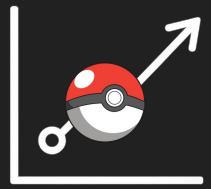
Death by Metrics

How Numbers Can Kill Your Security

VM



Metrics are measurements used to track performance, progress, or trends.

$ whoareyou?

Raise your hand if…

1. You are in a leadership position
2. You are in a technical IC role
3. You are in compliance, risk management, etc
4. You are at the C-level
5. You are an auditor
6. You’re just here to wait for lunch
7. All of the above?
8. None of the above?

whoami

- Fiction author
- Staff Security Engineer and Metrics Queen at GitLab 👑
- Founder of the Women In Cybersecurity Community Association (WICCA)
- WICCON Organiser
- Music, Theatre, Hiking, D&D

These views are my own.

Why should I care about metrics?

Why should I care about metrics?

- Metrics shape decisions
- Without metrics, there are no KPIs
- Without KPIs, there’s no budget
- Without budget, there’s no Security
- Without Security, **you** don’t exist

What is a good metric?

A good metric is **measurable**, **actionable**, **relevant**, and provides **insights** that lead to informed decisions.

- Measurability: Can I make a number out of this?
- Actionability: What do I do with this information?
- Relevance: Why are you telling me this?
- Insights: What is this supposed to mean?

Predict outcomes. Assess risk.

Example: Mean Time to Detect

Meant to show how fast threats are being identified.

Reported as a sign of detection maturity.

- Measurability: Time-based metric, easily calculable.
- Actionability: Improve detection speed over time.
- Relevance: Reduce dwell time and limit potential damage.
- Insights: Reveals how quickly threats are detected.

MTTD helps us track response readiness and forecast (to an extent) future detection performance, good or bad.

So what is a bad metric?

Bad Metrics Recipe

You can’t do anything with it or about it.

It doesn’t mean anything to you.

It doesn’t tell you anything.

You’re not measuring or reading it right.

Bad Metrics Recipe

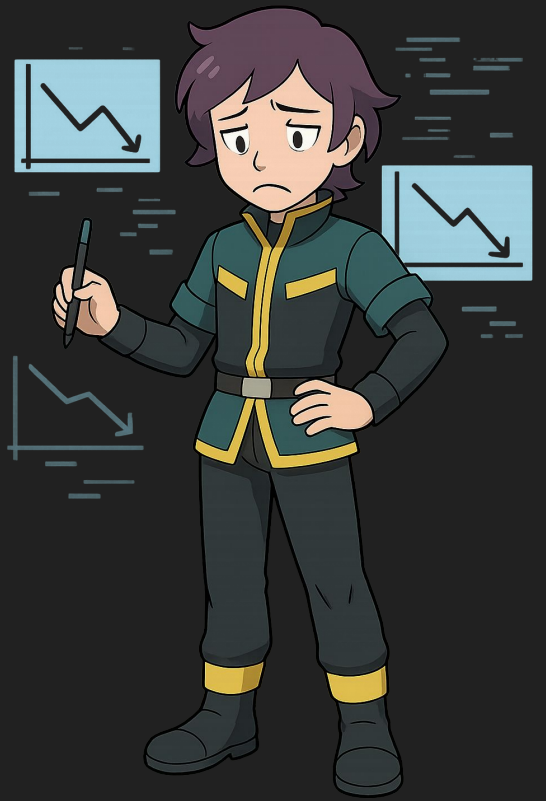
You can’t do anything with it or about it.

It doesn’t mean anything to you.

It doesn’t tell you anything.

You’re not measuring or reading it right.

Wrong maths and bad interpretations

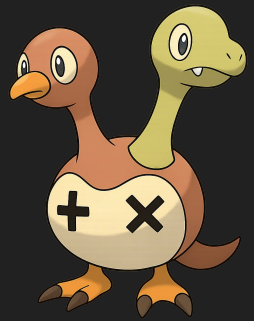


The Team of Metrics Failures

Selection Bias

Data Skews

Misleading Scales



False Correlations

Confounding Variables

Data

Presentation

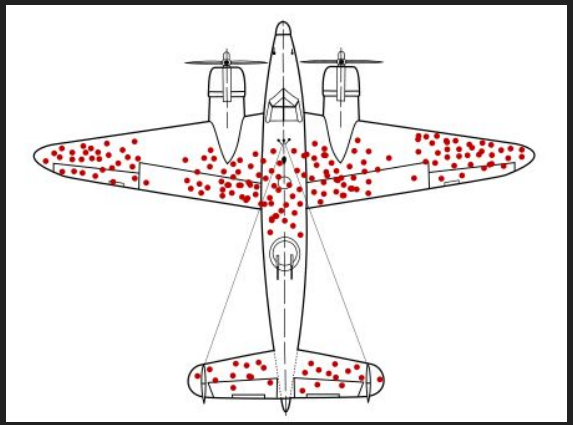
Interpretation

Selection Bias

Data is collected in such a way that some entries have a higher probability of being collected.

Selection Bias

Data is collected in such a way that some entries have a higher probability of being collected.



Selection Bias

Mean Time to Detect

1. Take all alerts/incidents
2. Determine the time to detect
3. Divide by the number of alerts/incidents

What are we missing?

Selection Bias

Mean Time to Detect

1. Take all alerts/incidents
2. Determine the time to detect
3. Divide by the number of alerts/incidents

What are we missing?

➔ Everything we didn’t detect!

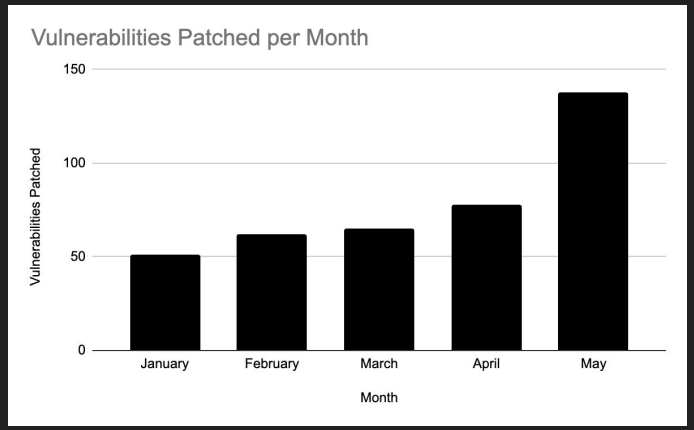
Tracking MTTD is good but it ignores everything you never detected. **It celebrates success, but hides failure.**

Data Skew

The distribution of data is uneven, causing metrics to reflect the majority rather than the most important or impactful cases.

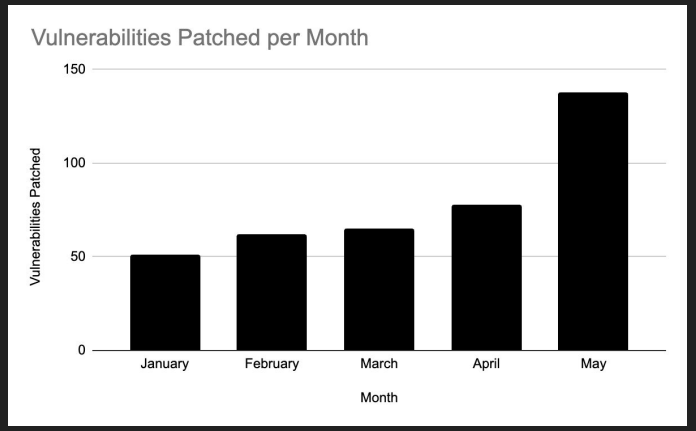
Data Skew

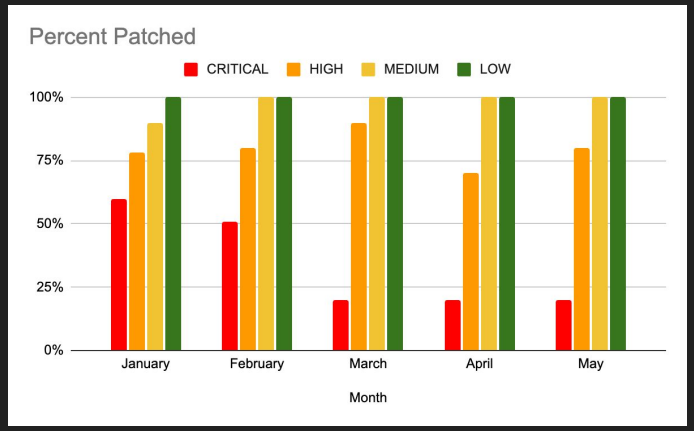
We patched 130+ vulnerabilities this month!



Data Skew

But we're not so great at patching S1s…





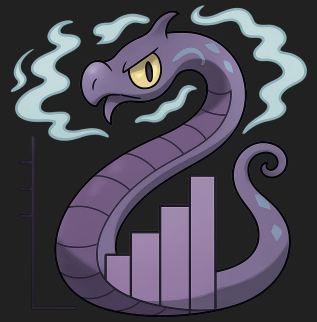
Critical issues remain unfixed but they are invisible in the numbers.

Data Skew

Data skews make security posture look better than it is, rewarding quantity over criticality.

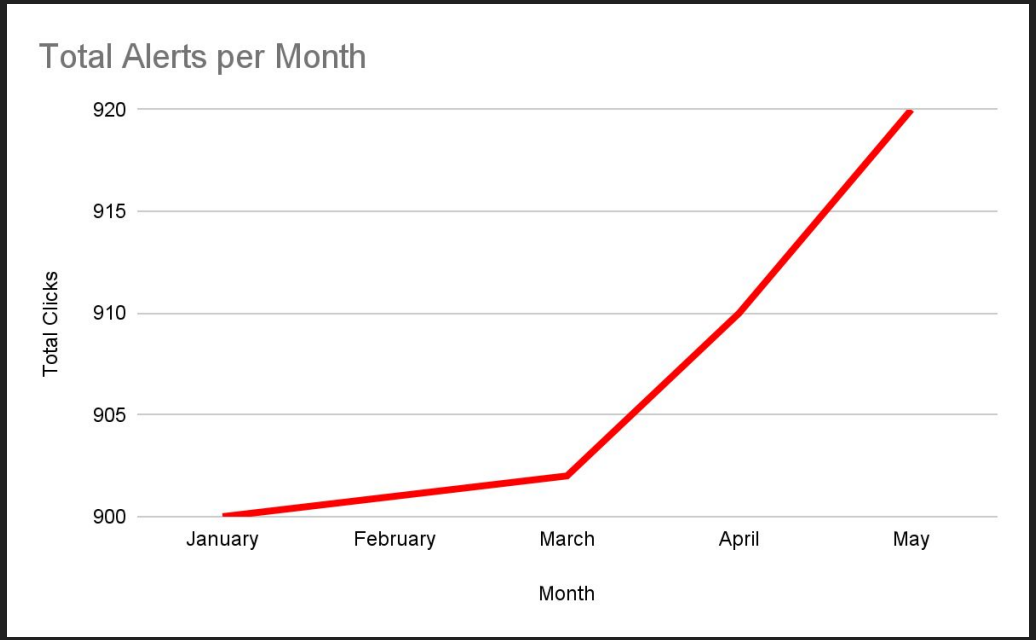
Misleading Scales

Charts or visuals distort the true meaning of data by manipulating axes or proportions.



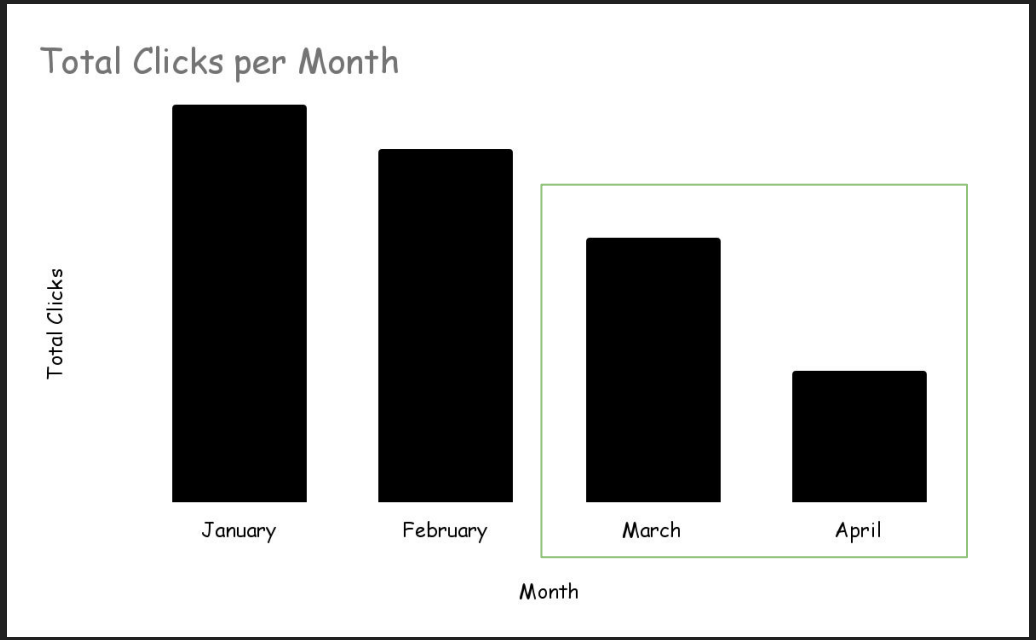
Misleading Scales

"We see a significant uptake in security alerts!"



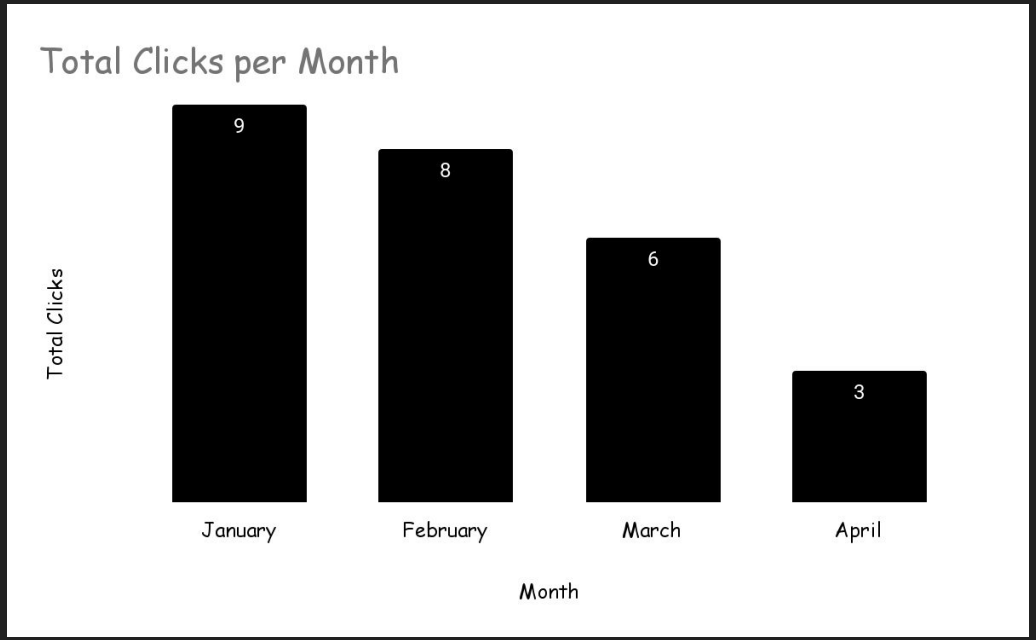
Misleading Scales

"We reduced phishing clicks by 50%!"

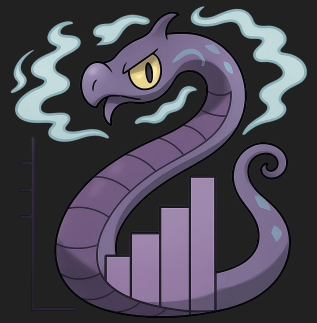


Misleading Scales

"We reduced phishing clicks by 50%!"



Misleading Scales



Using percentages when the sample size is small,

Skewing the y-axis to tell a different story,

All are examples of scaling that can mislead you.

It creates a false sense of progress or risk, making teams prioritise the wrong threats.

False Correlations & Confounding Variables

Two variables appear related but they're not. They're influenced by hidden or unmeasured factors.

False Correlations & Confounding Variables

We created an awesome security awareness training.

We did a phishing simulation exercise.

The results were significantly lower than the last time.

Our training must be **super effective**!

False Correlations & Confounding Variables

Possible confounders:

- The quality of the simulation
- Word-of-mouth security
- Better email filters
- More...

This can lead to overconfidence in user resilience and underinvestment in stronger controls.

Recap

How Numbers Can Kill Your Security

- Celebrating success, hiding failure
- False sense of progress or risk
- Prioritising the wrong threats
- Overconfidence in performance
- Rewarding quantity over criticality
- Making security posture look better than it is

How do I win at metrics?

Good Metrics: A Step by Step Guide

1. Why do you want this metric?
2. Does this metric answer the right question?
3. What will you measure?
4. Know your data:
    - Know what's inside
    - Watch out for skews!
    - Make sure it's complete!
5. Set thresholds or targets!
6. How will you use this metric?
7. Test & Iterate

Mission Statement:

Proposed metrics:

➔ Monthly count of Pokémon caught

Mission Statement:

Proposed metrics:

- ➔ Monthly count of Pokémon caught
    1. Why do you want this metric?

Mission Statement:

Proposed metrics:

- ➔ Monthly count of Pokémon caught
  1. Why do you want this metric?
     - To measure how many Pokémon we caught!

Mission Statement:

Proposed metrics:

- ➔ Monthly count of Pokémon caught
  1. Why do you want this metric?
     - To measure how many Pokémon we caught!
  2. Does this metric answer the right question?

Mission Statement:

Proposed metrics:

- ➔ Monthly count of Pokémon caught
  1. Why do you want this metric?
     - To measure how many Pokémon we caught!
  2. Does this metric answer the right question?
     - Well...

If your mission is to “catch ’em all”, how do you know you’ve indeed caught “’em all” if you just use raw counts?

Mission Statement:

A better metric:

➔ Pokémon Caught Ratio

Mission Statement:

A better metric:

➔ Pokémon Caught Ratio

- Counts distinct Pokémon caught against the total Pokémon count
- Gives us a numerical value for progress
- Tracks our progress to complete our mission
- Our target is 75% by EOY
- If we don't meet our target, we will invest in better Pokéballs

Death by Metrics: How do we survive?

- Bad metrics are dangerous. Avoid bad metrics.
- Are your numbers telling the truth or just a story?
- Follow the step-by-step guide when creating new metrics.
- Use your critical thinking skills.
- Ask questions.
- Evaluate your dataset using the concepts you learned.
- Graph ’em all!

Any questions?

"Every piece of software is a potential virus, you just need to find the right computer."


```
$ where me
```

- ➔ x/@vm00z
- ➔ linkedin/vm00z
- ➔ royalroad/lenagelis