Why not all metrics are created equal

Pedro Jimenez-Hernandez
@spapjh

About Me*

- 4 years of DFIR Experience
  - 2 at a MSSP
- 2 years as a SOC Analyst
- Previous XP as a Compliance Analyst

- Outside of work:
  - FM & Liquid Football, Motorcycles, 3D Printing and Crafts

**The opinions expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of Michigan Medicine.*

What this talk is not -

- No “universal truth” POV
- Not a highly detailed technical dive

What this talk is

- Conversation/Reflections about blue team metrics/KPIs/OKRs or whatever else you want to call them
- Sparked from Taz Wake's twitter (or X, I guess) thread

Two usual POVs

FROM TAZ's THREAD AND MY YEARS OF EXPERIENCE

TRADITIONAL METRICS

- **TOOL DRIVEN METRICS**
  - Vulnerabilities detected
  - Tickets over X days
  - Number of high alerts
- **CUSTOMER-ORIENTED METRICS**
  - Avg/Mean time to resolve a detection
  - Number of logs ingested in SIEM (lol)

COMPLETELY AGAINST METRICS

- *"I think most metrics are useless but I still track some of the traditional ones because the board/customer/senior leadership wants me to."*
- *"Metrics? Naaahhh…"*

The problem

WHY DO SO MANY BLUE TEAMERS FEEL SUCH APATHY TOWARDS METRICS

- **Most traditional metrics do not give a full and clear picture of a security team/program maturity. Why?**
    - Customer/Executive checkboxes
        - Worst Case Scenario:
            - Customer controls your team's maturity
    - Untold stories from tool telemetry
        - Is a high number of detections a good thing? Or a sign your tool needs tuning?
        - Is a high number of false positive a sign your tool needs tuning or that your analysts triaging is on point? Can also be used to inflate numbers for customers
        - Who is tracking false negatives?

The problem (II) -

- Most traditional metrics help spread blue teamer's burnout, which is already a widespread issue
    - Time-based metrics add on to existing pressure and do no take into account complexity or variance between incidents/detections
    - Traditional metric push analysts to not conduct thorough work and encourage other bad habits to just "get it done"
    - According to the '*Voice of the SOC*' poll conducted by Tines, 71% of the 468 cybersecurity analysts polled admitted to experience burnout. National Institute of Health 2021 survey said 35% of police officers experienced burnout

My POV -

- This is far too young of an industry for everything to be set in stone
- Many (too many) in senior leadership and mid-management are heavily reliant in Google results and traditional approach to metrics/KPIs/OKRs/+ due to not knowing any better (voluntarily or not)
- We can ensure proper delivery to customers (internal and external) without leaving a team's quality of life and a program's maturity aside
- A different or an additional approach involving **Quality of life (QOL) metrics** is crucial to the long term success of a security team/program, moving beyond day-to-day survival mode

No Affiliation to Gitlab

Gitlab's Approach

CUSTOMER DRIVEN + TOOLS DRIVEN + QOL = GOOD

- Items from a more traditional approach
  - Includes third party assessments
    - *3P pentests, SOC1/SOC2 audits, etc.*
  - Includes business basics
    - *Planned budget vs actual*
  - Includes other industry-wide stats *(i.e. estimated cost of incident)*

- **I get it, some traditional metrics are:**
  - Great info for board/execs
  - Great selling point for customers
  - Excelling in most of these can point to mature orgs/teams

https://about.gitlab.com/handbook/security/performance-indicators

Gitlab's Approach (II) -

- Tool-driven approach
  - Current vulnerability age
    - Full picture for analysts, mid-management, execs
  - Percentage of high risk/priority incidents
    - Can detect burnout
    - Can detect lack of proper incident prioritization
  - *Security incidents by category*
    - Full picture for analysts, mid-management, execs

- **Let's note that:**
    - No internal time-based tool metrics
      - Avg or mean time to perform X or Y

https://about.gitlab.com/handbook/security/performance-indicators

Gitlab's Approach (III)

- QOL metrics everywhere:
  - Team member on call volume
    - Helps detect burnout or identify insufficient staffing levels
      69% of Analysts said they are short-staffed (*Voice of the SOC*)
  - Team member retention over rolling 12 month period
    - Highlights the impact attrition can have in teams
  - Average age of open positions
    (incl. Time to hire and Time to Accept)
    - Highlights importance of filling open positions quickly
    - Treats candidates as external customers
  - Handbook update rate
    (via API with python script to run against merge requests in path to handbook)
    - Addresses the known "ever-changing" landscaping

https://about.gitlab.com/handbook/security/performance-indicators/

Gitlab's Approach (IV)

- QOL metrics everywhere (II):
  - Security Dpt discretionary bonus rate (manager nominated)
    - Encourages management to reward staff
  - Automation iteration average velocity
    - Targeted at solving 7 weighted issues or more every 2 weeks
    - Acknowledges the importance of automation to help ease burnout in cybersecurity teams
      (*66% of the 468 SOC Analysts of Tines' Voice of the SOC believed that ½ of their workload could be automated*)
  - Security Dpt promotion rate
    - Targeted at 12% in a rolling 12 month period

https://about.gitlab.com/handbook/security/performance-indicators/

Gitlab's Approach (V) -

- Why is this a big deal?
    - All of these QOL metrics come with a target and corrective action plans should those targets not be met, just as with any other metric
    - Publishing their metrics in public adds a whole new level of accountability for Gitlab's leadership
    - Most, if not all of these QOL metrics are fairly easy to track. Not really an excuse to not track them
    - Leadership teams like this are pushing new standards that we ought to keep an eye on

https://about.gitlab.com/handbook/security/performance-indicators/

QOL metrics can also involve tools

More QOL metrics

FROM TAZ's THREAD AND MY OWN POV

- % of deviation from SOPs during incident or project work
  - Let's track the usual "one-offs" mid-incidents or mid project work. Approved and documented is best.
- % of incidents/tickets where existing documentation was insufficient
  - Gaps in documentation, added stress on teams
- % of incidents/tickets that is repeated work
  - Burn out, fatigue rate
- % of incidents/tickets that is new work (manual escalation vs detection with existing solutions in place)
  - Gaps in detection, toll on team

TLDR -

- The majority of widely used blue team metrics help continue to spread burnout, promoting a culture of speed and quick fixes, over quality and long term mission. Surviving vs Thriving
- While some of those metrics are somewhat necessary (executive summaries, customer facing business, etc.), a balanced approach using these traditional metrics AND QOL metrics is needed in order to address the burnout epidemic and for teams to retain top talent long term
- QOL metrics are very easy to implement
- Not all metrics are created equal, we must take into account the impact that implementing/standardizing metrics can have in our team.

Takeaways

You know your environment best, can you come up with more QOL metrics?

- Senior Leadership / Execs
  - You simply do not get to say you care about your teams without implementing QOL metrics
  - QOL metrics are likely easier and less expensive to implement than traditional metrics, no excuse
  - Lots of turnover lately? It is not all about the money; QOL metrics may give you the reason
- Mid-Management and Team Leaders
  - Challenge leadership above you
    - Best case scenario: Create real impact on your team
    - Worst case scenario: Get to know sr. leadership doesn't care
  - Young industry, not everything is set in stone
- Analysts and those on the "trenches"
  - Challenge leadership above you
  - At a minimum, track some of those QOL metrics, can reveal a very telling picture of the place you work at

One last thing

- We need your voice, submit CFPs
- Slides: github.com/spapjh
- Blog: www.flaksec.com