SEI WEBINAR SERIES | Keeping you informed of the latest solutions

Software Engineering Institute | Carnegie Mellon University

Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003493

Secure Software Development Landscape

Mark Sherman
Technical Director, CERT

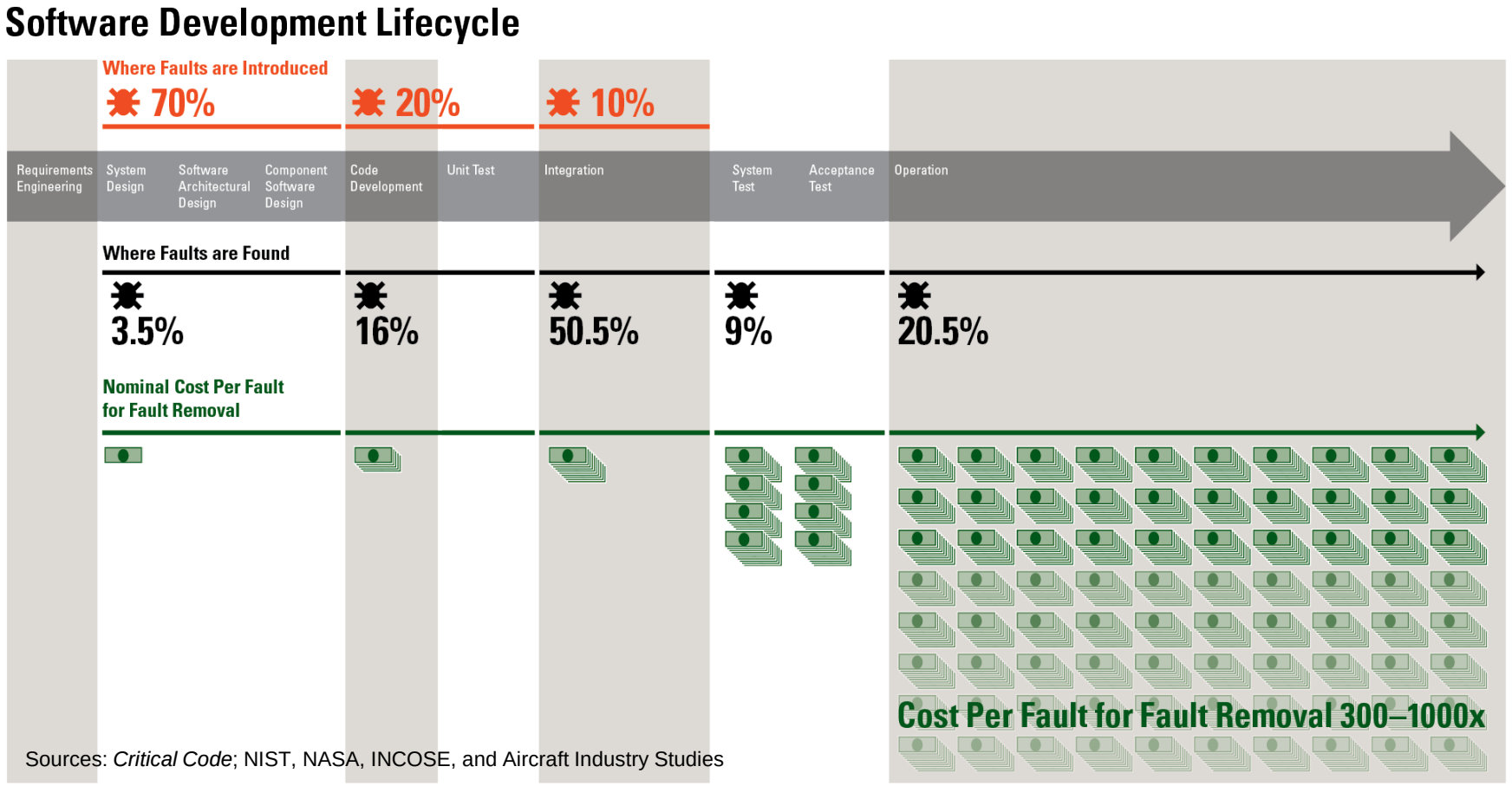
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

What did the Jeep experience illustrate

- Running out of date software
- Wide attack surfaces
- Not understanding or appreciating interconnections
- Components used in new operational situations
- Assumed or misunderstood authentication and authorization needs
- Lost opportunity to mitigate damage through disclosure
- “Security through obscurity” is not enough

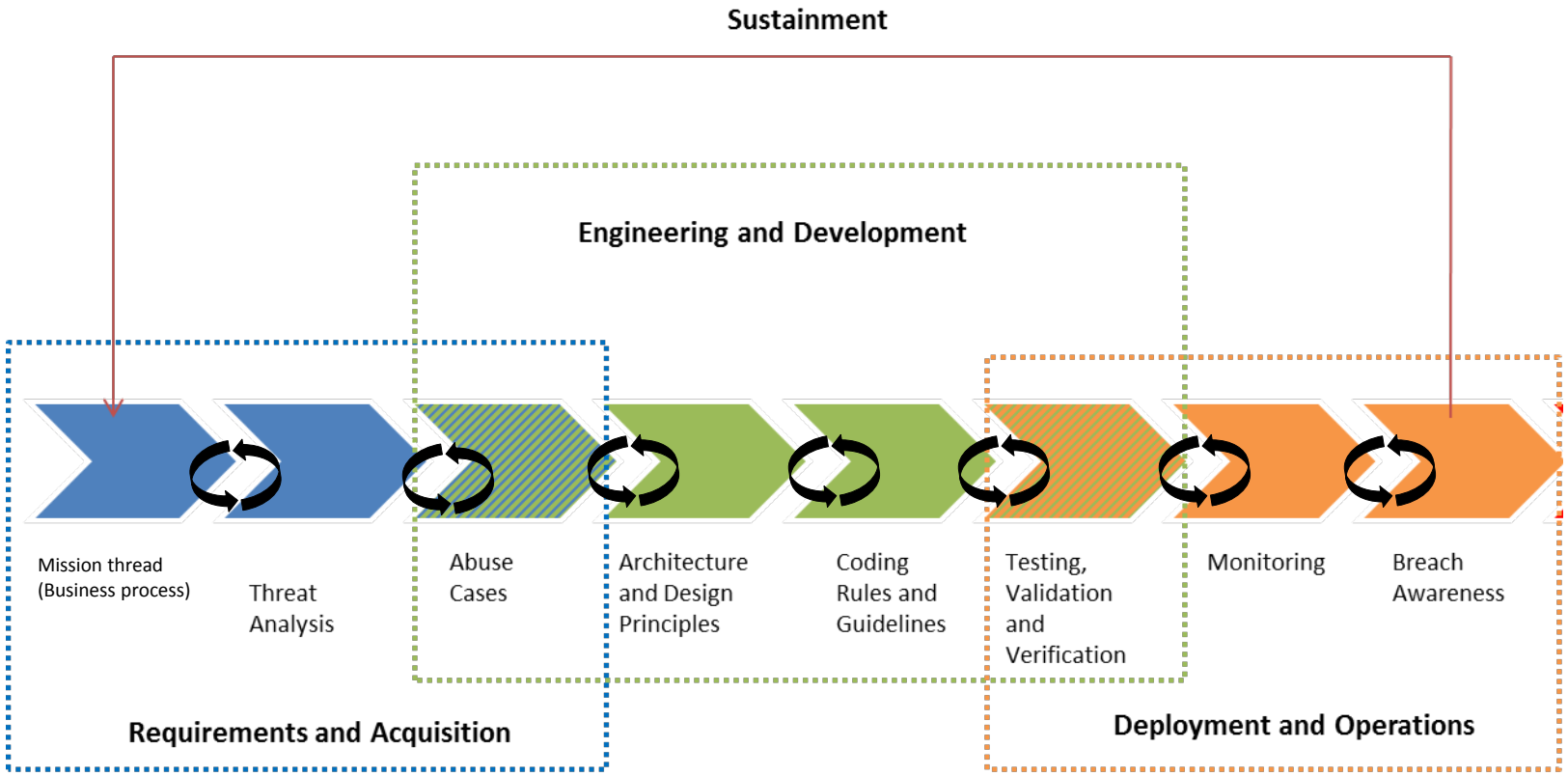
Catching software faults early saves money

Faults accounts for 30–50% percent of total software project costs



Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

Security is implemented across life cycle



Polling Question

What tools do you use to support secure development?

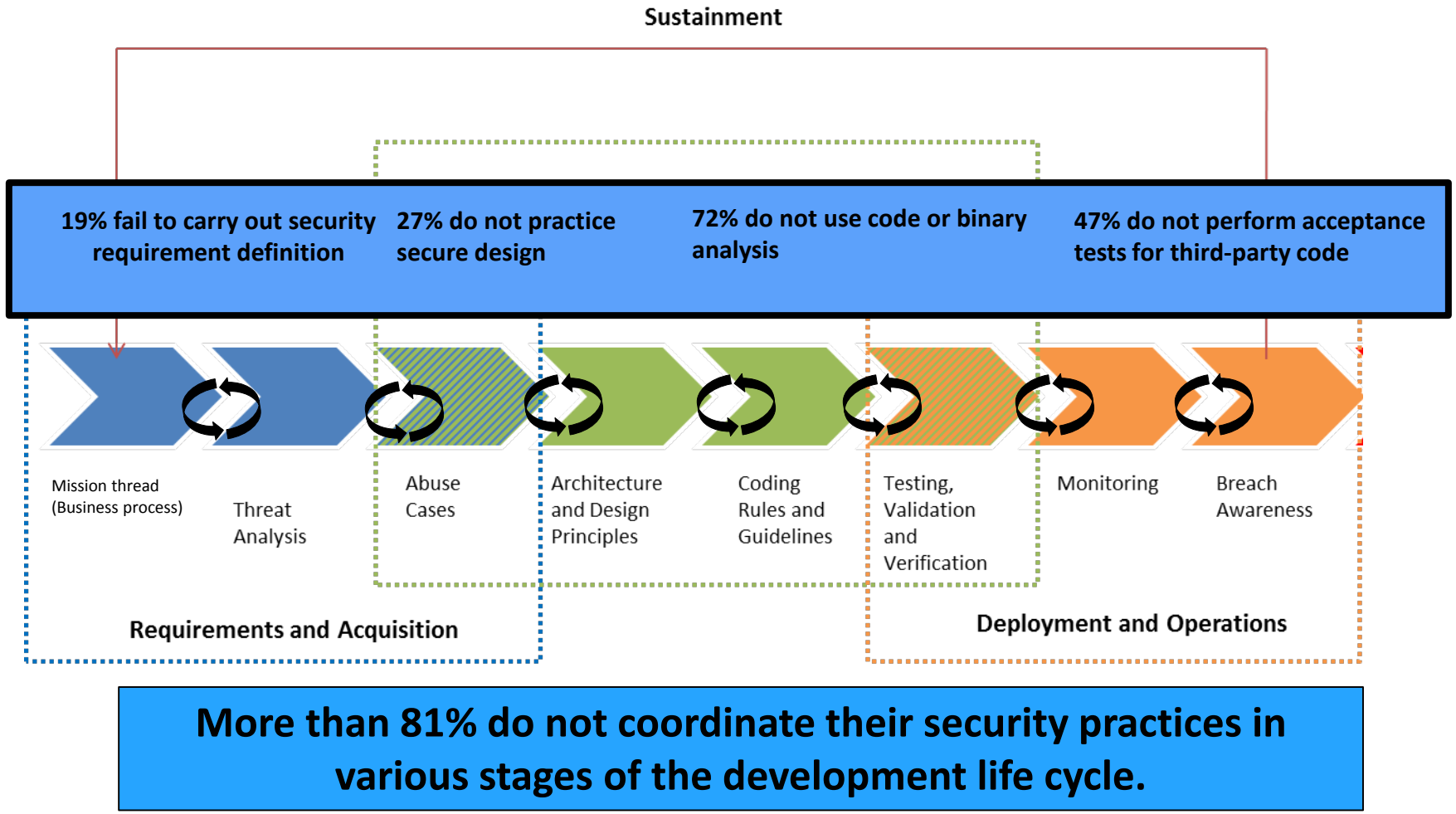
Security requirements management tool?

Source code analyzers?

Dynamic fuzz or penetration testing?

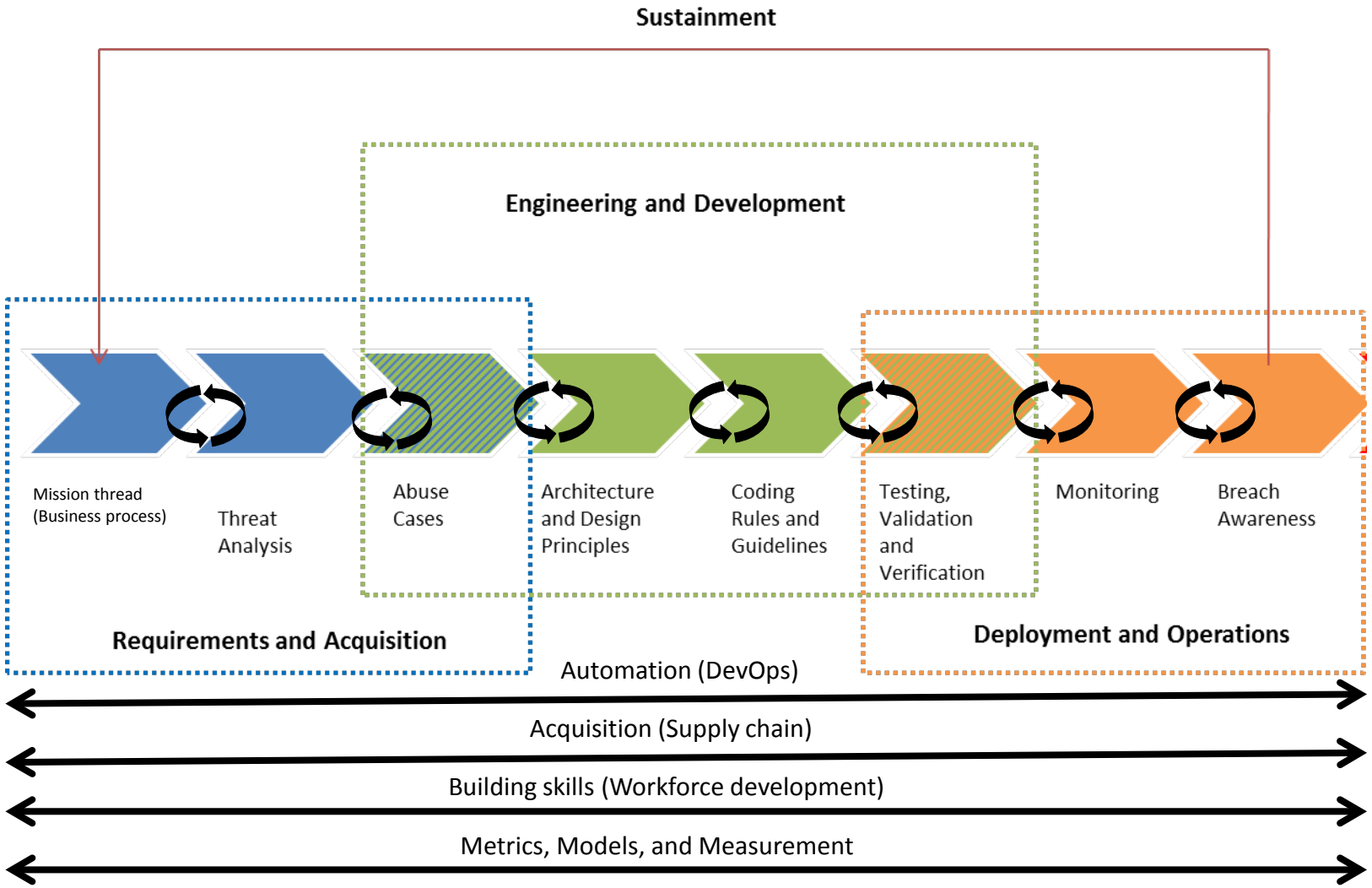
Others?

Room for improvement



Sources: Forrester Consulting, "State of Application Security," January 2011; Wendy Nather, Research Director, 451 Research, "Dynamic testing: Why Tools Alone Aren't Enough, March 25, 2015"

Cross life cycle issues



Software Engineering Institute | Carnegie Mellon

Contact Information

Mark Sherman

(412) 268-9223

mssherman@sei.cmu.edu

Web Resources (CERT/SEI)

http://www.cert.org/

http://www.sei.cmu.edu/