# Secure Software Development Lifecycle

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Mark Sherman, PhD
Technical Director, CERT
mssherman@sei.cmu.edu

12-Jun-2014



© 2014 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

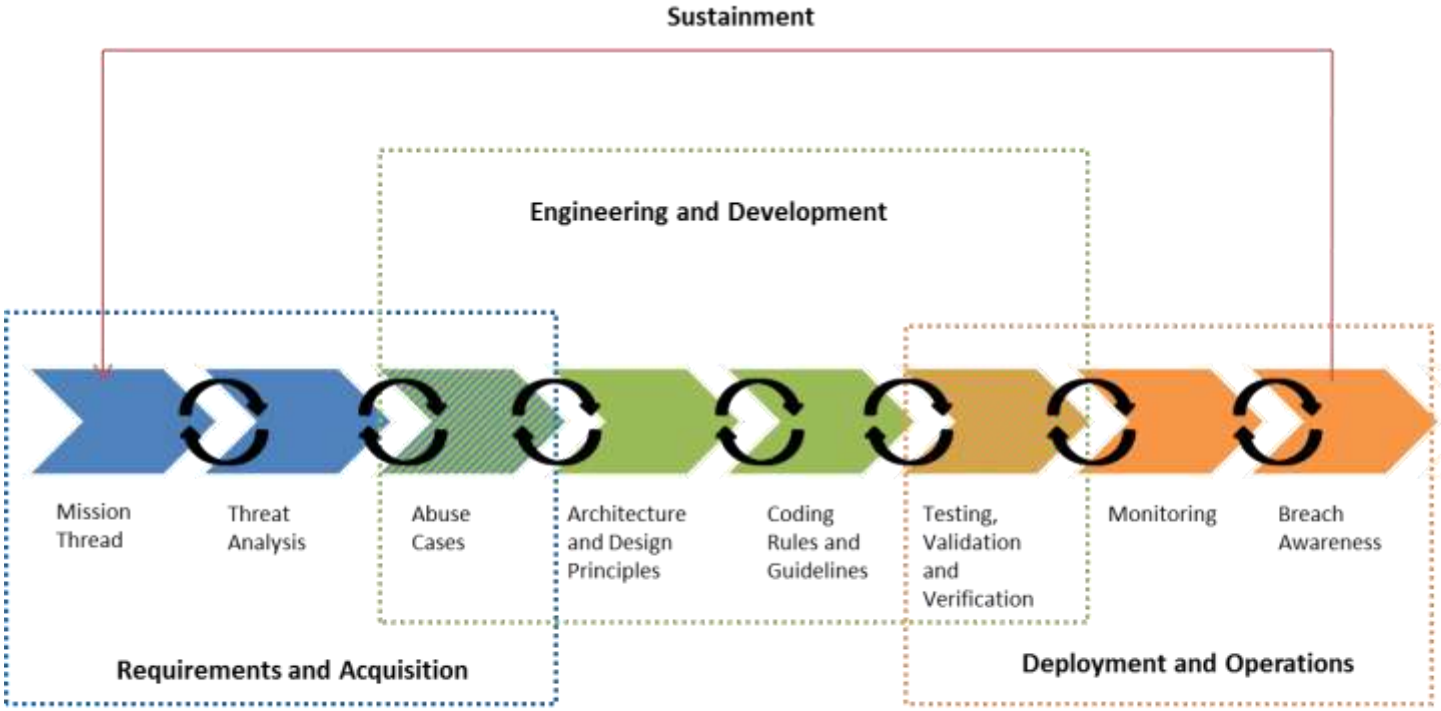
Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

PSP℠ and TSP℠ are service marks of Carnegie Mellon University.

DM23-0178

# Security is a lifecycle issue

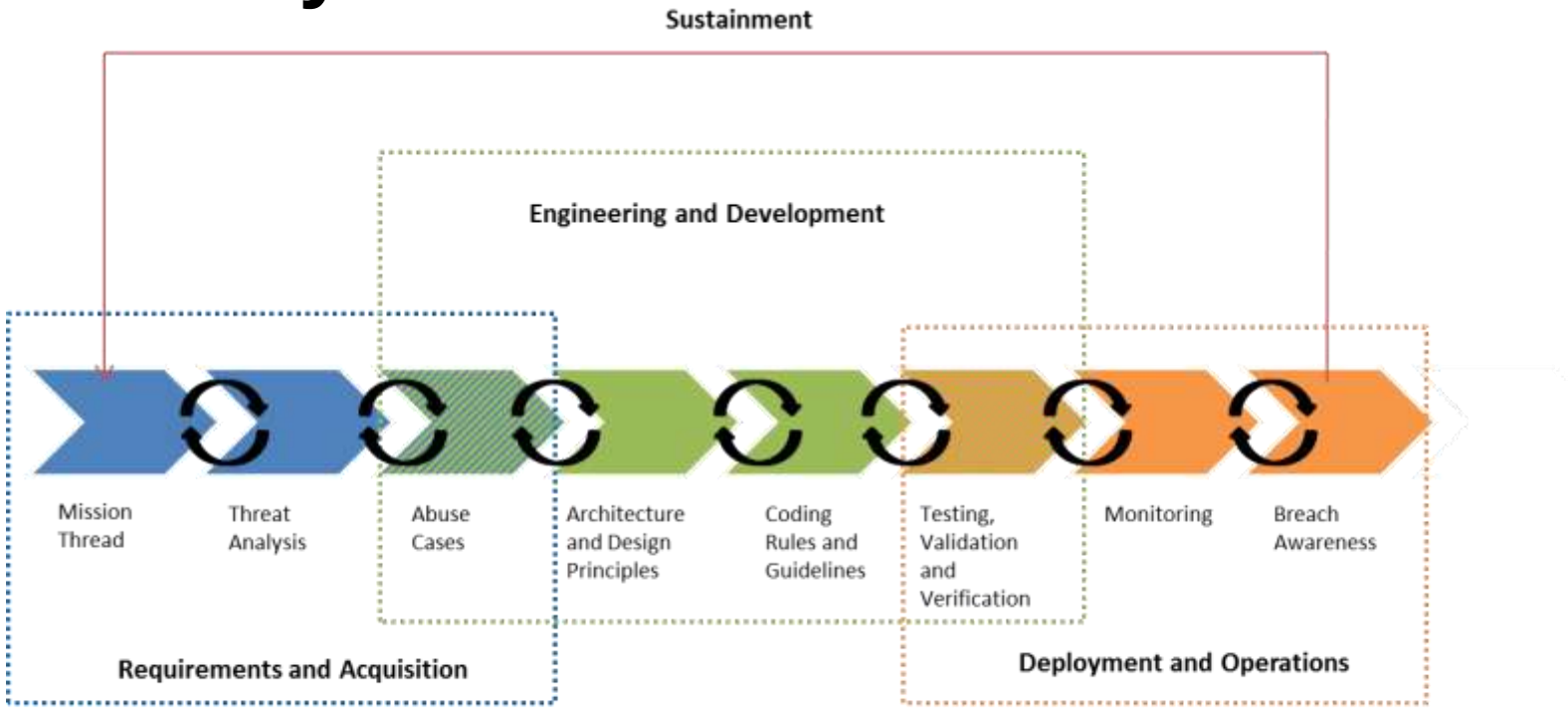
**Focus on the need to develop the theory, processes, practices and technology to support the agile construction and maintenance of secure software**






[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

# Cross lifecycle issues




Automation (devsecops)

Acquisition (Supply chain)

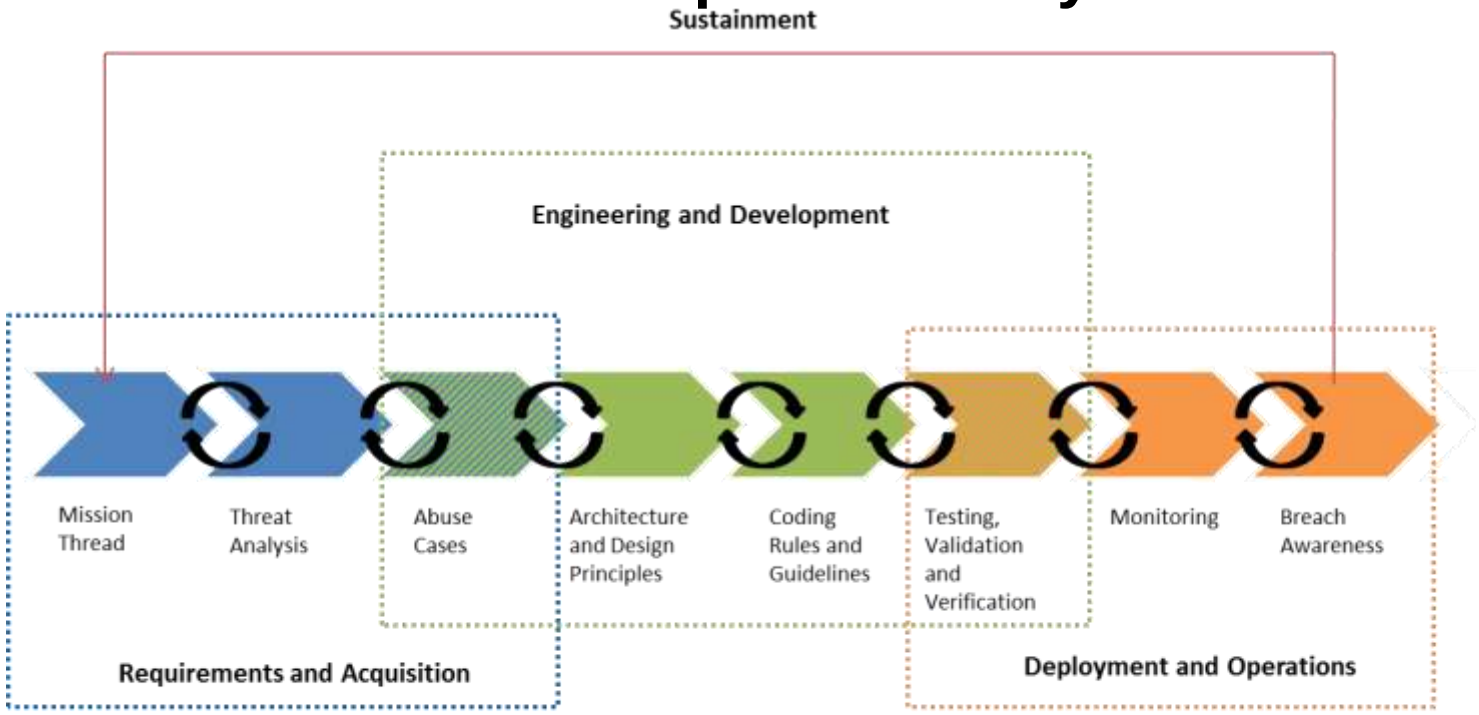
Building skills (Workforce development)

Metrics, Models, and Measurement



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

# Review: theory, processes, practices and technology for Secure Software Development Lifecycle




Automation; Acquisition (Supply chain); Building skills (Workforce development); Metrics, Models, and Measurement

*Software Assurance Framework*

*Mission Risk Diagnostic; Threat Modeling; SQUARE; Security Engineering Risk Analysis*

*Architecture Analysis & Design Language*

*Team Software Process; Secure Agile; Secure Coding; SCALe*

*Run time support; Vulnerability Analysis*

*Forensic Operations & Investigations*



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

# Contact Information


***Mark Sherman***

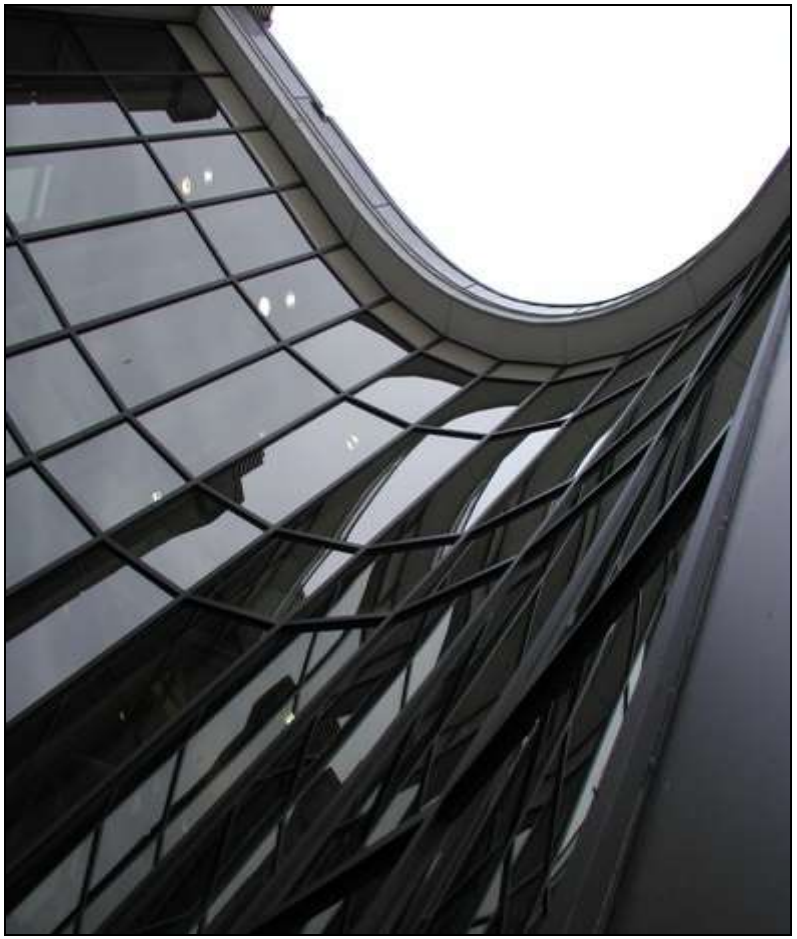
(412) 268-9223

mssherman@sei.cmu.edu


***Web Resources (CERT/SEI)***

http://www.cert.org/

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






[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.