SafeStack

Training Catalog

2024

Table of Contents

Overview

The SafeStack Model

Learn

Learn the skills and processes needed to software security risk, design patterns and approaches.

Courses
Labs
Seminars

Act

Take steps to prevent, detect and respond to security challenges and reduce the risk our applications face.

Playbooks
Templates
Integrations

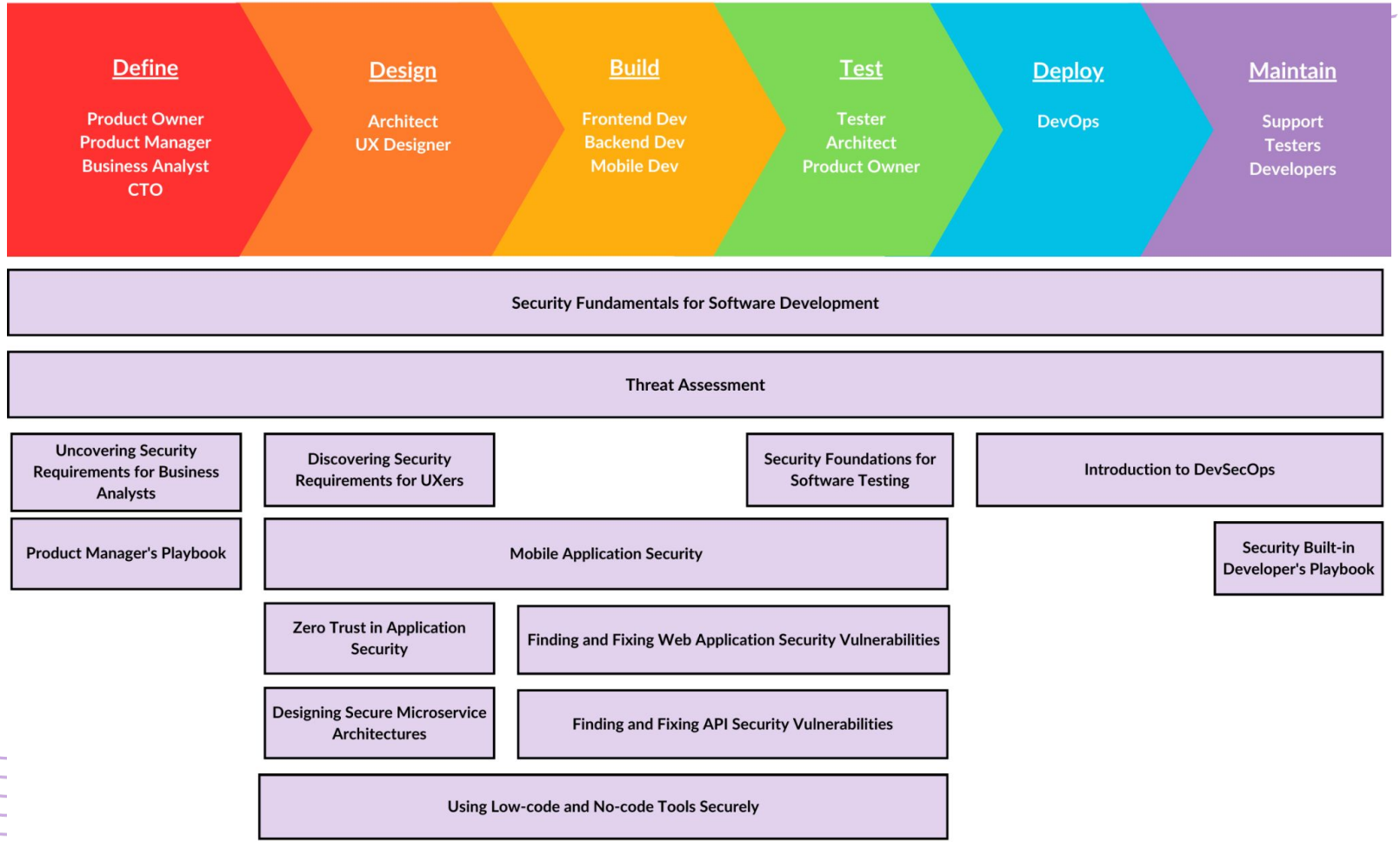
Measure

Understand and measure our teams engagement in software security initiatives and adapt our approaches based on the results.

Reporting
Learning Paths

Full Courses

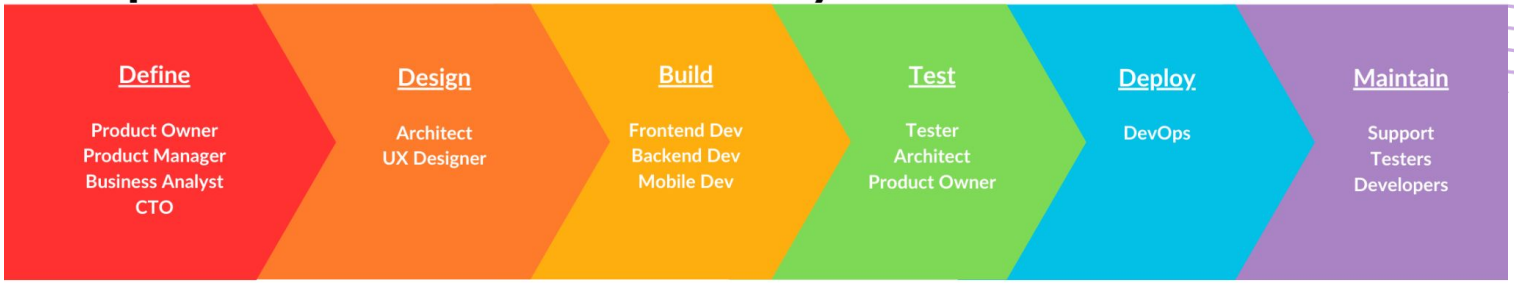
- Between 1 hour and 5 hours in length.
- Broken up into modules and lessons.
- Many include resources, playbooks or hands on labs
- 14 courses, totalling 50 hours of taught content mapped to roles and SDLC stage.


Define
Product Owner
Product Manager
Business Analyst
CTO
Design
Architect
UX Designer
Build
Frontend Dev
Backend Dev
Mobile Dev
Test
Tester
Architect
Product Owner
Deploy
DevOps
Maintain
Support
Testers
Developers
Security Fundamentals for Software Development
Threat Assessment
Uncovering Security Requirements for Business Analysts
Discovering Security Requirements for UXers
Security Foundations for Software Testing
Introduction to DevSecOps
Product Manager's Playbook
Mobile Application Security
Security Built-in Developer's Playbook
Zero Trust in Application Security
Finding and Fixing Web Application Security Vulnerabilities
Designing Secure Microservice Architectures
Finding and Fixing API Security Vulnerabilities
Using Low-code and No-code Tools Securely

Seminars

- Less than 1 hour in length
- Single topic, taught to a live audience and recorded for learners worldwide.
- Focused on practical, relevant and timely topics.
- 34 seminars, totalling 30 hours of taught content

Example live and on-demand Community Seminars



Security Metrics 101

Planning for Secure DevOps

★ Key to AppSec: Encryption

Hands-on with Container Security

AWS Threat Modeling

GitHub Actions for AppSec

★ Getting started with AI and Security

Over 30 On-Demand SafeStack Community Seminars Available

★ Includes interactive / useable templates

SafeStack helps companies meet their goals

Improve internal capability

- Reduce pressure on internal specialists
- Build security culture
- Grow security champions
- Integrate practices throughout your SDLC

Meet compliance requirements

- PCI DSS
- ISO 27001
- SOC2
- NIST 800-53
- APRA
- StateRamp/FedRamp

Progress against maturity frameworks

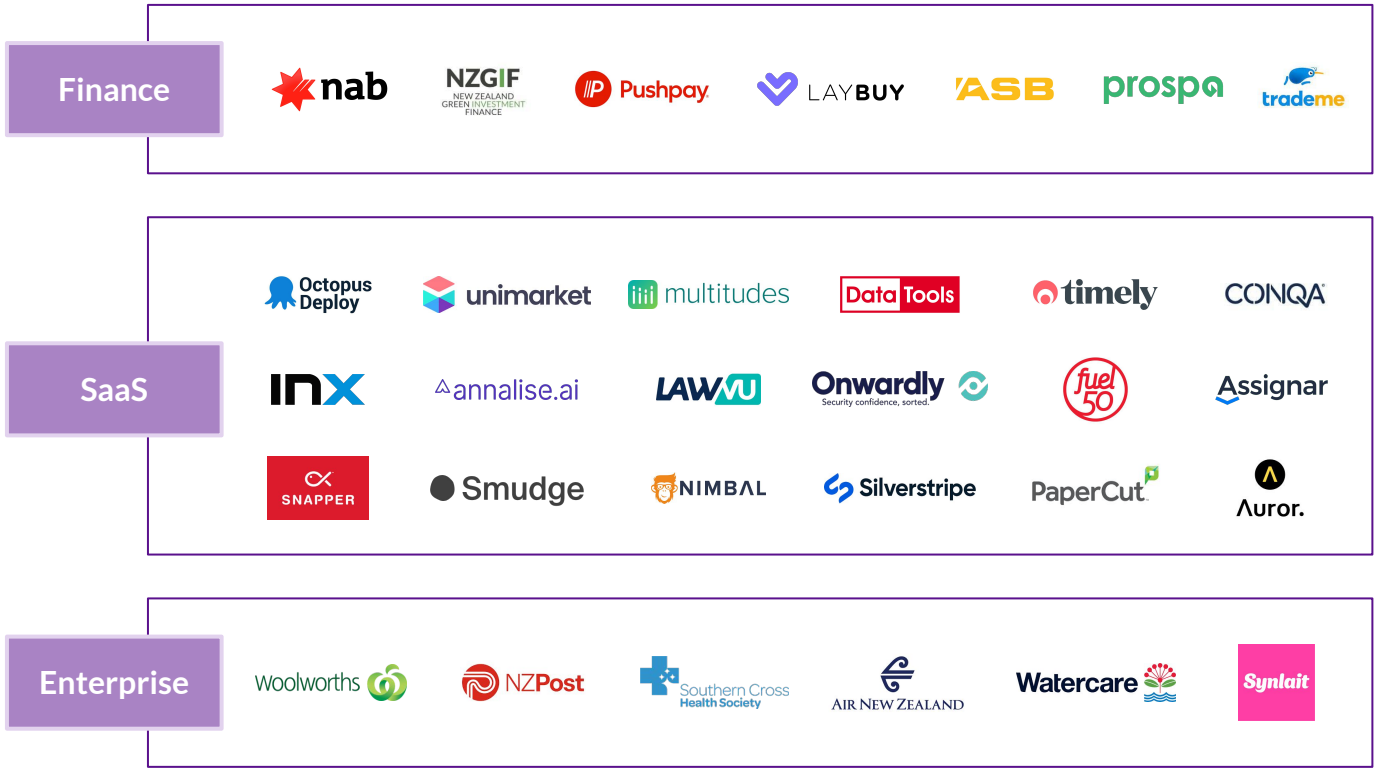
- SAMM
- BSIMM
- SSDF
- Technology specific frameworks
- Bespoke frameworks

Education that levels up your entire team

"Sometimes security training is a matter of ticking a box, but with Safestack you genuinely feel like you're levelling up your teams skills, which puts you in the best place to defend from real attacks, no matter what's "on paper"

"With so many of our company's customers expecting a high standard of security and compliance, SafeStack's platform ensures my team are trained in best practice at every level from junior through to senior software contributors."

Proudly training innovative development teams worldwide



Complete Course Syllabuses

COURSE OVERVIEW

Security Fundamentals for Software Development

Course Description

Security isn't just about tools and vulnerabilities. Security is a very human field, born from the idea that everything has value and some people will go to great lengths to acquire that value for themselves.

Course Objectives

- Understanding and calculating security risk and the impact it can have on our people, data and systems.
- Identifying the groups and individuals that pose a threat to our security, what drives them and how we can use this information to plan our defenses.
- The challenges with defending applications and organizations and the steps you can take to become a security champion

Credential

Security Fundamentals: Level 1

Roles

All Roles

Total Duration

55 minutes

COURSE SYLLABUS

Security Fundamentals for Software Development

Title	Total Duration	Structure
Introduction to Security Fundamentals for Software Development	2 minutes	1 lesson
Understanding Vulnerability and Risk	18 minutes	3 lessons
Threat Actors and Motivation	24 minutes	3 lessons
Why Security Matters	11 minutes	3 lessons
Threat Actor Characteristics Reference Sheet	-	Resource

COURSE OVERVIEW

Zero Trust in Application Security

Course Description

While application security is always evolving, right now we are going through a large paradigm shift that will define the next generation of secure software development and architecture. As we move away from centrally managed applications and trusted zones towards a cloud-centric technology environment, we need to approach security differently.

Zero Trust is a principled approach that can help application development teams decide on the right security architecture for their solutions and organizations. Zero Trust architectures are also an approach being mandated by governments and clients across the globe.

Course Objectives

- Learn the basics of Zero Trust architecture
- Understand what Zero Trust maturity looks like, how to assess it, and how to scale it
- Dive into how Zero Trust can be implemented in application development

Credential

Security in Practice: Zero Trust

Roles

Architect

Total Duration

2 hours 58 minutes

COURSE SYLLABUS

Zero Trust in Application Security

Title	Total Duration	Structure
Introduction to Zero Trust	34 minutes	3 lessons
Embedding Zero Trust	46 minutes	4 lessons
Zero Trust for developers	90 minutes	9 lessons
Zero Trust Course Summary	8 minutes	1 lesson

COURSE OVERVIEW

Introduction to DevSecOps

Course Description

DevOps is commonly embraced by technology teams looking to deliver value to their customers, faster. While the combination of software development and IT operations may introduce new risks, it also provides many opportunities to implement automated, continuous security.

Secure DevOps, or DevSecOps, is about making sure you're embedding the right amount of security throughout your DevOps processes and teams.

Course Objectives

- Introduce the concept of DevSecOps,
- Secure your cloud environments
- Embed automated security throughout your software development pipelines.
- Understand resilience, and incident response in a DevOps world.
- Learn how to strategically grow your secure DevOps capabilities

Credential

Security Fundamentals: Level 2

Roles

DevOps

Total Duration

3 hours 19 minutes

COURSE SYLLABUS

Introduction to DevSecOps

Title	Total Duration	Structure
DevOps Culture and Processes	36 minutes	4 lessons
Cloud Security	58 minutes	6 lessons
Securing Source Code and Deployment Pipelines	56 minutes	5 lessons
DevOps Defence	26 minutes	3 lessons
Strategically Growing DevSecOps	23 minutes	3 lessons

COURSE OVERVIEW

Finding and Fixing Web Application Security Vulnerabilities

Course Description

Vulnerable software is big business for cyber criminals. Identifying vulnerabilities early and knowing common pitfalls to avoid can make a big difference to the resilience of your applications. Every year new classes of web application security flaws are uncovered. Keeping across all these vulnerabilities can help prepare you, and your systems, against abuse.

This course will help you to understand, identify and avoid common software security vulnerabilities in your code.

This course includes hands on labs.

Course Objectives

- Common web application security vulnerabilities, and how to find them
- Approaches to avoid or reduce these vulnerabilities and how they work
- The challenges and trade-offs we face when implementing these controls

Credential

Secure Development: Level 1

Roles

Developers
Testers

Total Duration

4 hours 33 minutes

COURSE SYLLABUS

Finding and Fixing Web Application Security Vulnerabilities

Title	Total Duration	Structure
Introduction to Finding and Fixing Web Application Security Vulnerabilities	4 minutes	1 lesson
Object Access Vulnerabilities	15 minutes	2 lessons
Enumeration Vulnerabilities	26 minutes	2 lessons
SQL Injection Vulnerabilities	27 minutes	2 lessons
Configuration Vulnerabilities	13 minutes	2 lessons

COURSE SYLLABUS

Finding and Fixing Web Application Security Vulnerabilities

Title	Total Duration	Structure
Operating System Injection Vulnerabilities	20 minutes	2 lessons
Passwords and Authentication	37 minutes	4 lessons
Session Vulnerabilities	33 minutes	2 lessons
Cross Site Scripting Vulnerabilities (XSS)	22 minutes	2 lessons
Using Components with Known Vulnerabilities	27 minutes	2 lessons

COURSE SYLLABUS

Finding and Fixing Web Application Security Vulnerabilities

Title	Total Duration	Structure
Path Traversal Vulnerabilities	16 minutes	2 lessons
Return of the SQL Injection	17 minutes	1 lesson
XML External Entity (XXE) Vulnerabilities	16 minutes	2 lessons

COURSE OVERVIEW

Threat Assessment

Course Description

We all want to build security into our applications. While many of our approaches to application security rest with the specific syntax we write, this focus at the lower levels of our application often blind us to the security risks posed to the entire system.

Threat Assessment allows us to use Systems Thinking to understand our systems as they are designed and then as they are built and identify common threats to the confidentiality, integrity and availability of the components within it.

Course Objectives

- Understand the value of threat assessment.
- Apply a threat model to our systems using Microsoft STRIDE
- Use Attack Trees to group and prioritize the threats faced by our systems
- Understand the fundamentals of preventative, detective and responsive controls for defending software systems

Credential

Security Architect: Level 1

Roles

All Roles

Total Duration

1 hour 59 minutes

COURSE SYLLABUS

Threat Assessment

Title	Total Duration	Structure
Introduction to Threat Assessment	2 minutes	1 lesson
The Value of Threat Assessment	8 minutes	1 lesson
Understanding your system and environment	22 minutes	2 lessons
Applying a threat model	43 minutes	7 lessons
Using Attack Trees	15 minutes	3 lessons

COURSE SYLLABUS

Threat Assessment

Title	Total Duration	Structure
Applying Controls and Reducing Risk	22 minutes	3 lessons
Getting the most from Threat Assessment	7 minutes	1 lesson

COURSE OVERVIEW

Finding and Fixing API Security Vulnerabilities

Course Description

It's no surprise that microservices and APIs are gaining in popularity. They enable organisations to build and maintain their systems in ways that allow them to scale bigger, deploy faster, and be more resilient than their monolithic counterparts. This also means securing them is slightly different and requires us to focus more on specific areas like authentication, authorisation, alerting, and resource hardening.

This course will introduce different ways to apply security concepts and controls to the way you build and manage your microservices and APIs.

This course includes hands on labs.

Course Objectives

- Review and discover common microservice and API security vulnerabilities
- Learn approaches to apply security concepts and controls to reduce risk
- Discover further resources applying these security concepts to specific technologies and contexts

Credential

Secure Developer: Level 2

Roles

Developers
Testers

Total Duration

2 hours 29 minutes

COURSE SYLLABUS

Finding and Fixing API Security Vulnerabilities

Title	Total Duration	Structure
Applying Security Concepts to Development and Operations	28 minutes	3 lessons
Introduction to API Vulnerabilities	3 minutes	1 lesson
Broken Authentication	25 minutes	2 lessons
Broken Authorisation	14 minutes	2 lessons
Data Exposure	15 minutes	2 lessons

COURSE SYLLABUS

Finding and Fixing API Security Vulnerabilities

Title	Total Duration	Structure
Resource Limitations	14 minutes	2 lessons
Mass Assignment	9 minutes	2 lessons
Injection	12 minutes	2 lessons
Misconfiguration and Mismanagement	16 minutes	2 lessons
Transitioning To Microservices or Hybrid Architectures	13 minutes	1 lesson

COURSE OVERVIEW

Designing Secure Microservice Architectures

Course Description

Microservice-based architectures follow some different design principles than the ones we may be used to following with other, monolithic models. Different design principles means different and new ways to consider threats and security too.

This course will help you understand these differences, and how you can use the tools and techniques you already know to incorporate security into microservice-based designs.

Course Objectives

- Introduce and understand microservice-based architectures
- Explain the design principles followed and how security can add value
- Highlight specific threats and security risks to consider for microservices and API
- Discuss challenges, benefits, and tips with applying secure design principles

Credential

Security Architect: Level 2

Roles

Architect

Total Duration

50 minutes

COURSE SYLLABUS

Designing Secure Microservice Architectures

Title	Total Duration	Structure
Terminology, Technology, and Principles	15 minutes	2 lessons
Challenges and Benefits of Microservice Architectures Models	6 minutes	1 lesson
Case Studies	5 minutes	1 lesson
Security Risks and Threats	14 minutes	1 lesson
Tips for Designing Microservices Securely	5 minutes	1 lesson

COURSE OVERVIEW

Security Foundations for Software Testing

Course Description

Security testing is a type of software testing that allows you to uncover potential vulnerabilities or weaknesses. These weaknesses lead to security risks – which could impact the system, data, or users.

In this course, we're going to learn a bit more about what security testing is, and specifically how we can integrate it into every aspect of our software development life cycle.

Course Objectives

- Understand the value of security testing and see where it can fit in our software development lifecycle.
- Review some common types of security testing, when they should take place, who should be involved, and what tools can help.
- Identify different challenges and strategies that you can use to create test cases to help you test functionality for security weaknesses.

Credential

Security Tester: Level 1

Roles

Tester

Total Duration

1 hour 29 minutes

SYLLABUS

Security Foundations for Software Testing

Title	Total Duration	Structure
Introduction – Security Testing	4 minutes	1 lesson
The Value of Security Testing	6 minutes	1 lessons
The Types of Security Testing	17 minutes	2 lessons
Preparing your test cases	23 minutes	2 lessons
Challenges with Security Testing	5 minutes	1 lesson

SYLLABUS

Security Foundations for Software Testing

Title	Total Duration	Structure
Actioning Test Outcomes	17 minutes	2 lesson
Security Testing Tools	17 minutes	2 lessons

COURSE OVERVIEW

Security Built-in Developer's Playbook

Course Description

The Security built-in Developer's Playbook course is a growing playbook-styled series of modules to help learners do their jobs with security built-in.

This course is a collection of modules to help provide guidance and playbooks for common developer tasks, providing job aids and curated resources to help make better decisions.

Course Objectives

- Provide actionable guides and playbooks to solve common developer security challenges.

Credential

-

Roles

Developer

Total Duration

1 hour 6 minutes

COURSE SYLLABUS

Security Built-in Developer's Playbook

Title	Total Duration	Structure
Securing Cloud Accounts	5 minutes	1 lesson
Technical Playbook: Securing Cloud Accounts	1 hour	Resource

COURSE OVERVIEW

Product Manager's Playbook

Course Description

The Product Manager's Playbook course is a playbook-styled series of modules to help learners do their jobs with security built-in.

This course is a collection of modules to help provide guidance and playbooks for common Product Management tasks, providing job aids and curated resources to help make better decisions.

Course Objectives

- Provide actionable guides and playbooks to help product managers bring security to their roles.

Credential

-

Roles

Product Manager

Total Duration

24 minutes

SYLLABUS

Product Manager's Playbook

Title	Total Duration	Structure
Prioritizing Security for Product Managers	6 minutes	1 lesson
RICE Template	-	Resource
RICE Worked Example	-	Resource
RICE Worked Example Walkthrough	18 minutes	1 lesson

COURSE OVERVIEW

Using Low-code and No-code Tools Securely

Course Description

Low-code and no-code development approaches are flexible and help us build solutions - quickly. This also introduces security risk. The level of security risk depends on the solution we are building, as well as the decisions we make along the way in planning, development, and maintenance.

This course is interactive and is designed to be re-used for each low-code or no-code project you have. That way you only have to go through the learning that you need so you can get your solution built - quickly and securely.

Course Objectives

- Highlight the key decisions we are making that have a security impact.
- Focus on turning our security decisions from implicit to informed, and
- Equip ourselves with the information needed to get this work done.

Credential

Security in Practice - No Code, Low Code

Roles

All Roles

Total Duration

47 minutes

COURSE SYLLABUS

Using Low-code and No-code Tools Securely

Title	Total Duration	Structure
Overview of Low-code, No-code, and Security	17 minutes	1 lesson
Low-code No-code Security Interactive Questionnaire	30 minutes	Resource
Low-code and No-code Security Work Plan	-	Resource

COURSE OVERVIEW

Uncovering Security Requirements for Business Analysts

Course Description

As a Business Analyst, figuring out where to start with uncovering security requirements can be a challenge. In this course, we equip you with key concepts and questions for you to ask, as part of your requirements elicitation workflow.

This course will help bootstrap some key ideas you can take into your requirements discovery, elicitation, and planning discussions. These will help you better navigate these conversations, and support you in uncovering the security requirements.

You will also have the details necessary for writing user stories for the backlog, and any subsequent prioritization activities your team takes.

Course Objectives

- Helping with your preparation & requirements gathering process
- Identifying relevant stakeholders for the security work to be done
- Asking the right questions to help get these details.

Credential

Business Analyst Essentials

Roles

Business Analysts

Total Duration

45 minutes

COURSE SYLLABUS

Uncovering Security Requirements for Business Analysts

Title	Total Duration	Structure
Uncovering Security Requirements for Business Analysts	28 minutes	1 lesson
Worksheet - Uncovering Security Requirements for Business Analysts	-	Resource

COURSE OVERVIEW

Discovering Security Requirements for UXers

Course Description

Great UX for our products is a key component of software development. It means we connect with our users and customers, which builds trust.

Alongside UX sits security. With an increasing security compliance landscape we all want to make sure we can do both: thoughtful and empathetic UX, alongside being secure. This course is here to help you discover security requirements as part of the work you do, and in collaboration with your wider team.

This content includes two resources.

Course Objectives

- Use security as a key contributor toward quality, and understand how it directly contributes to usability
- Design a plan for which stakeholders to speak to, and why
- Organize security-focussed topics to partner with stakeholders, in order to discover security requirements.

Credential

UX Security Essentials

Roles

All UX/UI design roles

Total Duration

1 hour

COURSE SYLLABUS

Discovering Security Requirements for UXers

Title	Total Duration	Structure
Discovering Security Requirements for UXers	1 hour	1 lesson
Discovering Security Requirements for UXers - Job Aid	-	Resource
Discovering Security Requirements for UXers - Reference Sheet	-	Resource

Seminars

SEMINAR CATALOG

Key to Appsec: Secrets Management

Secrets come up a lot in our work and are one of the higher-risk pieces of data we handle.

In this seminar, we will cover all the different types of secrets that we come across when building software or services. For each type of secret, we will talk about practical advice on how they should be generated, stored, and handled.

45 minutes

Key to AppSec: Encryption

Encryption has been around for as long as we have had information we want to keep secret. It has always been a key security control for application security, and even more so now, as our users become more privacy-aware and conscious of who they share their data with. In this seminar, we will cover the fundamental basics of encryption when it comes to application security. We will discuss the concepts of encryption-at-rest and encryption-at-transit, the characteristics of encryption that make it secure, and pragmatic advice for incorporating it into your team's work.

40 minutes

Security and Usability: how can we do both?

We know that secure development practices are key to the work we do, and alongside that, ensuring a focus on the usability of our work. But sometimes these two things are in tension. Different areas of the business will likely be thinking from different perspectives in what we're trying to achieve and how we get there. That can mean a lot of conflict in these conversations - whether that's around the usability of authentication, unhelpful prompts, or introducing additional risk in third party services. How can we focus on both? Join Laura Bell Main in a conversation about security and usability, including practical outcomes and how we can get there.

30 minutes

SEMINAR CATALOG

Question time with a Penetration Tester

We often hear about penetration testing when talking about security. Especially, if you're in a compliance driven environment such as PCI-DSS. You might have been on the receiving end of a Penetration Test report, and just wondered, how does penetration testing fit into the bigger picture of security, and our product security workflow? Or maybe, how you can make the pentest process work better for you?

30 minutes

The software teams guide to compliance

So you need to comply with a standard such as ISO? Or perhaps you are entering a new market that comes with some form of regulation? Join us this month for a seminar led by Laura Bell Main, our SafeStack Co-Founder and CEO. We will take a look at where compliance fits into your software team, the common requirements and how to engineer your way to a pain-free compliance journey.

45 minutes

Onboarding a SAST tool (with minimal disruption)

We have talked a lot about Static Application Security Testing (SAST). We have discussed what it looks like and how valuable it can be. We have even talked about how these tools can fit into your workflows and pipelines. We know introducing new rituals like SAST to your existing lifecycles can be challenging. There is a bunch of context we need to consider for our own environments, it can be hard to find the path of least resistance and get started without adding excessive amounts of work onto our plates. In this seminar, we step through onboarding a SAST tool in our test app together.

50 minutes

SEMINAR CATALOG

Getting started with AI and Security

he latest tech trend of artificial intelligence (AI) means a lot of us are faced with learning new concepts, like neural network architecture and machine learning models. On top of learning those foundational concepts, many of us have to figure out how to apply these concepts to our jobs (and how to do so securely). It is a lot to learn!
In this seminar, join Erica Anderson (SafeStack Co-Founder and COO) as we set those foundational AI concepts together. We will go through the terminology, share resources you can use and share after, and then highlight the important parts where we need to focus our time on when it comes to security.

40 minutes

AI (eh? aye.) - How did we use it securely?

The Artificial Intelligence (AI) hype is real. It's like the early days of the internet and SaaS all over again! At SafeStack, we were faced with a resource constrained problem to solve, which led us to exploring the use of AI in our production workflow. How did we go about it?

In this seminar, we share our experience, and thought process as we go through trying to use AI securely ourselves. This month's community chat, join Dan Ting, Senior Secure Development Specialist at SafeStack; for a peek behind the curtain, and learn from our experiences.

30 minutes

Secure your things: IoT security for dev teams

This month's community chat, Shaun Bettridge, Secure Development specialist at SafeStack, discusses security as it relates to Internet of Things devices. This seminar is a great topic for the whole development team from software engineers through to product owners and managers who are building, or thinking of building, software for devices in the home, office or jobsite. In this seminar we will discuss some of the intricacies of building and deploying software on IoT devices and the security considerations you and your team should be making.

30 minutes

SEMINAR CATALOG

Intro to Paved Roads and Guardrails

The world of development has embraced DevOps which means we have much more control over every component of the software we build and its infrastructure. It is a lot of work to handle all this responsibility while also making sure we are doing it securely at the same time.

To manage this friction, the community has coined the concept 'paved roads' and 'guardrails' - meant to help teams move fast, reduce friction, and build securely. This month's community chat is focused on understanding what paved roads and guardrails are and what they look like in practice.

60 minutes

Security Metrics 101

All of us strive to make better decisions, right? Often, we dream of having all the data we need at our fingertips so we can make better choices of what to prioritise and what to do, to make most use of our time and resources.Especially for those of us trying to drive better security, we want data to support our case and demonstrate how important it is! What data should we be looking at? What data is unhelpful and distracting?
This month's community seminar is all about security data and metrics. Erica Anderson,, will share some stories of what has helped her and other organizations and will share some advice and pitfalls to avoid.

60 minutes

Utilizing OWASP ASVS as Application Developers

We know that secure development practices are key to the work we do, and alongside that, ensuring a focus on the usability of our work. But sometimes these two things are in tension. Different areas of the business will likely be thinking from different perspectives in what we're trying to achieve and how we get there. That can mean a lot of conflict in these conversations - whether that's around the usability of authentication, unhelpful prompts, or introducing additional risk in third party services. How can we focus on both? Join Laura Bell Main in a conversation about security and usability, including practical outcomes and how we can get there.

44 minutes

How to make friends and influence Security Champions

Communication is one of the bigger (and usually undervalued) skills in security. Researching and understanding a technique or concept is relatively easy compared to getting development team members to adopt new, secure ways of working and building software. There are a lot of different things to consider, and influencing others is hard! Surely that is why Dale Carnegie's 1936 action-book is so popular!

In this seminar, Erica Anderson will talk you through lessons learned from acting as a security champion and helping development teams add security into their workflows.

40 minutes

Dropping the SBOM

Sometimes as software development teams we get caught up in the day-to-day development of our application and forget to look at our software security from a higher level. An SBOM, or software bill of materials, looks at the supply chain of your code. From this perspective you can assess security concerns across the entire code lifecycle with a focus on dependencies and tooling used to build your software app.
In this seminar, Shaun Bettridge, is going to discuss how you can prepare your own SBOM and why this might be useful. We will also explore some technology solutions for improving the security maturity of your software development supply chain.

50 minutes

Planning for Secure DevOps

At the strategic layer, models from NIST, US DoD and ASD are commonly used by CISOs to plan ideal overarching cyber security targets. In the application security space both BSIMM and SAMM are well known approaches that can help define a target state for how to achieve maturity in software security. But what about DevOps practitioners?
This seminar we looked at maturity models and planning frameworks that can help with getting the right amount of security into your DevOps teams and processes. We also looked into OWASP's DevSecOps Maturity Model (DSOMM) and other tools to help you focus on the right things to uplift your DevOps security.

50 minutes

SEMINAR CATALOG

You down with SOP

This seminar we peek under the hood at one of the most critical and complicated security controls in modern web development. The seminar will cover the Same-origin Policy, Cross-origin Resource Sharing, Universal XSS, Site Isolation and more.

50 minutes

Secure Front-End Development

With the mainstream adoption of web based tools, and the advancement of web frameworks and libraries, we expect this trend to continue for the foreseeable future. Securing your web applications has never been more critical.
JavaScript has been around for over 25 years but the JavaScript of today is not that simple browser-based language of yesteryear, used to make rudimentary style changes. Today we take full advantage of the latest web frameworks and libraries to build feature rich web apps. But with all the advances in JS development we need to keep up with security best practices, and that can be difficult, so let us help.

50 minutes

Hands-on Container Security

Many paradigm shifts in computing have occurred in the past ten years. And the explosion of containers may seem like just another technology fad that will fizzle out in time. But it's undeniable that it's difficult to avoid conversations about containers, Kubernetes or other orchestrators when looking to build scalable tech. Join us as we go hands-on with some open source tools to help secure container environments.

This month's seminar, will briefly go over common container and orchestrator risks and how automated technology can help address some of those challenges.

50 minutes

SEMINAR CATALOG

AWS Threat Modeling

In this month's seminar, join Principal Developer Advocate Christian Frichot and Secure Development Specialist Shaun Bettridge. We're going to work together on a threat model for a newly designed solution that's going to be deployed onto the cloud.
We'll decompose the solution, and use some common threat modeling techniques to identify and prioritize security issues that we'll need to focus on. For those that have experience performing threat models, we welcome your assistance! For those that are new to this, the exercise is a great step forward.

56 minutes

GitHub Actions for AppSec

Automating vulnerability identification is one of the north star goals for many DevOps teams. Whether you're looking for vulnerable dependencies, forgotten secrets, or SQL injection there's many open source and commercial offerings out there that can integrate into your code pipelines.
In this month's seminar, join Christian Frichot as he goes hands on with automating common security tasks with open source tools on top of GitHub Actions. Don't worry if you're an Azure DevOps or GitLab user though, many of the examples can be integrated into those platforms too.

52 minutes

Understanding the bug - Log4Shell

The Log4Shell vulnerability, which affected Apache's Log4j Java-based logging utility, gained a lot of attention, and the first thing you might have thought of is “should I worry about this?”.

In this seminar, join us as we talk through the Log4Shell vulnerability and look at it from a development team's perspective.

46 minutes

SEMINAR CATALOG

Detecting security attacks in our software products

We all know that security is an important aspect of building high quality software, and it is a balancing act between having security controls that help us prevent and detect events, versus working at speed. Sometimes we can prevent a security event from happening by making conscious decisions in how we design, develop, and manage our software. And sometimes we just need to be ready to detect and handle an attack.

In this seminar, we discuss how security attacks happen and what your development team can do to detect them.

71 minutes

Measuring your Software Security Maturity

Releasing software products involves many people and teams, often at an increasing velocity,Applying security throughout this process, including having to consider overarching obligations, such as privacy and other regulatory requirements, is a difficult task.

In this seminar, we explain software security maturity models, and how building a measurable plan to elevate the security of your people, processes and technology can help your organization navigate the challenges of embedding security throughout your software development lifecycles.

56 minutes

Preventing Security Nightmares: Account Takeover

Attackers and scammers are always looking for ways to “take over” accounts. Once they assume an identity, they could create havoc in your name. When they do this at scale, they can cause nightmares for your team and leave your organization with a massive product misuse problem. Providing easy, accessible and secure access for your users' legitimate needs is an important part of a modern software product or service.
In this seminar, we explain how these “account takeover attacks” work and how your teams can prepare for this inevitable nightmare to make it a lot less scary.

55 minutes

SEMINAR CATALOG

Get your SAST on

Sometimes, despite our best efforts to avoid them, security vulnerabilities still make their way into our applications. Perhaps you accidentally hard-coded credentials in your code, or maybe your JSON parser is susceptible to denial of service attacks. Static Application Security Testing (SAST) tools can automatically analyze your code to find these (and more) known security vulnerabilities, before they get deployed. In this seminar, we highlight the need for SAST in software development, talk through SAST tools you can use to help find security flaws and how some of these tools can be adopted into a typical software development life cycle.

34 minutes

Security Culture in Business

Join us as we walk through how to introduce and grow a thriving security culture.

During the session, you will have an opportunity to discuss specifics about security culture in your organization, reflect on your understanding of it, and think about possible improvements to your processes.

45 minutes

Breaking the Software Supply Chain

We are starting to see a lot of news and incidents relating to supply chain-related attacks - incidents relating to network management software like SolarWinds, to virtual administrative tools like Kaseya, even Microsoft have accidently signed (or "verified a file as safe") for a malicious driver or two.

In this seminar we talk about where in your lifecycle or workflow supply chain risk can crop up, how to vet this software before we use it, and how you can prepare yourself in case that software pops up in advisories or headlines.

62 minutes

SEMINAR CATALOG

Can You Keep A Secret?

Intuitively, the best way to keep a secret — such as a password or a key — is never to tell it to anybody. Perhaps this is why we're often unprepared when we actually need to share one.

In this seminar, we go through some coping mechanisms to safely share secrets with your applications, servers, and pipelines. In this seminar, we will focus on some coping mechanisms to safely share secrets with your applications, servers, and pipelines.

41 minutes

OWASP, Beyond the Top Ten

You'll hear us talk about the OWASP Top Ten a few times in our courses, but what else does the Open Web Application Security Project have to offer and how can it help you?

In this seminar, we highlight resources, community chapters, online conferences, and other ways you can get involved.

33 minutes

In Dependencies We Trust

As developers, testers, and tech enthusiasts, we depend heavily on code we didn't write and applications we have no control over. Supply chain attacks and security issues through third party applications are a genuine threat that need our focus and attention.

In this seminar, we highlight common security issues the development world is facing today, introduce ways to investigate and analyze Software of Unknown Provenance (otherwise known as SOUP), and highlight dependencies that may be overshadowed by more prominent third party applications.

49 minutes

SEMINAR CATALOG

An AppSec Guide to Incident Response

What is Incident Response? How do we do it? Why do we need to know? Secure code, strong auth, added logging, and practicing social engineering scenarios are all things that can both help mitigate incidents and add a level of preparedness for when the bad things do happen.

In this seminar, we go through what Incident Response is, and how and why development teams can help.

68 minutes

Capture the Fun in your Security Program

Whether you're just starting your security journey or you're well beyond the basics, there's always time for fun when it comes to security learning. Capture the Flag (CTF) is a friendly competition where you search for 'flags' hidden in security flaws or application code.

In this seminar, we cover what CTFs are, how to create your own CTF program, some resources for further learning

65 minutes

The Alphabet of Cloud Security

Do you find yourself 'lost in the clouds' when it comes to cloud solution security? Maybe you're in a complicated cloud migration at the moment, or you're thinking of moving to the cloud in the future and you want to know more about it. It can all be a little overwhelming regardless of where you are in the process. If you could do with some advice and guidance, check out this seminar covering the shared responsibility model, identity and access management, multi-factor authentication, resource monitoring, host-based security, and layers (like WAF, VPN, CDN, and SIEM). Plus, a special appearance from Count von Count.

63 minutes

Level Up Your Personal Security

From work and personal devices to neat third party applications, we walk through achievable actions to take you to the next level with your personal security and OpSec.

46 minutes

Want to know more?

Let’s talk.

Laura Bell Main

laura@safestack.io
@lady_nerd
www.safestack.io