Modeling Alert Quality

Moshe Zadka – https://cobordism.com

Acknowledgement of Country

Belmont (in San Francisco Bay Area Peninsula)
Ancestral homeland of the Ramaytush Ohlone

What are alerts?

Good or bad

Monitoring

System → Aggregator

Event

Aggregator query

Event

Aggregator query atypical value

Low priority alert

Bad event (not urgent)

High priority alert

Break-fix needed!

High priority alert

Break-fix needed!
Focus of this talk

What is alert quality made of?

What is alert quality made of?

True alarms

What is alert quality made of?

True alarms
False alarms

What is alert quality made of?

True alarms
False alarms
Missing alarms

True Alarm

True Alarm

- Start to detect

True Alarm

- Start to detect
- Detect to acknowledge

True Alarm

- Start to detect
- Detect to acknowledge
- Acknowledge to diagnosis

True Alarm

- Start to detect
- Detect to acknowledge
- Acknowledge to diagnosis
- Diagnosis to remediation

Missing Alarm

- Start to detect

Missing Alarm

- Start to detect
- Detect to acknowledge

Missing Alarm

- Start to detect
- Detect to acknowledge
- Acknowledge to diagnosis

Missing Alarm

- Start to detect
- Detect to acknowledge
- Acknowledge to diagnosis
- Diagnosis to remediation

False Alarm

Detect to acknowledgement

False Alarm

Detect to acknowledgement
Acknowledgement to diagnosis

Alerting costs

False alarm

Alerting costs

False alarm
Useless alarm

Non-alerting costs

Extra time to remediate

Non-alerting costs

Extra time to remediate
Broken down

Alert quality as value

Cost of alerting

Alert quality as value

Cost of alerting
plus cost of not alerting

Alert quality as value

Cost of alerting
plus cost of not alerting
Negated

Alert quality as value

Cost of alerting
plus cost of not alerting
Negated
Plus a constant

Breaking down alerting costs

Data → Estimation

False alarm

Number of people

False alarm

Number of people
Time

Alarm convenience

Off business hours?

Alarm convenience

Off business hours?
Delaying critical project?

People diagnosing and remediating

Interaction with other teams?

People diagnosing and remediating

Interaction with other teams?
Finding responsible party?

Work diagnosing and remediating

Work to diagnose

Work diagnosing and remediating

Work to diagnose
Work to test

Work diagnosing and remediating

Work to diagnose
Work to test
Work to deploy

Incident cost

Separate from work on incident

Time to detect

Unknown problem

Time to acknowledge

Time until confirmation of detection

Time to remediate

Known problem

Cost

Immediate

Cost

Immediate
Reputational

Immediate cost

SLA missed

Immediate cost

SLA missed
Business missed

Reputation cost

Customer feedback

Reputation cost

Customer feedback
Customer continued business

Reputation cost

Customer feedback
Customer continued business
New customer acquisition

Secondary incidents cost

Any degradation caused by remediations/mitigations

Balancing cost

What would constitute ”better”?

Gather data

Estimate when you need to

Priorities

Strategy

Priorities

Strategy
Tactics

Tracking quality

Actual quality:

Tracking quality

Actual quality:Lagging indicator

Tracking quality: immediate

Approximate quality

Tracking quality: immediate

Approximate quality
Track that

Tracking quality: black swans

Take into account wide ”safety margins”

Tracking quality: Goodhart's law

Not a target

Tracking quality: Goodhart's law

Not a target
Feedback

Summary: Alert quality matters

Burn out

Summary: Alert quality matters

Burn out
Customer satisfaction

Summary: Alert quality difficult to track

Time and effort!

Summary: Alert improvement

Measure

Summary: Alert improvement

Measure
Fix

Summary: Alert improvement

Measure
Fix
Iterate