Can We Have Top 5 Security Metrics, Pleeeeeeese?

Dr. Anton Chuvakin
Research Director
Gartner for Technical Professionals
"90% of people are NOT in the Top 10 Percentile!"
The Idea: Metrics Starter Pack

- **Metrics starter pack** for those who'd otherwise measure nothing,
  
- **NOT:**
  - a set of "The Metrics"
  - "Top 237 Metrics you can never figure out"

- Should be usable within weeks for “unenlightened organizations”

- Include technical and non-technical metrics
Pros/Cons

Progs

• Starting from the starter pack is better than from in-depth analysis (*)
• There must be some "useful commonality" that can be measured
• Usable partial solution is better than no solution
• Discussion starter value

Cons

• Organizations are too different
• Needs for measuring security are too different
• Data collection is often lacking altogether, and there is a risk of picking easy metrics only
Examples

- # of detected/remediated incidents
- # of high risk items in your risk register
- Time to detect an incident
- Vulnerability counts and remediation time
- Some “proxy metrics” for security process effectiveness (e.g. patch speed -> overall program maturity)
- Coverage of security team / technology (reach)
- Outside known information metrics (reported breaches)
- *One metric per broad domain*: identity management, vulnerability management (e.g. patching speed), security monitoring, etc
Discussion?

Yay / Nay?
It is worth creating?
Can it work?
Will you use it?