Metricon 7 – M7 Useful or Bust!

Lessons Learned

Dr. Anton Chuvakin
Program Committee Chairman

FINAL Agenda

Introduction to Metricon, security metrics and workshop goals by *Anton Chuvakin* (9:00-9:30)

"Even Giant Metrics Programs Start Small" by *David Severski* (9:30-10:30)

Break (10:30-10:45)

PANEL: "Rules of the road for useful security metrics" (10:45-11:30)

"Measuring security with SecQua" by *Constantinos Patsakis* (11:30-12:00)

Lunch break (12:00-1:00)

"What we want to see in security metrics" by *Christopher Carlson* (1:00-2:00)

PANEL: "What we know to work in security metrics" (2:00-2:30)

"Application Security Metrics We Use" *Steve Mckinney* (2:30-3:00)

Break (3:00 – 3:15)

"Threat Genomics and Threat Modeling" by *Jon Espenschied* (3:15-4:15)

Discussion time, everybody shares lessons, highlights, etc (4:15-5:00)

Conclusions, results and action items by *Anton Chuvakin* (5:00-5:15)

Happy hour (sponsored) (5:15-6:15)

Key Insights Pile I

- **Culture** (such as “evidence-based”) helps security metrics if borrowed from other domains
  - 'Evidence-based security' needs credible evidence!
- **Spend more time defining the goals**, e.g. what "well-performing" and “useful” means
- Need to **measure both** “do they do as they are told” AND “are they being told the right things”
- **GQM (goal/question/metric)** is useful for creating and running metrics
- It **is easier to track ‘are we better or worse?‘** over time than 'what is good/best?‘

Key Insights Pile II

- **Accountability**, including personal, drives metrics use and metric programs sustainability
- "**Metricophobia**" is being scared of metrics due to personal accountability
- **Available data drives metrics**; measure what you understand first
- **GQM works**; goal->collect is great, but collect-> goal is also not wrong
- Know the audience before baking the metrics; **think "A-GQM“**
- Identify and use **“deep metrics”**

Key Insights Pile III

- **Process clarity** is really important for metrics success
- **Good is better than perfect**, diminishing returns come quick to metric tasks
- **Action, status and deadline measures** are more useful than "environment metrics“
- **Cause and effect in security is fuzzy**, thus metrics are hard
- **Standard metrics for industry**: tactical - yes, high-level - probably not or not soon

FAIL Highlights

- I want to measure X? – Hmmm ….WTH is X?
- Metric program sustainability
  - Shelfware metrics programs
- "Gimme top 5"
- Avoid 4D visuals ☺

FINAL Agenda

Introduction to Metricon, security metrics and workshop goals by *Anton Chuvakin* (9:00-9:30)

"Even Giant Metrics Programs Start Small" by *David Severski* (9:30-10:30)

Break (10:30-10:45)

PANEL: "Rules of the road for useful security metrics" (10:45-11:30)

"Measuring security with SecQua" by *Constantinos Patsakis* (11:30-12:00)

Lunch break (12:00-1:00)

"What we want to see in security metrics" by *Christopher Carlson* (1:00-2:00)

PANEL: "What we know to work in security metrics" (2:00-2:30)

"Application Security Metrics We Use" *Steve Mckinney* (2:30-3:00)

Break (3:00 – 3:15)

"Threat Genomics and Threat Modeling" by *Jon Espenschied* (3:15-4:15)

Discussion time, everybody shares lessons, highlights, etc (4:15-5:00)

Conclusions, results and action items by *Anton Chuvakin* (5:00-5:15)

Happy hour (sponsored) (5:15-6:15)