Creating a Virtual-First Line of Defense for Secure Software Development

AUTHOR:
MICHAEL BERGMAN

REVIEWED BY:
ROBERT FINDLAY

Creating functioning software is a challenge at the best of times, but ensuring that it is also secure is time consuming, requires fairly scarce skills and, frequently, is not effective. Therefore, a contribution to the topic that sets out to show how this can be achieved more effectively and efficiently, as Michael Bergman's book *Creating a Virtual-First Line of Defense for Secure Software Development: Automating a Software Security Risk Assessment* does, is something to be welcomed.

Based on Bergman's career as a software developer, the book aims to show how the problems of delaying software to ensure that it is secure, including the sheer volume of workload created, can be addressed by virtualizing the second- and first-line functions to semiautomate a software security risk assessment and integrate it into the development process.

The book is divided into three key sections: developing secure software, developing secure code, and measuring and improving, which, in effect, takes the reader through the setup of a framework for secure coding and measuring its success.

Because this is a short-format book, it is impossible for the author to provide comprehensive steps to achieve the goal. Instead, it lays out a theoretical framework with some practical examples interspersed in the text. For example, when the author is detailing how to identify the best automation tool for code reviews, he specifies one of the criteria, identifies the security controls it needs to automate, and gives a few examples of those controls and how they could be assessed.

At this stage, the author is assuming a certain degree of background knowledge. It may be difficult for anyone without a strong knowledge of COBIT®, US National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO) industry literature to get the most from this book, but the author makes that clear at the outset. However, this means the audience for a book of this nature, which lays out a concept based on a large volume of IT control documentation, is limited to experienced auditors or information security specialists or developers. In fact, the author does not explain specifically where the example controls come from, so the reader must already know or research the controls themselves.

However, the references at the back of the book are quite comprehensive with regard to the sources for valid controls and are a good set of documents, but the book would be enhanced with more guidance.

One other caveat is that the very informative section on developing secure code assumes the reader's organization has a data classification policy and has implemented it. Although the book is still interesting if the reader is not in this position, the practical implementation of the knowledge here would be very difficult without this significant piece of work having already been carried out.

It is a very approachable book for those interested in this topic, and its size means it is digestible. The most valuable parts are where good examples are given, such as when the author lays out an example set of baseline controls to secure AWS Amazon Simple Cloud Storage Service and Relational Database Service (RDS).

*Creating a Virtual-First Line of Defense for Secure Software Developmen*t is an interesting read, especially for anyone who has been presented with the problems of securing code before, but it is not a practical how-to guide for implementation; therefore, the more experienced reader will get the most value from it.

ROBERT FINDLAY

Is the global head of IT audit at Irish dairy leader Glanbia. He has more than 30 years of global IT, audit and security experience, including programming, project management and data center operations. He also has significant experience as an IT auditor, chief information security officer and head of IT. Findlay has set up and managed IT audit functions in global businesses such as British Airways, Aer Lingus, ARYZTA, Paddy Power and EY. He has been a presenter at numerous ISACA® and The Institute of Internal Auditors (IIA) conferences in Asia, Europe and North America. Findlay is an *ISACA® Journal* reviewer and a contributor to #IamISACA.