The “R” in PSIRT

Beverly Finch | Lenovo PSIRT

29th Annual FIRST Conference on Computer Security Incident Handling

About…

Lenovo

- Top PC maker, leading server provider + mobile
- $45B global technology leader, 55K employees, customers in 160 countries
- Product security led from US

Beverly Finch

- Program Manager and Coordinator, Lenovo PSIRT
- 22 years in the PC industry, PMP® certified
  - Operational Efficiency
  - Dashboard Metrics
  - Executive Communication
  - Software Project Management
  - Section 508 Accessibility Compliance
  - Lean Six Sigma

Lenovo Product Security Incident Response Team

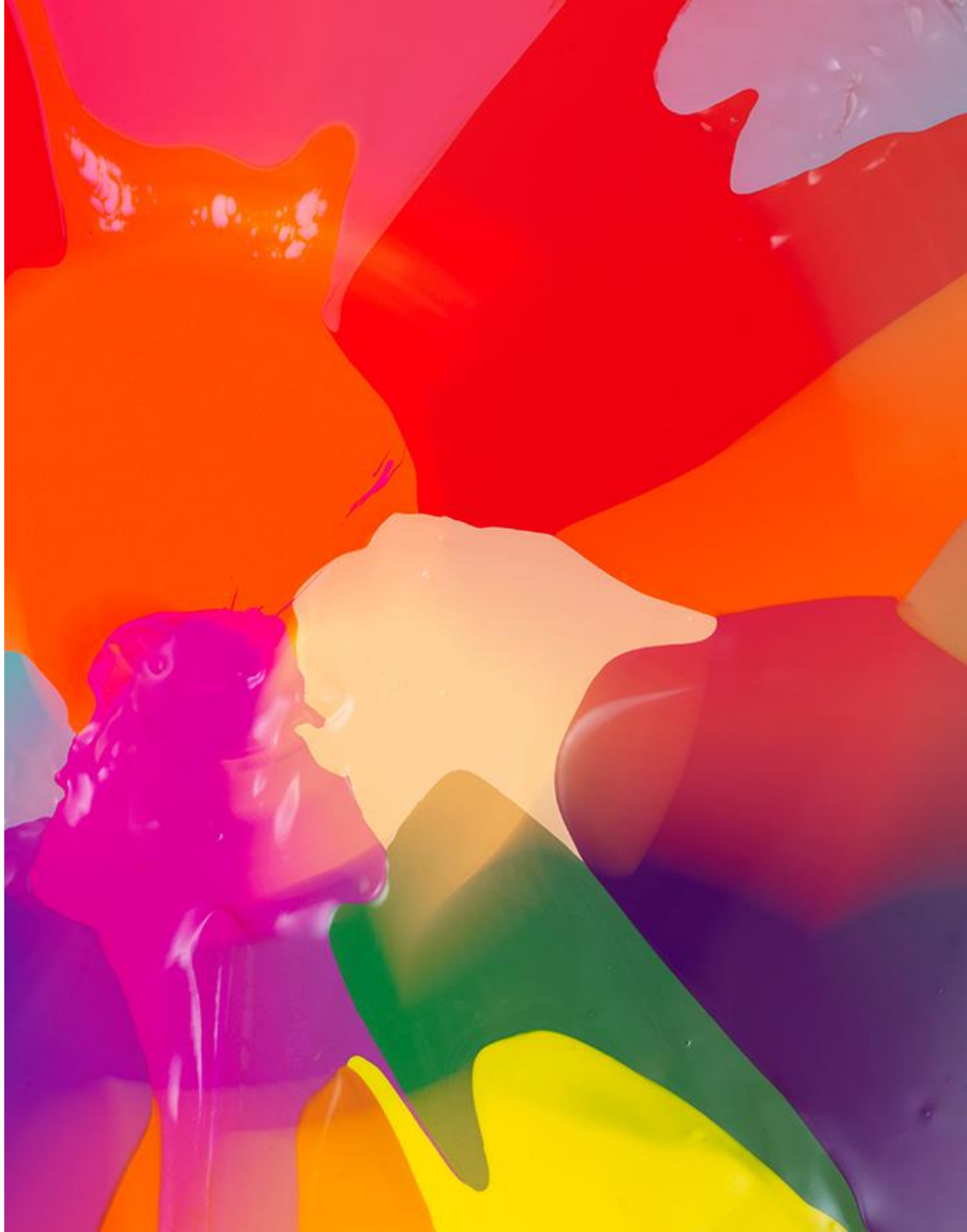
Mission Statement

"Improve customer trust and awareness in the security of Lenovo product offerings in order to gain and keep customers' confidence in Lenovo as their solutions provider."

Program Manager PSIRT Coordinator	• Daily Operations and Program Management • Metrics Reporting • Advisory Coordinator/Exec notifications • Manage Tool requirements
Technical Project Manager	• Triage & Assign cases • Advisory draft & review of PR deliverables • Communicate with customers & researchers • Drive Lessons Learned, as needed
Security SMEs	• Vulnerability reproduction, as needed • Penetration Testing, as needed • Support brand development teams
Supporting Functions Comms + Legal + Support	• Advisory scheduling/review/approval • Reactive statements (Internal + Media) • Support for legal matters • Provide direction to customer-facing support
Product Security Leaders Business Units	• Impact assessment for supported products • Fix target plans for affected products • Timely release of remediation • Review advisories, as needed

Objectives

- Explain how Lenovo uses metrics to improve PSIRT responsiveness.
- Understand the metrics Lenovo uses to measure responsiveness at various phases of the fix timeline.
- Review a sample PSIRT Dashboard report.



The “R” in PSIRT

No response is a response.

Establish Metrics

Data

- Plentiful
- Does not change behavior

A Good Metric is:

- Simple
- Comparative
- Behavior Changing

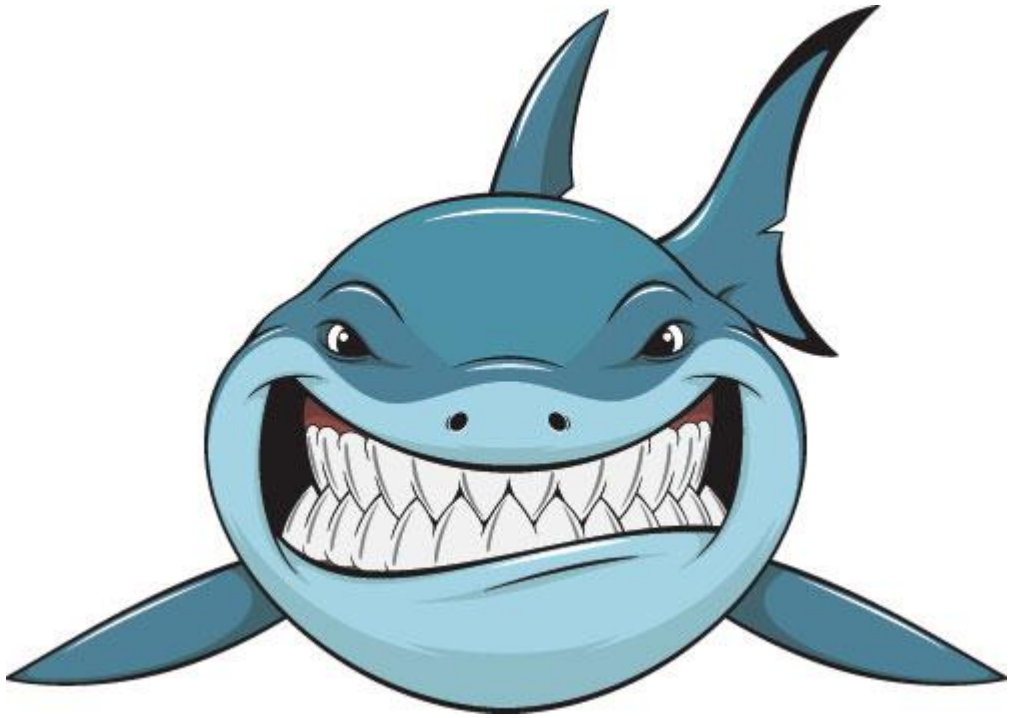
The difference between what <u>can</u> be counted and what <u>really</u> counts separates data from metrics.

Key Data Driving “R”-enabling Metrics

Impact Assessment	• Many products with different attributes across multiple business units • Critical to understand scope of impact for you and your customers
Fix Plan Ready	• For publicly known vulnerabilities, customers want fix release date • Delayed fix plan results in agitated customers and business execs
Fix Date - Planned	• Planned date when fix will be released to your customers • Important to track weekly to understand added risks as plans change
Fix Release - Actual	• Measure actual performance of development teams • Address schedule misses by performing lessons learned

The more time that passes between logging the issue and understanding scope of impact, the greater the risk that fixes will be extremely slow in coming.

Give Your Metrics Some Teeth



- Develop a Service Level Objective
- Considerations
  - Severity/priority
  - Active exploit
  - Legal/Privacy impact
  - Nature of finder/researcher
  - Media attention

Your metrics reflect your definition of success.

Target Remediation SLO Template

Phase	Severity				
	Critical	High	Medium	Low	Code Red (Active exploit, Media or Legal Impact)
CVSS 3.0	CVSS 9.0-10	CVSS 7.0-8.9	CVSS 4.0-6.9	CVSS .1-3.9	
Impact Assessment					
Fix Plan Ready & Approved					
Fix Release (Plan/Actual)					

Aim for big commitments.

How do you want to be perceived?

This?

- Bold
- Energetic
- Trusted
- Valued Partner
- Vigorous
- Zealous

Or This?

- Indifferent
- Unresponsive
- Idle
- Lethargic
- Slow
- Uncaring

Be BOLD!

Sample Dashboard (not actual data)

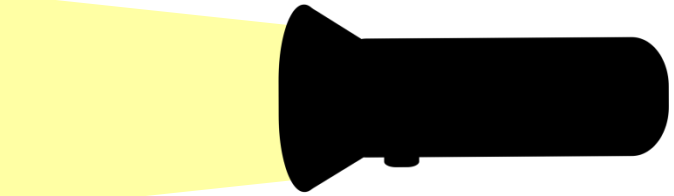
Business Unit	Total Open Cases	Impact Assessment	Approved Fix Target Plan	
		% SLA Achieved	% On Track (SLA)	Previous Month Closed Cases % SLA Achieved
		Active Impact Assessment SLA achieved/Total Active	Active Fix Plan SLA achieved and approved/Total Active	Prior Month Fix Release SLA achieved/ Total Closed
Group 1	10 =	100% ↑	100% ↑	82% ↑
Group 2	8 ↓	100% ↑	100% =	None closed
Group 3	34 ↑	54% ↓	67% ↓	None closed
Group 4	30↓	65% ↓	85% =	78% ↑
Group 5	58 ↑	70% ↑	65% ↑	86% ↑
Group 6	69 ↑	84% ↑	80% ↑	83% ↑
Group 7	24 ↓	82% =	59% ↓	67% ↓
Group 8	84 =	100% ↑	71% ↑	68% ↑

>80% = Green 60%-79% = Yellow <59% = Red

"Simplicity is the ultimate sophistication"—Leonardo Da Vinci

How Dashboards Help Management

- Red/Yellow/Green coding quick and easy to grasp
- Case volume could indicate intrinsic product security problems - or not
- Trend changes week to week by using ↑ and ↓ arrows
- Investigate poor/declining metrics with team to uncover problem areas
  - Issue owner sick or on vacation with no backup?
  - Unbalanced resource
  - Suppliers are slow to respond
  - Priorities out of order
  - Development missing target dates
  - Unnecessary process gates
  - Other teams not providing adequate support
- Celebrate successes!



No Metrics? No Problem!

Summary

- Don’t focus solely on Volume or Time to Fix.
- Data is great for performing deep dives and uncovering issues.
  - Does not change behavior
- Measure responsiveness at various points in the total timeline to uncover potential risks.
  - Impact assessment
  - Fix Plan
  - Fix Date – Planned
  - Fix Release – Actual
- Establish SLOs that drive your teams to achieve your company’s definition of success.
- Construct a simple dashboard to keep management engaged and informed.


Q&A

Different is better

Lenovo™