Managing Application Risk in Enterprises – Thoughts and Recommendations

Security as a Business Enabler

GLOBAL CAPABILITY.
PERSONAL ACCOUNTABILITY.

Thierry Zoller
Practice Lead EMEA
Threat & Vulnerability Management

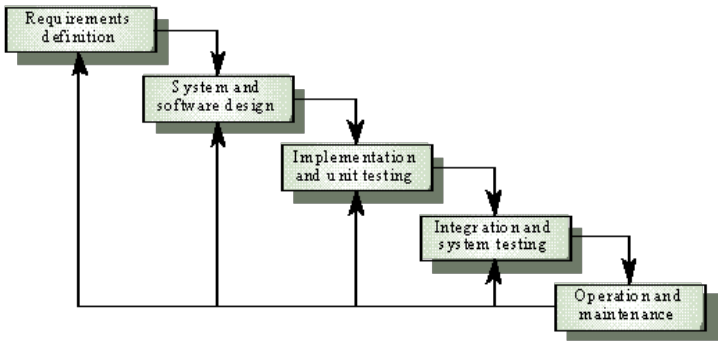
ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

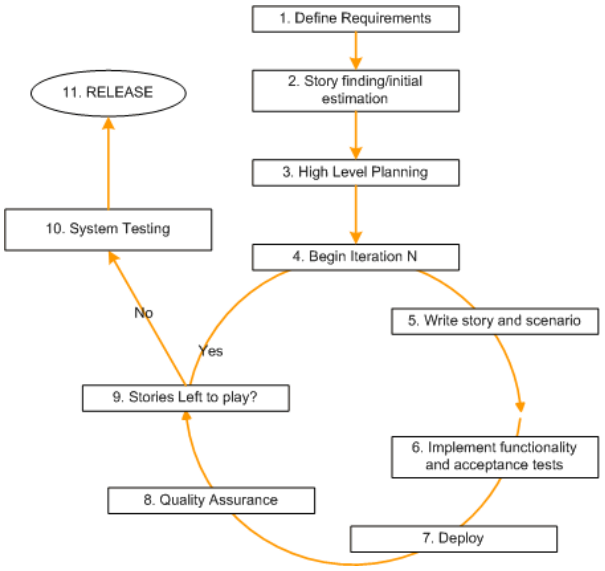
verizonbusiness

Secure Development Lifecycle

Development Lifecycles

- Waterfall Model and Agile Software Development (SCRUM, Devops..)



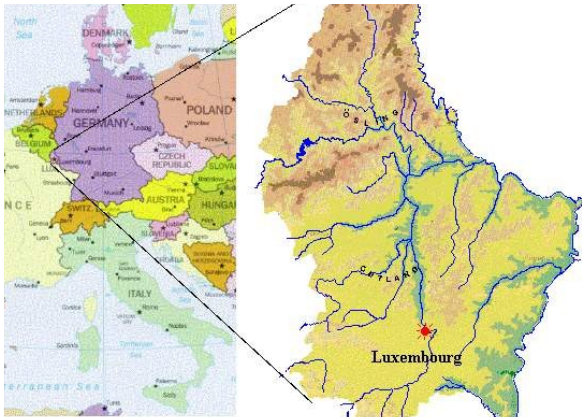


- Others: Spiral Development
- Realistically speaking I have seen a mix all of all of these, with some companies unable to name what type of cycle they use.

Agenda - ברוכים הבאים כולם

Who am I ?

- Thierry Zoller - Luxembourg
- Pratice Lead EMEA for Verizon Business
- Discovered and coordinated over 100 Software vulnerabilities
- ISC2 CSSLP Evangelist
- Former Director of Product Security at n.runs AG



Who is Verizon / Verizon Business ?

- Offices in over 129 countries (overall)
- Data Breach Report (2011 to be out soon)
- Broad consulting services worldwide (GRC, Business Optimisation, Application Security, Forensics ..)
- Over 1100 dedicated security professionals worldwide

WHO IS BEHIND DATA BREACHES?

70%	resulted from external agents (-9%)
48%	were caused by insiders (+26%)
11%	implicated business partners (-23%)
27%	involved multiple parties (-12%)

verizon business

Agenda

What this talk is about

- Different forms of Application Risk Management
- Types of Development Lifcycles
- Get upper management support for an SDLC Program
- Most effective methods to establish such a Program
- Experience Pitfalls / Traps
- How to measure success, which metrics to use

What this talk is **not**

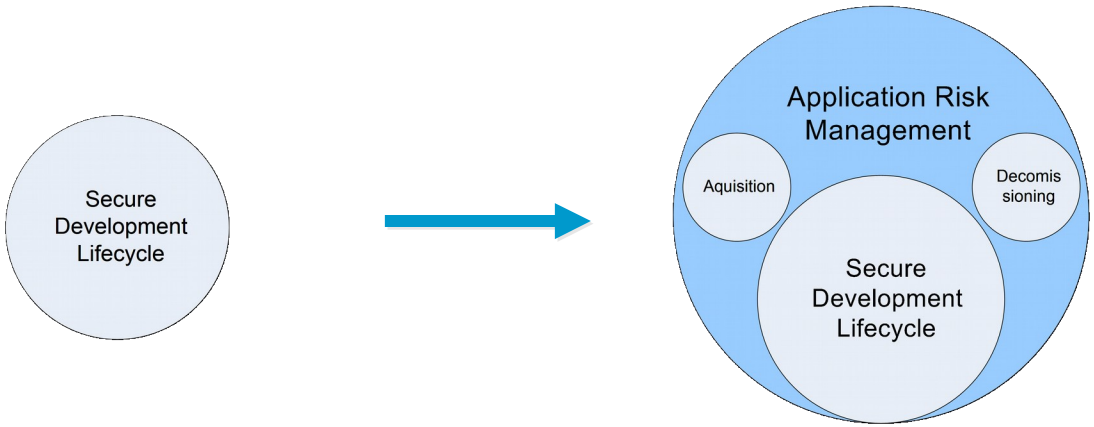
- Review of source code analysis tools
- Reports on effectivness of Penetration Tests or Fuzzing Tools
- Threat modeling or Vulnerabilities
- Sun Tzu

verizon business

Application Risk Management

What is “Application Risk Management”

“The Art of creating, acquiring and maintaining Applications while guaranteeing a defined level of Security Assurance and allowing Risk management to happen ” - Me

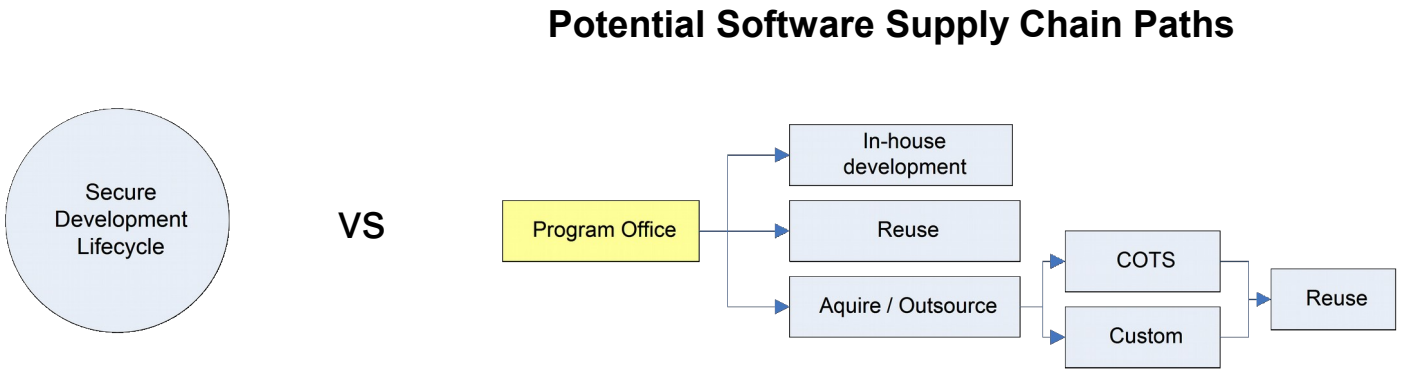


verizon business

Application Risk Management

What is “Application Risk Management”

- Vendor perspective vs. Enterprise



- Encompasses a broader Spectrum
- Assurance needs to be given to all Applications not only those developed in-house

Application Risk Management

An effective Application Risk management Program allows you to answer these types of requests a bit more coherently :

Dear CISO -

- We'd like to open this web application up to the internet ? Can you give us the go ahead ?
- We need to add transactional features to our current HR platform and we still need remote access – what's your advice ?
- We'd like to develop a custom Front Office - Back Office Solution and would need your requirements beforehand.

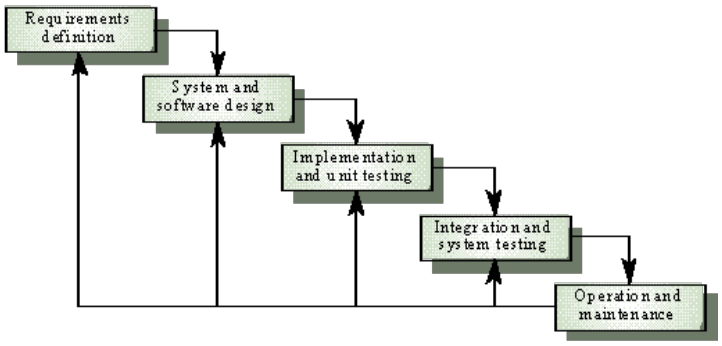
Oh by the way, we need an answer today, we knew since 2 month, but we forgot, hmmk

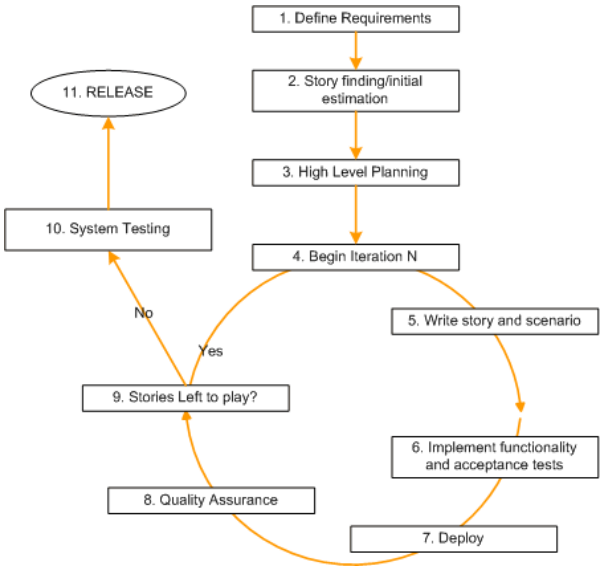
verizon business

Secure Development Lifecycle

Development Lifecycles

- Waterfall Model and Agile Software Development (SCRUM, Devops..)

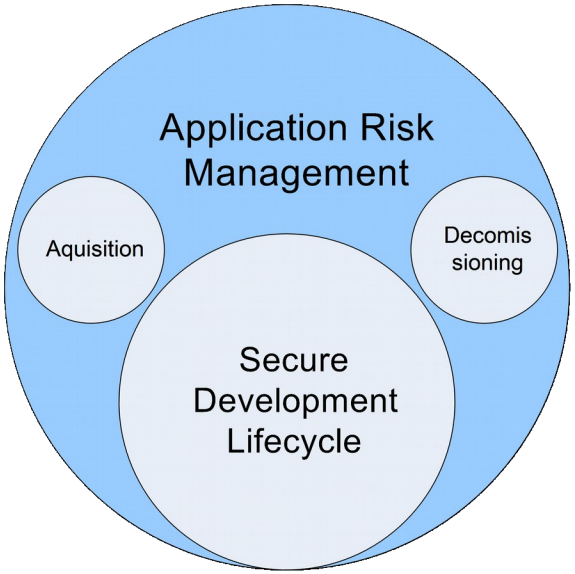




- Others: Spiral Development
- Realistically speaking I have seen a mix all of all of these, with some companies unable to name what type of cycle they use.

Secure Development Lifecycle

Secure Development Lifecycle

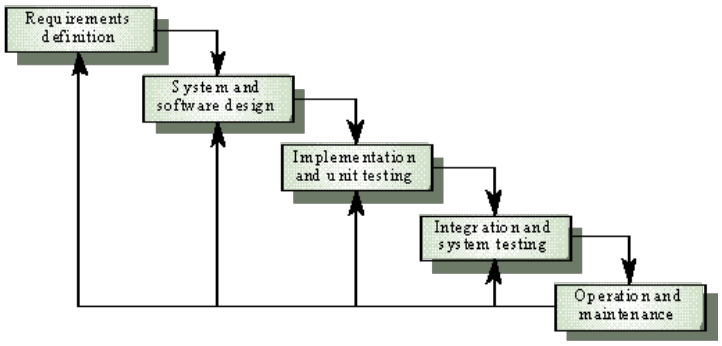


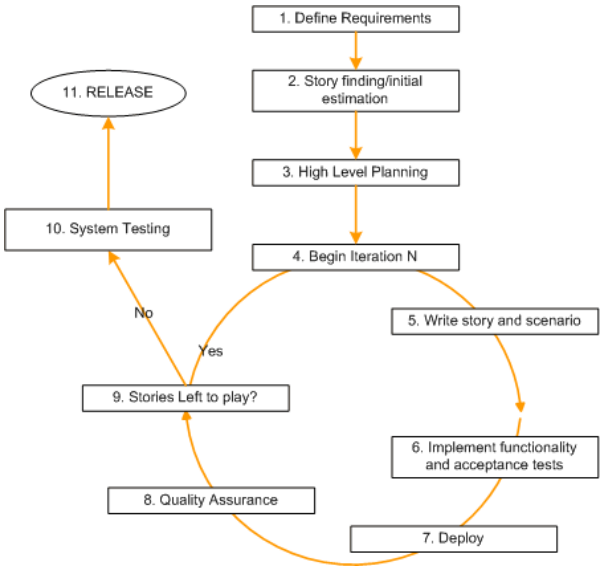
verizon business

Secure Development Lifecycle

Development Lifecycles

- Waterfall Model and Agile Software Development (SCRUM, Devops..)



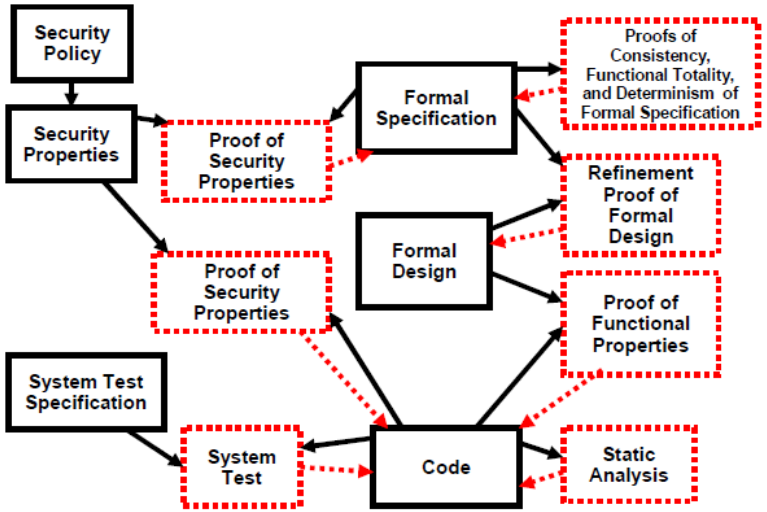


- Others: Spiral Development
- Realisticaly I have seen a mix all of all of these, with some companies unable to name what type of cycle they use.

Secure Development Lifecycle

A Secure Development Lifecycle

- Different shapes and colors - SDL, SDLC, SSDL, Software Assurance
- Types
  - Heavy Processes
    - [Hall 2002a] [NSA 2002, Chapter 3]
    - Clean Room and TSP-Secure
  - Lightweight Processes
    - Microsoft SDL
    - CLASP



Source: DHS

- They are all fine if they fit the needs of your enterprise / organization

Secure Development Lifecycle

A Secure Development Lifecycle

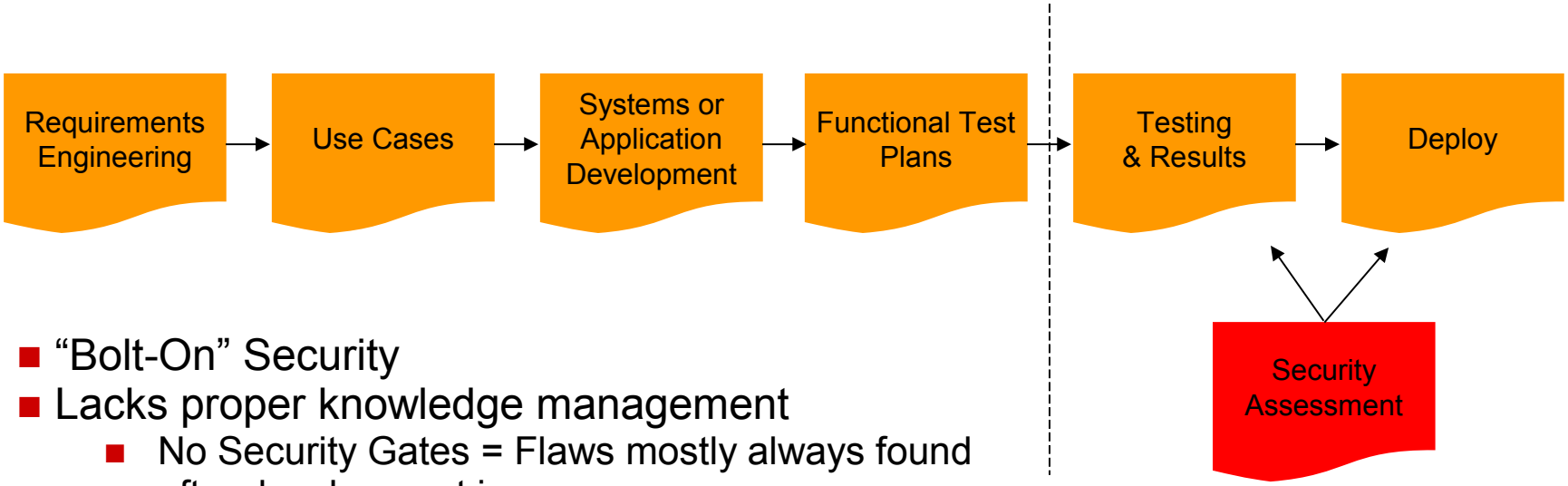
- Good experience with the Microsoft SDL approach
  - Have had good results
  - Is applicable to legacy code, not to heavy, formal and not too light
  - Adjustable to different Development Models (Waterfall, Spiral, RAD)
  - Feeds on years of experience
  - Knowledge and Training is key

- VzB EMEA is in the process of joining the Microsoft SDLPro Network

verizon business

Secure Development Lifecycle

Classical Development Lifecycle



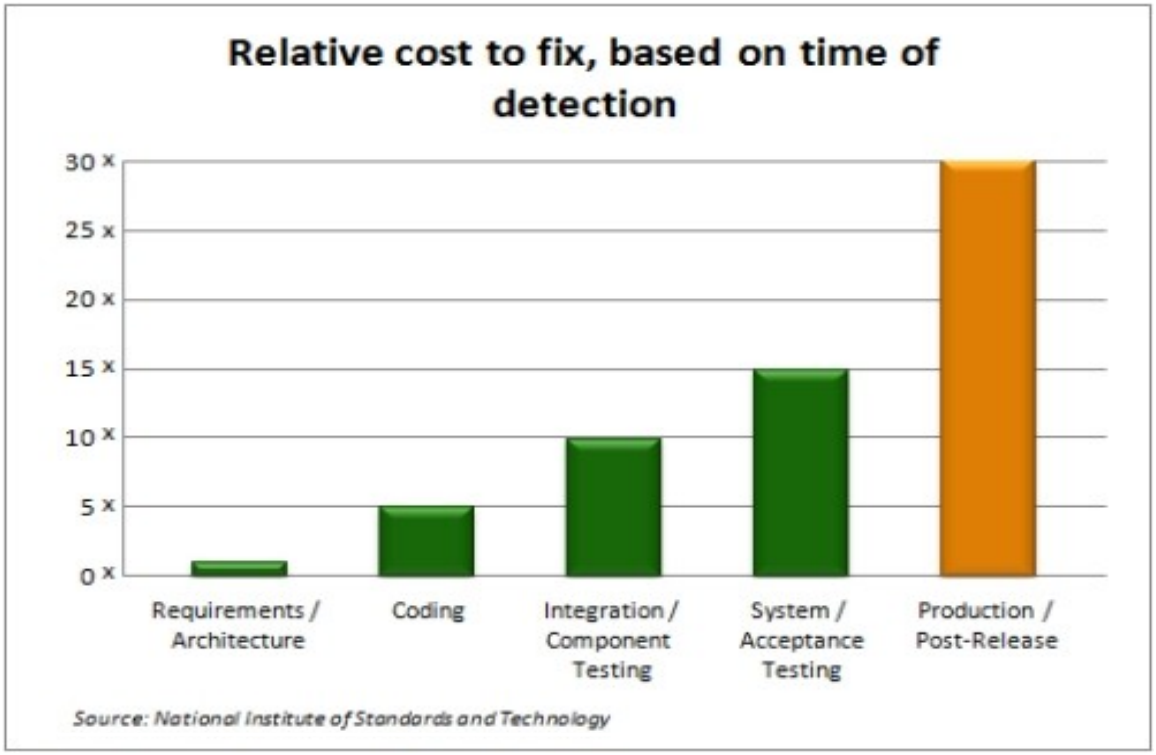
- "Bolt-On" Security
- Lacks proper knowledge management
  - No Security Gates = Flaws mostly always found after development is over
  - No knowledge management
- Risk management near impossible /
- Need to shift security and assurance to the left of the development cycle

verizon business

Agenda

Results in Increase of Costs

- Especially for Vendors, need to react and issue patches
- Major OS vendor calculated 200K USD costs per Bulletin published

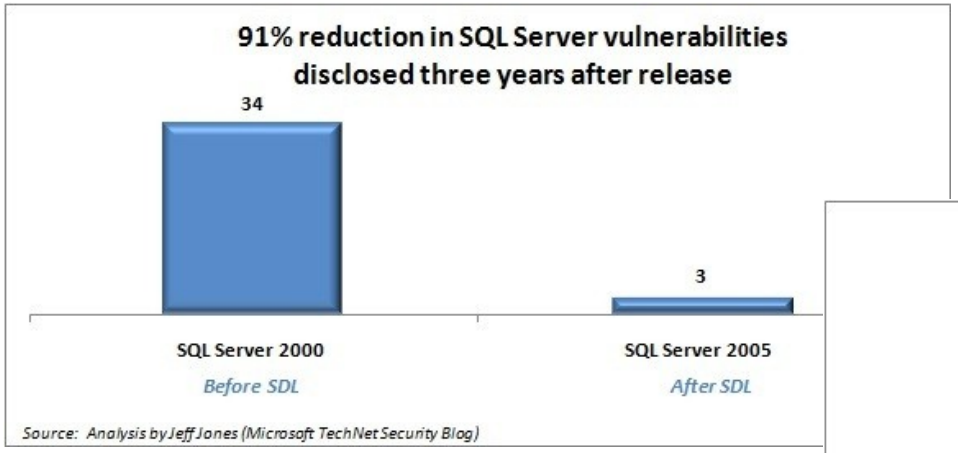


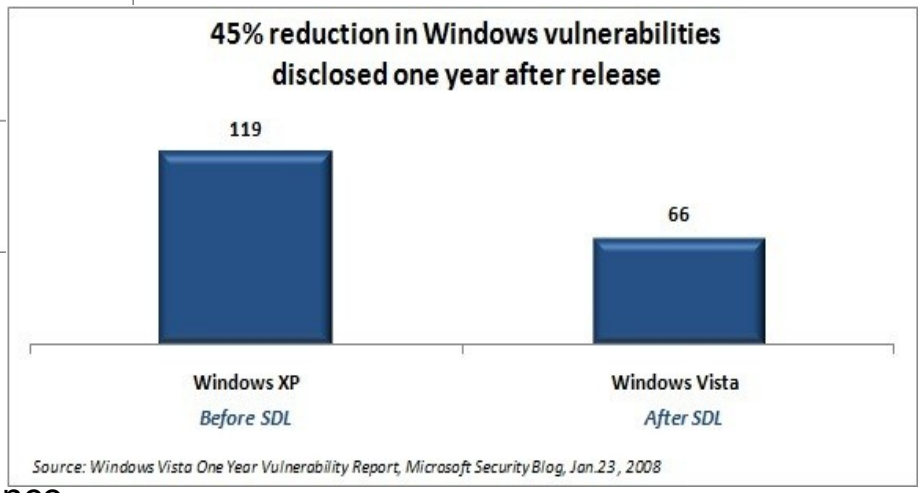
verizon business

Agenda

Results in Increase of Risk

- Statistics from Microsoft



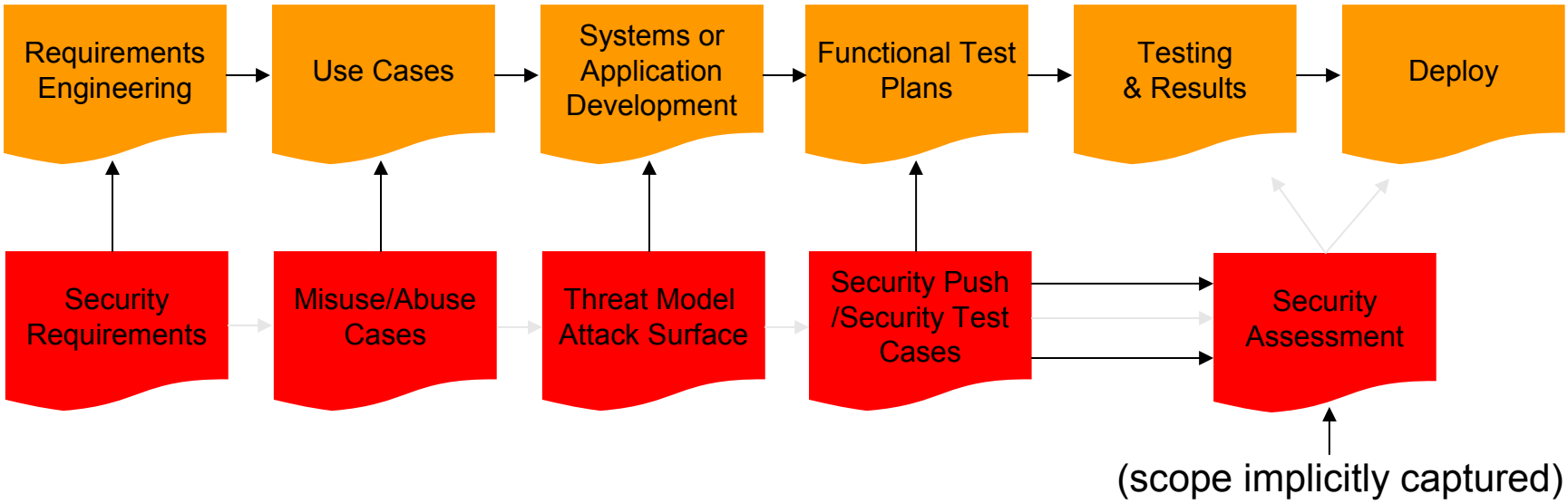


- Summary: Less Risk, Less Cost, Higher assurance – Holy Grail of Security ?

Secure Development Lifecycle

Security build-in Development Lifecycle

- A simplified example



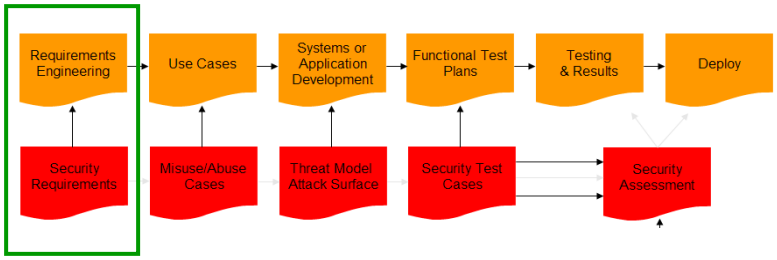
Secure Development Lifecycle

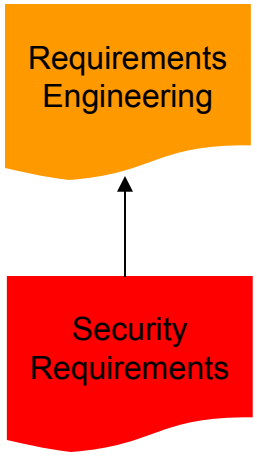
Requirements / Design Phase

- One of the most important phases
- Identify key security objectives
- Security Policies / Compliance
- Data Privacy

- Classify Application into Assurance Groups
  - Example : OWASP ASVS

- No more, “ Oh we needed PCI-DSS compliance ?! , at the end of Development.



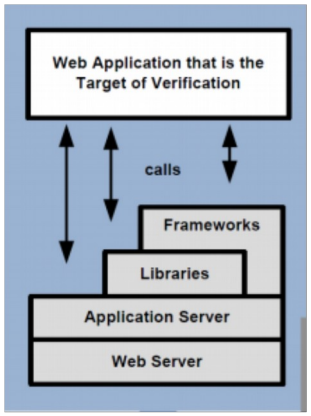
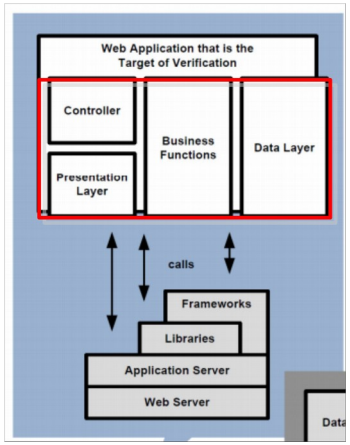
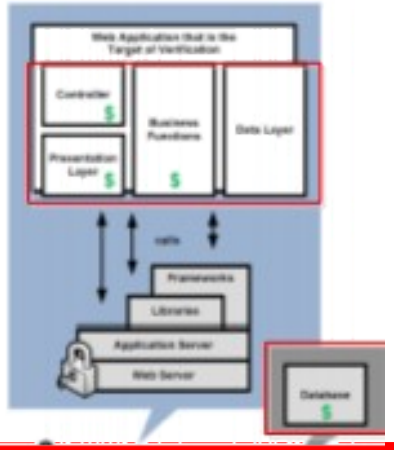
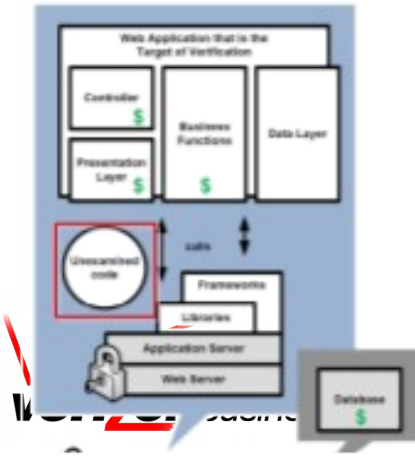


Agenda

Assurance Levels / Example

- Decide what Assurance Level the Application needs to fullfill
- Keeps effort down and effort relative to value of application and data

Generic Example only

	Assurance Level 1	Assurance Level 2	Assurance Level 3	Assurance Level 4
Techniques	Automated Manual (Verification of Automated findings only)	Manual Inspection + Level 1	Source Code Review Database Audit + Level 2	Architectural Review + Level 3
Scope				

Agenda

Assurance Levels / Example

- Decide what Assurance Level the Application needs to fullfill
- Keeps effort down and effort relative to value of application and data

Generic Example only

	Assurance Level 1	Assurance Level 2	Assurance Level 3	Assurance Level 4
Techniques	Automated Manual (Verification of Automated findings only)	Manual Inspection + Level 1	Source Code Review Database Audit + Level 2	Architectural Review + Level 3
Scope	**Provides Assurance against :** Opportunistic Attackers Limitations : **Does not cover application Logic**	**Provides Assurance against :** Unsophisticated **opportunists** such as attackers with **open source attack tools**.	**Provides Assurance against :** **Opportunists**, and **determined attackers** (skilled and motivated attackers focusing on specific targets using tools including purpose-builtscanning tools)	**Provides Assurance against :** Determined Attackers, Professional Attackers – Potentially State founded Attackers

Secure Development Lifecycle

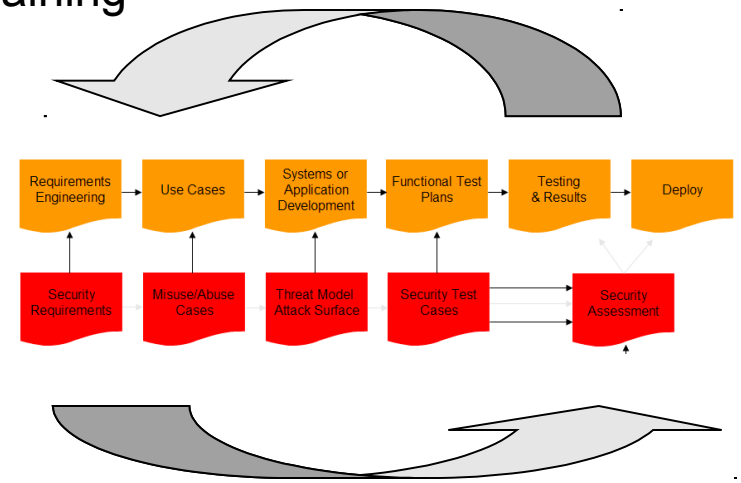
Key concepts

- Initial and *regular* Developer Trainings
- Product Manager / Architect Awareness Training
- Project Kick off Meetings

- Knowledge Base
  - Past issues
  - New vulnerability types / classes
  - Lessons learned

- Feed into :
  - Coding Guidelines
  - Application Security Requirements
  - Design Requirements
  - Coding Guidelines

- Reduced Attack Surface



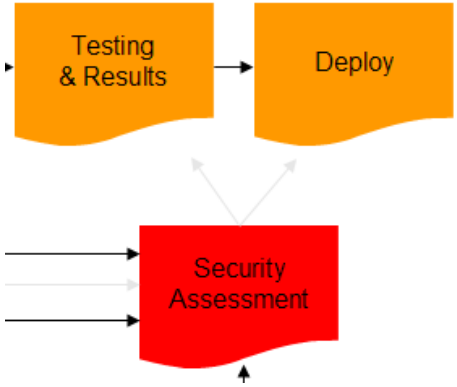
Knowledge management

Secure Development Lifecycle

Signs of Failure of a Secure Development Lifecycle

You are doing it wrong if :

- Simple Bug classes at later stages
  - XSS prior to deploying or in production
  - If your SDL works, there should be no “low hanging fruits”
- Architectural and Design bugs
  - CSRF at a late stage
  - Usually already covered at design/requirements stage



verizon business

Secure Development Lifecycle

Phases and Recommendations

Planning and Requirements

- Incorporate security activities into project plans
- Identify key security objectives
- Consider security feature requirements

Consider need to comply with industry standards and by certification processes such as the Common Criteria

- Consider how the security features and assurance measures of its software will
- integrate with other software likely to be used together with its software

Secure Development Lifecycle

Phases and Recommendations

Design

- Define security architecture and design guidelines
- Document the elements of the software attack surface
- Conduct threat modeling

Implementation

- Apply coding and testing standards
- Apply security-testing tools including fuzzing tools (if appropriate)
- Apply static-analysis code scanning tools
- Conduct code reviews

verizon business

Secure Development Lifecycle

Phases and Recommendations

Verification

- While the software is undergoing beta testing, conduct a “security push” that includes security code reviews beyond those completed in the implementation phase as well as focused security testing
- Not by members of the development team / can be external

Support

- Prepare to evaluate reports of vulnerabilities and release security advisories and updates when appropriate (Incident Handling)
- Conduct a post-mortem of reported vulnerabilities and take action as necessary
- Improve tools and processes to avoid similar future vulnerabilities (knowledge management)

verizon business

Secure Development Lifecycle

Implementing an SDLC Program

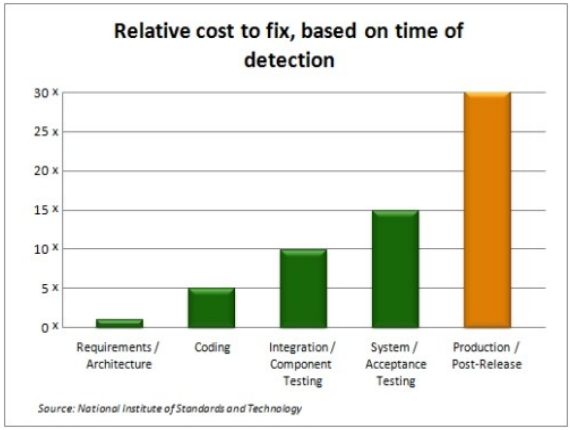
- Most important : Get upper management support
  - **Waste of time trying to implement a program using your budget with limited Senior management backing**
  - Too many stakeholder and political minefields
- Second most important step : Designate an SDLC Evangelist
  - Very important if new to SDLC
  - Responsible for bringing the stakeholders together
  - Monthly senior management meetings (Status, Roadblocks)
  - Can be insourced, should be stress resistant
- Create regular meetings
- Train and motivate
- Get everybody on board
- ….

Agenda

Ideas and Experiences on Budget and Funding

Barriers :

- The name itself “Secure Development Lifecycle “
  - Name is associated to increase in costs and TTM
- Product Management

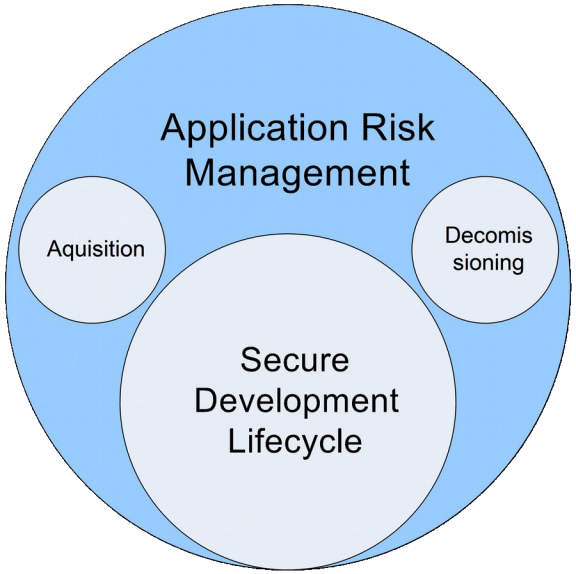


To leverage :

- Focus on Risk and Cost reduction (for once it’s real and we have it)
- Create a few business cases on real examples, use figures
- Compliance (PCI-DSS, you name it)

Application Risk Management

Aquisition



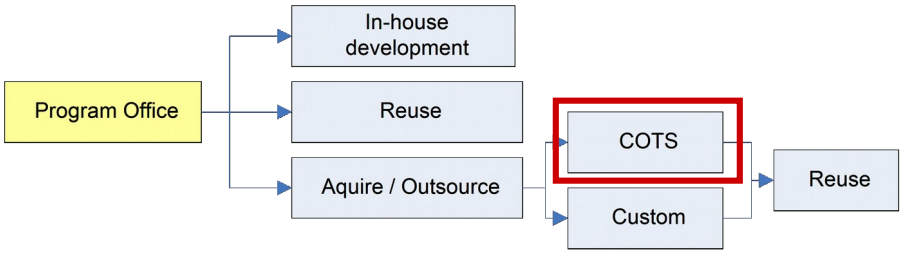
Aquisition

Building Security into the Aquisition Process

Due Diligence Questionnaires / Checklists

Should include :

- Security Track Record
- Financial History and Status
- Software Security Training and Awareness
- Development Process Management
- Foreign influences and interests



- Complete check list can be found :

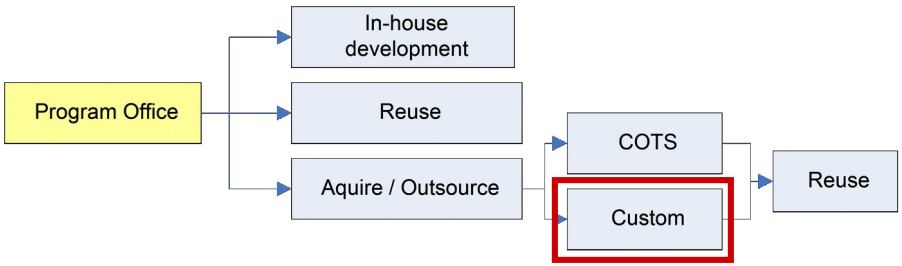
"Software Assurance in Acquisition: Mitigating Risks to the Enterprise"

Aquisition

Building Security into the Aquisition Process

Contractually require a Secure Development Lifecycle

- OWASP and US-CERT offer a template
- Visit them and have them show their Development Processes



- Make them liable as far as possible
- Don't forget the Sustainment (or Post-release Support)

- Require them to be audited by a trusted auditor
  - Audit in the large sense

verizon business

Agenda

Thank you

תודה לכם