cigital

“Right-Sizing” a Penetration Test

And Their Roles in a Larger SW Sec Program

Will Kruse

Senior Security Consultant
wkruse@cigital.com

cigital

Software Confidence. Achieved.

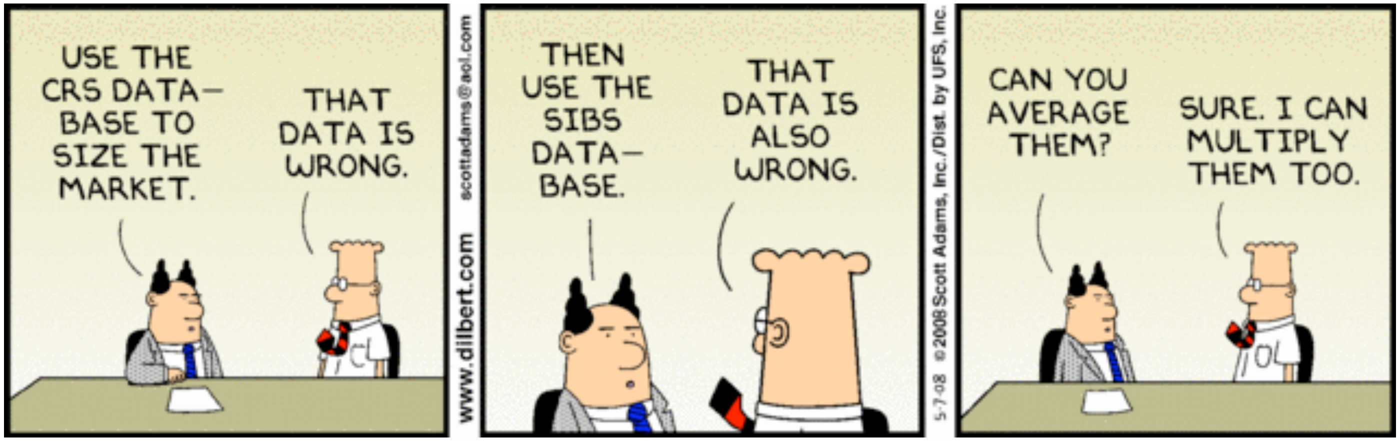
www.cigital.com
info@cigital.com
+1.703.404.9293

“I Hate Penetration Testing!”

- Why? Inefficiency and ineffectiveness…
  - Or so it seems…
- But it turns out there is value…
  - How much time do we spend per test?
  - What is its role in a larger sw sec program?
- Advantages
  - Low start-up cost*
  - Results are real*

Lies, Damn Lies…

- Question my data! It isn't perfect, it's just real
- Assumptions
  - We're only talking about web applications
  - Our goal is not completeness
  - We cannot control for "brokenness" of the application

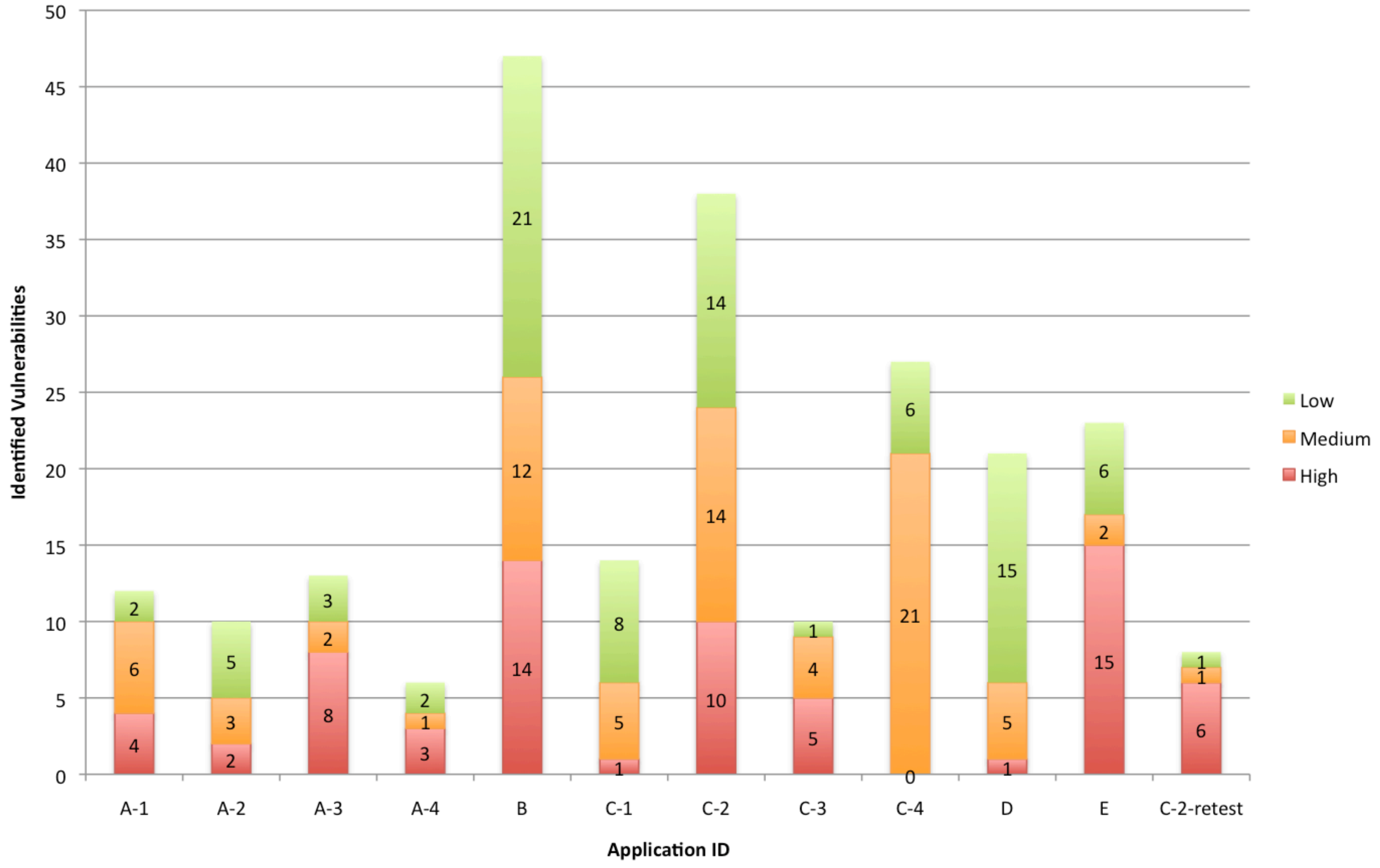

USE THE CRS DATA-BASE TO SIZE THE MARKET.
THAT DATA IS WRONG.
scottadams@aol.com
www.dilbert.com
THEN USE THE SIBS DATA-BASE.
THAT DATA IS ALSO WRONG.
5-7-08 ©2008 Scott Adams, Inc./Dist. by UFS, Inc.
CAN YOU AVERAGE THEM?
SURE. I CAN MULTIPLY THEM TOO.

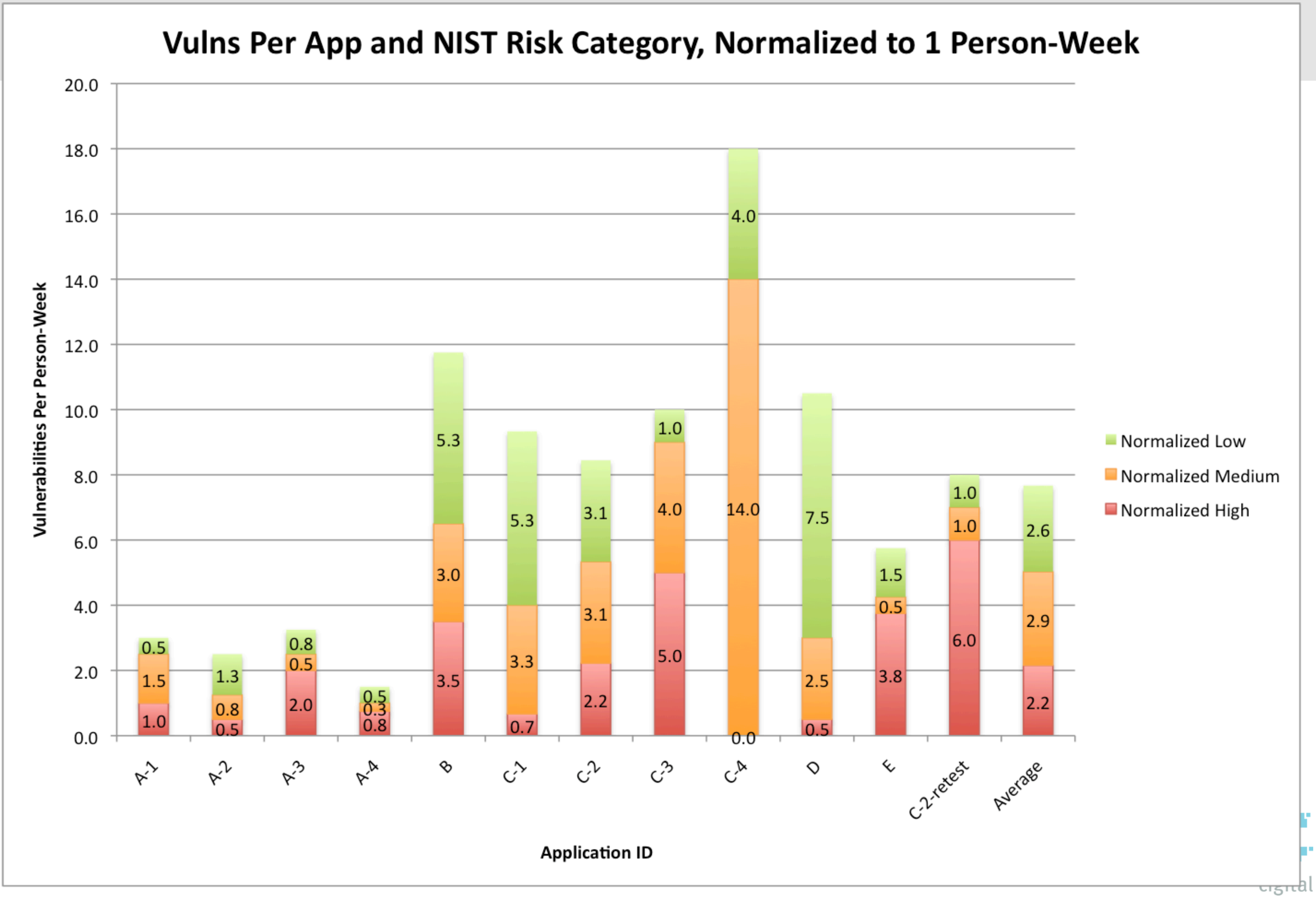
One of my favorite Dilbert comics. Copyright Scott Adams

Introduction to the Data

- 12 web applications
  - Pen tested over the course of 6 months
- Performed under various contracts
  - Letters indicate a single client
- Risk rated according to NIST 800-30
- I will present
  - The vulnerability breakdown per app
  - The vuln counts, normalized to 1 person-week
  - The count of just the highs, normalized to 1 person-week

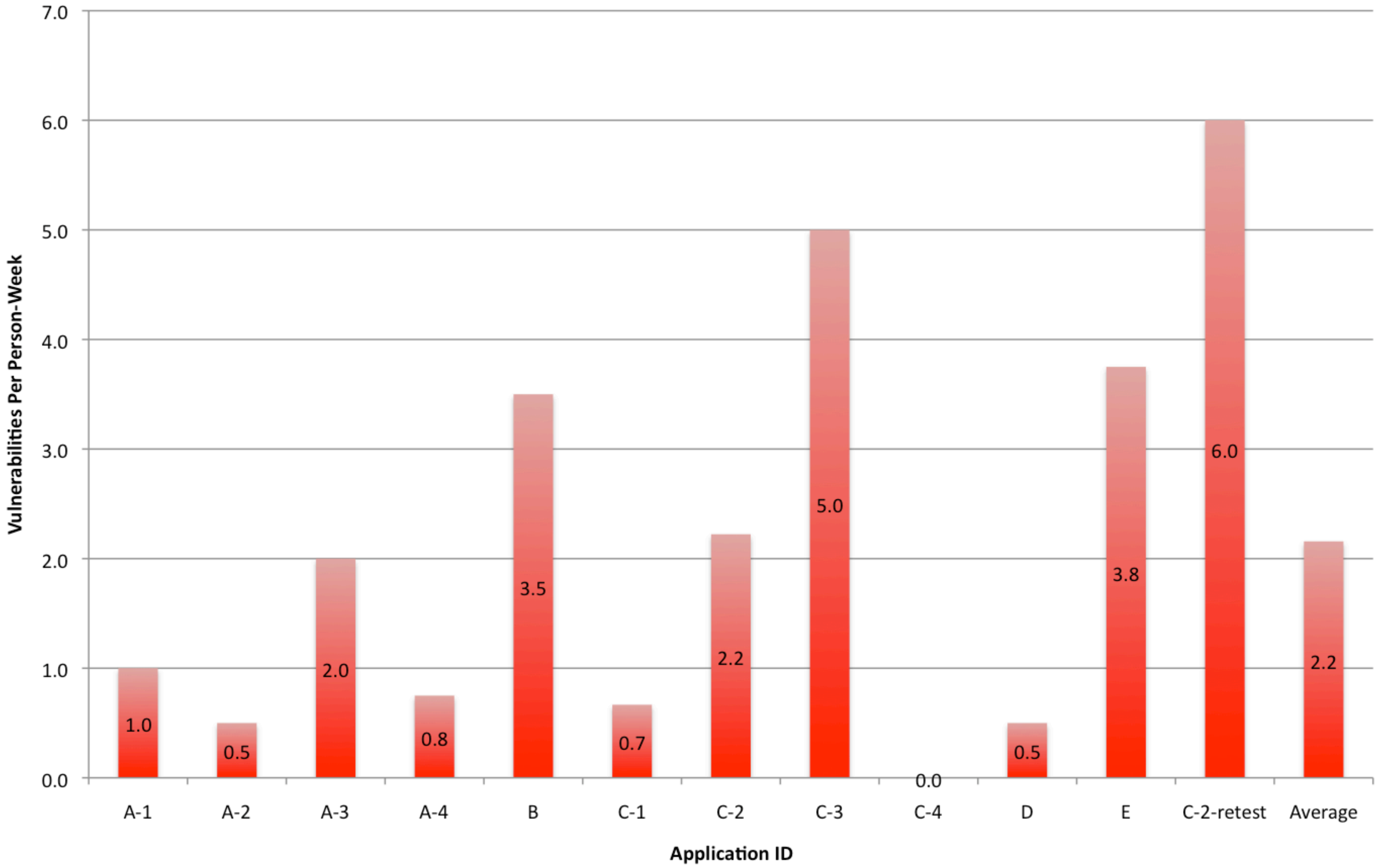
Vulnerabilities Per App and NIST Risk Category





Vulns Per App and NIST Risk Category, Normalized to 1 Person-Week

Highs Normalized to LOE - Because Who Cares About Anything Else?



Conclusions around “Right-Sizing”

- What are your goals?
  - “Show blood?” LOE in person-hours:
    - Average = 35, Std Dev = 28.7
      - Spend a week
  - Find some sort of problem?
    - Average = 8.6, Std Dev = 7.3
  - Find all high-risk problems?
    - Good luck… story time…
- What about a pen test as a quick and dirty “badness-o-meter” to determine whether further analysis is necessary?