NSC42

2020
Training Catalogue

NSC42

2020
Training Catalogue

Application Security

- Modern Devsecops – Assessing and building secure applications
- Modern Devsecops for managers
- Advanced DEVSECOPS
- IronClad Development: Building Secure Web & Web Service Applications
- Application for Security Managers
- Application Security for User Interface Developers & Designers
- Pragmatic Web Security
- Threat Modelling for Developer

Cloud Security

- Cloud Security Foundation (prep for CCSK and CCSP)
- AWS Security from zero to hero
- DEVSECOPS in the cloud

The Instructors

Francesco Cipollone

Founder – NSC42 LTD

Cybersecurity & Cloud Expert. Public Speaker, researcher and Chair of Cloud security Alliance UK, Researcher and associate to ISC2.
I've been helping organizations define and implement cybersecurity strategies and protect their organizations against cybersecurity attacks

FC-LinkedIn E-Mail Website Articles NSC42 LinkedIn

Francesco works hard for the benefit of the wider infosec community. He also works hard at keeping his own technical skills sharp with both a breadth and depth of knowledge across an impressive array of technologies.

David Boda CISO UK National Lottery

Francesco is one of the best Security Architects I had the pleasure to work with.

Florin Daniel Preda Lead Architect New Signature UK

WEB & API SECURITY CLASSES

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

ADVANCED WEB SECURITY CLASSES

Philippe de Ryck

Philippe De Ryck is a trainer in web security, with a specific focus on Angular applications. Philippe holds a PhD in web security from the university of Leuven, which lies at the basis of his in-depth knowledge of the web security landscape. Philippe is a frequent speaker on web security best practices at various developer conferences. Philippe is also the main author of the *Primer on Client-Side Web Security* (Published by Springer). He also built the university's *Web Security Fundamentals* course, a highly-rated online course.

PRAGMATIC WEB SECURITY | 1-3 DAYS, HANDS ON

"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

"The course consists of high-quality course material. Philippe's lectures cover the theory in a clear an concise manner. The practical labs in between provide a useful way to get practical experience.

We have learned a ton of new security practices, which we will immediately adopt within our development team. The course is highly recommended."

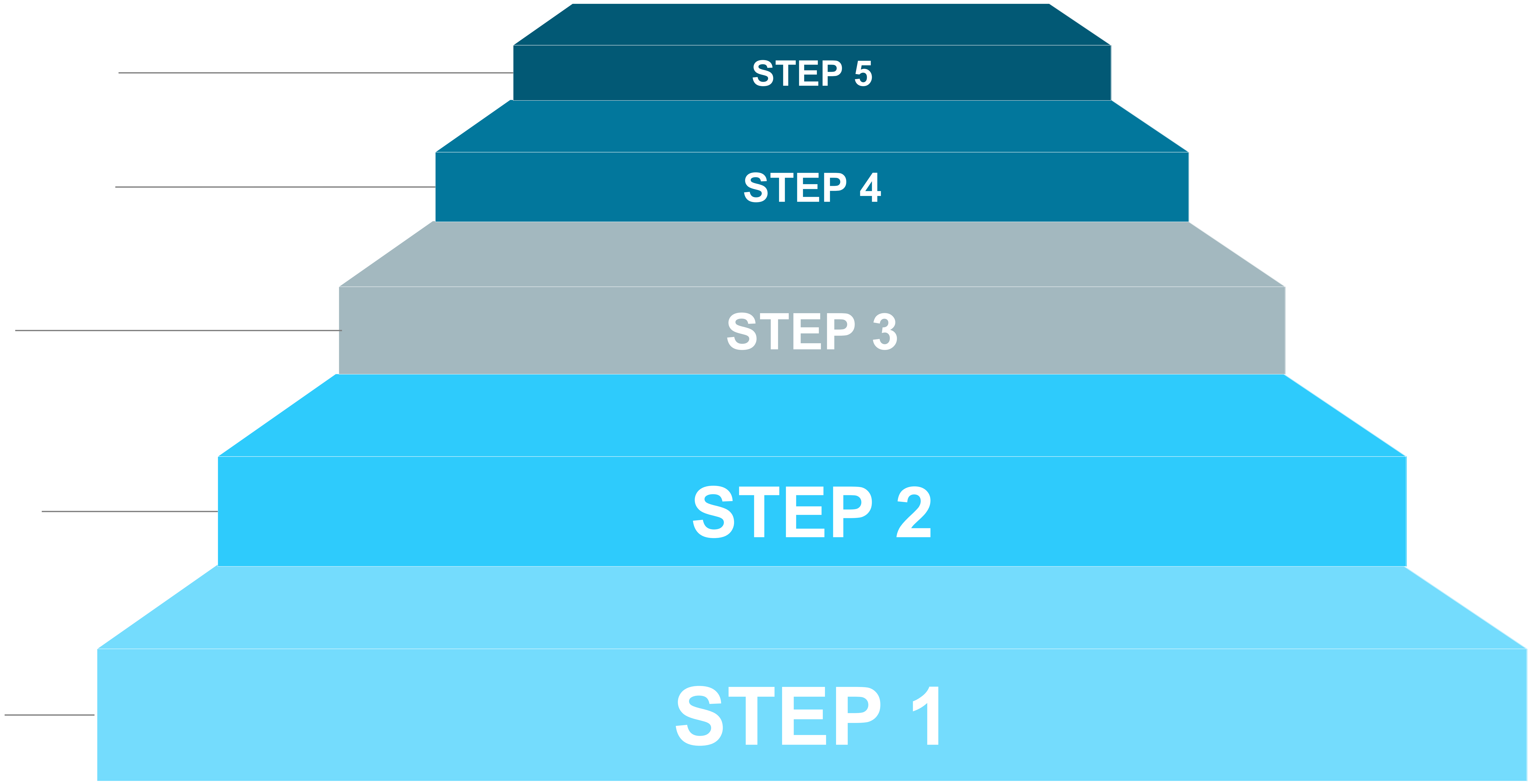
MATTIAS VANHOUTTE

"Philippe explains very thoroughly, yet in a very interesting and clear fashion how elementary it is for the malicious users to exploit a vulnerability. Obviously and most importantly, countermeasures are presented to help us engineers fix the problems systematically and protect our valuable software systems.

The seminars switch between a top-down solid theory behind the security problems and their solutions and hands-on sessions to demonstrate those problems and try the countermeasures in practice.

ARAM HOVSEPYAN

Training Curriculum – DEVSECOPS - DEV -



Cloud Security

Threat Modelling For developers

DEVSECOPS in Cloud

Advanced Devsecops

Basic DEVOPS

Training Curriculum – Cloud Security

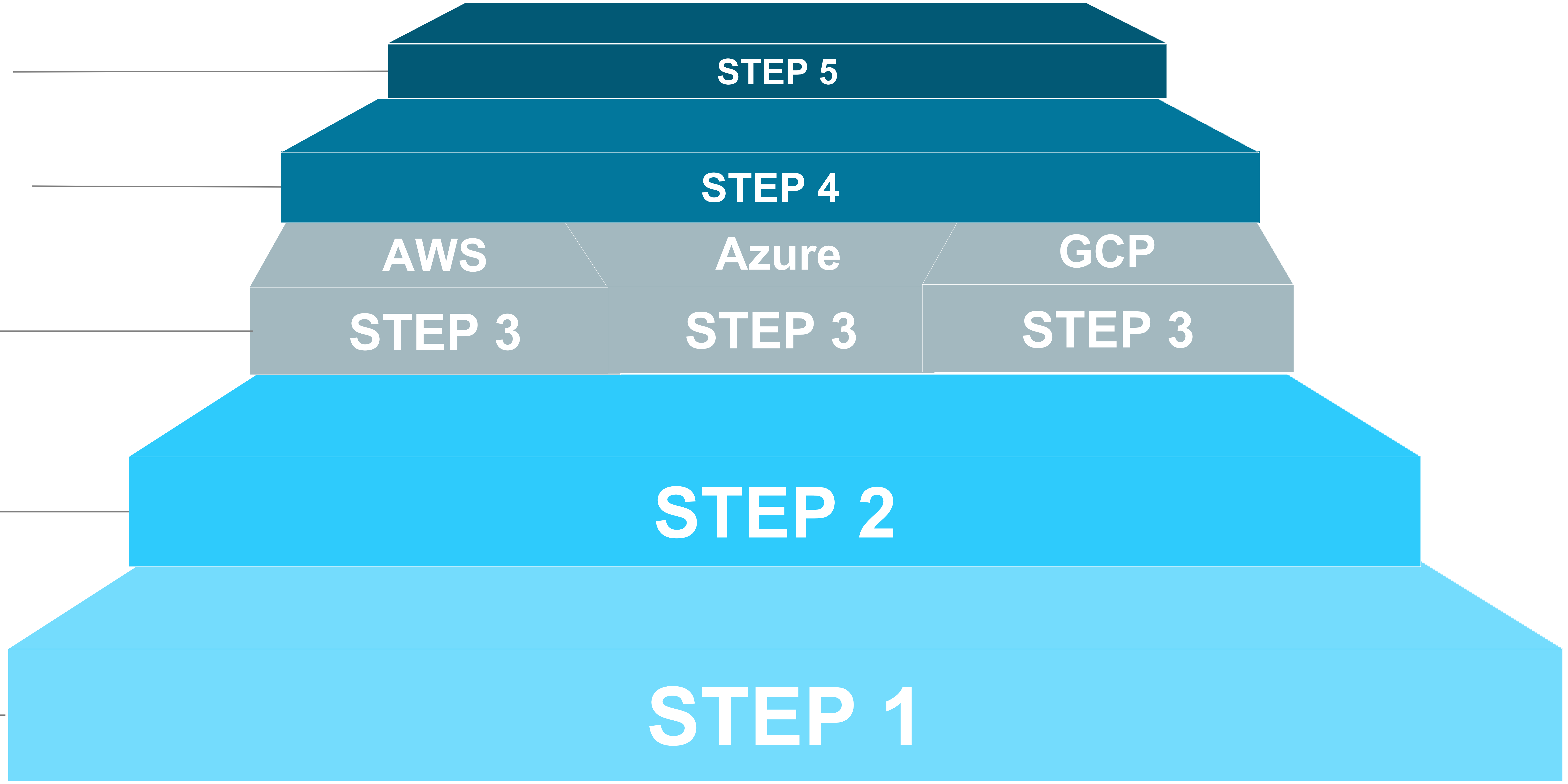
Application Security (opt)

DEVSECOPS for Cloud

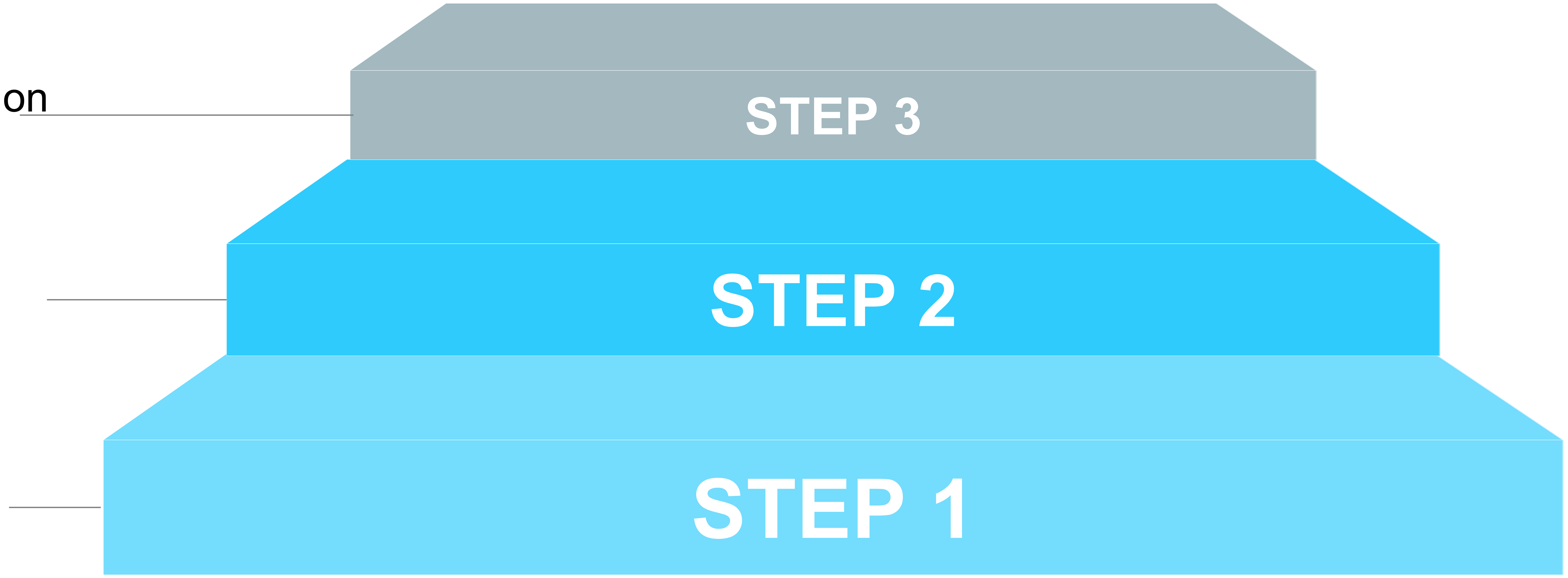
Cloud Specific Security Curriculum

Advanced Cloud Security

CCSK – Basic Cloud Security



Training Curriculum - DEVSECOPS - Managers



Cloud Security Foundation
For managers

Application Security for
Managers

Modern Devsecops
For Managers

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.

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

USER INTERFACE SECURITY

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

IDENTITY & ACCESS MANAGEMENT

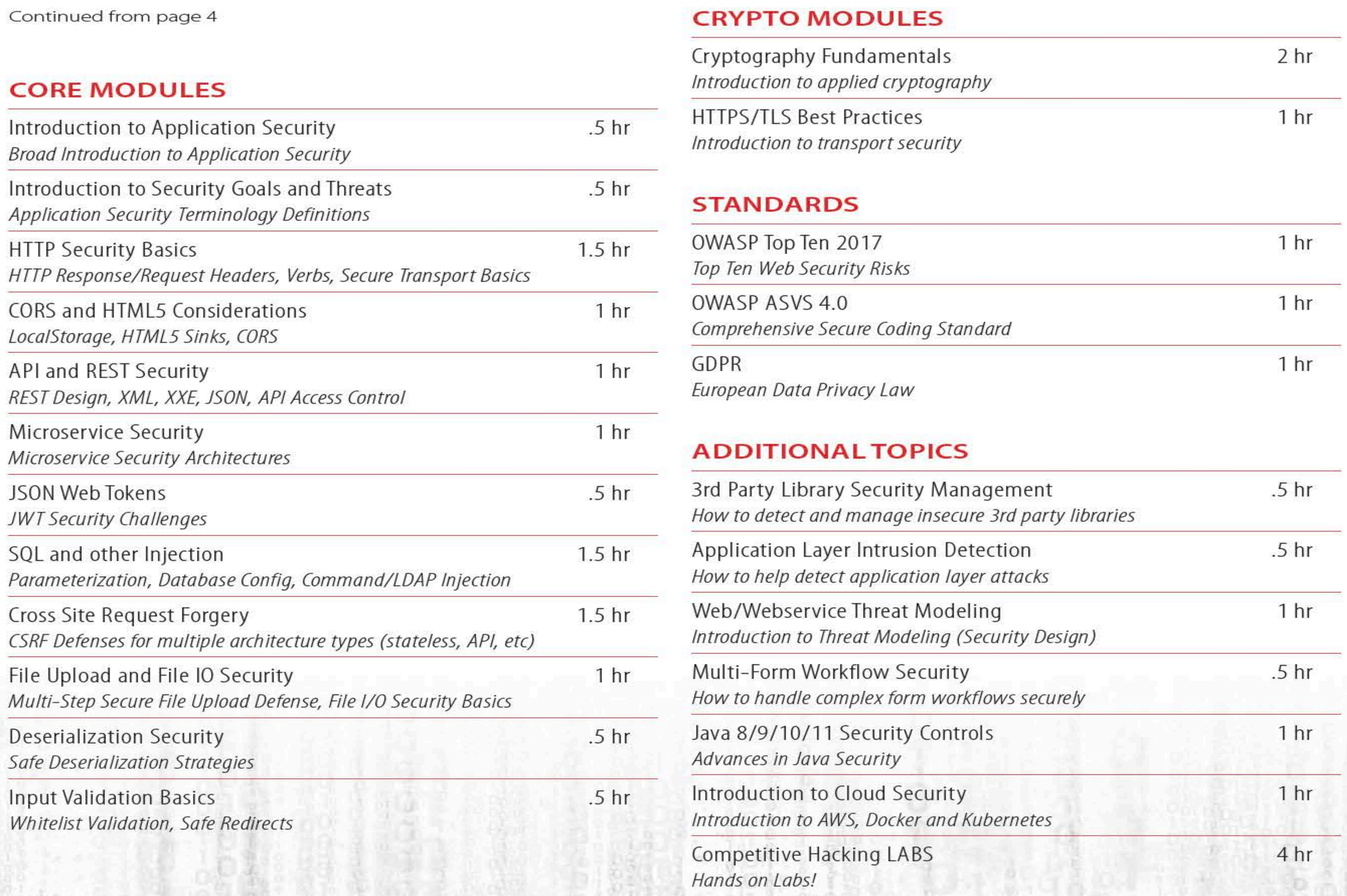
Authentication Best Practices *Best practices of web authentication*	1 hr
Session Management Best Practices *Best practices of web session management*	1 hr
Secure Password Storage *How to store user passwords for authentication securely*	1 hr
Access Control Design *How to design modern multi-tenant access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

PROCESS

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

Continued on page 5

Training Details – Iron Clad Development



Continued from page 4

CORE MODULES

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

CRYPTO MODULES

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

STANDARDS

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

ADDITIONAL TOPICS

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

APPLICATION FOR SECURITY 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

PRAGMATIC WEB SECURITY

Instructor: Philippe De Ryck

Course Length: 1-3 Days, Hands On

Skill Level: Intermediate

Laptop Requirements: To participate in the lab sessions, participants need to bring a laptop capable of executing a Virtual Machine.

Building secure applications is more critical than ever. Unfortunately, distributing a couple of cheat sheets among developers does not get you very far. The key to building more secure software is knowledge. Knowledge of the current security landscape. Knowledge of relevant threats and their corresponding mitigation techniques.

This course helps developers grasp the full security picture. Not only do they yield direct results, but they also gear up developers to recognize security issues in future scenarios.

The lab sessions are based on a custom-built training application. This way, participants can try out attacks and defenses in a realistic setting. The traditional training application consists of a servlet-based backend and a JSP-based frontend. The web pages use HTML5 and JavaScript.

Participants are not expected to write chunks of code on the spot. All labs are prepared up front. Security features can be enabled and disabled through configuration files. In all cases, sample solutions are provided.

The training course is custom built from the modules listed below. A training day consists of approximately 6 hours of classes (lectures and labs). During the labs and the breaks, there is plenty of time to answer detailed questions or discuss individual scenarios.

CORE SECURITY

The Security Model of the Web *Browser security mechanisms, security principles, dependencies*	1 hr
The Basics of HTTP Security *HTTP headers, input validation, authorization*	1 hr
Server-Side Injection Vulnerabilities *SQL injection, Command injection, other types of injection*	1 hr
The Impact of HTTPS on an Application *HTTPS basics, mixed content, SSL Stripping, HSTS*	1 hr
The Modern TLS Certificate Ecosystem *Certificate weaknesses, certificate transparency, public key pinning*	1 hr

API SECURITY

Common API Security Pitfalls *Overview of common mistakes*	1 hr
JSON Web Tokens (JWT) *JWT basics, signatures, encryption, key management*	1 hr
REST APIs, Sessions and Security *Cookies, Authorization header, tokens*	1 hr
Cross-Origin Resource Sharing (CORS) *Cross-origin communication, pitfalls, common mistakes*	1 hr
Introduction to OAuth 2.0 & OpenID Connect *The difference between OAuth 2.0 / OIDC, their purpose*	1-1.5 hr
Advanced OAuth 2.0 / OIDC Topics *Using it as a client, using it in an API, scopes, permissions*	1-2 hr

Continued on page 15

Training Details – DEVSECOPS for Managers

Instructor: Francesco Cipollone

Course Length: 1 Day

Skill Level: Basic/Intermediate

Laptop: Not required. Whiteboard and workshop sessions

Building an application security is complex
Figuring out the difference between various roles and the complexity of the modern applications is getting more and more complex

This course helps building pragmatic APPSEC and DEVSECOPS transformation programmes with lesson learned and use cases

Participants are invited to share their ideas and challenges in the organization

The course aims to leave the participant with measurable outcomes, a step by step maturity matrix and a plan to execute

Core Security

- Strategy and pillars – 1h
- Team and differences - 1h
- Vulnerabilities and numbers – 1h
- Vulnerability division and risk – 1h

APP/OP sec

- Risk Vulnerabilities in operations – 1h

- Standards – 1h
  - OWASP top 10
  - ASVS

KCI & Metrics

- Metrics to measure application security – 1h
- Metrics to measure operation security measure team performance -1 h

Training Details – DEVSECOPS - Developers

Instructor:	Francesco Cipollone
Course Length:	1 Day
Skill Level:	Basic/Intermediate
Laptop:	Not required. Whiteboard and workshop sessions

Including security in the application is growing in complexity.
Pentesting application does not deliver speed that the business requires.
There is a whole stream of tooling that create more confusion than not in application development team.
This training will help making sense of the tooling, understanding what are the common vulnerabilities and how to address.

Participants are invited to share their ideas and challenges in the organization

Process – 3h

- Secure SDLC
- Tooling integration at which stage
- OWASP/Open source tools
- Static code analysis – when and where
- Dynamic application analysis – when and where
- Library dependency check – when and where

Open Security Standards – 5h

- OWASP Top Ten – 1h
- OWASP ASVS - 1h
- NIST Cybersecurity Framework -1h
- GDPR/Shield – 1h
- Vulnerability division and risk – 1h

Training Details – DEVSECOPS - Developers

People – 3h

- Roles in DEVSECOPS
- Team and tooling
- What is a security champion
- Risk management
- Triage, False Positives, Context

Threat modelling (light Touch) -2h

- The basics - CIA
- Standards STRIDE and DREAD

APP/OP sec

- Risk Vulnerabilities in operations – 1h

KCI & Metrics

- Metrics to measure application security – 1h
- Metrics to measure operation security -1 h
- Metrics to measure team performance – 1h

Training Details – DEVSECOPS - Developers

Instructor:	Francesco Cipollone
Course Length:	1 Day
Skill Level:	Basic/Intermediate
Laptop:	Not required. Whiteboard and workshop sessions

Including security in the application is growing in complexity.
Pentesting application does not deliver speed that the business requires.
There is a whole stream of tooling that create more confusion than not in application development team.
This training will help making sense of the tooling, understanding what are the common vulnerabilities and how to address.

Participants are invited to share their ideas and challenges in the organization

Process – 3h

- Secure SDLC
- Tooling integration at which stage
- OWASP/Open source tools
- Static code analysis – when and where
- Dynamic application analysis – when and where
- Library dependency check – when and where

Open Security Standards – 5h

- OWASP Top Ten – 1h
- OWASP ASVS - 1h
- NIST Cybersecurity Framework -1h
- GDPR/Shield – 1h
- Vulnerability division and risk – 1h

Training Details – DEVSECOPS - Developers

People – 3h

- Roles in DEVSECOPS
- Team and tooling
- What is a security champion
- Risk management
- Triage, False Positives, Context

Threat modelling (light Touch) -2h

- The basics - CIA
- Standards STRIDE and DREAD

APP/OP sec

- Risk Vulnerabilities in operations – 1h

KCI & Metrics

- Metrics to measure application security – 1h
- Metrics to measure operation security -1 h
- Metrics to measure team performance – 1h

Contacts

NSC42

WHEN YOU ARE CYBERSAFE WE ARE CYBERHAPPY

Thank you

Get in touch:

https://uk.linkedin.com/in/fracipo

Francesco.cipollone (at) nsc42.co.uk

www.nsc42.co.uk