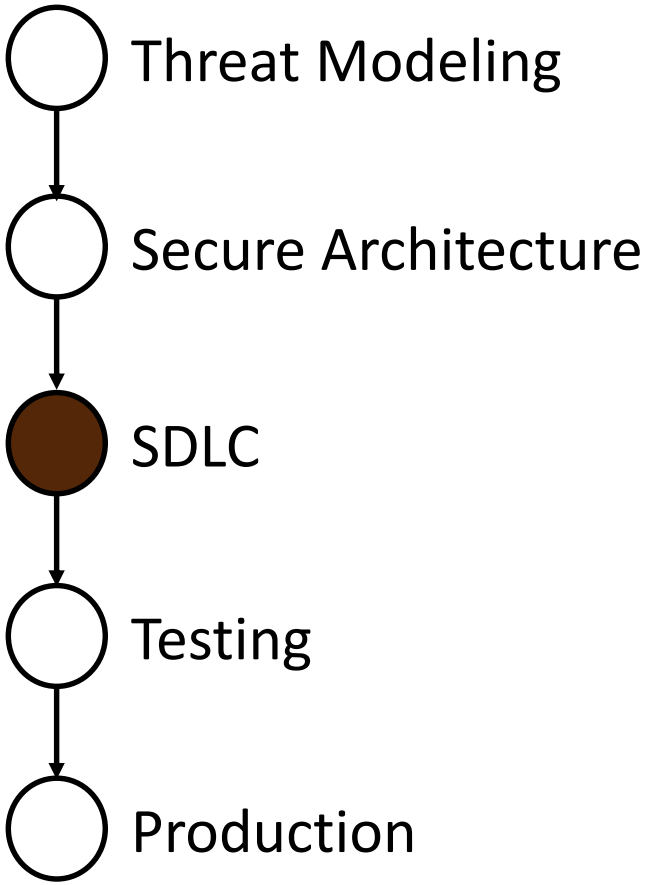
SDLC

Memi Lavi
www.memilavi.com

Secure Architecture Process



SDLC

Be Aware / Recommend

Goal: Integrates security and privacy considerations into the development lifecycle

Participants:
- Architect
- Dev Manager
- Developers
- QA

SDLC

- Secure Development Life Cycle
- Sometimes called just SDL
- Not to be confused with Software Development Lifecycle

What is SDLC?

- A methodology developed by Microsoft in 2002
- Integrates security and privacy throughout all phases of development process
- We'll focus on the development phase

History of SDLC

So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid e-mail-borne viruses. If we discover a risk that a feature could compromise someone's privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services.

- The internet i
- Windows 200
- Windows XP released

ites the

Computing

ting SDLC

Microsoft OSes around the world, causing $635 Million in damages and slows the internet

https://www.wired.com/2002/01/bill-gates-trustworthy-computing/

SDLC Process

- A collection of methodologies and practices to enhance security of software
- Not all of them mandatory
- Not all of them development oriented
- We'll review some of them
- https://www.microsoft.com/en-us/securityengineering/sdl/practices

Practice #1 – Provide Training

- Provide basic security training to everyone in the team
- Not everyone has to be security experts, but everyone must understand the attacker's perspective
- Is a must

Practice #7 – Manage 3rd Party Components

- 3rd party components can present security risks
- Need to manage accurate inventory of 3rd party components in use
- Plan a response when new vulnerabilities are discovered in them

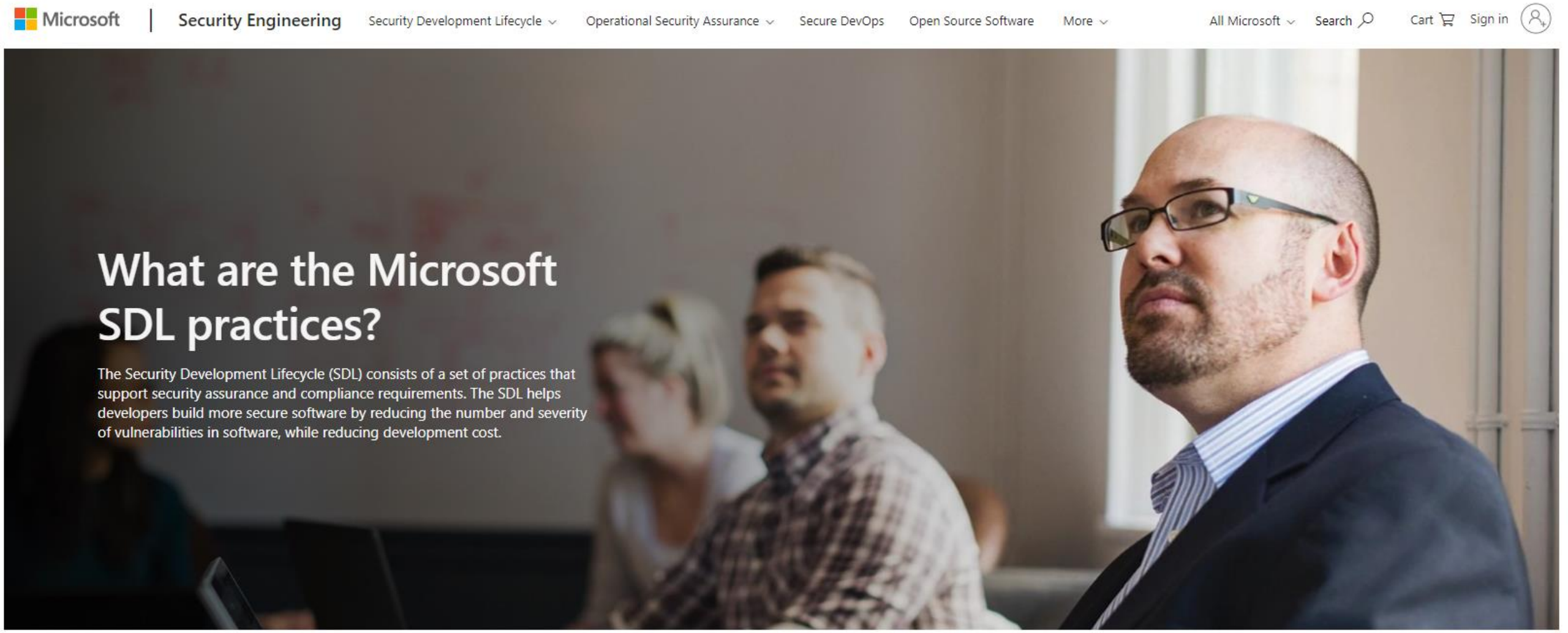
Practice #8 – Use Approved Tools

- Define a list of approved tools to use
- Research risks associated with each tool
- Strive to use the latest version of each tool

Practice #12 – Prepare Standard Response Plan

- Prepare standard incident response plan for addressing new threats
- Should include:
  - Who to contact
  - Protocol for security servicing
- Should be tested

Full SDLC Practices



https://www.microsoft.com/en-us/securityengineering/sdl/practices

SDLC and the Architect

- Must make sure there are trainings for the team
- If there is an active SDLC process in the project – join it
- Work with the team and make sure the secure architecture is implemented
- Be very active in the design and threat modeling phase