

APPLICATION SECURITY TRAINING PROGRAM



Content

Title Page	p01
Executive Summary	p03
Background	p03
Application Security Training Program	p04
Application Security Course Catalog	p05
Application Security Microdegrees	p08
Thank You	p10




EXECUTIVE SUMMARY

BACKGROUND

Infrared Security, LLC. has for many years worked closely with organizations to build out application security training programs tailored to the organization. Infrared Security has used this experience to build out a formal Application Security Training Program (herein "Program") offering targeting all technical stakeholders within the Software Development Lifecycle (herein "SDLC"), including: Software Engineers, Software Architects, and Software Managers. This Program consists of multiple curriculums that are unique to the roles and responsibilities of the technical stakeholders. Furthermore, this Program allows for the customization of course content to reflect organization specific application security practices. Adoption of such a program would not only facilitate the dissemination of preferred application security practices, but would also cement its managing business unit as an Application Security Center of Excellence.


APPLICATION SECURITY TRAINING PROGRAM

Infrared Security, LLC. offers a formal Application Security Training Program targeting all technical stakeholders within the Software Development Lifecycle. Such technical stakeholders include but are not limited to:




Software Engineers

individuals whose primary responsibility is the software implementation of project specifications.



Software Architects

individuals whose primary responsibility is defining and influencing high level project architectures and corresponding specifications.



Software Managers

individuals whose primary responsibility is overseeing and guiding execution of software development processes.

The Program consists of curriculums that are specific to the roles and responsibilities of the participant. Upon completion of the curriculum(s), the participant shall be awarded a certificate of completion in the form of a microdegree from Infrared Security. Participant may obtain more than one microdegree through the Program. Adoption of such a program would not only facilitate the dissemination of preferred application security practices, but would also cement its managing business unit as an *Application Security Center of Excellence*.



APPLICATION SECURITY COURSE CATALOG

The Program provides a wide variety of training courses specifically designed to suit the needs of the organization's technical stakeholders. This course catalog is organized in a way that is inline with the roles and responsibilities of applicable technical stakeholders. Furthermore, this catalog should allow for growth overtime to accommodate structural and technical changes within the organization.

OWASP TOP TEN FOR DEVELOPERS

Duration: 5 hour(s) of content, approximately 8 hour(s) to complete

Audience: Software Engineers, Software Architects and Software Testers

Overview: Participants of this course will gain a foundational understanding of application security and secure programming practices based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Top Ten document.

OWASP TOP TEN FOR MANAGERS

Duration: 1 hour of content, approximately 1.5 hour(s) to complete

Audience: Software Managers

Overview: Participants of this course will gain a foundational understanding of Application security based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Top Ten document.

DEFENSIVE ENTERPRISE REMEDIATION

Duration: 1 hour of content, approximately 1.5 hour(s) to complete

Audience: Software Engineers, Software Architects and Software Testers

Overview: Participants of this course will gain a foundational understanding of mitigating specific classes of vulnerability with emphasis on the Java and C# programming languages.

THREAT MODELING

Duration: 1 hour of content, approximately 1.5 hour(s) to complete

Audience: Software Architects and Security Engineers

Overview: Participants of this course will gain an understanding of the threat modeling process and how it is used to identify and prioritize threats.

BUILDING SECURE ASP.NET APPLICATIONS

Duration: 1 hour of content, approximately 1.5 hour(s) to complete

Audience: Software Engineers and Software Architects

Overview: Participants of this course will gain a foundational understanding of writing secure software on ASP.NET based platforms.

BUILDING SECURE MOBILE APPLICATIONS

Duration: 1 hour of content, approximately 1.5 hour(s) to complete

Audience: Software Engineers and Software Architects

Overview: Participants of this course will gain a foundational understanding of how to build secure mobile applications targeting the iOS and Android platforms.

BUILDING SECURE JAVA EE APPLICATIONS

Duration: 1 hour of content, approximately 1.5 hour(s) to complete

Audience: Software Engineers and Software Architects

Overview: Participants of this course will gain a foundational understanding of writing secure software on Java Enterprise Edition based platforms.

BUILDING SECURE JAVASCRIPT APPLICATIONS

Duration: 1 hour of content, approximately 1.5 hour(s) to complete

Audience: Software Engineers and Software Architects

Overview: Participants of this course will gain a foundational understanding of writing secure software using JavaScript for both the client and the server.



APPLICATION SECURITY MICRODEGREES

Participants of the Program who complete a curriculum shall be awarded a microdegree from the customer. Microdegree is defined as follows:

A microdegree is a credential focused upon a specified professional or career discipline and typically comprises one or more sources of accelerated educational experiences. microdegrees are considered to be "certificates" requiring a lower level of commitment and rigor than a traditional degree program but serving an important role as a vocational credential.

Wikipedia, <https://en.wikipedia.org/wiki/Microdegree>

The customer's microdegrees shall not only certify the advanced understanding of an area of software security, but they shall also provide its participants with Continuing Education Credits (CEC) that can be applied to industry-recognized certifications

The Program shall initially make the following microdegrees available:

SECURE SOFTWARE ENGINEER

Audience: Software Engineers and Software Architects

Description: Participants of this track will obtain a strong understanding of secure programming patterns and practices tailored specifically for software implementation.

Required Courses	Elective Courses (at least two)
OWASP Top Ten for Developers Defensive Enterprise Remediation	Building Secure JavaEE Applications Building Secure ASP.NET Applications Building Secure Javascript Applications Building Secure Mobile Applications

SECURE SOFTWARE ARCHITECT

Audience: Software Architects

Description: Participants of this track will obtain a strong understanding of secure architectural patterns and practices tailored specifically for software design.

Required Courses	Elective Courses (at least one)
OWASP Top Ten for Developers Defensive Enterprise Remediation Threat Modeling	Building Secure JavaEE Applications Building Secure ASP.NET Applications Building Secure Javascript Applications Building Secure Mobile Applications

SECURE SOFTWARE MANAGER

Audience: Software Managers

Description: Participants of this track will obtain a strong understanding of application security processes tailored specifically to the Software Development Lifecycle.

Required Courses	Elective Courses
OWASP Top Ten for Managers	N/A



THANK YOU

Infrared Security would like to formally thank you for providing us with an opportunity to work more closely with you and your organization. Please do not hesitate to contact us with any questions, comments or concerns. We look forward to working with you to build out this Program.