castle)

Yes.

Web Application Security programs have been known to fail in spite of their success…

Security Metrics Primer

INFORMATION SECURITY HAS HAD A ROUGH RELATIONSHIP WITH METRICS

Three core issues with metrics in security:

1. Very little actuarial data to support initiatives
   - Virtually no data supporting likelihood of being successfully attacked
2. Incorrect, hasty use of metrics as intelligence
   - Vulnerabilities being used as risks
   - Metrics – math without context
3. "It hasn't happened to me" being used as a metric
   - Many victims don't know, or won't admit it

Information Security hasn’t capitalized on available metrics … can KPIs save the day?

KPI Primer

A **key performance indicator** (**KPI**) is a measure of performance, commonly used to help an organization define and evaluate how successful it is, typically in terms of making progress towards its long-term organizational goals.

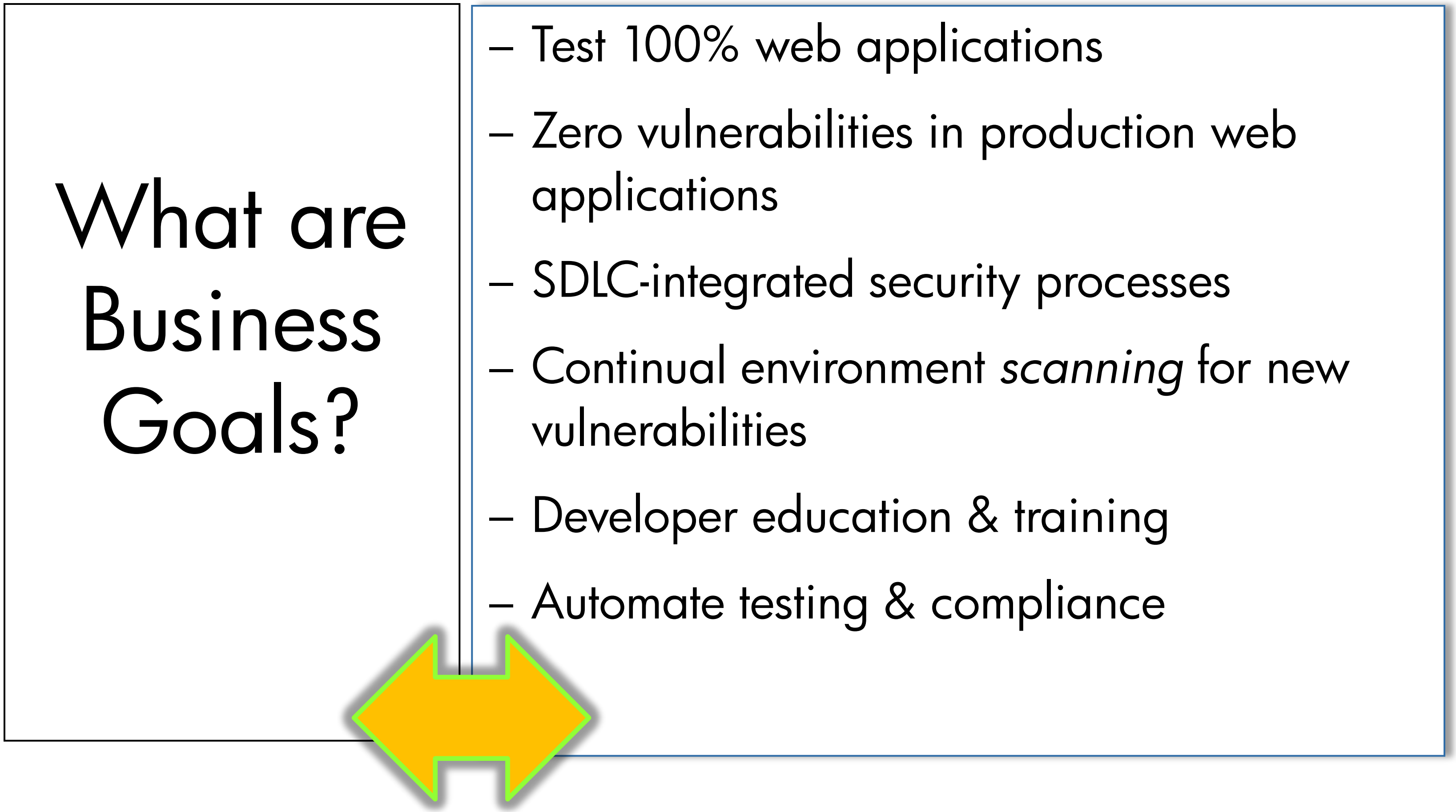
KPI Primer

A **key performance indicator** (**KPI**) is a measure of performance, commonly used to help an organization define and evaluate how successful it is, typically in terms of making progress towards its long-term organizational goals.

Business vs. IT Goals

Business Goals

IT Security Goals [Web App Sec]



What are Business Goals?

- Test 100% web applications
- Zero vulnerabilities in production web applications
- SDLC-integrated security processes
- Continual environment *scanning* for new vulnerabilities
- Developer education & training
- Automate testing & compliance

Business thinks in terms of risk.
Risk is bad, seen in shades of gray.

Web application vulnerabilities contribute to IT risk
IT risk is a factor of overall business risk

Business goal: Reduce IT risk to acceptable level.

Mindset reset

Tough Questions

Will it be possible to perform an analysis of 100% of enterprise web applications?

Will a zero vulnerability metric be reachable, practical or even desirable?

Is vulnerability reduction the same as risk reduction?

Enterprise Application Security Program Challenges

Challenges

– Get funded → Justify required resources

– Find vulnerabilities → Bugs in business critical apps

– Removing defects → Decrease risks with a budget

– Proving success → How do you prove success?

Resources

– Security vulnerability metrics

– Application registries

– Defect tracking systems

– Data from tools, human testing

Essential KPIs

Proving Success with Advanced Metrics

The 5 Key Performance Indicators (KPIs)

WRT – Weighted Risk Trend

DRW – Defect Remediation Window

RDR – Rate of Defect Recurrence

SCM – Specific Coverage Metric

SQR – Security to Quality defect Ratio

- KPIs provide business-level context to security-generated data
- KPIs answer the “so what?” question
- Each additional KPI indicates a step forward in program maturity
- None of these KPIs draw strictly from security data

KPI #1 – Weighted Risk Trend

Maturity Rank: 1

A business-based representation of risk from vetted web application security defects over a specified time-period, or repeated iterations of application development.

Formula: $[(\text{Multiplier}_{\text{critical}} \text{ x defects}) + (\text{Multiplier}_{\text{high}} \text{ x defects}) + (\text{Multiplier}_{\text{medium}} \text{ x defects}) + (\text{Multiplier}_{\text{low}} \text{ x defects})] \text{ x } {*}\text{Criticality}_{\text{business}}$

Requirements

– Web application registry with business-level criticality assigned

– *Pull *business criticality* rating from DR documents

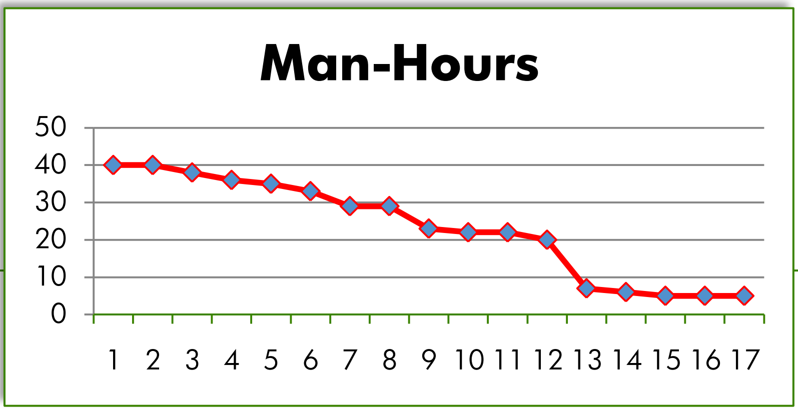
– Vetted web applications security defects by criticality level

– Mathematic plot capability

KPI #2 – Defect Remediation Window

Maturity Rank: 2

The length of time from when a vetted web application security defect is identified until it is verified closed.



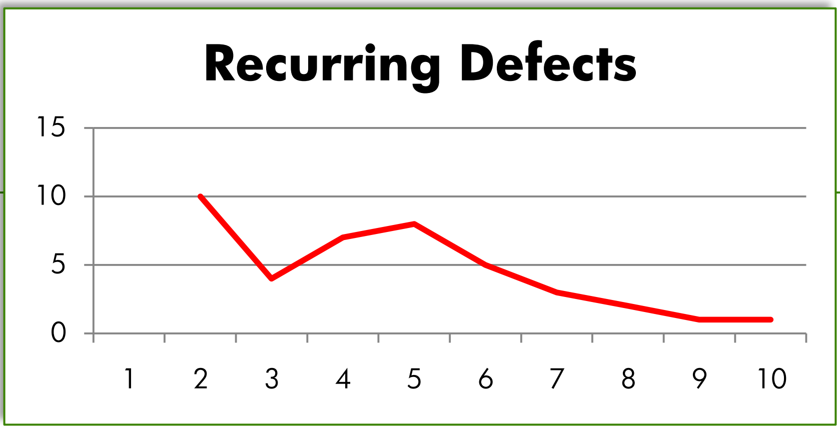
Requirements

- Defect tracking system, tracking web application security vulnerabilities in development, testing, and production environments
- Self-service testing, bug tracking, and reporting capabilities
- Cooperative security enablement thru development, QA, OPS teams

KPI #3 – Rate of Defect Recurrence

Maturity Rank: 3

The rate, over time, at which previously closed web application security defects are re-introduced into a given application, organization, or other logical unit.



Requirements

– Advanced defect tracking system

– Advanced web application security testing capabilities

– Capabilities to identify similar or *like* defects across an application or logical trackable unit

KPI #4 – Specific Coverage Metric

Maturity Rank: 4

The flow-based or component-based coverage of *total functionality* that web application security testing has achieved.

Total functionality = known functionality + discovered functionality*

Requirements

– Method for measuring total application surface (UI, API, code-level coverage methods) plus *advanced application discovery tools

– Advanced security testing capabilities using flow-based, data-driven methodology for completeness

– Integration with Quality Assurance for functional specification coverage

KPI #5 – Security to Quality Defect Ratio

Maturity Rank: 4

The ratio of security defects to the total number of software quality defects being generated (functional + performance + security).

Formula: $\frac{D_s}{D_t}$ D_s = Total Security defects; D_t = Total Overall Quality defects

Requirements

– Mature defect reporting system (tracking combined quality defects)

- Security as a quality defect
- Performance as a quality defect
- Functional (+related) as a quality defect

– Tight cooperation of Information Security & Quality Assurance

KPI Facts

KPI: WRT

- Metric is best graphed
- Risk trend will decrease over time similar to $^1/_x$
- Each defect criticality must have a non-linear factor assigned
  - Critical = 10
  - High = 5
  - Medium = 2
  - Low = 1
- Application business criticality must be rigidly defined
  - Business critical
  - Critical
  - Important…

KPI: DRW

- #1 most critical KPI
- DRW will be potentially very large at first
- Critical to shrink this metric as quickly as possible
- Can be used to target education where needed
- Important to note *type* of defect remediated (complex defects take longer to fix)

KPI: RDR

- Reappearing defects measure internal development confusion
- Recurring defects should prompt a systemic investigation into root-cause
- Critical for identifying poorly-run development organizations

KPI Facts

KPI: SCM

- Most difficult KPI to achieve
- Most organizations cannot identify even *known* attack surface coverage
- Flow-driven & data-driven methodology is required to fully test known attack surface
- Exploratory testing required to discover “unknown functionality”

KPI: SQR

- Final step in organizational maturity with respect to security testing
- Demonstrates security adoption as a component of overall software quality

Applications

Applying the KPIs

Applying KPIs to Web Application Security Programs

What You Have

What You Want

Failures of Common Metrics

Common Metrics

1. Number of vulnerabilities found
2. Number of pages scanned/tested
3. Critical vulnerabilities found
4. Critical vulnerabilities fixed

Failure Mode(s)

1. So what? No context!
2. So what? Do “pages” matter?
3. Business-critical? Or IT-critical? Or…?
4. Business-critical? Or IT-critical? Or…?

Options?

Business Context.

KPIs provide business context to standard metrics reporting practices.

When Metrics Aren't Enough

Objective

- Conclusively prove that risk is being reduced through program effort
- Remove subjectivity of metrics by providing business context
- Bring IT Security into higher-level business discussion
- Unify "testing" methodologies

KPIs Answer

- Combine metrics with business-level **context**
- Provide direct **feedback** to the business to target ongoing effort
- Track program **effectiveness** including education, corporate remediation strategies
- Consolidate technical metrics into business-level dashboards
- Successfully break the "security silo"

Practical

Real-life KPI use-case

Example Application "the large financial"

Current Situation

- 1,500 web applications
- Security testing some web applications pre-production
- Difficult to halt critical applications
- Metrics collected, reported ad-hoc (per test)

Complaints

– No way to prioritize effort

– Difficult to demonstrate if program spend is making a positive impact

– Impossible to have business-level conversation on security vulnerabilities in go-live applications

– No way of knowing what *actual coverage* is being achieved by security testing

– **Result**: Business down-plays security's role

Example Application
"the large financial"

Right Now

Applied KPI – Weighted Risk Trend (**WRT**)

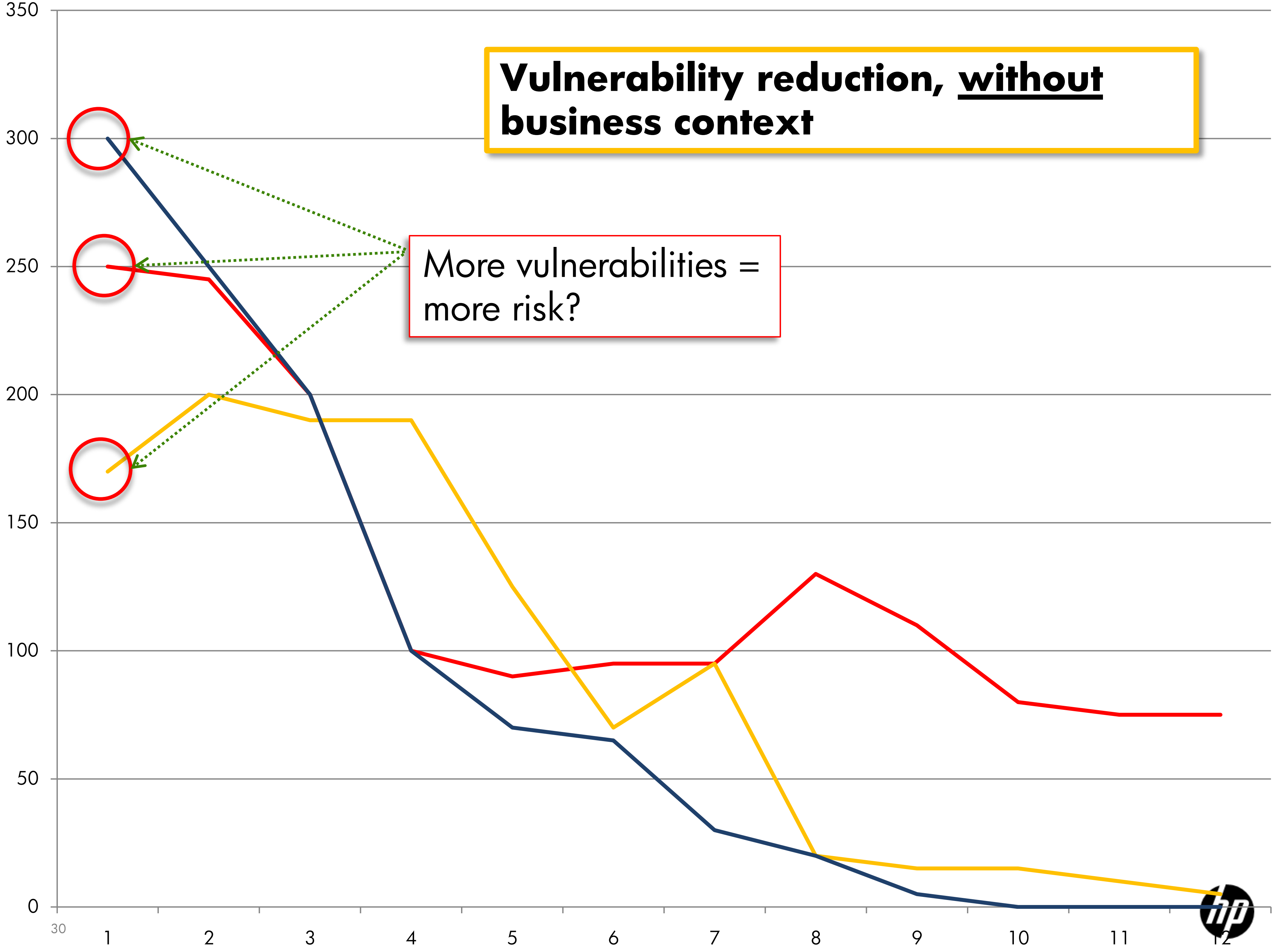
- Application registry + business ranking to prioritize application testing
- Business context to go/no-go decisions for critical defects
- Demonstrate risk reduction in business-critical applications over time
- Demonstrate program spend effectiveness

Near Future

Applied KPI – Defect Remediation Window (**DRW**)

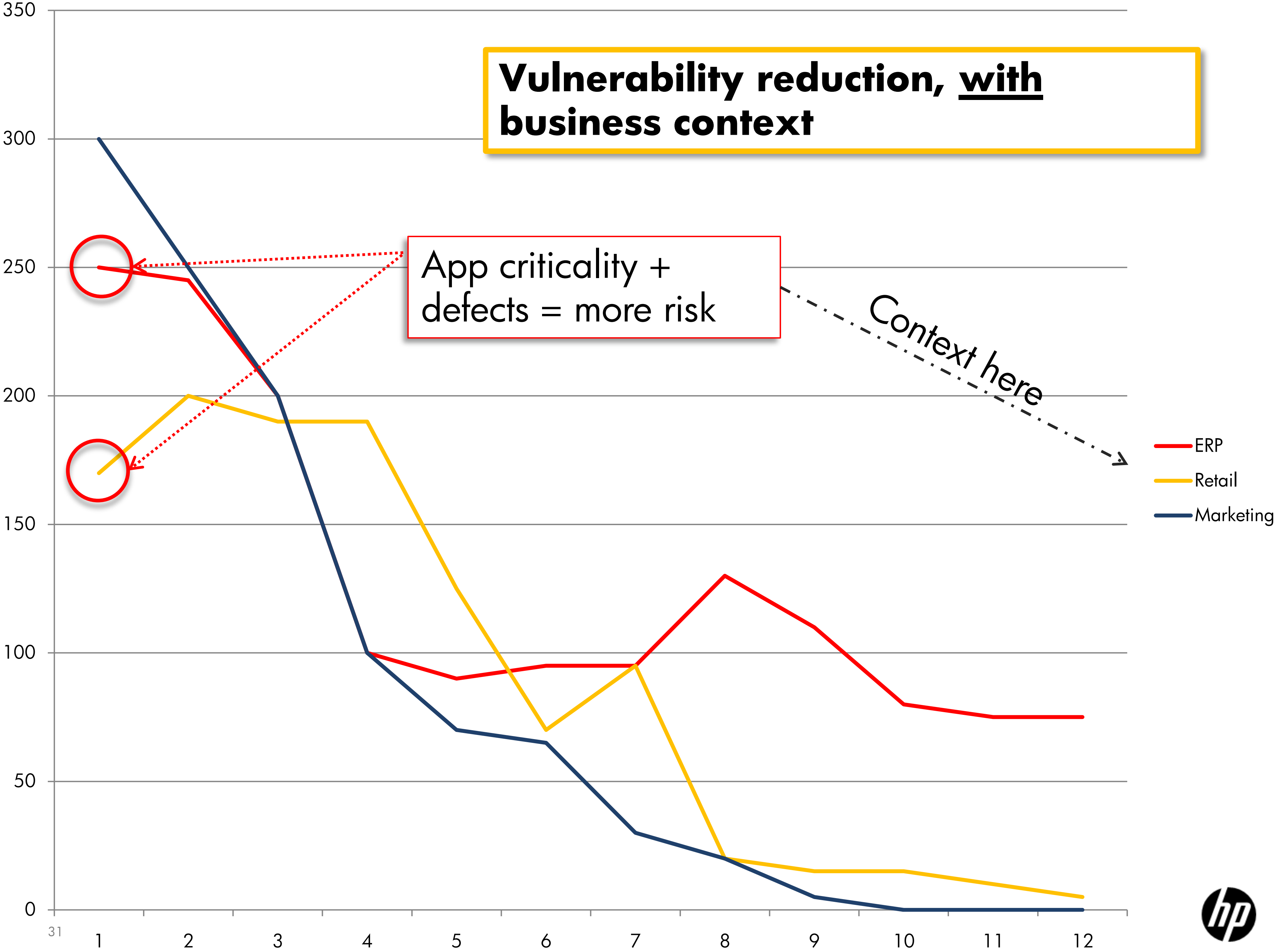
- Produce baseline for defect remediation times
- Implement program plan to prevent security defects from making it to production
- Demonstrate program effectiveness by shrinking remediation window(s)

Vulnerability reduction, without business context



More vulnerabilities = more risk?

Vulnerability reduction, with business context



App criticality + defects = more risk

Context here

Example Application
“the large financial”

KPIs mean measurable gains

– Break the “security silo”

– Improve security team’s posture in the business

– Apply business context to measure risk

– Make key go/no-go decisions intelligently with business support

Data is raw information

Metrics are refined data

KPIs are metrics with business-context

Business context makes security **relevant**.

The 5 Key Performance Indicators (KPIs)

WRT – Weighted Risk Trend

DRW – Defect Remediation Window

RDR – Rate of Defect Recurrence

SCM – Specific Coverage Metric

SQR – Security to Quality defect Ratio

KPIs are the difference between technical data points, and the actionable intelligence that information security needs.

Rafal Los - Security Evangelist, HP

Email: Rafal@HP.com Direct: +1 (404) 606-6056

Twitter: Twitter.com/Wh1t3Rabbit
Blog: HP.com/go/White-Rabbit