Security Investment Dashboard

Business leaders are becoming more aware of the need to invest in information and software assurance—to meet compliance requirements and optimize their total cost of ownership for software-intensive applications and systems. The Security Investment Decision Dashboard (SIDD) helps business leaders make decisions by evaluating and comparing several candidate security investments using business-based criteria. A foundational principle of the dashboard is that the priorities for candidate investments are driven by the organization's desired outcome for any given investment, not just security investments.

The SIDD defines seven decision criteria categories, each supported by three or more indicators. Categories and indicators are ranked and applied to a series of investments, and individual investment scores are presented for discussion and evaluation. The SIDD is designed so that categories and indicators can be changed, added, and deleted, and the dashboard will continue to present meaningful comparisons.

For more information about our research, visit the CERT website:

www.cert.org

Additional information about these projects is also available at

http://www.cert.org/research/2008research-report.pdf

https://buildsecurityin.us-cert.gov/

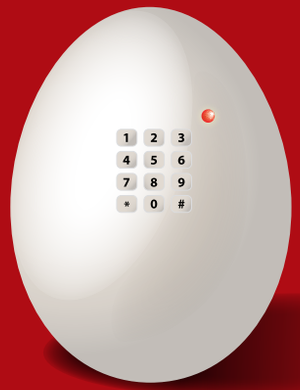
About CERT

CERT engages in cutting-edge research and development and also provides robust training and education programs focused on ensuring that software developers, internet security experts, network and system administrators, and others are able to resist, recognize, and recover from attacks on networked systems.

The CERT® Program is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania.

CERT
Software Engineering Institute
Carnegie Mellon

CERT
Software Engineering Institute
Carnegie Mellon



Addressing Security Early in the System Lifecycle

Laying the Groundwork

CERT has developed a number of techniques aimed at addressing security early in the system lifecycle. This early focus will result in more secure and robust systems, more effective use of development funding, and more predictable security improvements. We have developed three approaches—SQUARE, SoSAF, and the Security Investment Dashboard—that can be used individually or together.

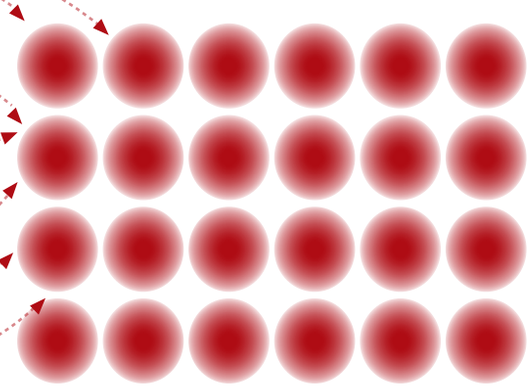
SQUARE

Requirements problems are the primary reason that projects are significantly over budget and past schedule, have significantly reduced scope, deliver poor-quality applications, are little used once delivered, or are cancelled altogether. In particular, system quality requirements, such as security, are often poorly expressed and little analyzed, leading to inappropriate and incomplete system designs and implementations.

The Security Quality Requirements Engineering (SQUARE) project involves identifying and assessing processes and techniques to improve requirements identification, analysis, specification, and management. It also focuses on management issues associated with the development of good security requirements. SQUARE has been field tested in a series of client case studies, and prototype tools have also been developed to support the process. More recently, we have included privacy requirements (P-SQUARE) and developed a version for use in acquisition (A-SQUARE). SQUARE will not only improve the predictability of schedules and costs but will also lead to more secure, survivable systems.

SoSAF

Business processes are often connected and structured to include many organizational units, and technology support is multi-system. However, few analysis techniques support this kind of structure, so organizations cannot identify and address the growing challenges of systems of systems. The System of Systems Assurance Framework (SoSAF), a structured view of people, process, and technology, helps organizations characterize the complexity of multi-system and multi-organizational business processes.

SoSAF provides a structure for organizing information about a business process so that gaps between systems are readily identifiable. It is designed to

- identify potential problems with existing or near-term interoperations among networked components
- highlight the impact on survivability as constrained interoperation moves to more dynamic connectivity
- increase assurance that the business process can survive in the presence of stress and possible failure