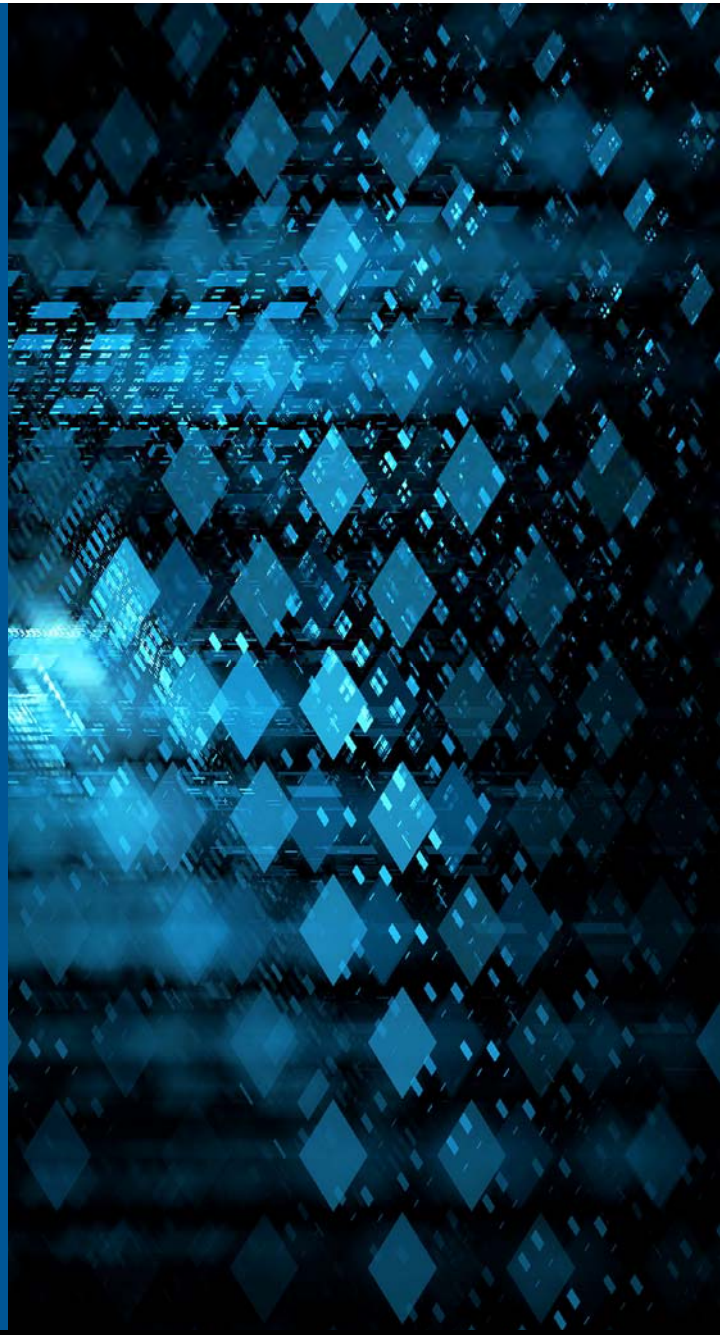
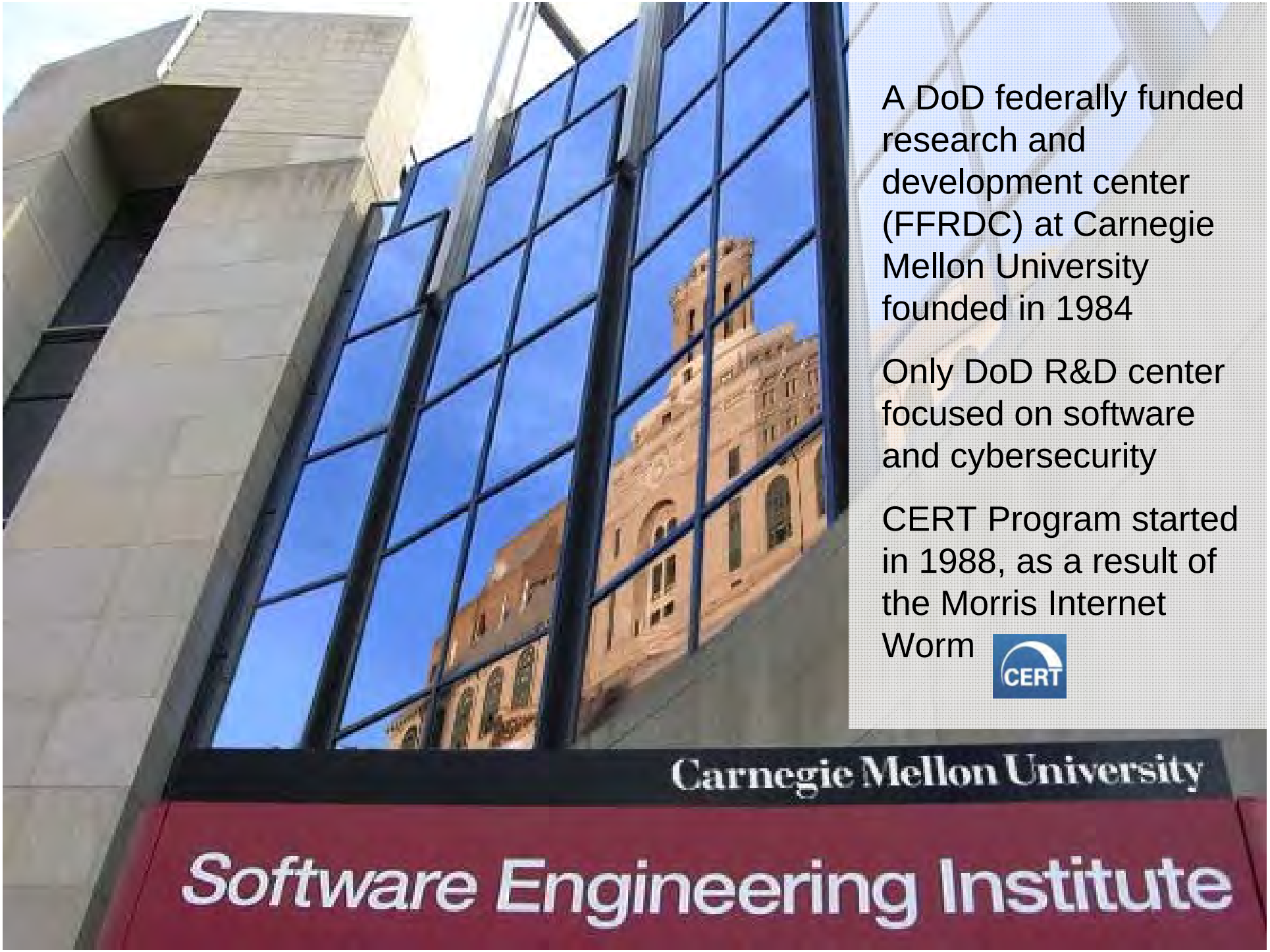
SEI Research Program

Dr. Kevin Fall

Deputy Director, Research, and CTO

kfall@sei.cmu.edu





A DoD federally funded research and development center (FFRDC) at Carnegie Mellon University founded in 1984

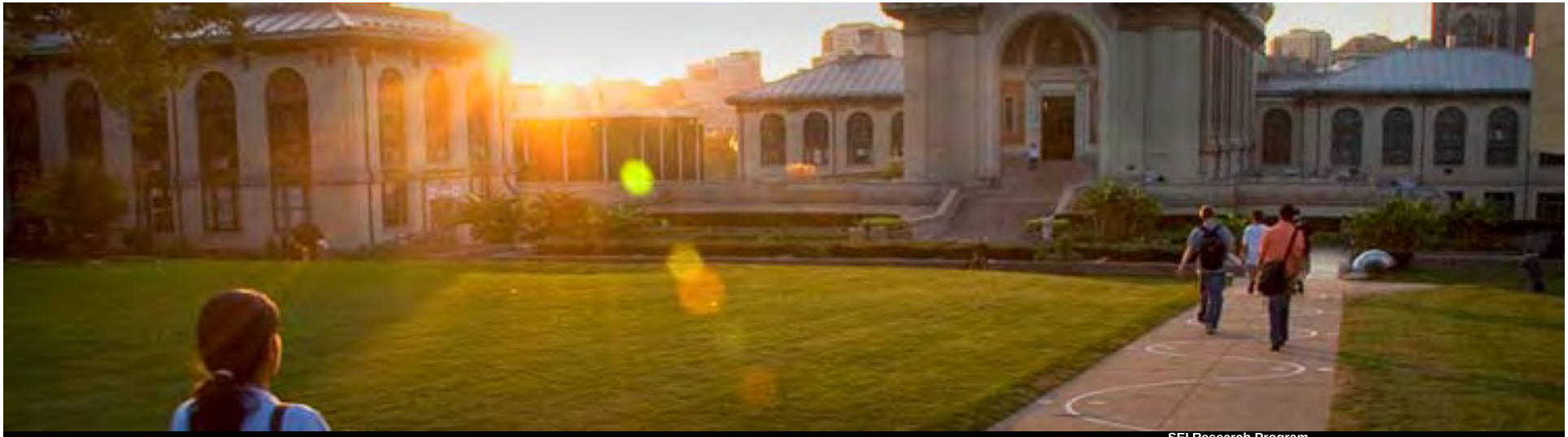
Only DoD R&D center focused on software and cybersecurity

CERT Program started in 1988, as a result of the Morris Internet Worm

SEI and CMU

Within CMU, we resemble a “school” or “college” in the org chart

- Such as: Computer Science, Engineering, Fine Arts, Humanities/Social Science (Dietrich), Business (Tepper), Science (Mellon), Public Policy and Information Science (Heinz)
- Our ~600 employees are CMU staff members
  - Some hold additional academic titles (researcher, adjunct faculty)



“The DoD is in the software business”

Software provides for the capabilities and flexibility needed to sustain DoD strategic advantage.

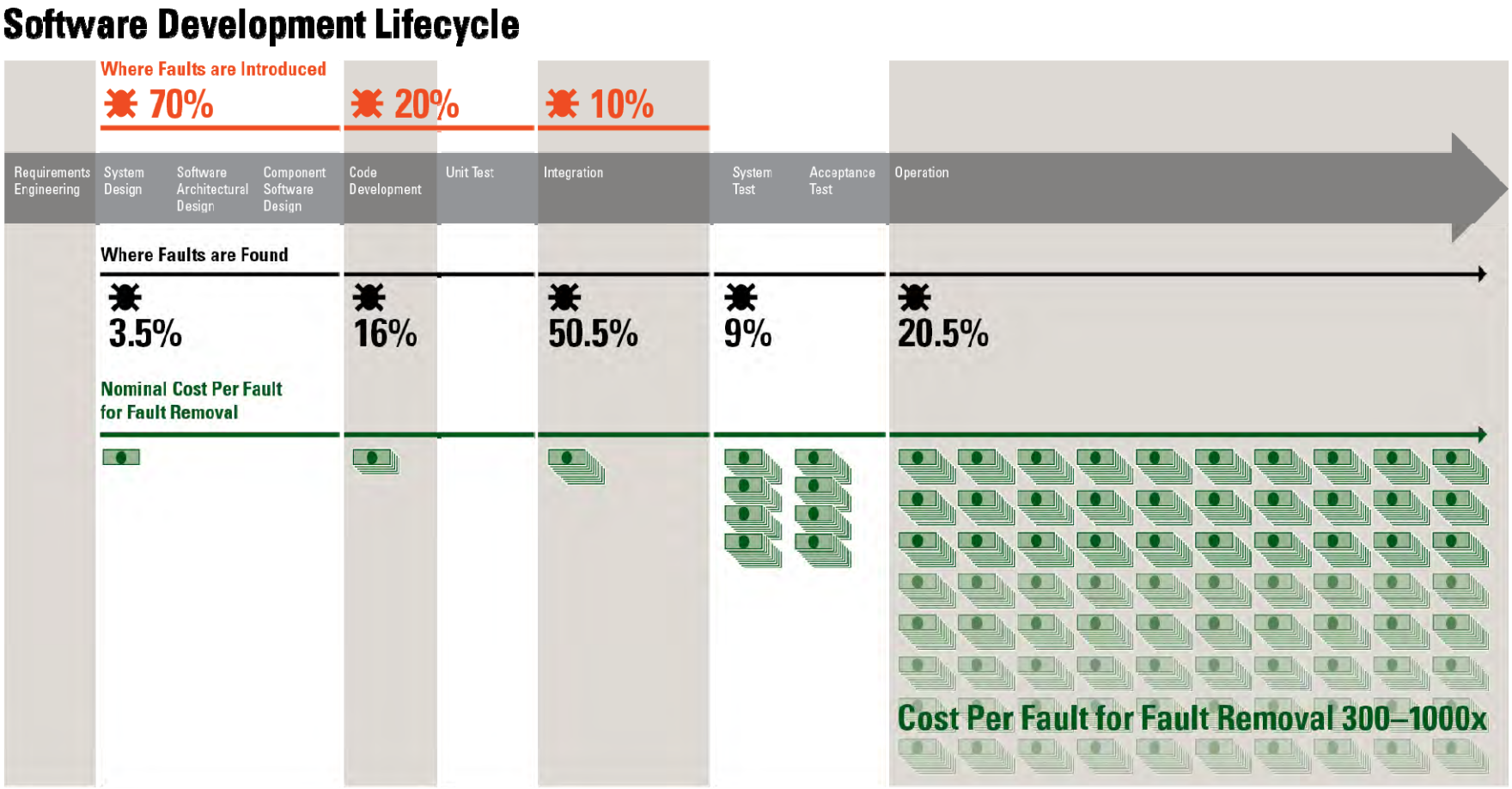
“The B-52 lived and died on the quality of its sheet metal. Today our aircraft will live or die on the quality of our software.” —Air Force General

Quotes: “Delivering Military Software Affordably,” *Defense AT&L*, March-April 2013

Image: 091209-F-6680C-140.jpg (Wikimedia commons)

DoD Concern: Software Complexity & Costs

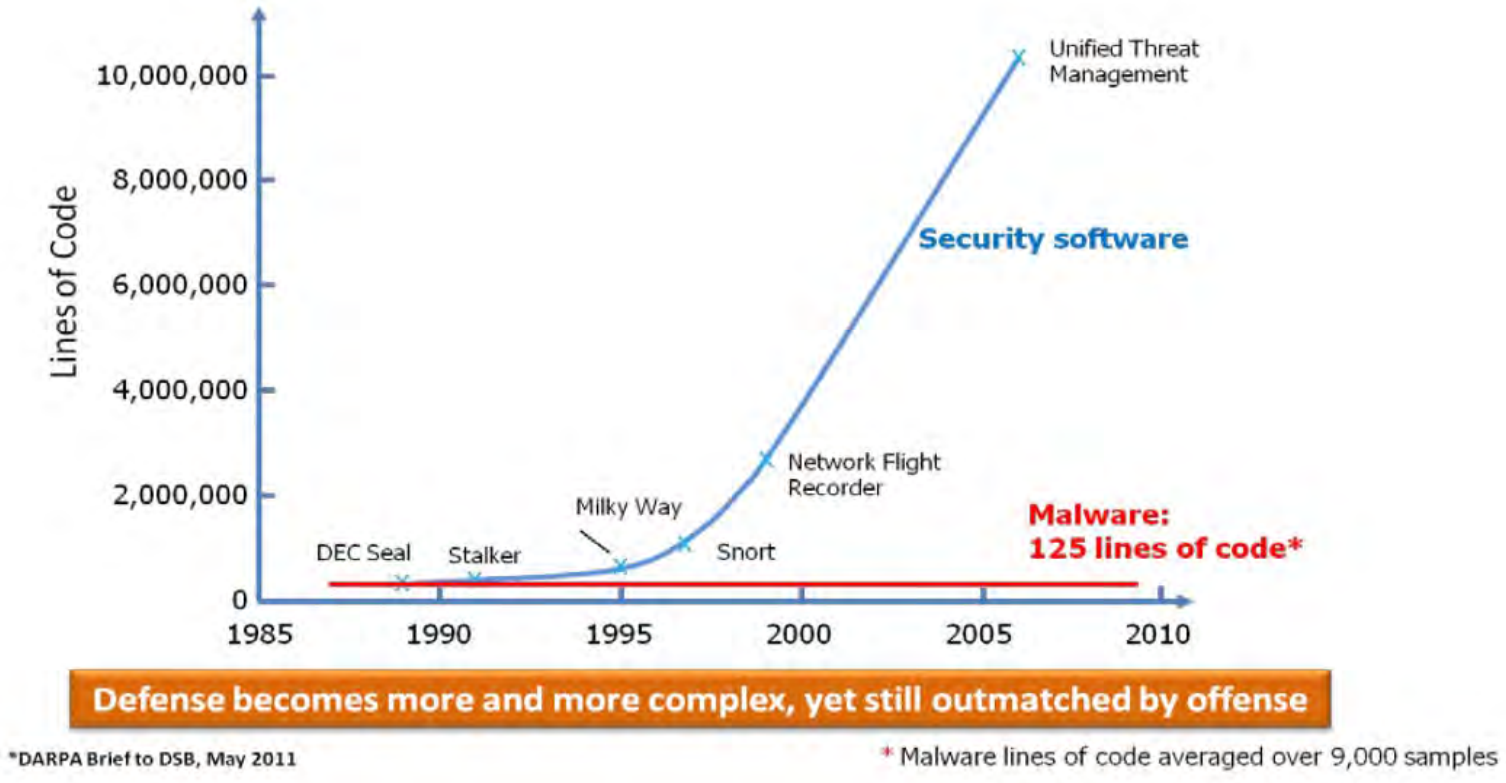
Finding faults early or avoiding them can produce major savings.



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

DoD Concern: Cybersecurity and Risk

Software complexity, interconnectedness, and a global supply chain contribute to risks associated with cybersecurity.



Source: DSB, *Resilient Military Systems and the Advanced Cyber Threat*

DoD Concern: Workforce Development

A surge in hiring cyber workforce calls for skills to understand cyber threats, write secure code, and analyze network traffic for intrusions and software for vulnerabilities.

Managers and acquisition professionals must likewise understand these concerns.

Source: http://www.arcyber.army.mil/g1.html

The Technical Landscape

Growing ability to program things that were once fixed-function

sensor networks, FPGAs, SDR, SDN, NFV,
smart grid, IoT, autonomous operations, etc…

Systems of [networked] systems and components

cloud, apps, virtualization, MapReduce/Spark
increased complexity of distributed s/w systems

Software development environments and methods

rich data sets, “big data,” and machine learning
a need for validation and accreditation

Greater capabilities bring greater complexity and assurance concerns

Motivation: Capabilities with Confidence

Software provides a growing percentage of functionality…
and is the building material for cybersecurity

Software capabilities are assembled from components
often from unknown sources and with little validation

- At least 75% of organizations rely on open-source software, and it is not immune from seemingly simple problems; neither is closed source

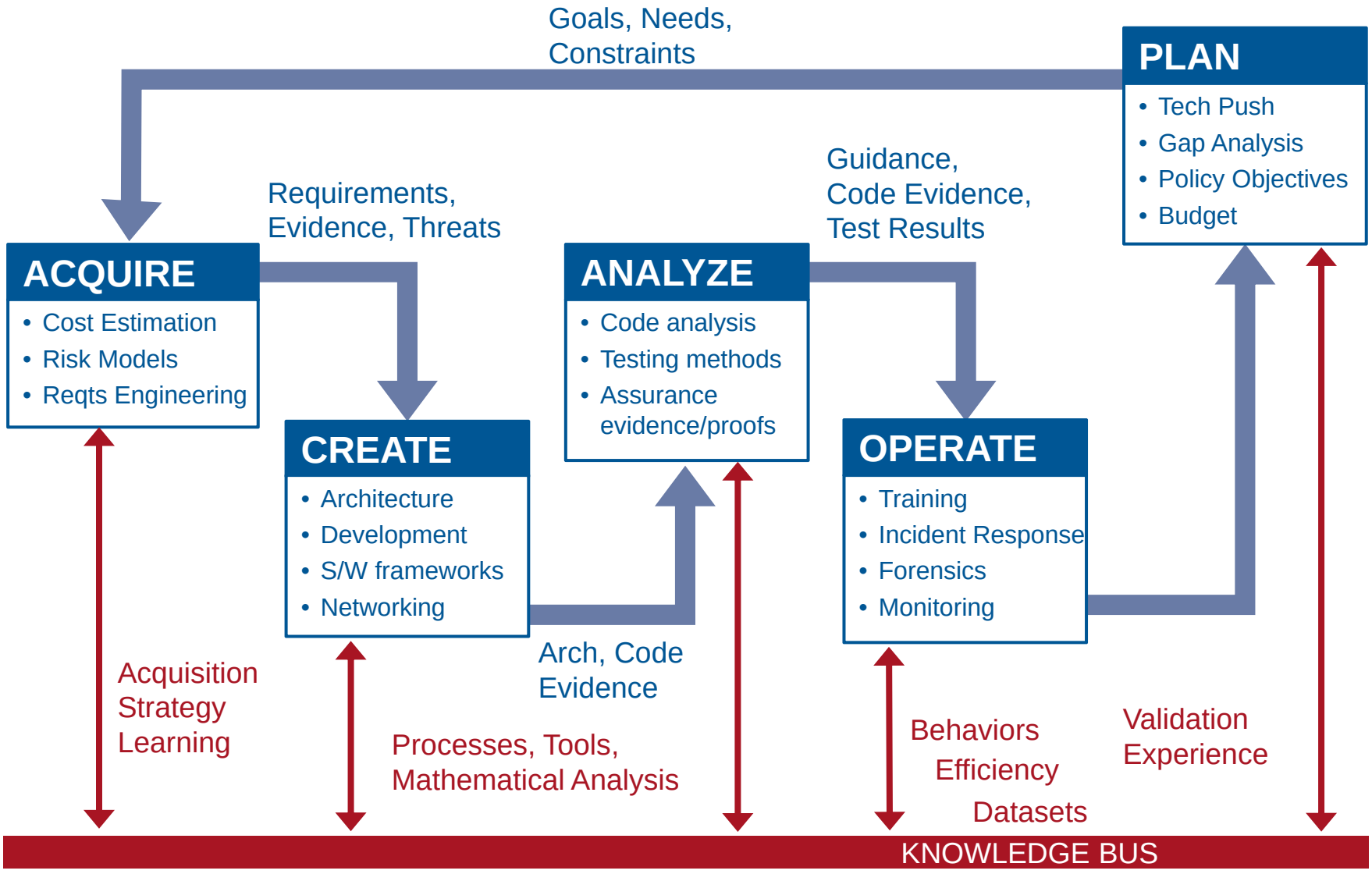
Composing [even simple] software components leads to complexity that is difficult to reason about and secure

- IoT will likely increases the challenges
- different expertise, use cases, security needs, privacy issues

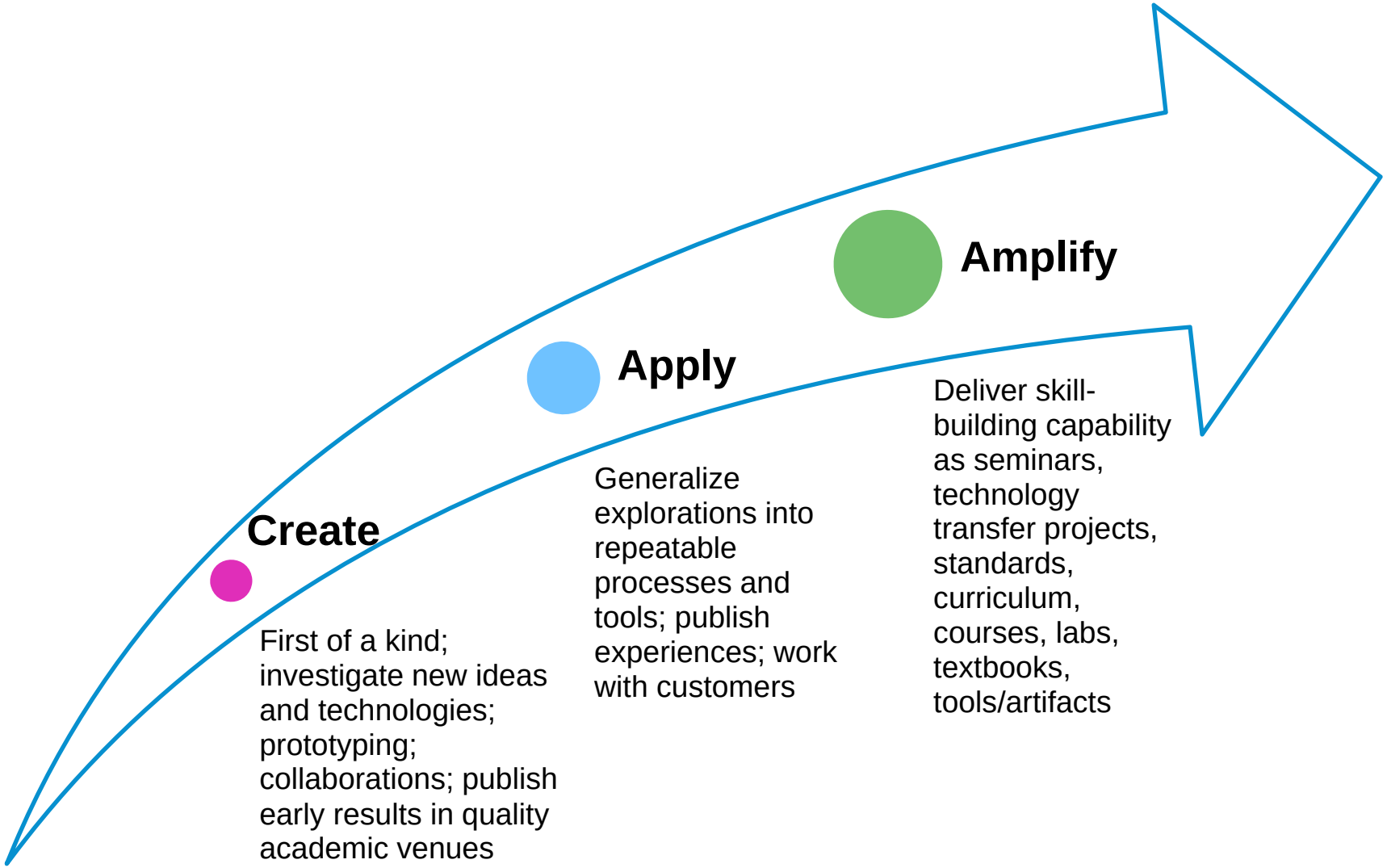
How to buy, make, operate, and improve software systems

… with unprecedented levels of assurance and confidence?

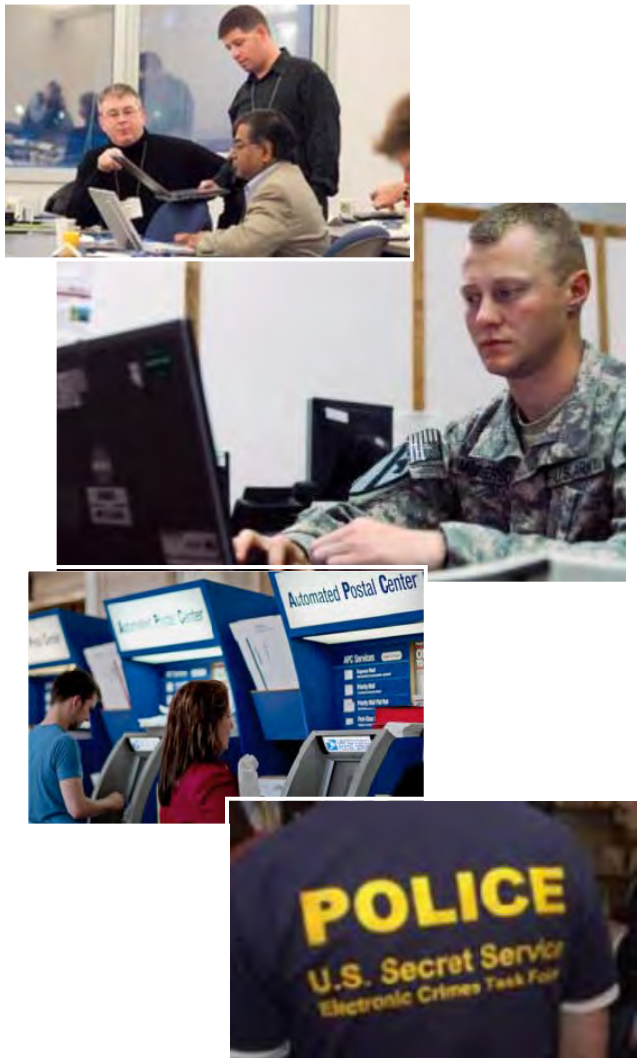
Technical Strategic Framework



Notional Technology Maturation Pipeline



R&D Work at SEI



Line funded projects ("line" and "LENS")

- LENS = Line-funded Exploratory New Starts
- One- and two-year projects, with collaborators

Project work (with individual "customers")

- PWP (Project Work Plans) for work with government agencies
- Collaborative agreements for work with industry organizations

As a DoD FFRDC, we are subject to 'ceiling' (called "STE")

- Applies to our entire DoD-supported work

Technical Focus Area 1 (TF1): Lifecycle Assurance

- Statistical modeling of cost estimation
- Model-based engineering
- Model checking
- Technical debt analysis
- Vulnerability discovery
- Malware analysis

Acquisition lifecycle

Software development and validation

Operations, security, remediation, etc.

Policy and risk management

Human factors and performance

Technical Focus Area 2 (TF2): “PED to the Edge”

Production, Exploitation, Distribution of Information, including challenged environments

(using results from TF1)

- Frameworks for software development and analysis
- Networking and protocols
- Edge components – data analysis, power, security
- Algorithms, ML, “big data” systems

Architecture-Centric Virtual Integration Process (ACVIP)

Create

Apply

Amplify

1998
SEI first to research Virtual Integration

2004
With SEI technical leadership, AADL standard published

2005-current
Line-funding/ sponsored work: ACVIP, based on AADL/OSATE workbench

2006-current
Army pilots ACVIP (e.g., CH-47F)

2008
Aircraft makers choose AADL, OSATE for Virtual Integration initiative

2010-12
ASSIP & Apache Upgrade: Virtual Upgrade and Reliability Validation

2014-15 ACVIP shadow exercise: SEI rapidly detected more than 85 potential integration issues early in JMR development that traditional approaches missed. Led to ACVIP adoption by JMR contractors and its inclusion in RFPs for FY2016/17 projects.

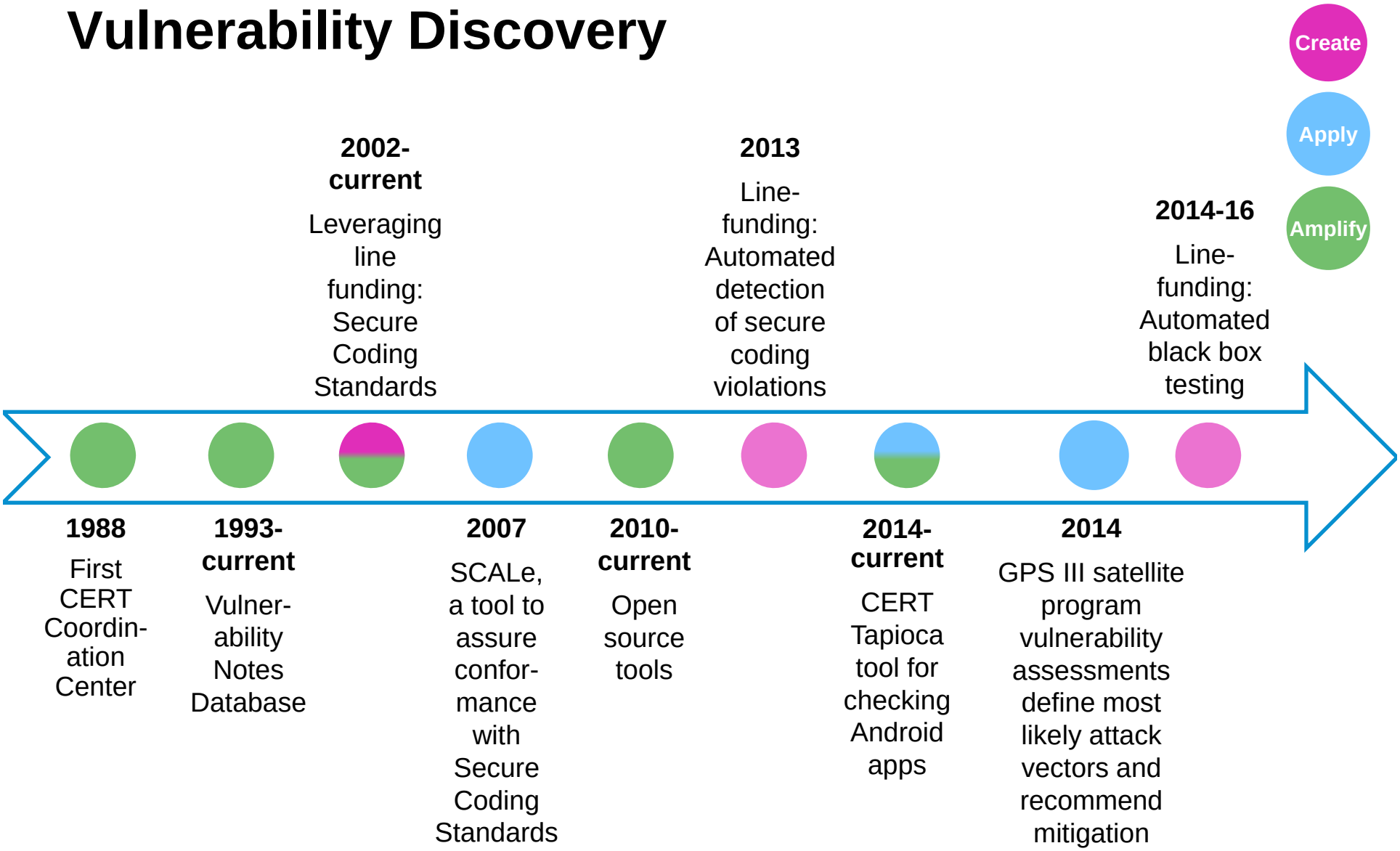
2015
Line-funding: AADL in auto code generation

2015-16
Line-funding: Lifecycle assurance based on ACVIP

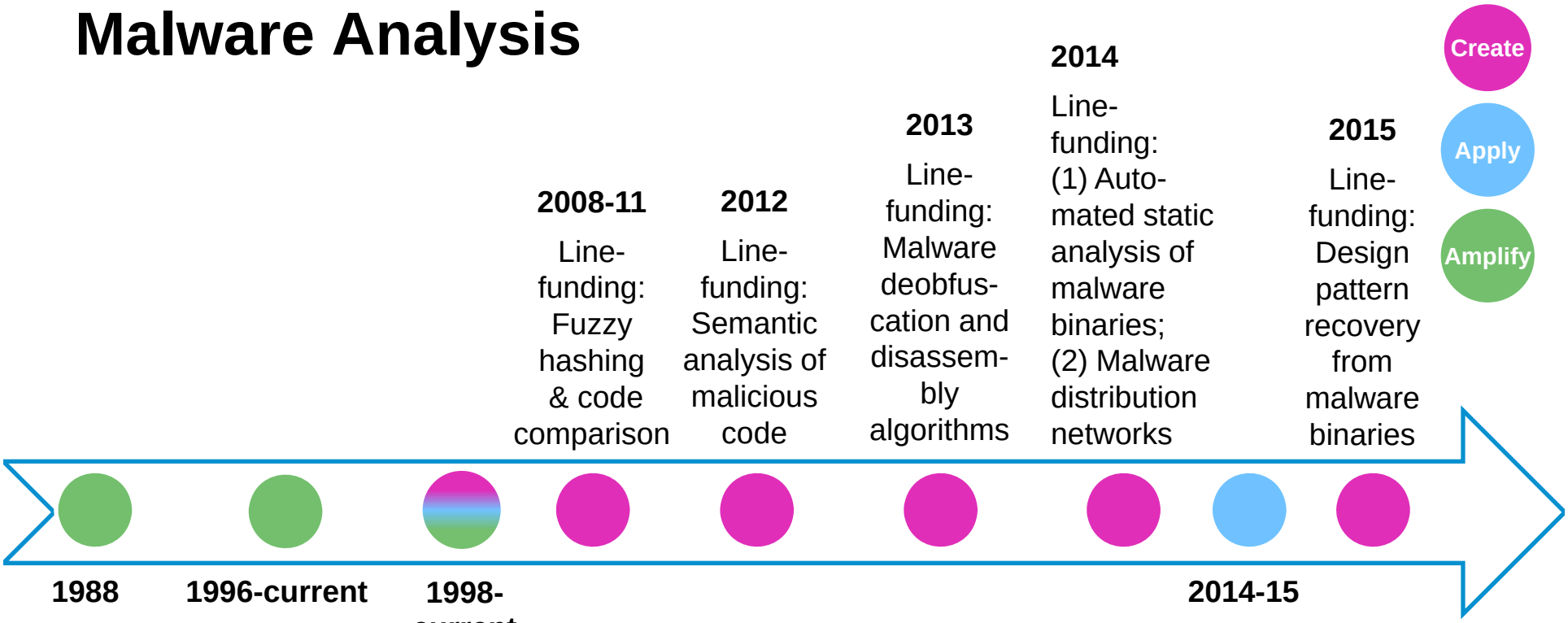
2015-18
ACVIP in Future Vertical Lift acquisition

AADL= Architecture Analysis & Design Language; OSATE = Open Source AADL Tool Environment

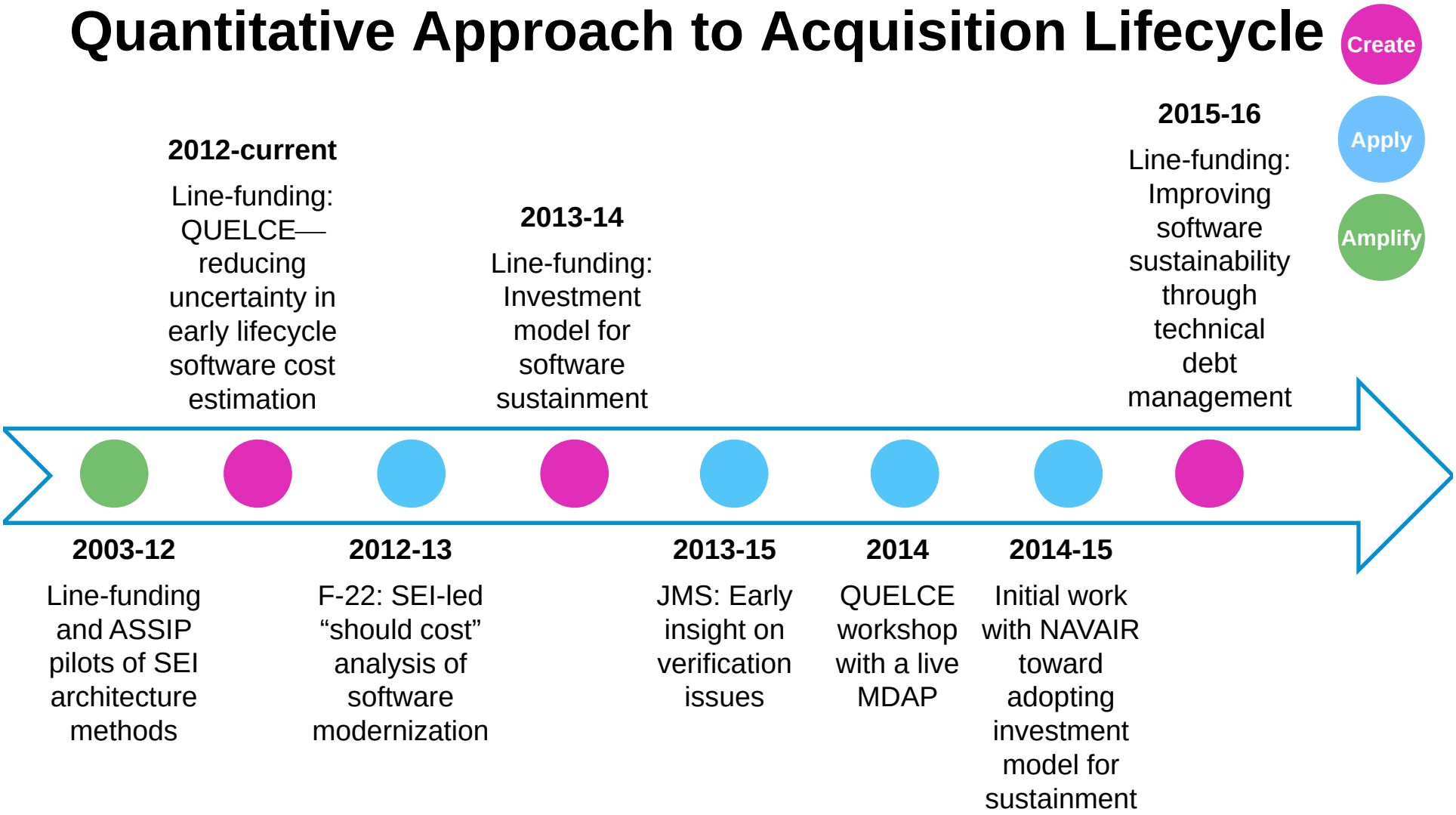
Vulnerability Discovery



Malware Analysis



Quantitative Approach to Acquisition Lifecycle



QUELCE = Quantifying Uncertainty in Early Life-Cycle Cost Estimation; JMS = Joint Space Operations Center (JSpOC) Mission System
MDAP = Major Defense Acquisition Program; COE = Common Operating Environment

Cyber Workforce Exercises and Simulations

Create

Apply

Amplify

2001

Line funding: Virtual Training Environment (VTE) platform

2002

Web-based VTE platform used for the first Service academy Cyber Defense Exercises

2007

Web-based cyber exercise system, CERT Exercise Network (XNET)

2009-current

XNET: AF cyber readiness program & exercises for Army's distributed ARCERTs, TNOSCs

2012

R&D of CERT Simulation, Training, and Exercise Platform (STEP)

2013

Transition of VTE to Govt. as FedVTE

Estimated Government annual training cost savings: $10M

2013

US-CYBERCOM chooses STEP to manage its joint persistent training environment

2014-15

Line-funding: Automated Cyber Readiness

2015-16

Line-funding: Human-computer decisions

ARCERT = Army Computer Emergency Response Team; TNOSC = Theater Network Operations and Security Center

Cyber Risk and Resilience

Create

Apply

Amplify

2003

OCTAVE method to assess organizational security needs

2007

Resilience Management Model (RMM), foundation for operational resilience management improvement

2008

Smart Grid Maturity Model

2010

RMM capability appraisals

2011

Cyber Resilience Review (CRR), to examine cybersecurity practices in critical infrastructure organizations

2012

Risk and vulnerability assessment (RVA), to provide agency-specific risk analysis

2014

Third-party risk assessment (supply chain)

2015

Cyber Risk insurance symposium

Gov. Tom Ridge, first Secretary of Homeland Defense, keynoted the May 2015 CERT Cyber Risk Insurance Symposium

OCTAVE is the Operationally Critical Threat, Asset, and Vulnerability Evaluation method

Summary: SEI Highlights

Pausch Bridge and The Gates Center at CMU

One of DoD's only two R&D FFRDCs (at CMU and MIT)

600+ Staff in DC, Pittsburgh, and Los Angeles

A primary focus on software engineering and cybersecurity

Affiliation with Carnegie Mellon University, a globally recognized research university and #1 in computer science

Extensive databases and access

Ability to work with industry, government, and academia

From work intended for academic publication to sensitive government programs

Contact Information

Kevin Fall

Email: kfall@sei.cmu.edu

Telephone: +1 412-268-3304

Customer Relations

Email: info@sei.cmu.edu

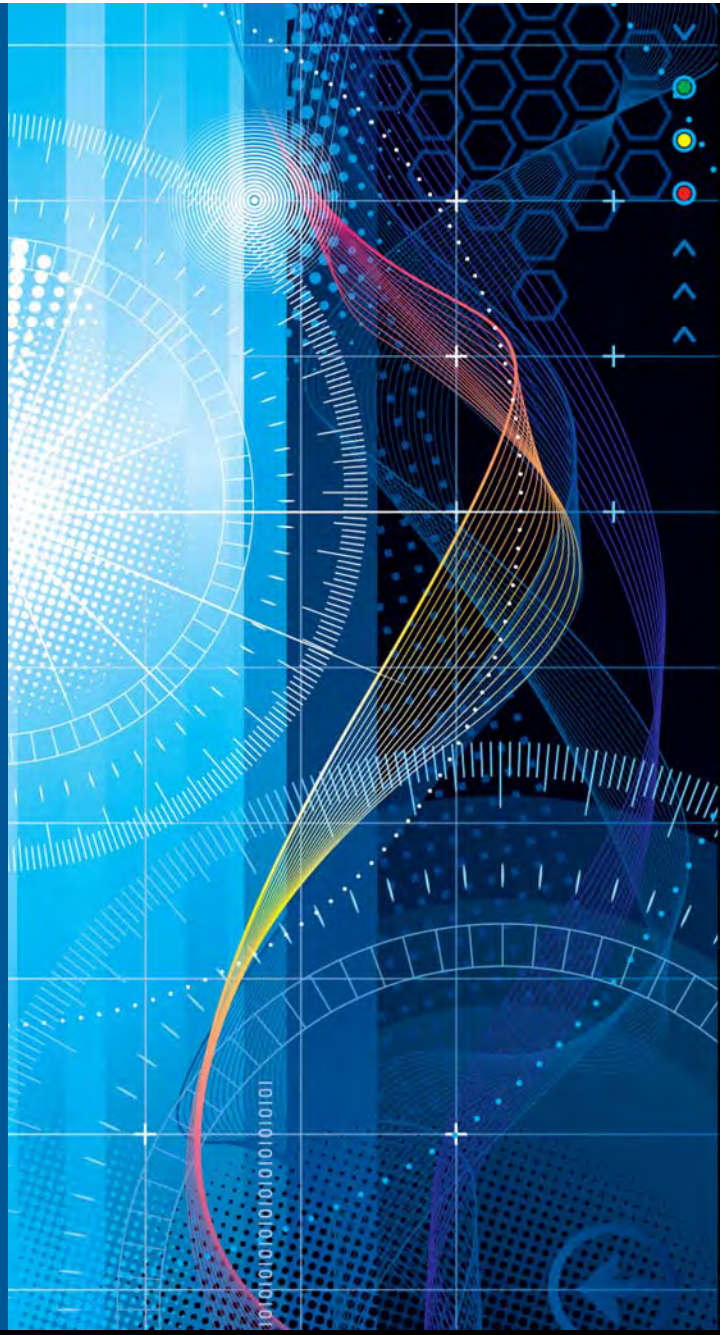
Telephone: +1 412-268-5800

U.S. Mail

Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612 USA

Website

www.sei.cmu.edu/contact.cfm



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-0003058

Extra

Risk and Vulnerability Assessment

8 areas of assessment

- Network mapping
- Vulnerability scan
- Penetration test
- Phishing assessment
- Wireless assessment
- Web application assessment
- Operating system security assessment
- Database assessment

Cyber Flag Exercises

Cyber Flag-15 demonstrated the first transition of STEP tier I and tier II operational responsibilities to a transition partner

CERT has facilitated Cyber Flag FY12-FY15

Exercise network powered by the SEI-developed Simulation, Training, and Exercise Platform (STEP)

FY15 Cyber Flag incorporate 700+ distributed participants in environment composed of 7,000+ virtual machines and 200+ hardware appliances

F-22 Modernization Program

Issue

The Air Force Aeronautical Systems Center wishes to understand software development in the F-22 modernization program

Action

SEI performed a should-cost analysis of the program's software acquisition

Result

Program Office negotiated a 15% reduction—$32 million—in cost and schedule improvements, as well as a reduction in defects and an improvement in productivity

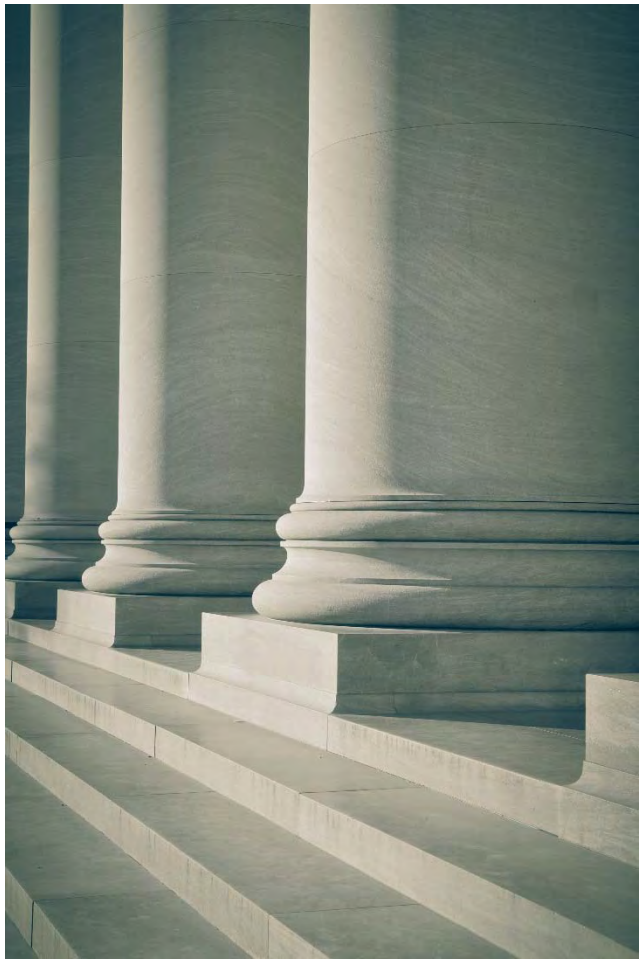
Semantics Analysis Tools

Line-funded research in semantic analysis of malicious code, initiated in FY2012

In FY2014-15, transition automated object oriented analysis and API call behavior identification tools to DoD malware analysts

- Tools operate at 2 orders of magnitude faster than manual analysis

Our Value Proposition



Giving open/unbiased support for the Nation's defense

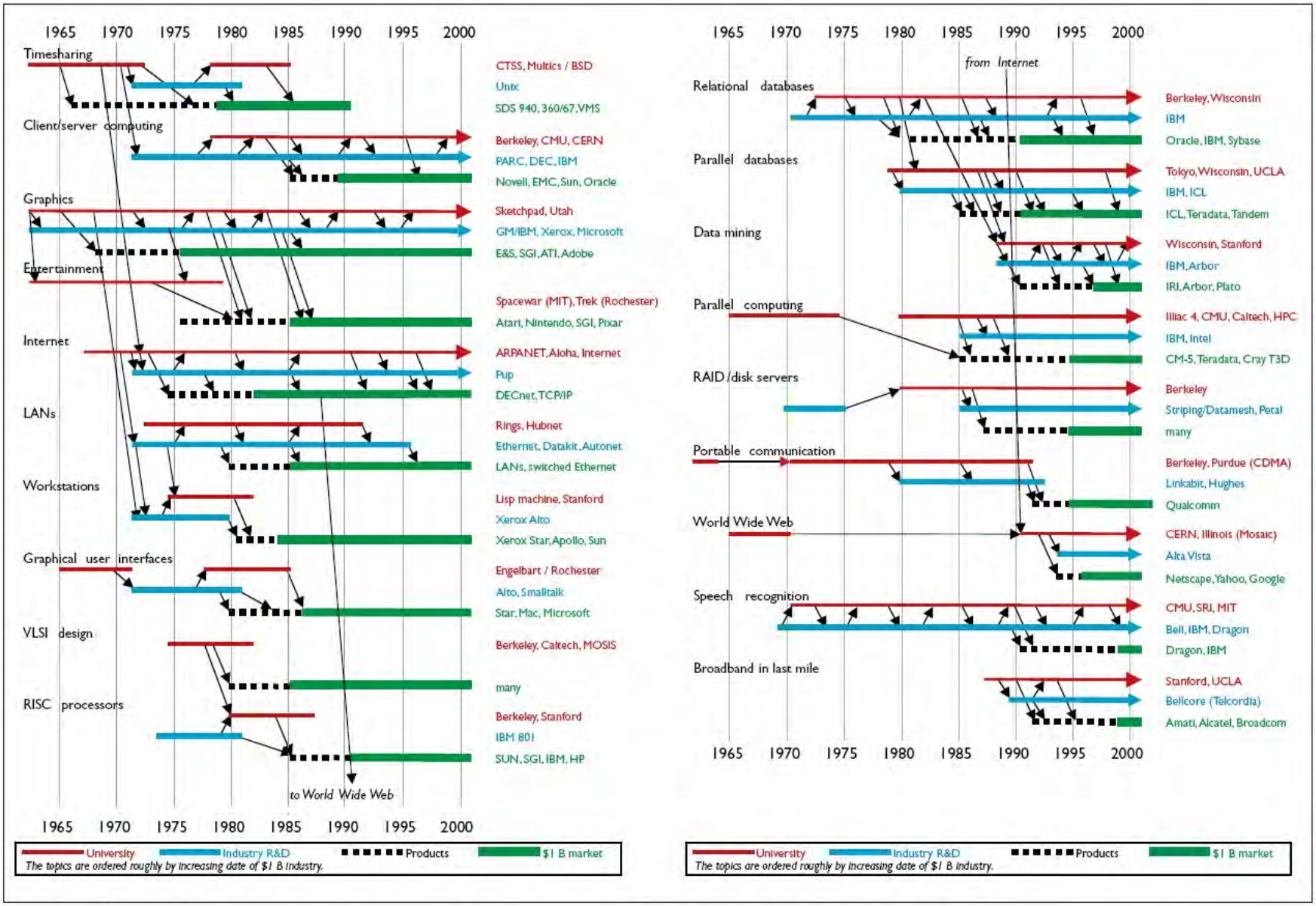
Maintaining technical expertise in our core competencies across the acquisition and software lifecycles

Catalyzing innovation found across industry, academia, and government

Promoting technology transfer to industry

Developing non-competitive relationships with industry

Establishing long-term software/cyber technology awareness



Source: From [6], reprinted with permission from the National Academy of Sciences, courtesy of the National Academies Press, Washington D.C. ©2003.

CH-47F Health Monitoring System Upgrade VI

Issue: Contractor could not assess integration risk early (before integration).

***Action*:** In shadow project, used virtual integration, which identified 20 major issues.

Result: Adjusted CDR Schedule to remediate / avoid failure

- Prevented 12 month delay in a 2-year project
- Current practice would not have identified the issues until 3 months before delivery.

Current practice: *design a system, build components, put the components together, and test to find problems.*

Virtual integration: *Use design and architectural modeling to make sure the components work together and then build components to conform to the model.*

Image: http://www.army.mil/

Android App Testing

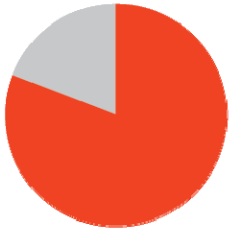
CERT Tapioca is a man-in-the-middle (MITM) proxy that operates on networks rather than applications

Checks for applications that fail to validate SSL certificate chains

Applied to wide-scale testing of Android apps

Tapioca has tested more than 1 million Android apps and identified more than 23,000 certificate-related vulnerabilities

Lifecycle View



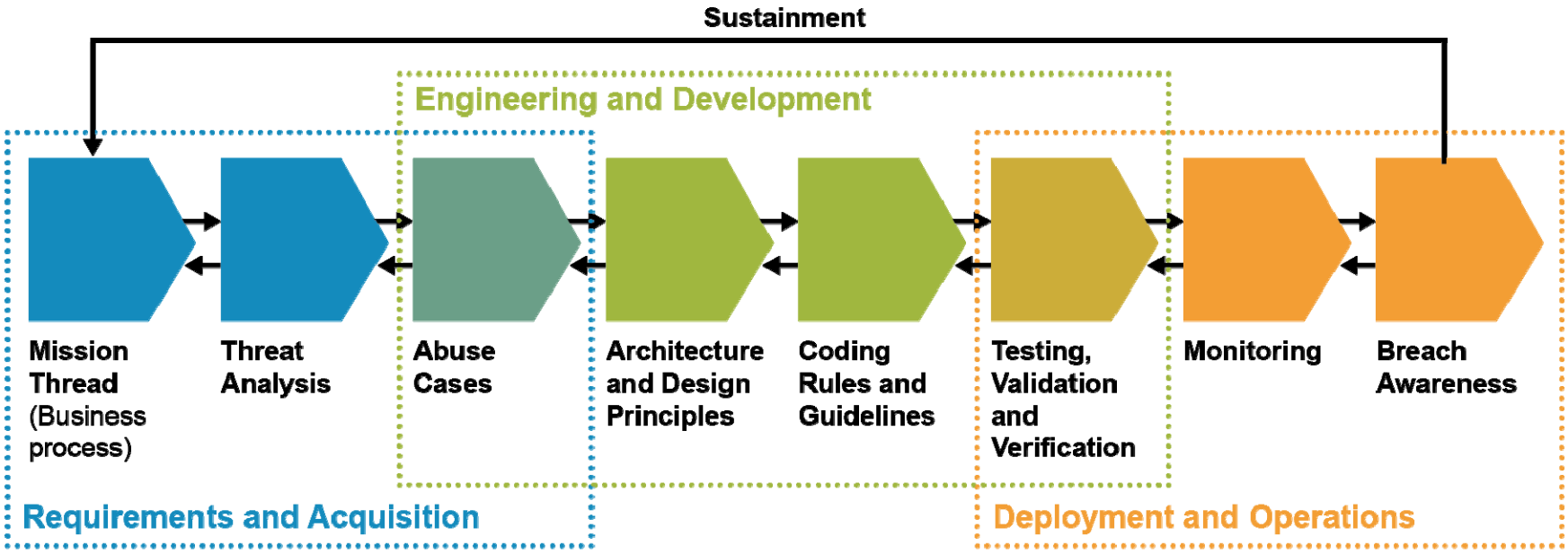
More than **81%** do not coordinate their security practices in various stages of the development life cycle.

19% fail to carry out security requirement definition.

27% do not practice secure design.

30% do not use static analysis or manual code review during development.

47% do not perform acceptance tests for third-party code.

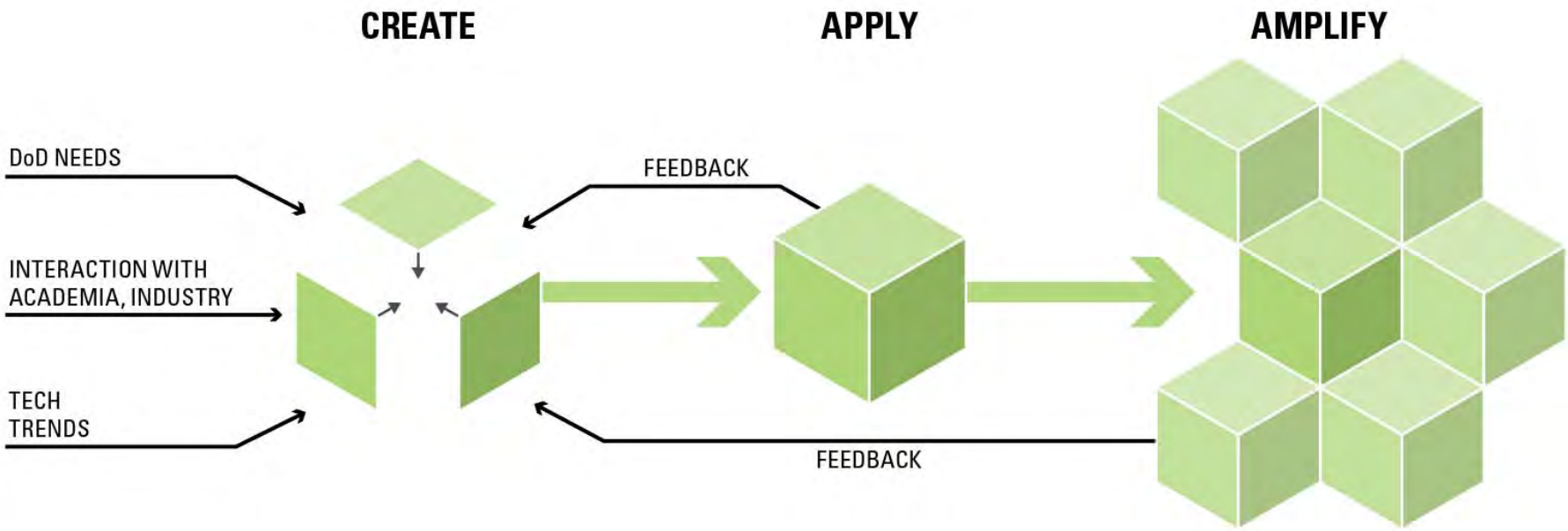


Source: Forrester Consulting, "State of Application Security," January 2011

SEI: Execution Strategy

Deliver across a spectrum from R&D, to prototyping, to adoption by DoD and the Defense Industrial Base

Provide technologies and practices that improve performance across the lifecycle of acquisition through sustainment



Summary

Software delivers the capabilities DoD needs to accomplish its mission goals.

SEI R&D aims to minimize risks associated with software requires attention across the acquisition and software development lifecycles.

Informed by DoD's needs and the technology landscape, SEI is pursuing research falling into two technical areas (TF1/TF2).