# MANICODE

SECURE CODING EDUCATION

# MANICODE
## SECURE CODING EDUCATION

# Jim Manico

Jim Manico is the founder of Manicode Security where he trains software developers on secure coding and security engineering. He is also the co-founder of the LocoMoco Security Conference and is a investor/advisor for BitDiscovery and Signal Sciences. Jim is a frequent speaker on secure software practices and is a member of the JavaOne rockstar speaker community. He is the author of *"Iron-Clad Java: Building Secure Web Applications"* from McGraw-Hill. For more information, visit *http://www.linkedin.com/in/jmanico*.

**IRONCLAD DEVLOPMENT: BUILDING SECURE WEB & WEB SERVICE APPLICATIONS** | 2-3 DAYS, HANDS ON
**APPLICATION SECURITY FOR MANAGERS** | 1 DAY, LECTURE
**APPLICATION SECURITY FOR USER INTERFACE DEVELOPERS & DESIGNERS** | 1 DAY, LECTURE

"Jim is a high energy talented programmer. I worked with him on a number of complex coding projects and he did show great skill in organizing and implementing these projects. He does understand the concepts of web development very well, in particular the need for and implementation of security measures. In addition, Jim communicates well and is a great team player."

**JOHANNES ULLRICH**

"Jim is extremely charismatic, energetic and highly technical. He has unparalleled skill in developing J2EE applications, which are both robust and secure. His knowledge of application security and security architecture is phenomenal, and he is leading a vigorous campaign to change the J2EE spec to make it more secure. I recommend Jim for any development, security or training project."

**JERRY HOFF**

"Jim taught one of the more recent security classes, and having observed many classes in action I can honestly say he really stood out as an instructor. He very successfully engaged the diverse demographics in the class and convinced all of them why the security issues pertained to their immediate job, and were the concerns of all information employees."

**JOSH BROWN**

# IRONCLAD DEVELOPMENT: BUILDING SECURE WEB & WEB SERVICE APPLICATIONS

**Instructor:** Jim Manico

**Course Length:** 2 Days, Hands On

**Skill Level:** Intermediate

**Student Requirements:** Familiarity with the technical details of building web applications and web services from a software engineering point of view.

**Laptop Requirements:** Any laptop that can run a web browser and updated client-side JVM.

Jim's secure coding training classes are designed to benefit any web developer, architect, security professional or other software development professional who needs to build and maintain secure web and web service software. Classes taught by Jim Manico are custom built from the following learning modules.  (Please note times are approximate.)

## USER INTERFACE SECURITY

| | |
|---|---|
| XSS Defense | 2 hr |
| *Client side web security* | |
| Content Security Policy | 1 hr |
| *Advanced Client side web security* | |
| Content Spoofing and HTML Hacking | .5 hr |
| *HTML based client-side injection attacks* | |
| Angular and AngularJS Security | .5 hr |
| *Coding Angular applications securely* | |
| React Security | .5 hr |
| *Coding React applications securely* | |
| Vue.js Security | .5 hr |
| *Coding Vue.js applications securely* | |

## IDENTITY & ACCESS MANAGEMENT

| | |
|---|---|
| Authentication Best Practices | 1 hr |
| *Best practices of web authentication* | |
| Session Management Best Practices | 1 hr |
| *Best practices of web session management* | |
| Secure Password Storage | 1 hr |
| *How to store user passwords for authentication securely* | |
| Access Control Design | 1 hr |
| *How to design modern multi-tenant access control* | |
| OAuth Security | 2 hr |
| *Introduction to the OAuth authorization protocol* | |
| OpenID Connect Security | 1 hr |
| *Introduction to the OpenID connect federation protocol* | |

## PROCESS

| | |
|---|---|
| Secure SDLC and AppSec Management | 1hr |
| *Processes around building secure software* | |
| DevOps Best Practices | 1hr |
| *Introduction to DevOps and DevSecOps with a CD/CI focus* | |

## CORE MODULES

| | |
|---|---|
| Introduction to Application Security | .5 hr |
| *Broad Introduction to Application Security* | |
| Introduction to Security Goals and Threats | .5 hr |
| *Application Security Terminology Definitions* | |
| HTTP Security Basics | 1.5 hr |
| *HTTP Response/Request Headers, Verbs, Secure Transport Basics* | |
| CORS and HTML5 Considerations | 1 hr |
| *LocalStorage, HTML5 Sinks, CORS* | |
| API and REST Security | 1 hr |
| *REST Design, XML, XXE, JSON, API Access Control* | |
| Microservice Security | 1 hr |
| *Microservice Security Architectures* | |
| JSON Web Tokens | .5 hr |
| *JWT Security Challenges* | |
| SQL and other Injection | 1.5 hr |
| *Parameterization, Database Config, Command/LDAP Injection* | |
| Cross Site Request Forgery | 1.5 hr |
| *CSRF Defenses for multiple architecture types (stateless, API, etc)* | |
| File Upload and File IO Security | 1 hr |
| *Multi-Step Secure File Upload Defense, File I/O Security Basics* | |
| Deserialization Security | .5 hr |
| *Safe Deserialization Strategies* | |
| Input Validation Basics | .5 hr |
| *Whitelist Validation, Safe Redirects* | |

## CRYPTO MODULES

| | |
|---|---|
| Cryptography Fundamentals | 2 hr |
| *Introduction to applied cryptography* | |
| HTTPS/TLS Best Practices | 1 hr |
| *Introduction to transport security* | |

## STANDARDS

| | |
|---|---|
| OWASP Top Ten 2017 | 1 hr |
| *Top Ten Web Security Risks* | |
| OWASP ASVS 4.0 | 1 hr |
| *Comprehensive Secure Coding Standard* | |
| GDPR | 1 hr |
| *European Data Privacy Law* | |

## ADDITIONAL TOPICS

| | |
|---|---|
| 3rd Party Library Security Management | .5 hr |
| *How to detect and manage insecure 3rd party libraries* | |
| Application Layer Intrusion Detection | .5 hr |
| *How to help detect application layer attacks* | |
| Web/Webservice Threat Modeling | 1 hr |
| *Introduction to Threat Modeling (Security Design)* | |
| Multi-Form Workflow Security | .5 hr |
| *How to handle complex form workflows securely* | |
| Java 8/9/10/11 Security Controls | 1 hr |
| *Advances in Java Security* | |
| Introduction to Cloud Security | 1 hr |
| *Introduction to AWS, Docker and Kubernetes* | |
| Competitive Hacking LABS | 4 hr |
| *Hands on Labs!* | |

# APPLICATION SECURITY FOR MANAGERS



**Instructor:** Jim Manico

**Course Length:** 1 Day, Lecture

**Skill Level:** Intermediate

**Course Goals:**
- Understand the various stages of a secure SDLC
- Understand the types of attacks specific to application security
- Prepare managers to build contracts and procure software with application security considerations
- Build a business case for application security investment

**Student Requirements:** Experienced software engineering managers or other software development leaders will benefit most from this class.

**Laptop Requirements:** Need only to take notes.

Application security excellence requires a wide range of management involvement and activity. From managing procurement, contracts, software development activities and more, application security management touches many aspects of business operations.

Managers need a solid understanding of both the technical and business justifications for these activities in order to be successful.

This one day course will prepare managers to take on a wide variety of challenges in order to successfully guide your organization towards application security excellence.

Classes are custom built from the following learning modules. (Please note times are approximate.)

### APPLICATION SECURITY MANAGEMENT TRAINING MODULES

| | |
|---|---|
| Secure SDLC and AppSec Management | 2 hr |
| Introduction to Threat Modeling | 1 hr |
| OWASP Top Ten 2017 | 1 hr |
| OWASP ASVS 3.1 | 1 hr |
| 3rd Party Library Security Management | .5 hr |
| Legal and Contract Issues | .5 hr |
| DevOps Best Practices | 1 hr |
| GDPR, PCI and other Compliance Issues | 1 hr |

# APPLICATION SECURITY FOR USER INTERFACE DEVELOPERS & DESIGNERS

**Instructor:** Jim Manico

**Course Length:** 1 Day, Lecture

**Skill Level:** Beginner

**Student Requirements:** Familiarity with the technical details of designing and building the user interface portion of web applications (HTML/CSS and some JavaScript).

**Laptop Requirements:** Any laptop that can run a web browser and updated client-side JVM.

This class is designed to teach web based designers how to build secure user interfaces. This class is primarily for the UI software engineer but any web developer, architect, security professional or other software development professional who needs to build and maintain secure web user interfaces will benefit.

We'll cover the many defensive strategies needed to defeat Cross Site Scripting. We'll also take a close look at building modern Content Security Policies as well as explore defending modern JS frameworks such as React and Angular.

Classes are custom built from the following learning modules.  (Please note times are approximate.)

## USER INTERFACE SECURITY TRAINING MODULES

| | |
|---|---|
| Content Spoofing and HTML Hacking | 1 hr |
| XSS Defense | 2 hr |
| Content Security Policy | 1 hr |
| Angular.JS Security | 1 hr |
| React.JS Security | 1 hr |
| XSS Labs | 2 hr |

# philippe de Ryck

Dr. Philippe De Ryck helps developers protect companies through better web security. As the founder of Pragmatic Web Security, he travels the world to train developers on web security and security engineering. His Ph.D. in web security from KU Leuven lies at the basis of his exceptional knowledge of the security landscape. Philippe is a Google Developer Expert and an Auth0 Ambassador/Expert for his community contributions on securing web applications and APIs.

## PRAGMATIC WEB SECURITY | 1-3 DAYS, HANDS ON

"The Advanced Application Security training was amazing! I would definitely take any class taught by Philippe again. He was the best instructor I've ever had (including a $5000 CISSP boot camp led by ISC2).

All the topics were extremely relevant, educational, and the hands-on labs were beneficial to put all the material we covered in class to practice. Excellent work!!"

**SOFTWARE ENGINEER
FORTUNE 500 COMPANY**

"Mastering OAuth2 and OpenID Connect was one of the best courses I attended. Philippe is a great instructor. He has the gift of explaining complex topics in a very understandable and structured way. The presentations were perfectly prepared.

I can recommend this course to anyone who is professionally involved with this topic. I am looking forward to the next course from Philippe. Great work. Thank you very much."

**JOCHEN HAMMANN
TECHNICAL LEAD, SERVICETRACE**

"Dr. Philippe De Ryck is a stellar secure coding instructor. He brings an immense body of web security knowledge to the classroom when teaching his various class offerings. His style is both focused yet inviting which encourages students to participate in class.

It's rare to find professionals who have both the technical ability and presentation skills it takes to be a successful instructor-led-trainer.

Dr. Philippe De Ryck has both and more in spades!"

**JIM MANICO
FOUNDER, MANICODE SECURITY**

# MASTERING OAUTH 2.0 AND OPENID CONNECT

**Instructor:** Dr. Philippe De Ryck

**Course Length:** 1-2 Days

**Skill Level:** Advanced

**Student Requirements:** Familiarity with engineering modern API-based applications

**Laptop Requirements:** Any device with a browser

OAuth 2.0 and OpenID Connect (OIDC) are crucial for securing web applications, mobile applications, APIs, and microservices. Unfortunately, getting a good grip on the purpose and use cases for these technologies is insanely difficult. As a result, many implementations use incorrect configurations or contain security vulnerabilities.

This course takes you on a step-by-step journey into the latest best practices in the world of OAuth 2.0, OAuth 2.1, and OpenID Connect. This course helps students understand the problems OAuth 2.0 and OpenID Connect solve, and how to use these technologies to address concrete application security requirements. Throughout the course, we discuss the various design and implementation decisions you will face, along with their trade-offs and current recommendations

This course is the product of hundreds of hours spent advising architects and developers on integrating, implementing, and securing OAuth 2.0 and OpenID Connect. After taking this course, students will be able to analyze their systems for potential weaknesses and apply the latest best practices.

The course format is a mixture of lectures, use case analysis, live demos, and interactive quizzes. All demos rely on real-world scenarios and OAuth 2.0/OIDC implementations.

## CONTENT

| | |
|---|---|
| Introduction to OAuth 2.0 and OIDC | 3 hr |
| *Overview of the technologies, security challenges and current best practices* | |
| User Authentication with OpenID Connect | 2 hr |
| *Designing and building a (federated) identity system* | |
| Using OAuth 2.0 and OIDC in Single Page Applications | 1 hr |
| *Recent changes in flow recommendations for frontend web applications* | |
| Securing Tokens in Single Page Applications | 1 hr |
| *Security patterns to enhance token security in the browser* | |
| Using Scopes, Roles, and Permissions | 1.5 hr |
| *Pitfalls and recommendations on handling authorization with OAuth 2.0* | |
| Securing APIs with OAuth 2.0 | 1.5 hr |
| *Practical guidelines on making API security decisions with access tokens* | |
| Hardening an OAuth 2.0 and OIDC Architecture | 2 hr |
| *Advanced architectural patterns to improve security* | |
| Advanced Attacks Against OAuth 2.0 and OpenID Connect | 2 hr |
| *Analysis of advanced attack scenarios and recommended mitigations* | |

# SECURING REACT APPLICATIONS



**Instructor:** Dr. Philippe De Ryck

**Course Length:** 1-3 Days

**Skill Level:** Intermediate-Expert

**Student Requirements:** Familiarity with engineering modern React-based applications backed by APIs

**Laptop Requirements:** Any computer with a browser



React applications disrupt the traditional web security landscape, and finding reliable security advice is hard. This course provides React developers with the answers to all their security questions.

With a mix of lectures, demos, quizzes, and hands-on labs, participants discover best practices for building secure React applications. We investigate how to use and configure security mechanisms available in modern browsers. We explore how React handles security, along with common mistakes that circumvent these protections. Additionally, we discuss scenarios that address common questions, including secure data storage in the browser and the use of OAuth 2.0 and OpenID Connect.

This course offers practical and immediately applicable security advice for React architects and developers. Throughout the course, Philippe is available to answer any questions, including concrete scenarios applying to your own applications.

The course consists of a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing participants to gain hands-on experience with offensive and defensive technologies..

## CONTENT

| | |
|---|---|
| The Security Model of React Applications | 1 hr |
| *Understanding the power and limitations of React security* | |
| Essential XSS Attacks and Defenses in React | 1.5 hr |
| *Secure coding techniques to avoid pitfalls with React's XSS defenses* | |
| Mitigating Advanced XSS Attacks in React Applications | 1.5 hr |
| *Finding and fixing advanced XSS problems in React applications* | |
| Defending React Applications with Content Security Policy | 1.5 hr |
| *Concrete guidelines on using CSP in React applications* | |
| Content Security Policy Beyond XSS | 1hr |
| *Use cases for CSP as an effective defense-in-depth mechanism* | |
| Securing Isomorphic and Server-side Rendered React | 1 hr |
| *Overview of security concerns with server-side rendering* | |
| Securing Tokens in Single Page Applications | 1 hr |
| *Security patterns to enhance token security in the browser* | |
| OAuth 2.0 and OpenID Connect Best Practices for SPAs | 1.5 hr |
| *Overview of the technologies, security challenges and current best practices* | |
| Circumventing OAuth 2.0 security | 1 hr |
| *Identifying and abusing weaknesses in the OAuth 2.0 security model for SPAs* | |
| Securing OAuth 2.0 with the Backend-For-Frontend Pattern | 1 hr |
| *In-depth look at securing OAuth 2.0 with the BFF pattern* | |
| Offensive and Defense Hands-on Labs | 4 hr |
| *Guided labs exploiting and solving application vulnerabilities* | |

# SECURING ANGULAR APPLICATIONS

**Instructor:** Dr. Philippe De Ryck

**Course Length:** 1-3 Days

**Skill Level:** Intermediate-Expert

**Student Requirements:** Familiarity with engineering modern Angular-based applications backed by APIs

**Laptop Requirements:** Any computer with a browser

Angular applications disrupt the traditional web security landscape, and finding reliable security advice is hard. This course provides Angular developers with the answers to all their security questions.

With a mix of lectures, demos, quizzes, and hands-on labs, participants discover best practices for building secure Angular applications. We investigate how to use and configure security mechanisms available in modern browsers. We explore how Angular handles security out-of-the-box, along with common mistakes that circumvent these protections. Additionally, we discuss scenarios that address common questions, including secure data storage in the browser and the use of OAuth 2.0 and OpenID Connect.

This course offers practical and immediately applicable security advice for Angular architects and developers. Throughout the course, Philippe is available to answer any questions, including concrete scenarios applying to your own applications.

The course consists of a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing participants to gain hands-on experience with offensive and defensive technologies.

## CONTENT

| | |
|---|---|
| The Security Model of Angular Applications | 1 hr |
| *Understanding the power and limitations of Angular security* | |
| Essential XSS Attacks and Defenses in Angular | 1 hr |
| *Secure coding techniques to leverage Angular's built-in defenses* | |
| Advanced XSS Attacks and Defenses | 1 hr |
| *Avoiding XSS pitfalls in Angular and using Trusted Types as a defense* | |
| Defending Angular applications with Content Security Policy | 1.5 hr |
| *Concrete guidelines on using CSP in Angular applications* | |
| Content Security Policy beyond XSS | 1 hr |
| *Use cases for CSP as a effective defense-in-depth mechanism* | |
| Securing Server-side Rendered Angular Pages | .5 hr |
| *Overview of security concerns with server-side rendering* | |
| Securing Tokens in Single Page Applications | 1 hr |
| *Security patterns to enhance token security in the browser* | |
| OAuth 2.0 and OpenID Connect Best Practices for SPAs | 1.5 hr |
| *Overview of the technologies, security challenges and current best practices* | |
| Circumventing OAuth 2.0 security | 1 hr |
| *Identifying and abusing weaknesses in the OAuth 2.0 security model for SPAs* | |
| Securing OAuth 2.0 with the Backend-for-Frontend Pattern | 1 hr |
| *In-depth look at securing OAuth 2.0 with the BFF pattern* | |
| Offensive and Defense Hands-on Labs | 4 hr |
| *Guided labs exploiting and solving application vulnerabilities* | |

# WEB APPLICATION SECURITY FUNDAMENTALS

**Instructor:** Dr. Philippe De Ryck

**Course Length:** 1-2 Days + Hands-on Labs

**Skill Level:** Beginner-Intermediate

**Student Requirements:** Familiarity with basic engineering concepts of web applications (HTTP, HTML, . . . )

**Laptop Requirements:** Any computer with a browser

Building secure web applications requires developer knowledge on security pitfalls and secure coding guidelines. This course provides developers with practical hands-on knowledge to build more secure web applications.

Academic-level security lectures ensure that developers grasp the causes of vulnerabilities and understand how mitigations work. Rather than providing developers with textbook solutions, this course empowers them to analyze the problem and apply the proper mitigation strategy.

During the hands-on lab sessions, developers are challenged to process and apply the learned concepts. In a custom-built competitive lab environment, developers need to solve offensive and defensive challenges against training applications. Doing so helps them understand the mechanics of both attacks and defenses. Hands-on labs are critical to ensure optimal retention of the security material.

At the end of this course, students are guaranteed to be able to find and fix vulnerabilities in their applications. They will have developed a security mindset and will have obtained an invaluable amount of practical security knowledge.

Various companies use this course as the starting point for their AppSec program. While many students are junior developers being introduced to secure coding, even senior developers have indicated that they have learned a ton of new information. In a nutshell, this course is a must-follow for every web developer in your organization.

The course format is a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing students to gain hands-on experience with offensive and defensive technologies.

## CONTENT

| | |
|---|---|
| The Security Model of the Web | 1 hr |
| *Foundational security principles for web applications* | |
| Security Fundamentals for HTTP Applications | 1 hr |
| *Common mistakes and best practices for securing web applications* | |
| Preventing Server-side Injection Vulnerabilities | 1 hr |
| *Deep-dive into injection vulnerabilities (SQLi, command injection, . . . )* | |
| Configuring Modern Security Headers | 1 hr |
| *Overview of security headers, their configuration, and their effect* | |
| Best Practices for End-user Authentication | 1 hr |
| *Common authentication pitfalls and modern best practices* | |
| Secure Password Storage | 1 hr |
| *Concrete guidelines for securely handling password-based secrets* | |
| Modern Multi-factor Authentication | 1 hr |
| *Modern MFA mechanisms, their security properties, and trade-offs* | |
| Best Practices for Session Security | 1 hr |
| *Defending against common threats, such as session hijacking and session fixation* | |
| The Impact of HTTPS on an Application | 1 hr |
| *Achieving 100% HTTPS deployments in modern browsers* | |
| The Modern TLS Certificate Ecosystem | 1.5 hr |
| *Modern certificate security techniques, such as transparency and key pinning* | |
| Essential XSS Attacks and Defenses | 1 hr |
| *Secure coding techniques to avoid introducing XSS vulnerabilities* | |
| Mitigating Advanced XSS Attacks | 1 hr |
| *Finding and fixing advanced XSS problems* | |
| Preventing XSS with Content Security Policy | 1 hr |
| *Concrete guidelines on using CSP as a second line of defense against XSS* | |
| Content Security Policy Beyond XSS | 1 hr |
| *Use cases for CSP as an effective defense-in-depth mechanism* | |
| Offensive and Defense Hands-on Labs | 8 hr |
| *Guided labs exploiting and solving application vulnerabilities* | |

# SECURING MODERN REST APIS IN NODEJS / SPRING BOOT

**Instructor:** Dr. Philippe De Ryck

**Course Length:** 1-2 Days + Hands-onLabs

**Skill Level:** Intermediate–Advanced

**Student Requirements:** Familiarity with building REST APIs and JSON-based APIs

**Laptop  Requirements:**  Any computer with a browser

API security is more important than ever, as illustrated by a dedicated OWASP top 10 for common API security vulnerabilities. This course provides API developers with the necessary knowledge to avoid these common vulnerabilities, but also goes a lot further than that.

The academic-level lectures in this course ensure students fully grasp the cause and consequences of each attack. The lectures also explain various mitigation strategies, along with potential trade-offs and best practices.

Unique hands-on lab sessions allow students to gain practical experience with attacks and defenses. A custom-built lab environment guides students as they solve challenges related to the course contents, all in a friendly competitive atmosphere.

At the end of this course, students will be able to assess their APIs' security and identify potential security vulnerabilities. Additionally, students will be able to make informed decisions about proper countermeasures and their impact on the system.

This course is the perfect follow-up for the "Web application security fundamentals" course. This course is available in a NodeJS Express version, and in a Java Spring Boot version.

The course format is a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing students to gain hands-on experience with offensive and defensive technologies..

## CONTENT

| | |
|---|---|
| API Authentication Techniques | 1 hr |
| *Strategies for secure user and service authentication* | |
| Enforcing API Authorization | 1 hr |
| *Designing and implementing robust authorization policies* | |
| REST APIs, Sessions and Security | 1 hr |
| *In-depth look at challenges with managing authentication state* | |
| Understanding Cross-Origin Resource Sharing | 1 hr |
| *Practical guidelines for deploying a secure CORS policy* | |
| Using JSON Web Tokens for Security | 1 hr |
| *Security challenges and patterns of using signed/encrypted JWTs* | |
| Configuring Modern Security Headers for APIs | 1 hr |
| *Overview of security headers, their configuration, and their effect on APIs* | |
| Preventing API Injection Vulnerabilities | 1 hr |
| *Deep-dive into API injection vulnerabilities (SQLi, JSON, . . . )* | |
| Advanced API Injection Attacks | 1 hr |
| *Defending against modern attacks, such as Server-Side Request Forgery (SSRF)* | |
| Introduction to OAuth 2.0 and OIDC | 2 hr |
| *Overview of the technologies, security challenges and current best practices* | |
| Using Scopes, Roles, and Permissions in OAuth 2.0 | 1.5 hr |
| *Pitfalls and recommendations on handling authorization with OAuth 2.0* | |
| Securing APIs with OAuth 2.0 | 1.5 hr |
| *Practical guidelines on making API security decisions with access tokens* | |
| Offensive and Defense Hands-on Labs | 4 hr |
| *Guided labs exploiting and solving application vulnerabilities* | |

# Jimmy Mesta

Jimmy Mesta is an application security leader that has been involved in Information Security for nearly 10 years. He is the chapter leader of OWASP Santa Barbara and co-organizer of the AppSec California security conference. Jimmy has spent time on both the offense and defense side of the industry and is constantly working towards building modern, developer-friendly security solutions. Jimmy's core focus has been in application and cloud security with an emphasis on secure architecture, automated testing, developer training and defensive techniques.

**KUBERNETES SECURITY TRAINING OUTLINE** | 1 OR 2 DAYS
**DEVOPS PIPELINE TRAINING OUTLINE** | HALF-DAY
**INTRODUCTION TO CLOUD SECURITY: AZURE OR AWS** | 1 DAY

"As Redspin's most senior and experienced web app pentester, Jimmy was frequently called on to break apps of all shapes and sizes, and as one of the most articulate members of the team, Jimmy always did a great job explaining specific findings and recommendations to clients."

**ERIC ROGERS**

"Over the nearly-three years that I had the pleasure of working with Jimmy, his positive attitude and technical skills constantly impressed me. As he grew professionally and moved up in our organization, his great attitude and ability to acquire new and relevant skills were a constant inspiration to his team."

**DAVID SHAW**

# KUBERNETES SECURITY TRAINING OUTLINE

**Instructor:** Jimmy Mesta

**Course Length:** 1 or 2 Days

**Skill Level:** Intermediate

**Laptop Requirements:** Modern Web Browser and a steady internet connection

The Cloud as we know it is changing. Containers have taken the center stage as the preferred method of developing and deploying software into production. As security practitioners, we must adapt to the latest technologies or be left in the dust. This course will focus on the ins and outs of building a modern cloud infrastructure capable of taking containers from a developer's laptop to production, in a secure manner. This course will help attendees of all backgrounds gain a practical understanding of containers as well as Kubernetes and help teams responsible for Kubernetes make sane security decisions when moving towards container-based deployments.

Some of the principals and techniques covered in this course will include:

DevSecOps Overview and Intro to Modern Infrastructure Security Topics

Introduction to Containers

Hardening Containers end-to-end

Introduction to Kubernetes Components and Core Concepts

Kubernetes Attack Surface

Kubernetes Network Policies

Securing a Cluster Using a Service Mesh

Role-Based Access Control (RBAC)

Storing Secrets in Kubernetes

Building DevSecOps Pipelines in Kubernetes

Data Security and Encryption

Logging, Monitoring and Alerting

Hands-on Kubernetes Attack and Defense Live Demonstration

*Heavier on container security if needed (Half-day focus)*

# DEVOPS PIPELINE TRAINING OUTLINE

**Instructor:** Jimmy Mesta

**Course Length:** Half-Day

**Skill Level:** Intermediate

Pipelines are an integral piece in moving towards DevOps workflows but can present challenges for security teams in both defending pipelines from attacks as well as utilizing pipelines to secure applications and infrastructure. This course will dive into both sides of the equation. We will clear up common terminology used in modern pipeline infrastructure and then explore ways to make use of pipelines to discover vulnerabilities early and often. Then, we will threat model modern pipeline implementations and learn how to harden the pipeline itself from developer laptop to production.

Some of the principals and techniques covered in this course will include:

CI/CD Overview

Lab Setup

Artifact Management and Supply Chain Security

Production Security Considerations

Auditing Pipelines

# INTRODUCTION TO CLOUD SECURITY: AZURE OR AWS

**Instructor:** Jimmy Mesta

**Course Length:** 1 Day

**Skill Level:** Intermediate

**Laptop Requirements:** Modern Web Browser and a steady internet connection

The cloud is here to stay. As development and software delivery moves rapidly towards cloud infrastructure it is imperative we are equipped to address the challenges of security and compliance. Learn common cloud terminology and how to navigate the vast array of security controls that need to be considered when moving to a cloud provider. By the end of this class, you should understand how to address the common security challenges presented when running your software in cloud infrastructure.

Some of the principals and techniques covered in this course will include:

Introduction to Cloud Security:
How the Cloud is Changing the Software Security Landscape

Infrastructure Security: Building a Secure Cloud-Native Infrastructure

Lab: Setup

Lab: Security Testing in CI/CD Pipelines

Data Security in the Cloud:
Demystifying Keys, Secrets, and Encryption in the Cloud

Lab: Data Storage

Serverless and Container Security:
Securing Modern Software Deployment and Delivery Mechanisms

Lab: Container and Kubernetes Security

Monitoring and Alerting:
Logging and Anomaly Detection in Modern Cloud Environments

Q&A

# Avi Douglen

AviD is a security architect and software developer, and has been involved in building secure products for close to 20 years. His research interests include efficient security engineering, usable security, and scaling enterprise security systems. As CEO of Bounce Security in Israel, Avi consults on software security to development teams of all sizes, and teaches them how to integrate security practices into their process. He is on the OWASP Board of Directors, a leader of the OWASP Israel chapter, and created the AppSecIL security conference. He is also a community moderator on *https://security.StackExchange.com/*, and a co-author of the *Threat Modeling Manifesto*.

## THREAT MODELING WORKSHOP | 1.5 DAYS, HANDS ON
## .NET SECURITY | 2 DAYS, HANDS ON

"Avi prepared a course for our architects at Amdocs on Threat Modeling. I must say, Avi is very pleasant to work with and has delivered high quality material. He conducted live training with a good rhythm, ease and fluency. He was very knowledgeable and provided practical examples on the topic at hand. The audience was very satisfied with the session and I am happy to recommend on Avi's services with much confidence."

**NADAV ATTIAS**

"I've been working with Avi for more than 3 years. As an experienced AppSec specialist, he brought high standards and high-quality work to our research group. Avi's keen eye for details and his clear vision of the big picture makes him a top-notch consultant while his deep technical knowledge with the ability to explain and simplify complex processes makes him a true mentor. I would recommend Avi anytime."

**EREZ YALON**

"Avi helped the school teachers in teaching networks, information security and operating systems courses, enriching the students with important topics. Additionally, Avi mentored the students in developing their final projects. His contribution to the learning process was significant and helped greatly to understand the material studied as well as the students' successes in the final projects. Avi made a good personal connection with the students, and created a positive and pleasant atmosphere."

**SARA SHARON**

# THREAT MODELING WORKSHOP

**Instructor:** Avi Douglen

**Course Length:** 1.5 Days, Hands On

**Skill Level:** Intermediate

**Student Requirements:** Some familiarity with development of a modern web-based application. Some coding experience (any modern language) preferred but not required.

You've decided that your products require a higher level of security, and now you need to start introducing security into your software design process. Threat Modeling is one of the most effective security activities that can be performed for a software application.

Threat modeling is a structured methodology for security-based analysis of a complex system. This can help you identify and prioritize potential threats and attack vectors, and understand the appropriate countermeasures. This can also empower the product teams to contribute to their own security, as well as build customer confidence.

In this hands-on, collaborative working session, the attendees all actively take part in creating the models. Your architects will take turns with each activity, and have an open dialogue around the models to evoke insight and examine our assumptions.

The interactive Workshop will kickstart your security design efforts, teach your teams the skills required to build their own threat models for their products, and train them with tangible hands-on experience so that they are confident to continue the secure design work and grow the ongoing threat models as a basis.

## Key Takeaways

After we're done, you'll have the foundation of a threat model for your software application, and your teams will have the ability to continue to build further on this initial model.

Attendees will have the skillset, knowledge, and practical experience to threat model their own applications. They will have done a full, but small-scale threat model process on their own features.

As an added benefit, you will receive the completed threat models for the features we already worked on during the sessions, documented and diagrammed. This will be an excellent starting point from which the architects can easily continue to build the threat model for the rest of their applications.

## Target Audience

Product security teams, software architects, senior developers, and security champions.

Threat Modeling Process

Universal Principles

Modeling Basics and Tools

Decomposing the Application

Identifying Threats

STRIDE and Other Models

Rating Risks

Designing Countermeasures

Retrospective

Lightweight Approaches

Integrating with Agile

Full Process Exercise

# .NET SECURITY

**Instructor:** Avi Douglen

**Course Length:** 2 Days, Hands On

**Skill Level:** Intermediate

**Student Requirements:** Familiarity C#, and experience developing web applications and services

**Laptop Requirements:** Visual Studio

The .NET Framework is an incredibly versatile software platform, and C# is very popular for building large enterprise systems and even lightweight startup websites. It has undergone substantial changes over the last few years, and is supported in a wide range of environments. This secure coding class is designed to teach anyone involved in software development - programmers, architects, QA, PM, or security professional – how to build and maintain secure web and web service software.

## CORE MODULES

| | |
|---|---|
| Introduction to Application Security | 1/2 hr |
| *Broad Introduction to Application Security* | |
| Introduction to Security Goals and Threats | 1/2 hr |
| *Application Security Terminology Definitions* | |
| HTTP Security Basics | 1.5 hr |
| *HTTP Response/Request Headers, Verbs, Secure Transport Basics* | |
| CORS and HTML5 Considerations | 1 hr |
| *LocalStorage, HTML5 Sinks, CORS* | |
| Security in ASP.NET MVC and Web API | 1 hr |
| *REST Design, XML, XXE, JSON, API Access Control* | |
| JSON Web Tokens | 1/2 hr |
| *JWT Security Challenges* | |
| SQL and other Injection | 2.5 hr |
| *Parameterization, EF/LINQ, Database Config, Command/LDAP Injection* | |
| Cross Site Request Forgery | 1.5 hr |
| *CSRF Defenses for multiple architecture types (stateless, API, etc)* | |
| File Upload and File IO Security | 1 hr |
| *Multi-Step Secure File Upload Defense, File I/O Security Basics* | |
| Deserialization Security | 1/2 hr |
| *Safe Deserialization Strategies* | |
| Input Validation Basics | 1/2 hr |
| *Whitelist Validation, Safe Redirects* | |

## USER INTERFACE SECURITY

| | |
|---|---|
| XSS Defense | 2 hr |
| *Client side web security* | |
| Content Security Policy | 1 hr |
| *Advanced Client side web security* | |
| Content Spoofing and HTML Hacking | 1/2 hr |
| *HTML based client-side injection attacks* | |

## IDENTITY & ACCESS MANAGEMENT

| | |
|---|---|
| Authentication Best Practices | 1 hr |
| *Best practices of web authentication* | |
| Session Management Best Practices | 1 hr |
| *Best practices of web session management* | |
| Password Policies | 1 hr |
| *What makes up a good password and how to enforce it* | |
| Secure Password Storage | 1 hr |
| *How to store user passwords for authentication securely* | |
| Access Control Design | 1 hr |
| *How to design modern multi-tenant access control* | |
| OAuth Security | 2 hr |
| *Introduction to the OAuth authorization protocol* | |
| OpenID Connect Security | 1 hr |
| *Introduction to the OpenID connect federation protocol* | |

## CRYPTOGRAPHY

| | |
|---|---|
| Cryptography Fundamentals | 2.5 hr |
| *Introduction to applied cryptography* | |
| Advanced Cryptography Usage | 1 hr |
| *Key management and certificate management* | |
| HTTPS/TLS Best Practices | 1 hr |
| *Introduction to transport security* | |

## PROCESS

| | |
|---|---|
| Secure SDLC and AppSec Management | 1hr |
| *Processes around building secure software* | |
| DevOps Best Practices | 1hr |
| *Introduction to DevOps and DevSecOps with a CD/CI focus* | |
| Introduction to Threat Modeling | 1 hr |
| *Overview of secure design and threat modeling for developers* | |

## POSSIBLE ADDITIONAL TOPICS

3rd Party Libraries

Standards (Top10, ASVS, GDPR, etc.)

Differences to ASP.NET Core

Azure Platform and Services

# Sven Schleier

Sven lives in sunny Singapore and is an application security expert and founder of S7ven Consulting. He has executed hundreds of penetration testing engagements and supported and guided software development projects for mobile and web applications during the whole SDLC. He is a core project leader and co-author of the *OWASP Mobile Security Testing Guide* (MSTG) and *OWASP Mobile Application Security Verification Standard* (ASVS), and has created the *OWASP Mobile Hacking Playground*.

Sven has given talks and workshops worldwide to audiences, ranging from developers to penetration testers and students. Check him out on *Linked In*.

## iOS MOBILE SECURITY | 1 DAY, HANDS ON
## ANDROID MOBILE SECURITY | 1 DAY, HANDS ON

"Sven is very well known in the security industry for his remarkable work done on the OWASP Mobile Security Testing Guide project. He is a hardcore technical leader who is passionate about security and knowledge sharing. I had the opportunity to work with him in many areas from pre-sales to project delivery and he has demonstrated his skills on client relationship management, people leadership and project management. It was a privilege working with him and given the opportunity it would be a pleasure working with him again. I highly recommend Sven to any organisation who wants to make a difference in their security culture!"

**— SUMAN SOURAV**
*https://www.linkedin.com/in/sumansourav/*

**FEEDBACK FROM STUDENTS:**

- High level of knowledge and willing to help the students, good job with the apps to test and the presentation.

- As a beginner in this field, I think the delivery was very good and helpful for me. The slides were easy to follow and to understand.

- The training was excellent although I don't have experience in Android or iOS apps it was a very good start for me.

- I like the pace and the instructor's patience to help everyone.

- Very hands on and practically useful skills. Take the theory and make it possible to put into practice!

- The training gave me a much better understanding of mobile security testing, and I now have a list of topics and tools to explore further. Thanks Sven for the training!

# iOS SECURITY

**Instructor:** Sven Schleier

**Course Length:** 1 Day, Hands On

**Lecture Skill Level:** Intermediate

**Student Requirements:**
Basic knowledge about the iOS ecosystem and mobile coding practices

**Laptop Requirements:**
- macOS device that can run latest Xcode
- An iOS hardware device is **NOT** needed

This course teaches you how to identify security vulnerabilities in (your) iOS Apps. Sven is offering an end-to-end experience where students are given the opportunity to do static analysis of the source code and IPA and do dynamic analysis by executing and analysing the app during runtime. We exploit vulnerabilities, identify best practices and verify their effectiveness. Sven will share his experience and many small tips and tricks to attack and defend mobile apps.

An iOS hardware device is not needed by the participants. The iOS hands-on exercises of the training will instead be executed in a cloud-based virtualised environment that allows attendees to access a jailbroken iOS device during the training. One iOS instance will be provided for each participant.

After successful completion of this course, students will have a better understanding of how to implement an iOS app securely and also how to test for vulnerabilities. The course is based on the OWASP Mobile Security Testing Guide (MSTG), with Sven being one of the main authors. The OWASP MSTG is a comprehensive, open source guide for both iOS and Android and is the de-facto industry standard for Mobile Security.

Classes are custom built from the following learning modules. (Please note times are approximate.)

## CORE MODULES

Introduction into mobile security…     .5hr
*…and it's differences to web application security*

Overview of the iOS Platform     .5 hr
*Security Architecture (Code Signing, Sandboxing etc.)*

Jailbreaking…     .5 hr
*… and why an attacker doesn't need it to attack your app*

Secure Networking     1 hr
*Analysing all (non-)HTTP traffic and making it secure with App Transport Security (ATS)*

Frida Crash Course     1 hr
*Understand how attackers use dynamic instrumentation to attack mobile apps*

Introduction into SSL Pinning     1 hr
*Best practices for using and implementing SSL Pinning*

Static Analysis     1 hr
*Automated static analysis of source code and 3rd party libraries*

Biometric Authentication     1 hr
*Making Touch and Face ID bulletproof*

Introduction into Reverse Engineering Attacks     1.5 hr
*Bypassing detection controls and best practices for implementing client-side security controls in general*

Sensitive Data in Local Storage     1 hr
*Secure usage of the KeyChain and best practices for storing data*

Stateless authentication in Mobile Apps     1 hr
*JSON Web Tokens (JWT) and it's security implications*

Deep Links     1 hr
*Avoid business logic vulnerabilities*

WebViews     .5 hr
*Secure configuration and common attacks*

Capture The Flag (CTF)     1 hr
*Investigate an app with the newly learned skills and win a prize!*

# ANDROID SECURITY

**Instructor:** Sven Schleier

**Course Length:** 1 Day, Hands On

**Lecture Skill Level:** Intermediate

**Student Requirements:**
Basic knowledge about the Android ecosystem and mobile coding practices

**Laptop Requirements:**
- Any laptop with at least 8GB Ram, 50GB of free storage and full administrative access
- An Android hardware device is **NOT** needed

This course teaches you how to identify security vulnerabilities in (your) Android App(s). Sven is offering an end-to-end experience where students are given the opportunity to do static analysis of the source code and APK and do dynamic analysis by executing and analysing the app during runtime. We exploit vulnerabilities, identify best practices and verify their effectiveness. Sven will share his experience and many small tips and tricks to attack and defend mobile apps.

An Android hardware device is not needed by the participants. The Android hands-on exercises of the training will instead be executed in a cloud-based virtualised environment that allows attendees to access a rooted Android device during the training. One Android instance will be provided for each participant.

After successful completion of this course, students will have a better understanding of how to implement an Android app securely and also how to test for vulnerabilities. The course is based on the OWASP Mobile Security Testing Guide (MSTG), with Sven being one of the main authors. The OWASP MSTG is a comprehensive, open source guide for both iOS and Android and is the de-facto industry standard for Mobile Security.

Classes are custom built from the following learning modules. (Please note times are approximate.)

## CORE MODULES

Introduction into mobile security…   .5 hr
*…and it's differences to web application security*

Overview of the Android Platform   .5 hr
*Security Architecture (Permission Model, Sandboxing etc.)*

Rooting…   .5 hr
*… and why an attacker doesn't need it to attack your app*

Secure Networking   1 hr
*Analyzing all (non-)HTTP traffic and making it secure*

Frida Crash Course   1 hr
*Understand how attackers use dynamic instrumentation to attack mobile apps*

Introduction into SSL Pinning   1 hr
*Best practices for using and implementing SSL Pinning*

Static Analysis   1.5 hr
*Manual and automated static analysis of source code to identify a Deeplink vulnerability; analysis of 3rd party libraries*

Biometric Authentication   1 hr
*Making it bulletproof*

Introduction into Reverse Engineering Attacks   1 hr
*Bypassing detection controls and best practices for implementing client-side security controls in general*

Sensitive Data in Local Storage   1 hr
*Secure usage of the KeyStore and best practices for storing data*

WebViews   .5 hr
*Secure configuration and common attacks*

Capture The Flag (CTF)   1 hr
*Investigate an app with the newly learned skills and win a prize!*

# Yiannis Pavlosoglou

Yiannis is a cybersecurity executive and founder of KIBERNA, a company specialising in data driven security for managing your cyber risks. With over 20 years of experience in Information Security, he has applied NIST, CERT RMM, and numerous ISO and BSI standards while helping businesses protect their digital assets. Coming from a technical background, he holds a PhD in designing routing protocols, has spent more than 5 years as a professional penetration tester and has committed over 10,000 lines of code for OWASP and others to the public domain. He has successfully held the position of CISO in two countries and is currently volunteering as an elected Board of Directors Member for (ISC)2 where he was elected in 2019 to oversee the CEO for a 3-year tenure. For more information, visit *https://www.linkedin.com/in/yiannisp/*.

## THE MINDSET OF THE CHIEF INFORMATION SECURITY OFFICER (CISO) | 1-2 DAY, HANDS ON
## CYBER RESILIENCE | 1-1 1/2 DAYS, LECTURE

"If you want real advice on how to be a better CISO, this course is for you"

— **CISO, UNDISCLOSED COMPANY IN ENERGY**

"Yiannis actually breaks down in layman's terms what it takes to practice Identify, Protect, Detect, Respond and Recover" and be good at it!

– **HEAD OF INFORMATION SECURITY**

"This course teaches you why cyber resilience is not just a buzz phrase of two words cobbled together, but the most likely next evolution of our industry"

– **OPERATIONAL RISK MANAGER**

# THE MINDSET OF THE CHIEF INFORMATION SECURITY OFFICER (CISO)

**Instructor:** Yiannis Pavlosoglou

**Course Length:** 1-2 Days, Hands On

**Lecture Skill Level:** Intermediate

**Student Requirements:**
Familiarity with the role and responsibilities of Head of Information Security, Information Security Officer, or Chief Information Security Officer.

**Laptop Requirements:**
Any laptop that can run a web browser and has Office applications for Word, Excel, and PowerPoint, or equivalent.

This class is designed for those entering, having recently being appointed to, or considering a future career in being a CISO. Key goal for participants is to become effective in their role. The fundamental contradiction we will tackle in this course is that the principles of confidentiality, integrity and availability often do not agree with the rule of business. This is especially true for organisations that are appointing a head of information security for the first time. As no two businesses have the same information security needs, this class is custom build from the following learning modules (times provided below are approximate).

## BEFORE TAKING ON THE ROLE

| | |
|---|---|
| Your reporting line | 1 hr |
| *Why who you report into is important and common reporting line models* | |
| Your budget | 1 hr |
| *Researching your potential future employer and what they spend in information security* | |
| Your team | 1 hr |
| *Who else works there will determine your capability* | |

## YOUR FIRST 100 DAYS

| | |
|---|---|
| Identify | 1 hr |
| *Your assets* | |
| Identify | 1 hr |
| *Your third parties* | |
| Protect | 1 hr |
| *Controls you can trust vs Controls you need to change* | |
| Detect | 1 hr |
| *Enterprise Logging & Monitoring* | |
| Respond | 1 hr |
| *Your first incident – what you need to prepare* | |
| Recover | 1 hr |
| *Never waste a good crisis* | |

## GOVERNANCE

| | |
|---|---|
| Popular Frameworks | 1 hr |
| C-Suite Buy-in | 1 hr |
| Committee Structure | 1 hr |

### CYBER BUSINESS AS USUAL (BAU)

| | |
|---|---|
| Pennies for the Organisation | 1 hr |
| Pennies for the Team | 1 hr |
| Return on Security Investment (ROSI) | 1 hr |

### CYBER CHANGE AS USUAL (CAU)

| | |
|---|---|
| Don't fall behind on your controls | 1 hr |
| Establish change governance | 1 hr |
| Return on Security Investment (ROSI) | 1 hr |

### CYBER RISK MANAGEMENT

| | |
|---|---|
| Committee Structure | 1 hr |
| Cyber Risk Appetite | 1 hr |
| Your team | 1 hr |

### AWARENESS & CULTURE

| | |
|---|---|
| Your presence each week, each month, each quarter | 1 hr |
| Managing feedback from phishing and other processes | 1 hr |
| Driving behaviors | 1 hr |

### 3RD PARTY PROVIDERS

| | |
|---|---|
| Your cloud providers | 1 hr |
| Security requirements | 1 hr |
| Driving the security industry forward | 1 hr |

### STRATEGY

| | |
|---|---|
| Your horizons | 1 hr |
| Business Model Canvas | 1 hr |

### SERVICES & PROCESSES

| | |
|---|---|
| Building your Service Catalog | 1 hr |
| Building the processes that support your services | 1 hr |
| Managing your service posture | 1 hr |

### YOUR TRANSITION

| | |
|---|---|
| Planning for your Exit | 1 hr |
| Order you Must Leave Behind | 1 hr |
| Handovers | 1 hr |

### YOUR TEAM

| | |
|---|---|
| Offering Technical & Non-Technical Career Paths | 1 hr |
| Managing your Managers | 1 hr |
| Open door policy and contact with the wider team | 1 hr |

# CYBER RESILIENCE

**Instructor:** Yiannis Pavlosoglou

**Course Length:** 1–1 1/2 Days, Lecture

**Lecture Skill Level:** Intermediate

**Laptop Requirements:**
Any laptop that can run a web browser and has Office applications for Word, Excel, and PowerPoint, or equivalent.

When you complete this class, you will have a firm understanding of Operational Resilience and Cyber Resilience. This class is for anyone who wants to help their organisation withstand disruptions and adopt their processes during stress or uncertainty. Common fallacy among information security professionals is that resilience is the job of another team, and we should be only concerned about the availability of systems. Looking at recent ransomware attacks, think again, cyber resilience is the key to prevent, adapt, recover and learn from such disruptions.

### OPERATIONAL RESILIENCE

| | |
|---|---|
| Your Organization's Mission and Business Services | 1 hr |
| Understanding and Setting Disruption Service Thresholds | 1 hr |
| Planning for Disruption Scenarios | 1 hr |

### UNDERSTANDING IMPACT TOLERANCE

| | |
|---|---|
| Service disruption definition | 1 hr |
| Threshold of service tolerances | 1 hr |
| Processes underpinning services | 1 hr |

### UNDERSTANDING CYBER RESILIENCE

| | |
|---|---|
| Withstanding an Information Security Event | 1 hr |
| Absorbing an Information Security Event | 1 hr |
| Recovering from an Information Security Event | 1 hr |

### RESILIENT THREAT MANAGEMENT

| | |
|---|---|
| Cyber Threats using the Diamond Adversary Model | 1 hr |
| Layer 8 Hacking | 1 hr |
| Recovering from an Information Security Event | 1 hr |

# Kostas Papapanagiotou

Dr Kostas Papapanagiotou is a cyber security consultant that helps organizations around the world improve their security posture. He has more than 20 years of experience in the field of cyber security both as a corporate consultant and as a researcher. Over those years he has led numerous projects ranging from penetration tests to the implementation of complex corporate security, compliance and data loss prevention solutions. He is passionate about teaching and has delivered courses to hundreds of students, security professionals and developers.

He has been involved in OWASP since 2004, leading the OWASP Greek Chapter and several educational initiatives. He is an Adjunct Lecturer at the Hellenic-American University in the field of Cyber Security. He holds a PhD and BSc in Cyber Security from the University of Athens and an MSc in Information Security with distinction from Royal Holloway.

**INTRODUCTION TO AZURE SECURITY** | 1-2 DAY, HANDS ON OR LECTURE
**INTRODUCTION TO AWS SECURITY** | 1-2 DAYS, HANDS ON OR LECTURE
**INTRODUCTION TO GCP SECURITY** | 1-2 DAYS, HANDS ON OR LECTURE

"Kostas combines a solid technical background with a unique capability to transmit knowledge to attendees, regardless of their skill level, from university students and beginners to the most technically advanced."

— **HEAD OF SECURITY & COMPLIANCE, ORGANIZATION IN THE PAYMENTS INDUSTRY**

"It is hard to find security professionals that have a very high level of technical expertise and, at the same time, can understand how to realistically address business needs. Kostas has an excellent understanding of the technical aspects of cyber security and a unique ability to effectively communicate them to business leaders and executives."

– **CISO, ORGANIZATION IN THE FINANCIAL SECTOR**

"I've worked with Kostas on a number of occasions and he always delivered with excellence and unmatched professionalism. Work with Kostas if you want a consultation that will lead to a deeper analysis and understanding of your cyber security issues."

– **HEAD OF DEVOPS**

# INTRODUCTION TO AZURE SECURITY

**Instructor:** Dr. Kostas Papapanagiotou

**Course Length:** 1-2 Days, Hands On or Lecture

**Skill Level:** Beginner/Intermediate

**Student Requirements:** Familiarity with building, deploying and running web applications

**Laptop Requirements:** Any laptop with web browser and a steady Internet connection

This course focuses on how to build and deploy secure software on the Microsoft Azure cloud platform. You will learn common Azure terminology and the basic components of a secure application architecture in Azure. We will explain how identity and access management work in Azure and how you can leverage Microsoft Identity Platform to manage your users. You will understand how to use Azure-specific features to ensure your application's production data is adequately protected and monitored. By the end of the course, you should understand how to set up a secure infrastructure using Azure, capable of deploying cloud-native web applications and services.

## SECURITY AND COMPLIANCE IN AZURE

| | |
|---|---|
| Shared Responsibility Model | 1 hr |
| Azure Reference Architectures | 1 hr |
| Azure Virtual Networks | 1 hr |
| Network Routes and Security Groups | 1 hr |
| Network Security and DDoS Protection | 1 hr |
| Identity and Access Management in Azure | 1 hr |
| Microsoft Identity Platform & Azure AD B2C | 1 hr |
| Access Management & Azure RBAC | 1 hr |
| Encrypting Data at Rest in Azure | 1 hr |
| Key Management in Azure and Azure Key Vault | 1 hr |
| Monitoring and Logging in Azure | 1 hr |
| Azure Security Tools & Services | 1 hr |

# INTRODUCTION TO AWS SECURITY

**Instructor:** Dr. Kostas Papapanagiotou

**Course Length:** 1-2 Days, Hands On or Lecture

**Skill Level:** Beginner/Intermediate

**Student Requirements:** Familiarity with building, deploying and running web applications

**Laptop Requirements:** Any laptop with web browser and a steady Internet connection

Amazon AWS is one of the most popular cloud platforms. This course goes through all you need to know in order to develop and deploy secure applications in AWS. We will present how you can build a secure cloud infrastructure in AWS. You will learn how to use AWS Identity and Access Management in order to manage your users and control access to your resources and data. We will demonstrate how to use AWS-specific tools and features to ensure your application's production data is adequately protected and monitored. By course end, you should understand how to set up a basic hardened AWS infrastructure capable of deploying a production web application.

## SECURITY AND COMPLIANCE IN AWS

| | |
|---|---|
| Shared Responsibility Model | 1 hr |
| AWS Reference Architectures | 1 hr |
| Virtual Private Cloud Security | 1 hr |
| Security Groups | 0.5 hr |
| Firewalls and ACLs | 1 hr |
| AWS WAF and DDoS Protection | 0.5 hr |
| AWS System Manager | 0.5 hr |
| VPC Security Strategy and Best Practices | 1 hr |
| Identity and Access Management in AWS | 1 hr |
| Access Control Policies and Policy Conditions | 1 hr |
| IAM Roles and User Policies | 1 hr |
| Protecting Data at Rest in AWS | 1 hr |
| Securing S3 Buckets | 1 hr |
| Key Management in AWS | 1 hr |
| Auditing and Logging in AWS | 1 hr |
| Using CloudTrail and CloudWatch | 1 hr |
| AWS GuardDuty, Security Tools & Services | 1 hr |

# INTRODUCTION TO GCP SECURITY

**Instructor:** Dr. Kostas Papapanagiotou

**Course Length:** 1-2 Days, Hands On or Lecture

**Skill Level:** Beginner/Intermediate

**Student Requirements:** Familiarity with building, deploying and running web applications

**Laptop Requirements:** Any laptop with web browser and a steady Internet connection

This course provides all the information you need to start setting up your Google Cloud Project environment in a secure way. You will learn how to securely build your Virtual Private Cloud in GCP and configure network security controls that Google provides. We explain how you can manage users, roles, identities and access in GCP and how you can leverage what Google Identity Platform offers for managing the identities of your customers. Protecting your data, whether in transit or at rest is critically important. We present how you can adequately safeguard them in GCP based on your data protection requirements. Finally, we demonstrate how logging works in GCP and how you can use tools that Google provides to monitor your GCP infrastructure and efficiently manage security. At the end of the course you will have gotten a thorough understanding of all the elements you need to take into account to secure your GCP environment.

## SHARED RESPONSIBILITY

| | |
|---|---|
| GCP resource hierarchy and key concepts | 1 hr |
| GCP reference architectures | 0.5 hr |
| Virtual Private Cloud Security | 1 hr |
| Routing, Load balancing and External Connectivity | 1 hr |
| Firewalling - the VPC firewall | 1 hr |
| Network Tags and Service Accounts | 1 hr |
| DoS protection and WAF - Google Cloud Armor | 0.5 hr |
| Identity and Access Management in GCP | 1 hr |
| GCP Roles and Policies | 1 hr |
| Google Cloud Identity & Google Identity Platform | 1 hr |

# John Steven

John has spent more than two decades making application security's rocket science problems practicable. As co-CTO of Cigital he led innovation of and brought to market the first static analysis tools, the practice of threat modeling, and the concept of building, measuring, and improving security initiatives. John continues this work as trusted advisor to security executives, startups, and venture funds. Check him out on *LinkedIn*.

**MODULE 1:  INTRODUCTION TO THREAT MODELING AND CONCEPTS**  | 0.5 DAY, LECTURE & EXERCISES
**MODULE 2:  PRACTICING THREAT MODELING**  | 0.5 DAY, LECTURE & EXERCISES
**MODULE 3:  DESIGNING FOR SECURITY BASED ON THREAT MODELING**  | 0.5 DAY, LECTURE & EXERCISES

# ADVANCED THREAT MODELING

**Instructor:** John Steven

**Course Length:** 0.5 - 1.5 Days

**Skill Level:** Intermediate

**Student Requirements:** Literacy in Web development and MVC/MVV architecture

This 3-part course is designed to demystify the myriad approaches to Threat Modeling offered in industry and provide practicable techniques and job aides that make accomplishing it possible for practitioners operating on their own. Learners will understand what they may draw from different schools of threat modeling, when to do so, and how. They will learn how to conduct incremental threat modeling activities as part of a Secure SDL, as well as how to build on activities conducted over time to create a the capability of anticipating risk and delivering secure design on the critical path of their business's schedule..

## MODULE 1

Introduction to Threat Modeling and Concepts          0.5 Day

Learners will understand the different schools of threat modeling in terms of their contributed strengths and weaknesses and be equipped to select from these the techniques necessary to apply and operate within their chosen secure development lifecycle. Learners will leave with the ability to answer questions such as:

- What threat modeling approaches exist; what are their strengths and weaknesses?

- How do I pick from and leverage techniques given my environment?

- When, within a software lifecycle, do I conduct threat modeling?

- What practices are common to most threat modeling approaches?

- What inputs make threat modeling effective?

- What outputs make threat modeling most impactful?

## MODULE 2

Practicing Threat Modeling          0.5 day

Learners will be introduced to practicable guidance and job aides necessary to execute on Module 1 topics. Exercises will give learners practice conducting threat modeling activities and applying guidance and aides. Learners will leave with:

- Generated content Including:
  - An enumeration of threat agents,
  - Key 'doomsday scenarios',
  - The basics of software and infrastructure diagramming, and
  - Threat traceability matrices.

- The ability to conduct threat modeling activities within a secure development lifecycle, as well as

- Insight Into where to look for help conducting threat modeling activities.

## MODULE 3

Designing for Security based on Threat Modeling          0.5 day

Learners will focus on the practical aspects of using a threat model as input to other activities within a secure development lifecycle, particularly test planning and secure design. Learners will practice working a draft threat model to completion, developing compensating security controls, and updating a threat traceability matrix accordingly. Learners will leave confident:

- As security champions or product security architects, designing security controls to meet threats.

- Making security and other design tradeoffs.

- Updating security artifacts, such as design diagrams, threat traceability matrices, and so on.

# Josh Grossman

Consulting on Application Security and IT Risk for over 15 years, Josh has provided guidance to multi-national software development organizations, Fortune 500 companies as well as early and mid-stage start-ups. This has also led him to work, speak and deliver training both locally and worldwide.

Josh is currently CTO for Bounce Security where he helps clients improve and get better value from their application security processes and provides specialist application security advice. In his spare time, he co-leads the OWASP Application Security Verification Standard project and is on the OWASP Israel chapter board.

**BUILDING A HIGH-VALUE APPSEC SCANNING PROGRAMME** | 2-4 HALF-DAYS
**SOFTWARE SECURITY REQUIREMENTS WITH THE ASVS** | 2-4 HALF-DAYS

"Josh delivered application security training based on the OWASP ASVS here in Finland. Josh got excellent feedback from the 30+ training participants who were also more than happy to recommend the training to their colleagues. Personally, I think that Josh is a star in the subject matter with exceptional trainer qualities. As one of the ASVS project co-leaders we were lucky to have him delivering the training and I would love to have Josh back any day!"

**LASSE KORVALA | ISACA FINLAND - VICE PRESIDENT**

"Josh worked with us providing application security support and expertise for two large product groups. I was impressed by his professionalism and how he integrated with the teams and adapted to their working styles despite being an external consultant. He demonstrated a wide range of security expertise along with an understanding of how business constraints would need to affect prioritization. He was also able to improve the knowledge of our security champions through engaging and relevant learning sessions."

**VP R&D | GLOBAL ENTERPRISE SOFTWARE ORGANIZATION**

# BUILDING A HIGH-VALUE APPSEC SCANNING PROGRAMME

**Instructor:** Josh Grossman

**Course length:** Can be flexed to 2-4 half-days depending on desired content.

**Skill level:** Intermediate

**Target audience:** Anyone with involvement in operating or running application security scanning tools/activities such as SCA, SAST, DAST or Penetration Testing.

**Laptop requirements:** Any laptop that can run a web browser and has Office applications for Word, Excel, and PowerPoint, or equivalent.

**Course Objective:** Be ready to work in a group, take part in discussions, and present your findings and leave the course with clear strategies and ideas on how to maintain velocity and get more value from these tools.

---

You invested in the tools, you have the findings, but now what? Many organizations find themselves drowning in possible vulnerabilities, struggling to streamline their processes and not sure how to measure how they are doing.

If you are involved in using application security scanning tools in your organization, these may be familiar feelings to you. In this course you will learn how to address these problems and more (in a completely vendor-agnostic way), with topics including:

- What to expect from these tools?
- Customizing and optimizing these tools effectively
- Building tool processes which fit your business
- Showing the value and improvements you are making
- Faster and easier triage through smart filtering
- How to focus on fixing what matters and cut down noise
- Techniques for various alternative forms of remediation
- Comparison of the different tool types covered.

To bring the course to life and let you practice what you have learnt, for each tool type you will work in teams on exercises which simulate:

- Process design – How to plan processes for a sample organization and justify your decisions to stakeholders
- Finding evaluation – How to eliminate noise and prioritize your remediation efforts.

For these exercises, you will work based on specially designed process templates (which we will provide) which you can use afterwards to apply these improvements within your own organization.

## OVERVIEW

Overview    .25 hr
*Setup training, share training goals and provide tools process overview.*

## LAYING THE GROUNDWORK

Introduction to Vulnerability Analysis    .75 hr
*How to analyze an application vulnerability, what common measurement systems are in used and some common pitfalls.*

Exercise 1: Vulnerability Analysis    .5 hr
*Practice analyzing vulnerabilities using common calculation methods including group discussion and consensus on results.*

Key Skills for AppSec processes    .75 hr
*Understand the key skills needed to best use application security scanning tools and analyze application vulnerabilities.*

Introduction to Application Security Tools/Testing    .5 hr
*Introduce 6 key types of application security tool and their basic characteristics.*

## SOFTWARE COMPOSITION ANALYSIS

Building a process around SCA    .75 hr
*More details on how SCA tools work, the need for an SBOM, measuring SCA effectiveness and how best to integrate the tool.*

Exercise 2: SCA Process    .5 hr
*Process design group activity for SCA.*

Addressing SCA findings    .5 hr
*Considerations for addressing SCA related issues (including security and license) including eliminating noise and how best to remediate.*

Exercise 3: Evaluating SCA findings    .5 hr
*Finding evaluation group activity for SCA.*

## STATIC APPLICATION SECURITY TESTING

Building a process around SAST                                1 hr

*More details on how SAST tools work, measuring SAST effectiveness and how best to integrate the tool.*

Exercise 4: SAST Process                                     .5 hr
*Process design group activity for SAST.*

Addressing SAST findings                                     .5 hr
*Considerations for addressing SAST findings including eliminating noise and how best to remediate.*

Exercise 5: Evaluating SAST findings                         .5 hr
*Finding evaluation group activity for SAST.*

## DYNAMIC APPLICATION SECURITY TESTING

Building a process around DAST                               1 hr

*More details on how DAST tools work, the differences between Enterprise and QA style DAST tools, measuring DAST effectiveness and how best to integrate the tool.*

Exercise 6: DAST Process                                     .5 hr
*Process design group activity for DAST.*

Addressing DAST findings                                     .5 hr
*Considerations for addressing DAST findings including eliminating noise and how best to remediate.*

Exercise 7: Evaluating DAST findings                         .5 hr
*Finding evaluation group activity for DAST findings.*

## PENETRATION TESTING

Building a process around Penetration Testing               .75 hr
*More details on the penetration testing process, how it can be most efficient, and how to integrate the process.*

Exercise 8: Pen Testing Process                              .5 hr
*Group activity to prepare a plan for arranging a pen test.*

Addressing Penetration Testing findings                      .5 hr
*Understanding the thought process to use and steps to take to address findings from penetration testing.*

Exercise 9: Evaluating Pen Test findings                     .5 hr
*Finding evaluation group activity for Pen Test results. Includes discussing with a simulated pen tester and preparing mitigation and prioritization advice and explanations*

## CONCLUSION

Overall comparison of tools                                  .5 hr
*Perform an overall comparison of different tool types to look at advantages and disadvantages*

Other types of AppSec scanning tools                         .5 hr
*Quick review of other options which exist such as IaC scanning, container scanning, secret scanning, cloud security scanning, etc.*

Product Security Incident Response overview                  .5 hr
*High level overview of Product Security Incident Response process*

## SUMMARY

Summary                                                     .25 hr
*Summarize the course and open up for questions.*

# SOFTWARE SECURITY REQUIREMENTS WITH THE ASVS

**Instructor:** Josh Grossman

**Software Engineer variant:** Delivered over 3-4 half-days, this variant is aimed at people in Product Management, Application Architect, or general Software Engineering roles. Students should be familiar with general software development practices and software architecture.

**Security Generalist variant:** Delivered over 2-3 half-days, this variant is aimed at people in general information security or compliance roles. Students should be familiar with basic information and application security concepts.

**Skill level:** Intermediate

**Laptop requirements:** Any laptop that can run a web browser and has Office applications for Word, Excel, and PowerPoint, or equivalent.

This training course is designed to provide you with a deep dive into how to design secure software including the mindset and approach for balancing the needs of security with practicality.

You will go beyond the standard OWASP Top 10 to discuss a wider range of issues, using the comprehensive OWASP Application Security Verification Standard (ASVS) as a baseline to understand the requirements for secure software over a variety of key areas.

For each area, there will be an in-depth table-top exercise where you take turns in using what you have learnt to either secure a sample application architecture or attempt to attack it in a red team vs blue team style.

You will learn how the ASVS can be customized and best suited to your use-case and not only the theoretical solutions but also practical options which are common in the industry for providing software security mechanisms.

You will also learn how the ASVS can be applied to a variety of situations such as Risk Assessment, Procurement and Software Development. Each situation will be accompanied by a practical case study where you need to work with your team to use the standard to make informed risk decision..

## LAYING THE GROUNDWORK

**Application Security Risk and What is the ASVS**          1.25 hr
*Explain application security risk in more detail. How does the ASVS fit in the context of other, better-known OWASP projects, how it is structured and what information does it contain.*

**Approach to Security in the Requirements process**          .75 hr
*Approaching the requirements stage of development with a security mindset, thought processes for into prioritization and trade-offs, and introducing to the exercises for software engineers.*

## ARCHITECTURE, AUTHENTICATION AND AUTHORIZATION

**ASVS V1: Architecture and building security from the start**          .5 hr
*Overview of this chapter in ASVS, key/interesting requirements and more in-depth review of architecture concepts.*

**ASVS V2-4: Authentication, Session Management and Access Control**          1.5 hr
*Modern authentication/authorization concepts including password storage, multi-factor authentication and federation, examples of interesting requirements, and common solutions for addressing these issues in real life.*

**Authentication/Authorization Exercise**          .75 hr
*Scenario of building a new access control mechanism for an existing app.*

## HANDLING BAD INPUT

**ASVS V5: Validation, Sanitization and Encoding**          1.5 hr
*Issues which relate to these requirements including injection attacks, Cross-site Scripting, Deserialization attacks, etc, examples of interesting requirements, and common solutions for addressing these issues in real life.*

**ASVS V7: Error Handling and Logging**          .5 hr
*Overview of this chapter in ASVS, key/interesting requirements and common solutions for addressing these issues in real life.*

Dangerous Input Exercise                           .75 hr
*Scenario of a social media application which lots of dangerous input types and functionality.*

## PROTECTING DATA IN TRANSIT AND AT REST

ASVS V6: Stored Cryptography, V8: Data Protection and V9: Communications                          1.5 hr
*Key cryptography concepts such as asymmetric/symmetric, algorithm modes, encryption parameters and TLS, examples of interesting requirements, and common solutions for addressing these issues in real life.*

Data Protection Exercise                           .75 hr
*Scenario of various sensitive data flows across untrusted networks which require protection.*

## SECURE CONFIGURATION AND BUSINESS LOGIC

ASVS V11: Business Logic and V12: Files and Resources       1.25 hr
*Key business logic attacks and file related attacks such as path traversal, file upload/download, SSRF, etc., examples of interesting requirements, and common solutions for addressing these issues in real life.*

ASVS V10: Malicious Code, V13: API and Web Services and V14: Configuration                       1.25 hr
*Security risks related to REST, SOAP and GraphQL, build-time security and security headers, examples of interesting requirements in these chapters, and common solutions for addressing these issues in real life.*

Business Logic Exercise                            .75 hr
*Scenario of a decision tree mechanism based on user input and business logic.*

## USING THE ASVS IN PRACTICAL SITUATIONS

ASVS in the SDLC                                   .75 hr
*How the ASVS can be used in the SDLC at various stages, how best to approach this activity, and an exercise to apply the ASVS in a simulated SDLC situation.*

ASVS in Procurement                                .75 hr
*How the ASVS can be used in procurement processes to either verify the security controls of a product or verify the protections it provides and an exercise to apply the ASVS in a simulated procurement situation.*

ASVS for Risk Identification                       1 hr
*How the ASVS can be used for risk identification such as during design reviews, penetration testing, etc., and an exercise to apply the ASVS in a simulated risk identification situation.*

MASVS overview                                     .5 hr
*Brief overview of the Mobile ASVS for comparison purposes.*

## SUMMARY

Summary and Questions                              .25 hr
*Summarize the course and open up the floor for questions.*

**MANICODE**
SECURE CODING EDUCATION

031422