

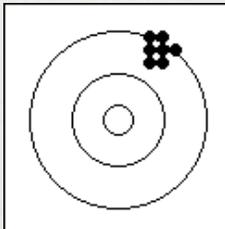
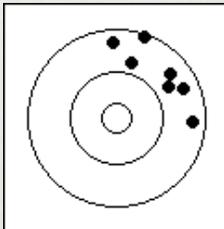
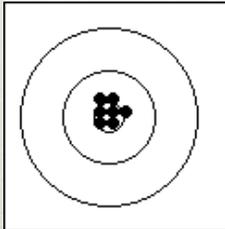
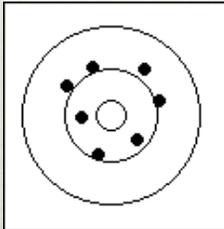
SHOES FOR
INDUSTRY

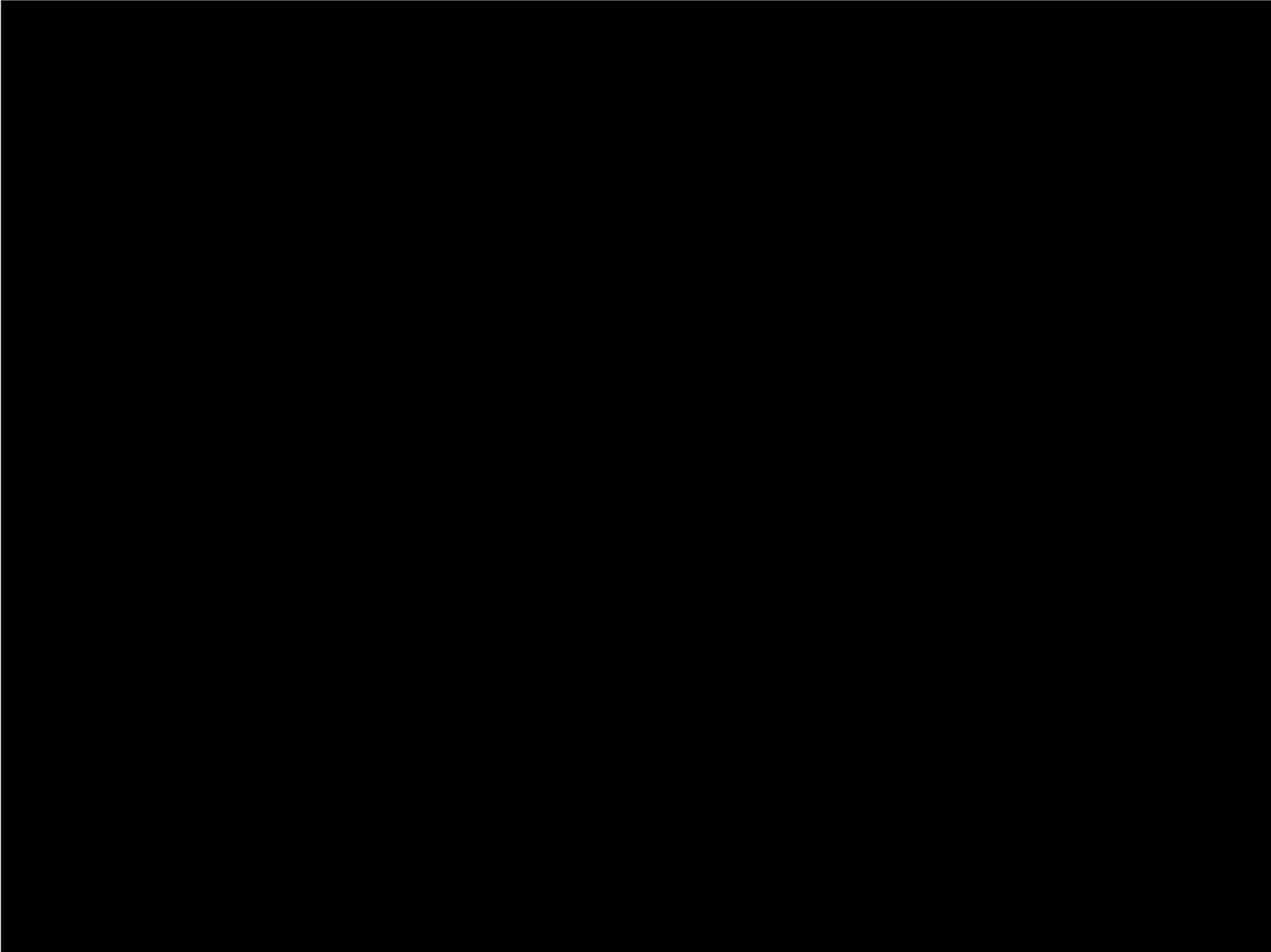
DAN GEER

13106

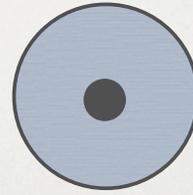


BIAS VS PRECISION

	precise	imprecise
biased		
unbiased		



CONSISTENCY



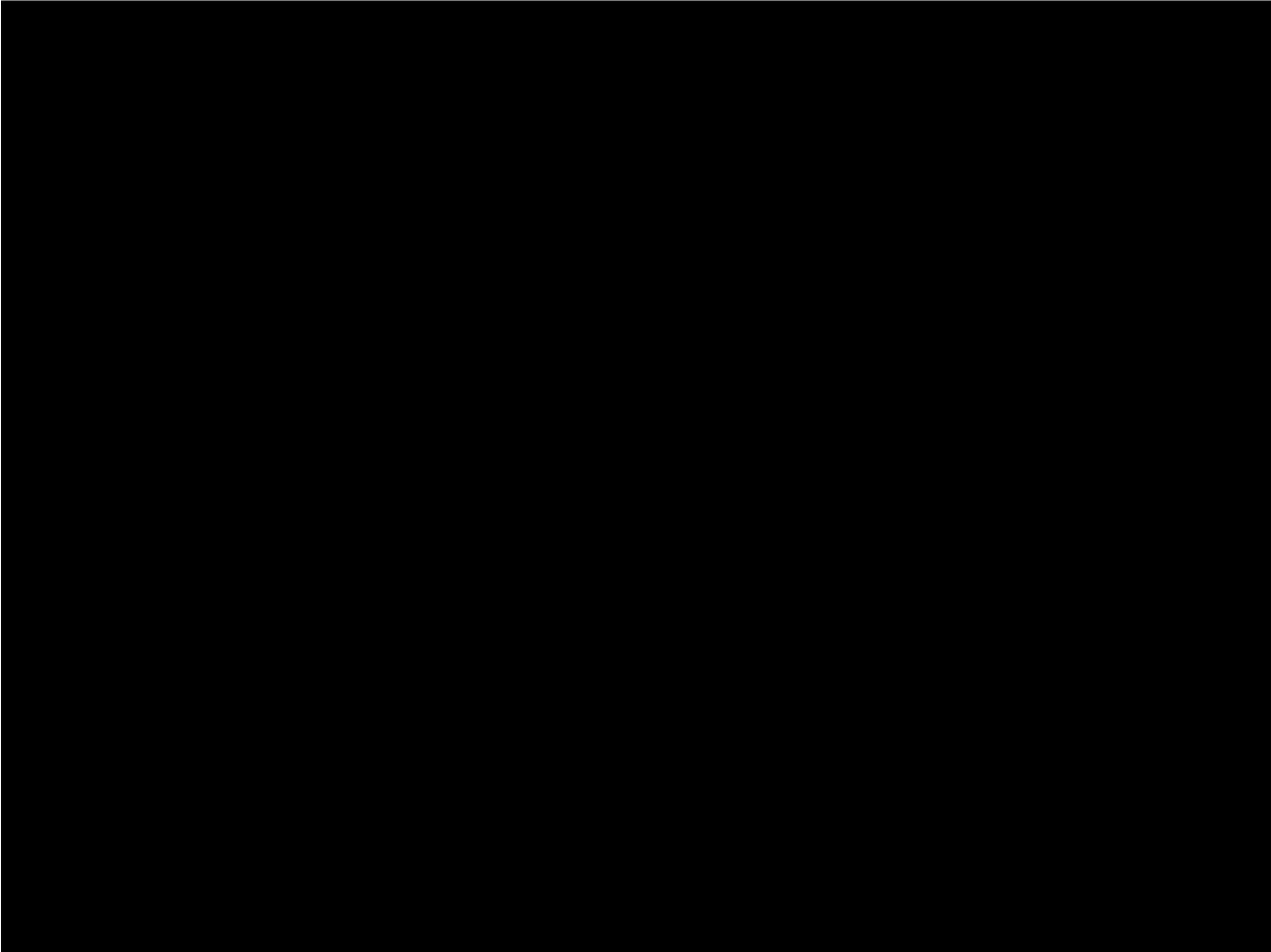


$$\text{ALE} = \text{exp}(\text{losses} / \text{yr}) * \text{exp}(\$ / \text{loss})$$

$$1 * \$1,000,000 \equiv 1,000,000 * \$1$$

↑
will file

↑
will not file
(or notice?)



NUMBERS GENERALLY

- ✱ $\Pr(\text{infection}|\text{exposure})$
- ✱ interval from infection to infectiousness
- ✱ interval of infectiousness
- ✱ interval from infection to symptoms
- ✱ duration of acquired immunity

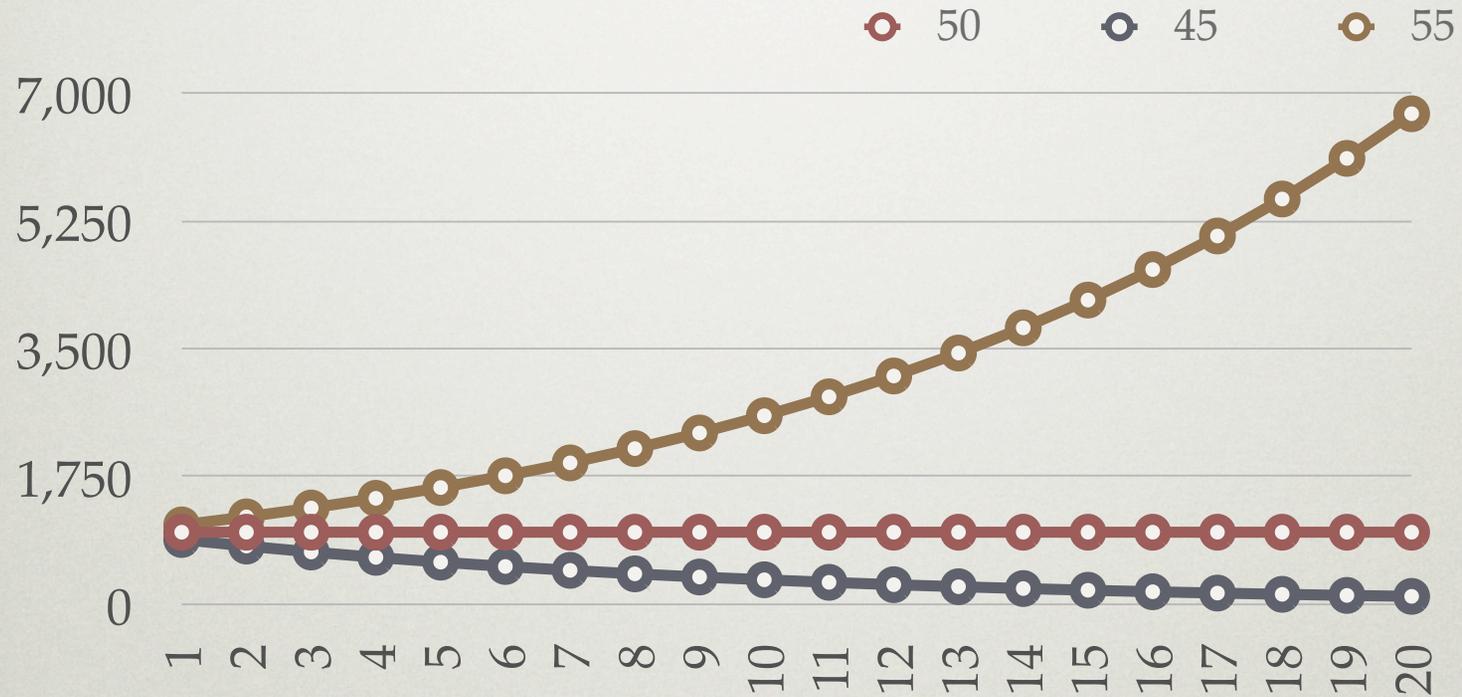
NUMBERS WORST CASE

- ✱ $\text{Pr}(\text{infection}|\text{exposure}) = 1.0$
- ✱ interval from infection to infectiousness = 0
- ✱ interval of infectiousness = open ended
- ✱ interval from infection to symptoms = indef
- ✱ duration of acquired immunity = 0 (mutates)



TIPPING POINT EXAMPLE

$PR(I|E)=2\%$, $N(E)=50\pm 10\%$



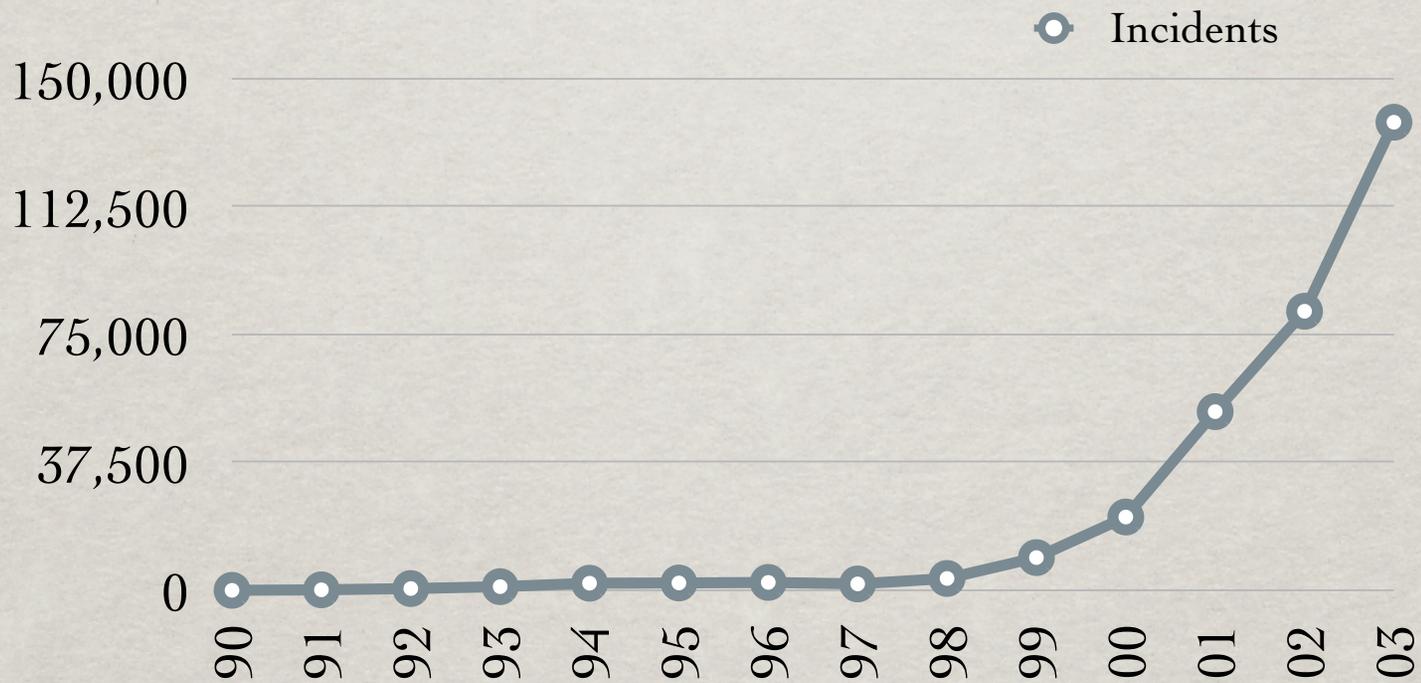


COMPLEXITY

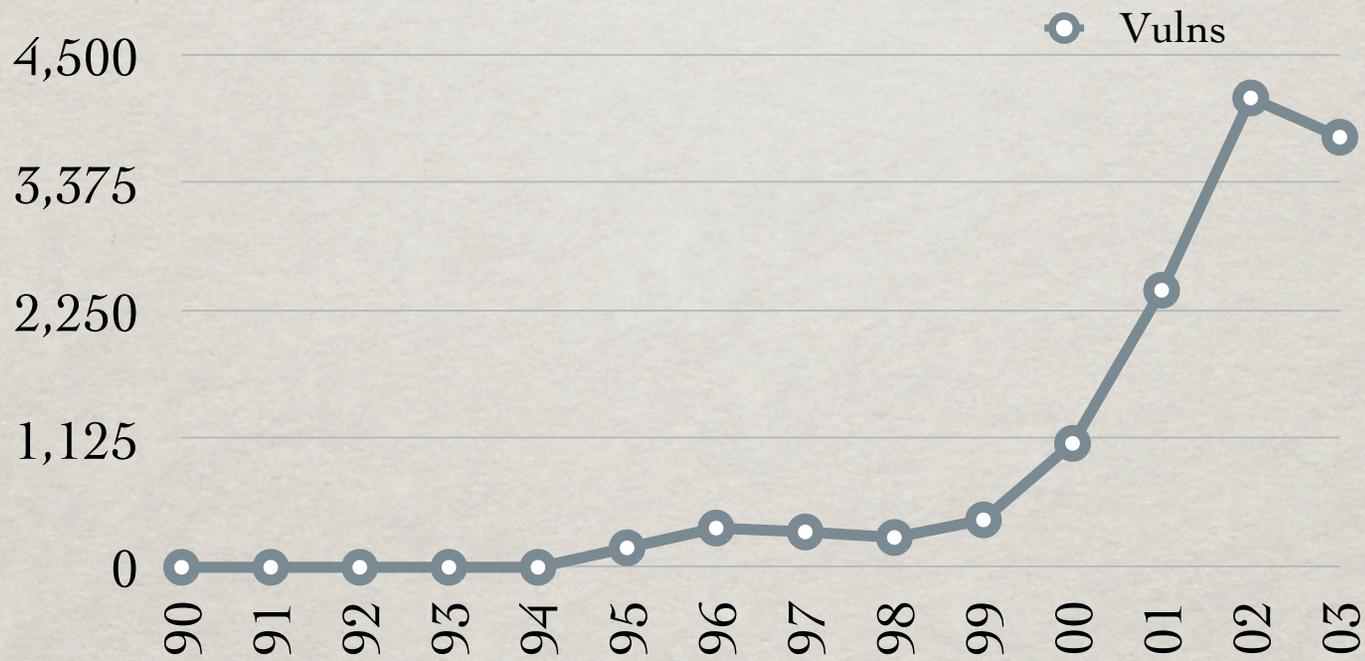
“There are two ways of constructing a software design. One way is to make it so simple that there are obviously no deficiencies and the other is to make it so complicated that there are no obvious deficiencies.”

C.A.R. Hoare

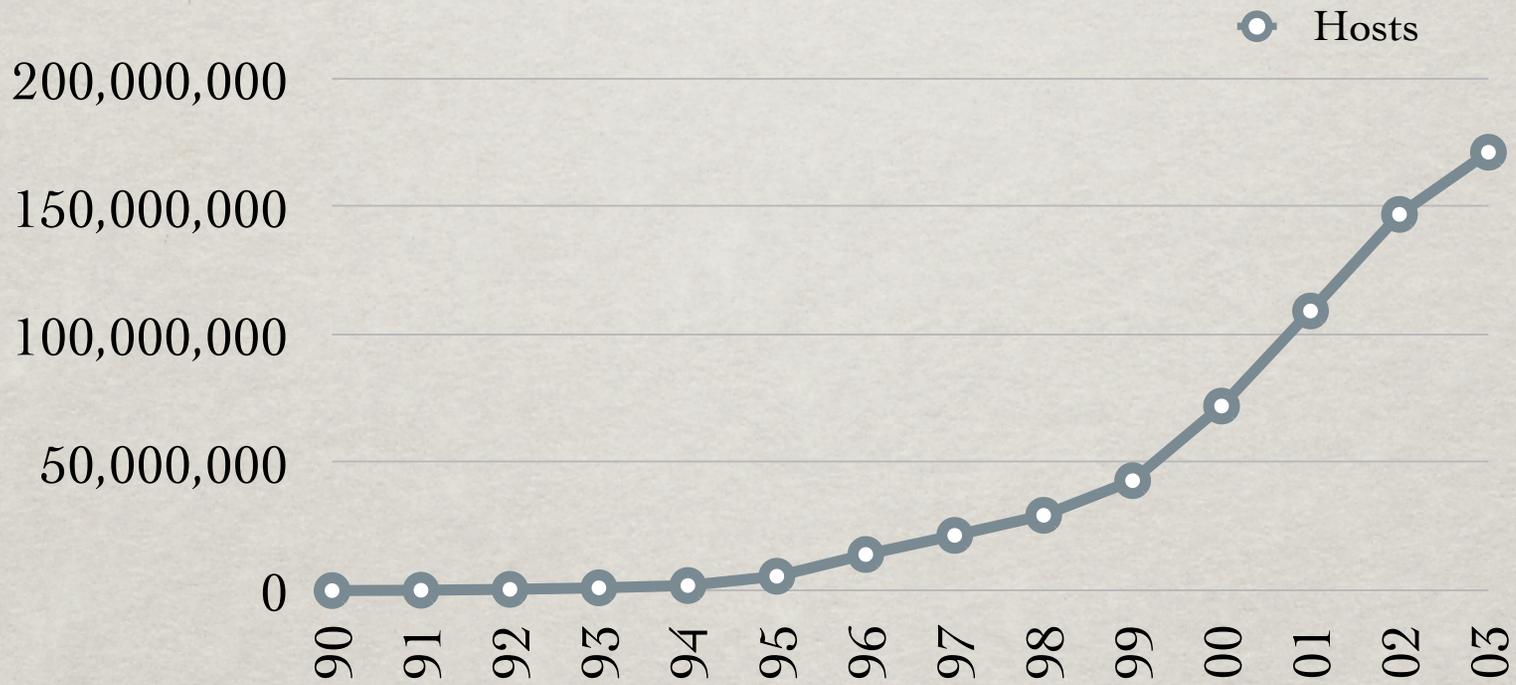
INCIDENTS (KNOWN)



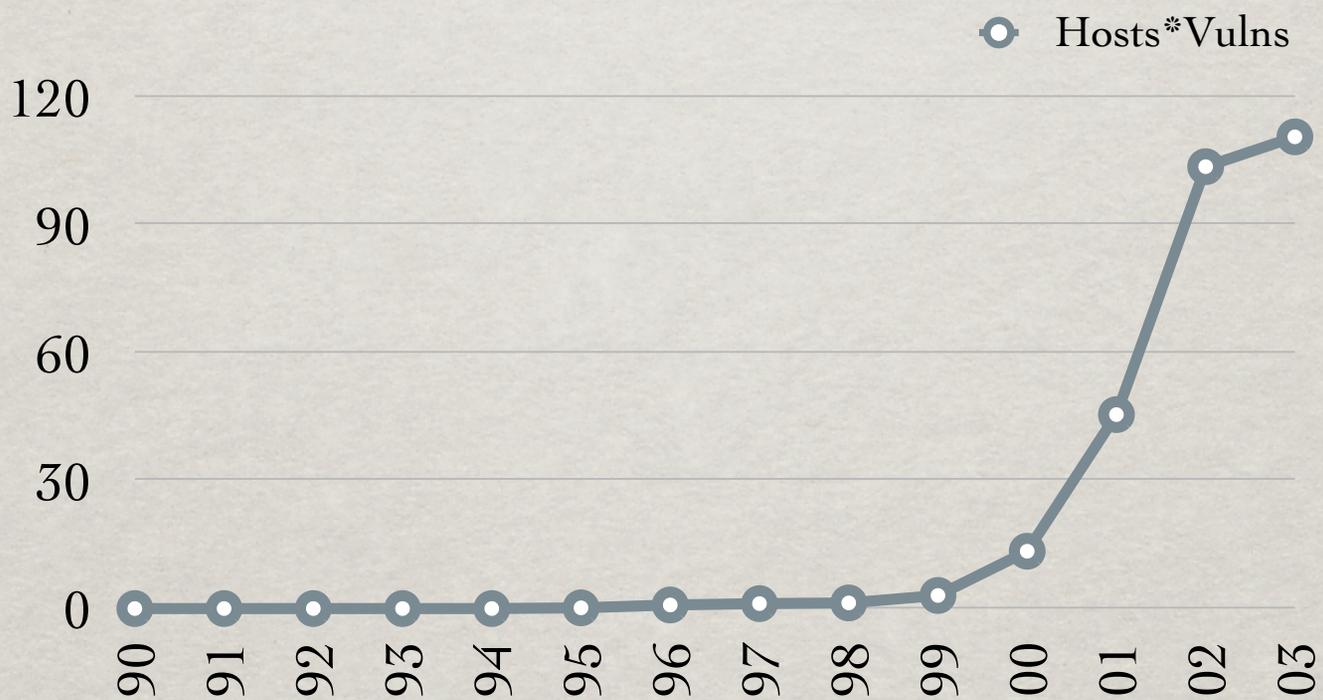
VULNERABILITIES (KNOWN)



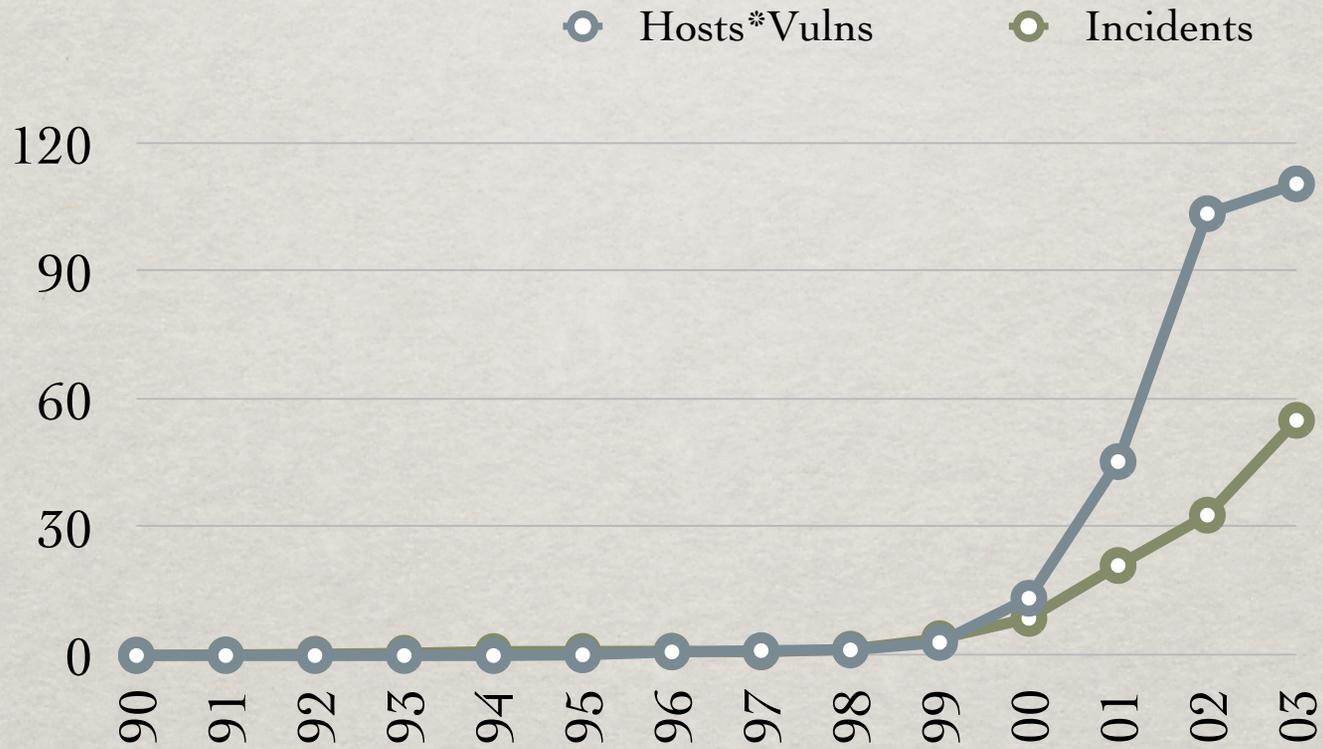
HOSTS (ESTIMATED)



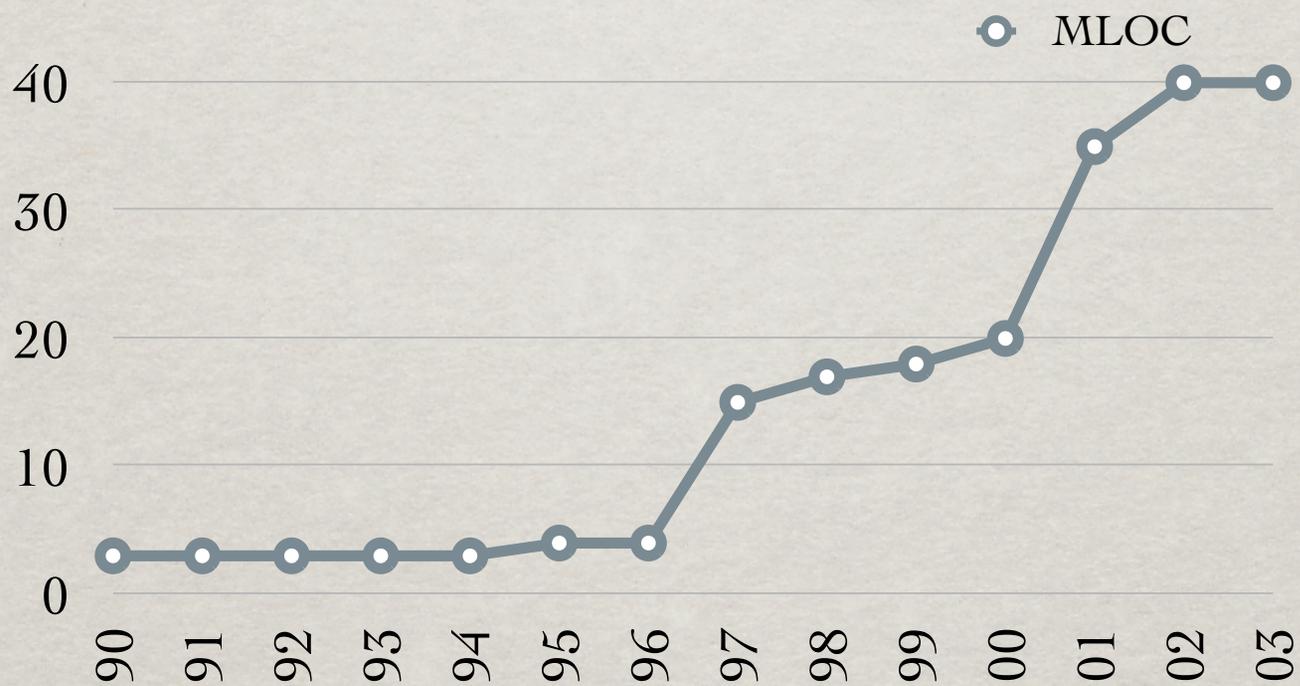
OPPORTUNITY (NORMALIZED)



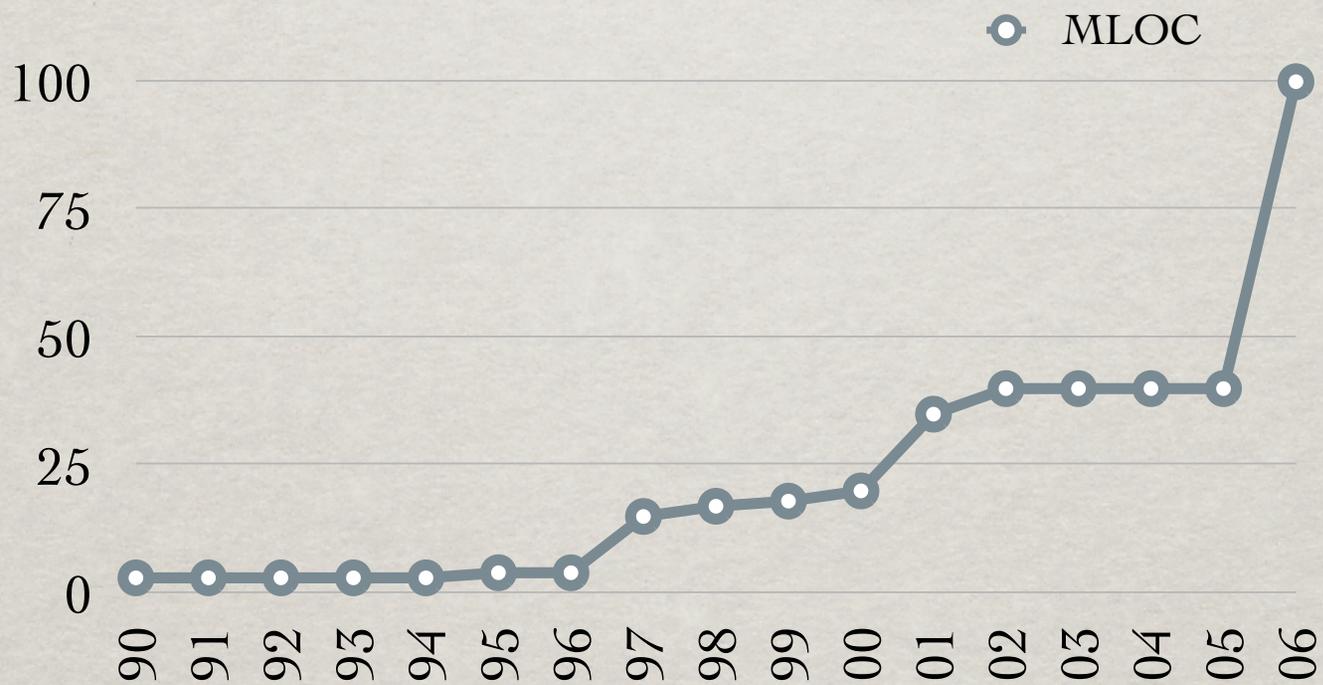
OPPORTUNITY “WASTED”?



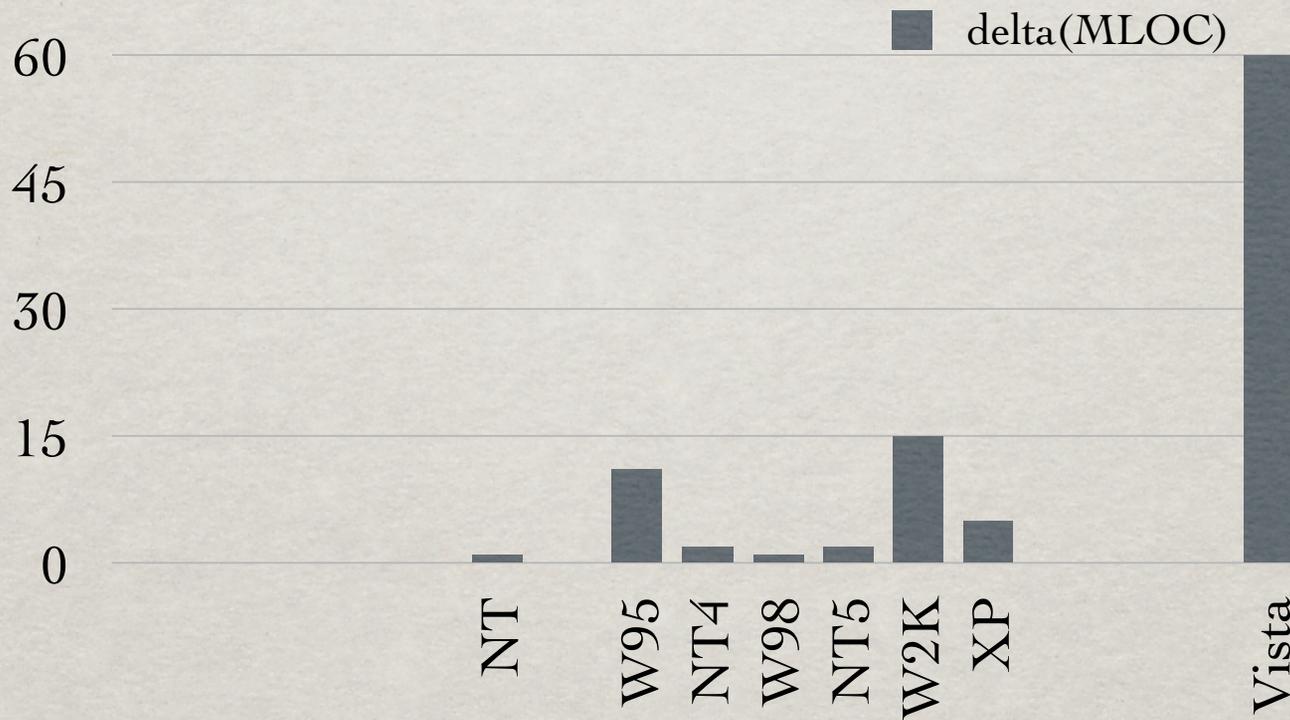
CODE VOLUME (94% SHARE)



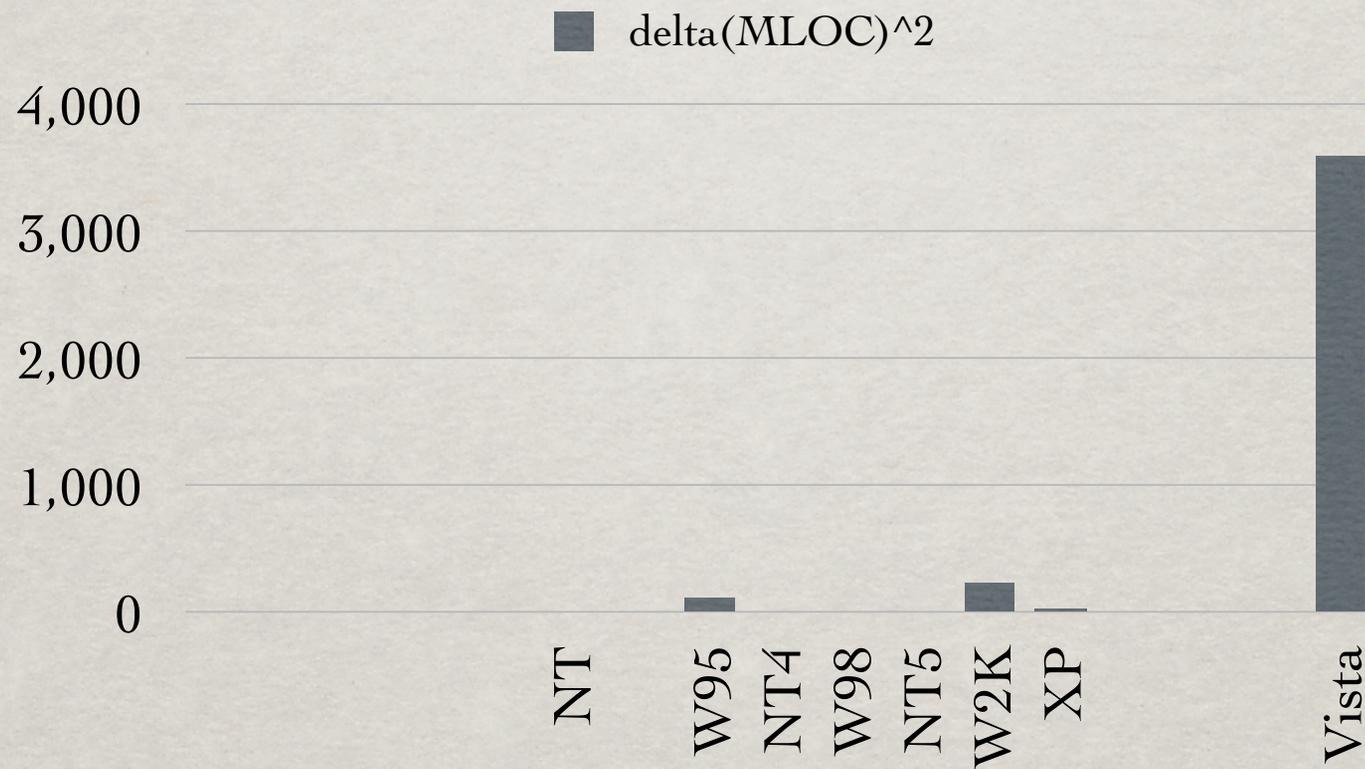
FIGHTING FIRE WITH FIRE?



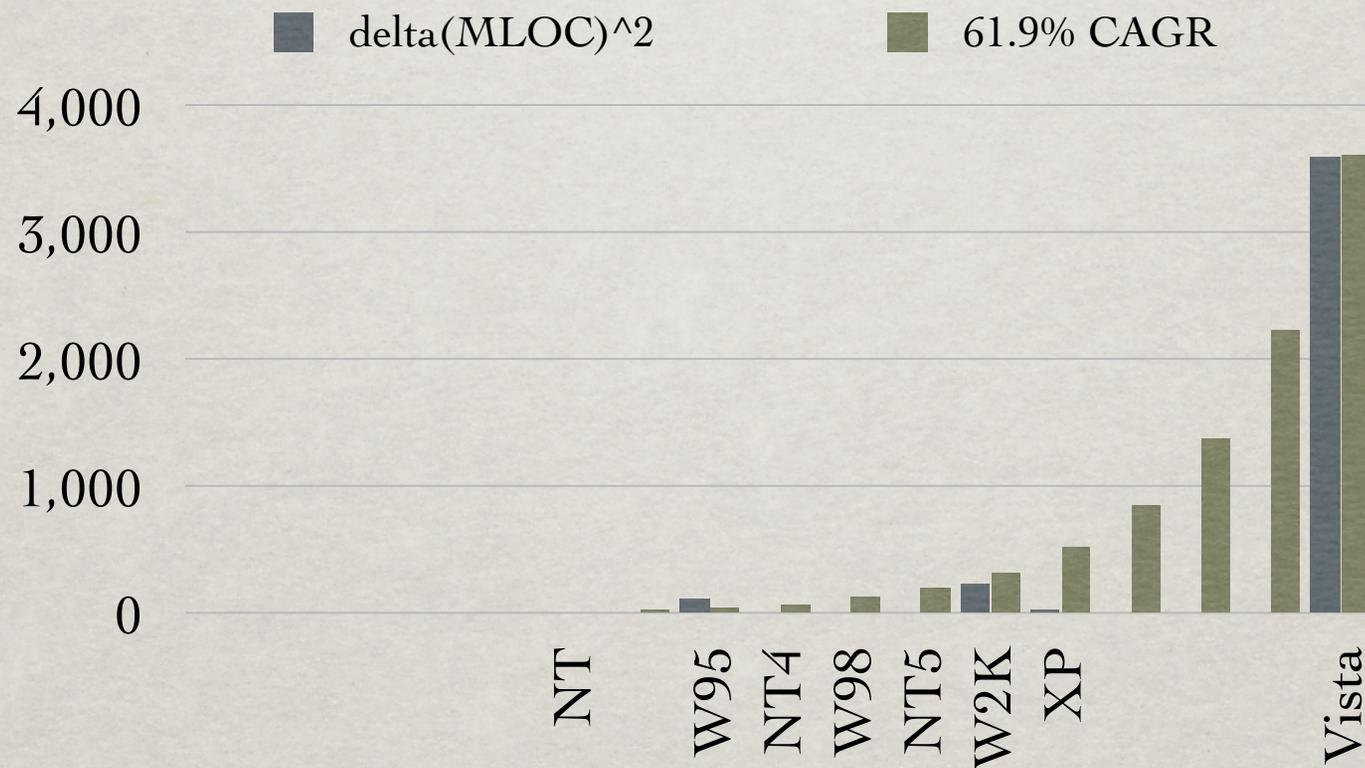
+CODE / UNIT TIME



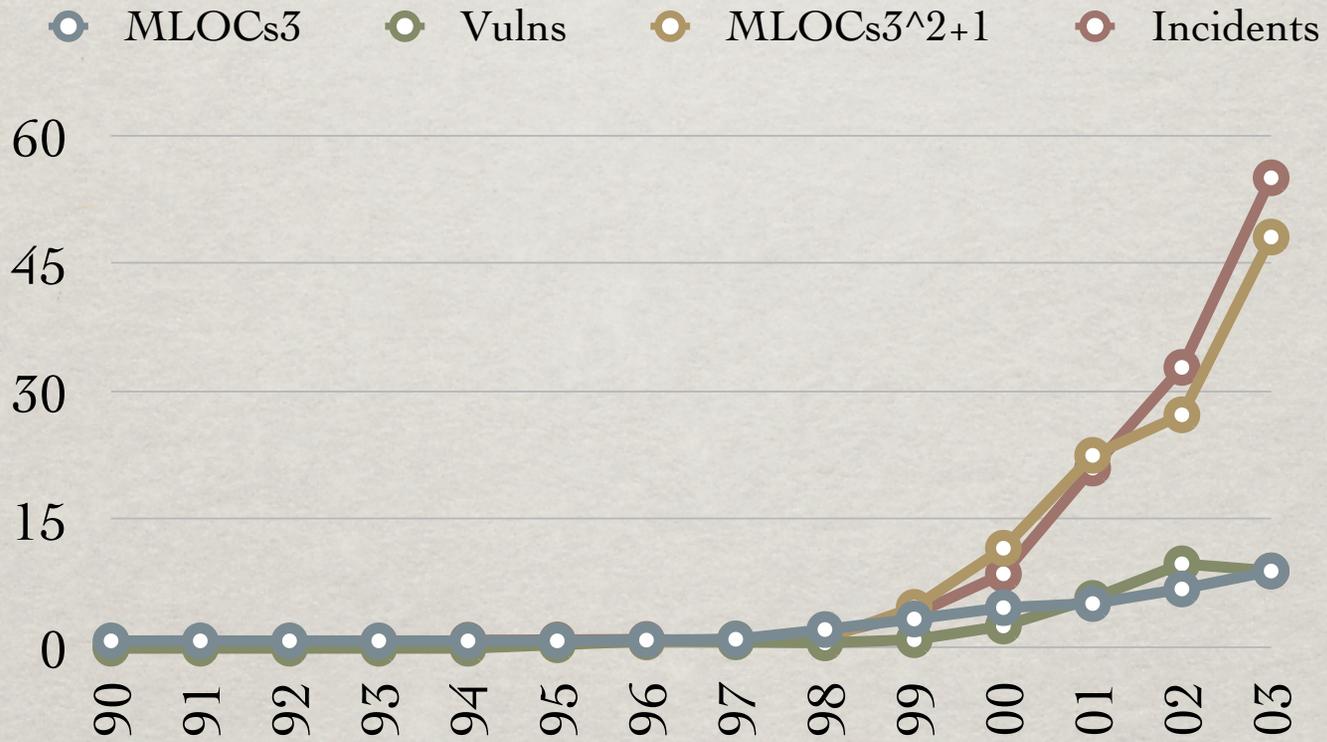
+COMPLEXITY / UNIT TIME

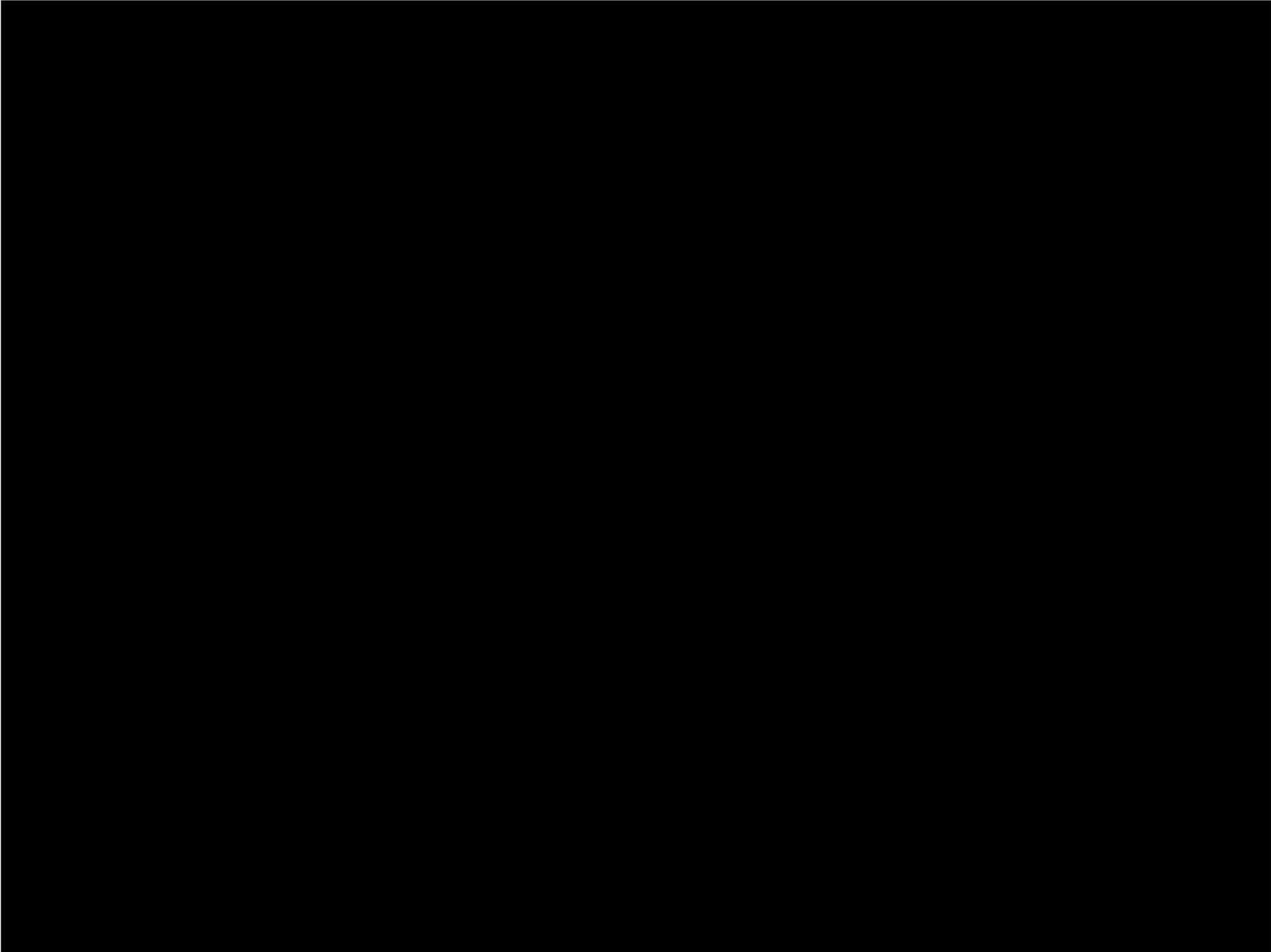


+COMPLEXITY / UNIT TIME



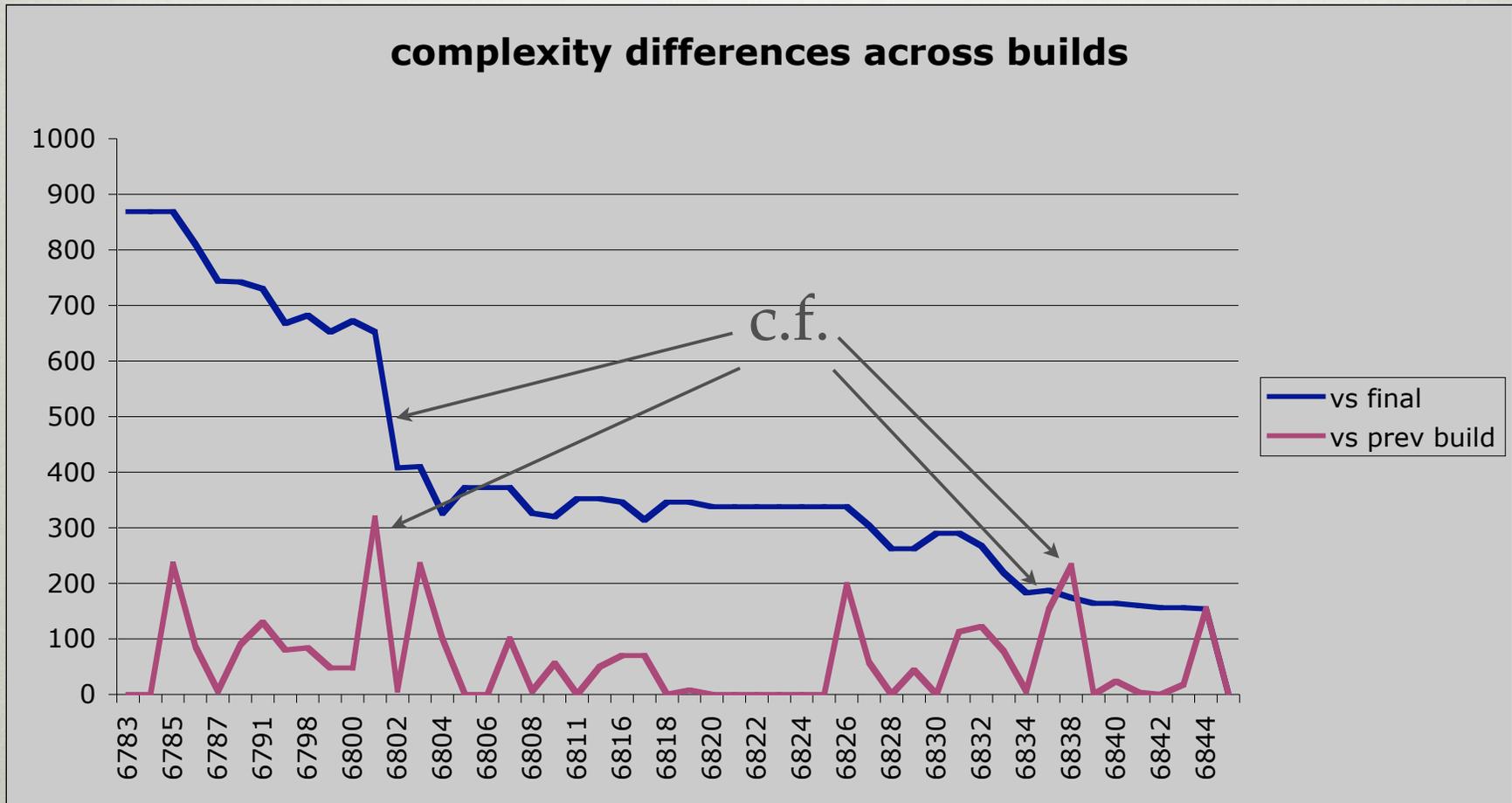
RISK DRIVERS

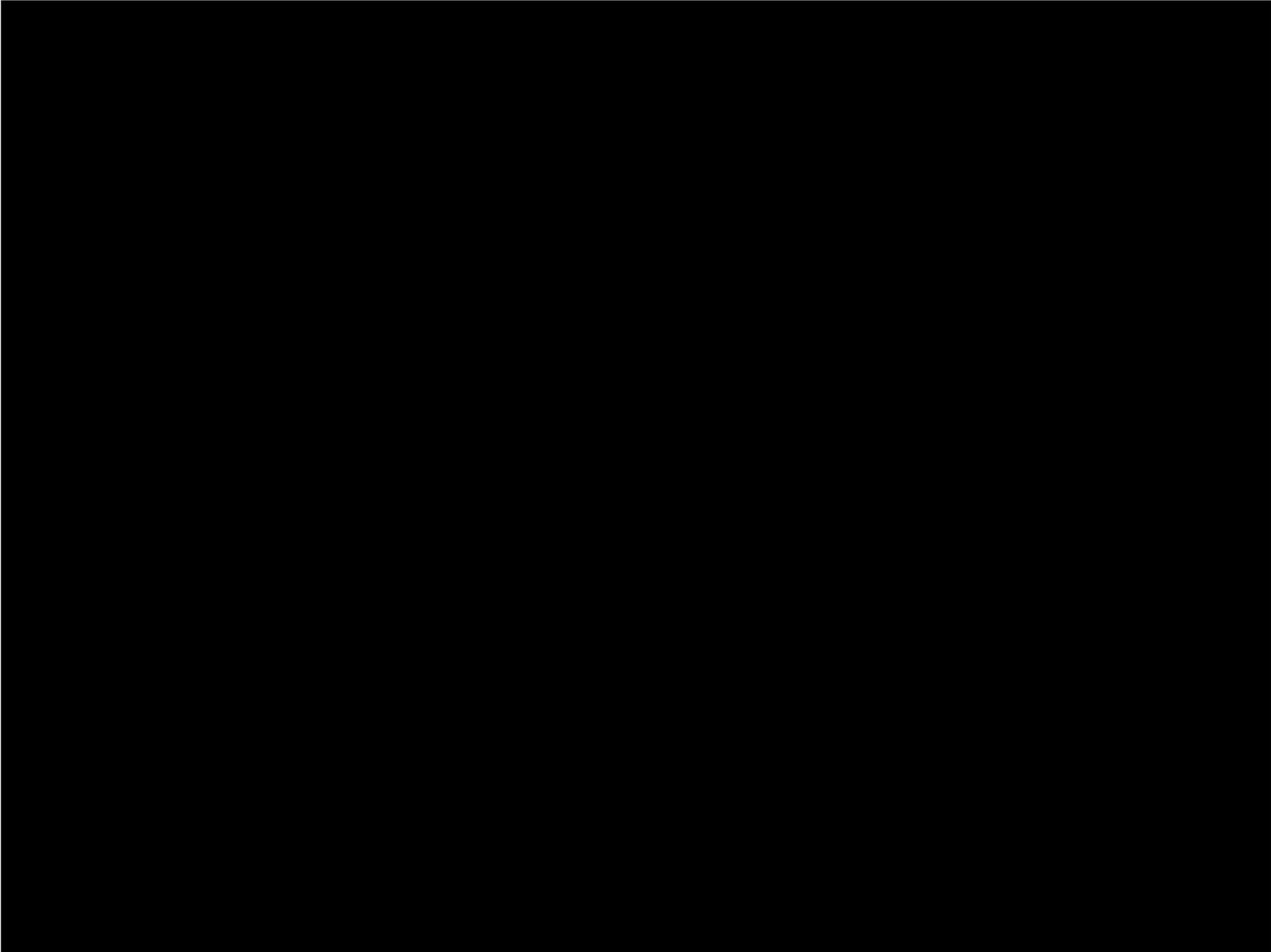




BUILD JITTER

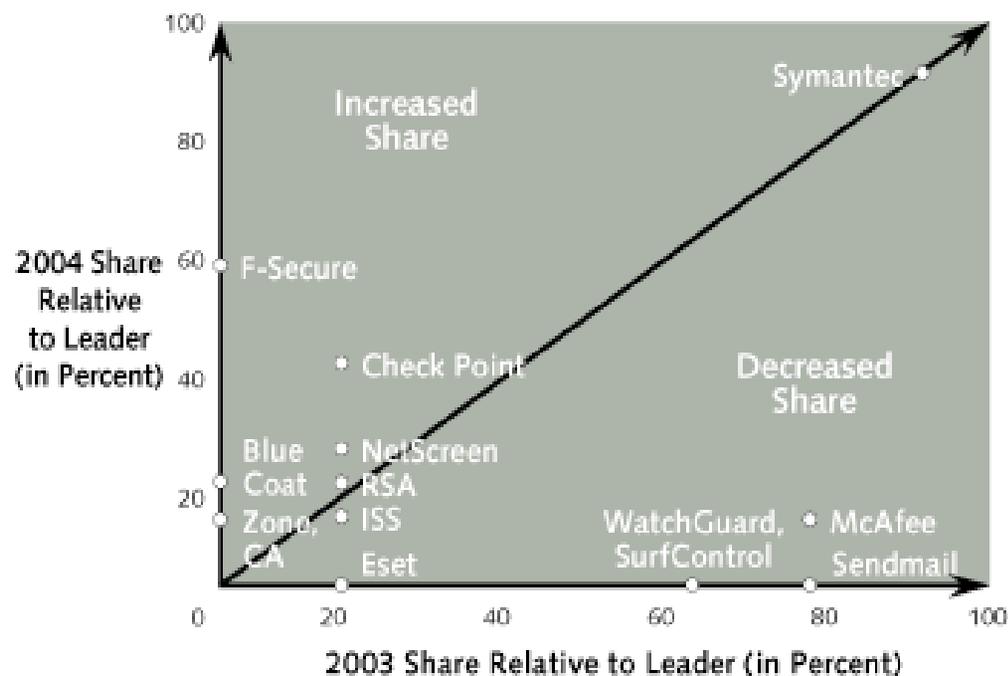
complexity differences across builds





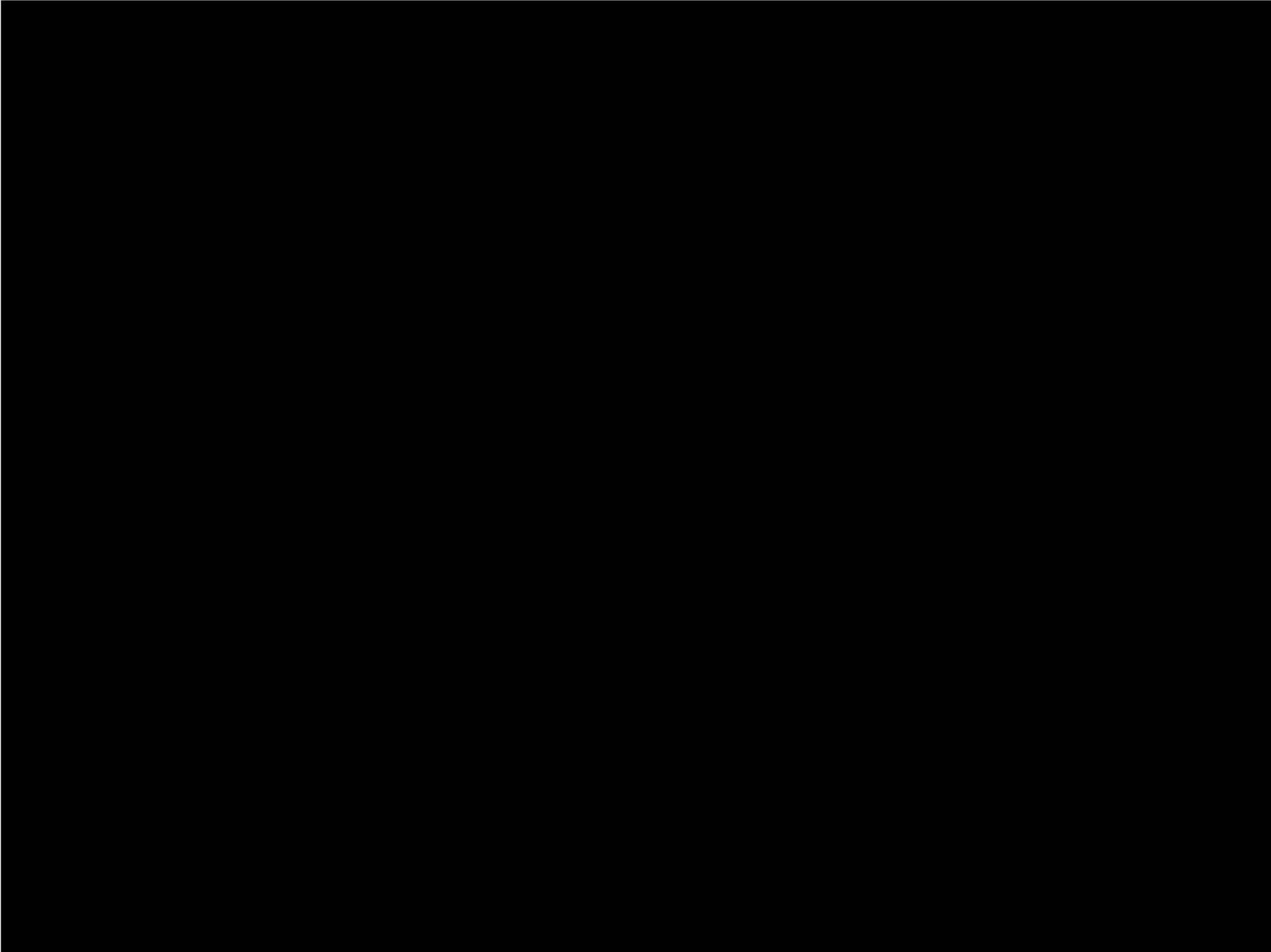
SECURITY TOOLS ARE TARGETED

Security Vendor Vulnerability Distribution
Number of CVE Advisories 2003-2004



SO WHO FINDS FLAWS?





DAN GEER
DAN@GEER.ORG
+1.617.492.6814

challenging work sought & preferred