Investing in Security Assuming Silver Bullets are Rare

David Schafer

10/17/2017

Silver Bullet Definition

Something that acts as a magical weapon; *especially* : one that instantly solves a long-standing problem

No Silver Bullets? – What do we do

Eyes on the Prize – Keep bad things from happening to Aviation

- Assumptions:
  - Current Approach isn't perfect
  - One solution (silver bullet) is rare/impossible
  - Resources are limited
- Use Many Lead Bullets
  - CT, AT ,AIT, Trace, Canine, BDO, Video,…
  - Vary operations requirements and procedures
- Investment options
  - Invest in making each approach better
  - Invest in new approaches
    - Specific subsets of the overall problem?
  - Use the lead bullets in coordinated fashion
    - Macro Security, Fusion, Information Technology
- Where should the focus be?

Beware of snake oil salesmen

- Test the science
  - If it can't work in the lab it won't work in the field
    - Time to scan
    - Cost to scan
    - Effect of stream of commerce on measurement
- Extrapolate the experience in other fields
  - Expert/Peer review

analogic

Best way to invest limited resources?

- Depends who you ask!!
- Different stakeholders have different viewpoints
  - Regulators
    - Threat intel - Current threats, new emerging threats
    - R&D for new emerging technologies
    - Macro security and security architecture
    - Con-Ops - dealing with false positives and false negatives
  - Equipment Vendors
    - Improvements to existing technology
    - Deploy best available qualified technology
  - TSO's – Invest in making it easier to do my job well
    - Human factors improvements, Common GUI, Con-ops, Education, Training
  - Inventors / Academia / National Labs
    - Research and NEW approaches
  - Public – Invest in making it safer, without making it more complicated, time consuming, expensive or annoying
    - Less divesting, better communication, education, special cases (medical, …)
  - Crossovers (Multiple stakeholder interests)
    - More agile testing and deployment of successful approaches

But are the resource really limited ?

- Limitation based only on commitment to problem and belief that it is still relevant
  - Regulators/Governments play key role
    - Budgets, Allocation
  - Maintain relevance as time goes on without incident?
- R&D funding
  - Focus on near and long term objectives
    - Near term – incremental improvements and deployment
    - Longer term – keep searching for better bullets
    - Require milestone achievement to continue consuming resources
- Deployment funding
  - Decisions have long tails
    - Equipment life is expected to be long
    - Replacement costs are high including infrastructure

Staying relevant to the problem

- Solutions competing for resources and attention
  - Detection?
    - Find the actual threat at the checkpoint
  - Deterrence?
    - Make it difficult – they will attack somewhere else
  - Other security risks
    - Soft targets
      - Public gatherings
      - Public transportation

Keep Trying

- Maybe someone's silver bullet will work?
  - Some portion of resources stay committed to long term
- Keep improving what we are doing
  - Better really is better

Thank You