



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÀI GIẢNG MÔN
AN TOÀN ỨNG DỤNG WEB & CSDL
CHƯƠNG 4 – BẢO MẬT
TRONG PHÁT TRIỂN & TRIỂN KHAI
ỨNG DỤNG WEB

Giảng viên:

Điện thoại/E-mail:

Bộ môn:

TS. Hoàng Xuân Dậu

dauhx@ptit.edu.vn

Khoa An toàn thông tin

NỘI DUNG CHƯƠNG 4

1. Đặt vấn đề
2. Thiết kế ứng dụng web an toàn
3. Xây dựng ứng dụng web an toàn
4. Đánh giá bảo mật ứng dụng
5. 10 lời khuyên trong thiết kế, phát triển và triển khai ứng dụng web an toàn

Đặt vấn đề

- ❖ Các ứng dụng web (website) là một trong các loại ứng dụng được sử dụng phổ biến nhất:
 - Facebook
 - Gmail
 - Tweeter
 - Google Search,...
- ❖ Các ứng dụng web là đối tượng của một lượng rất lớn các dạng tấn công đánh cắp thông tin, tấn công phá hoại:
 - Tấn công DoS/DDoS
 - Tấn công XSS
 - Tấn công chèn mã SQL,...

Các vấn đề bảo mật/lỗ hổng trong ứng dụng web

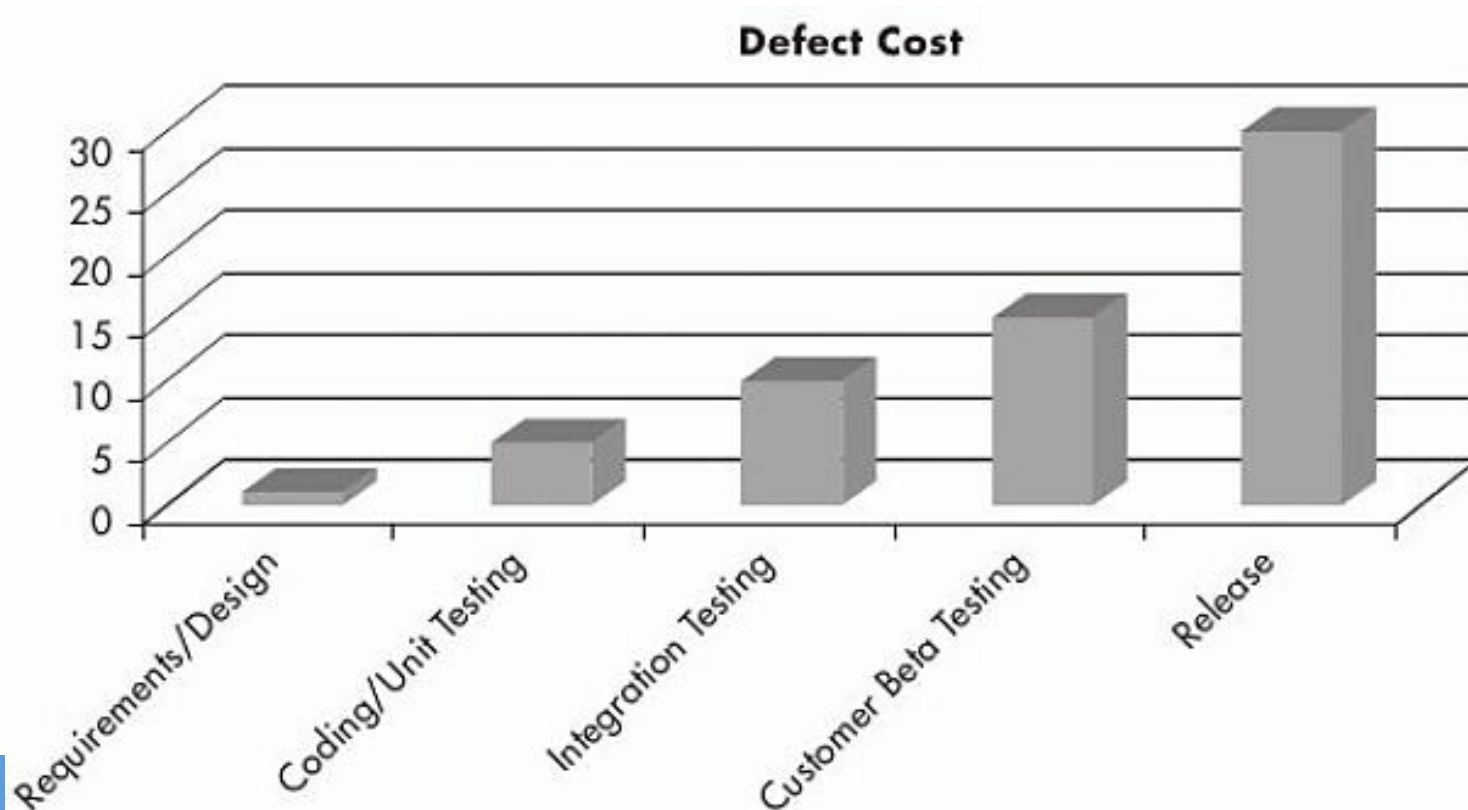
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Đặt vấn đề

- ❖ Các biện pháp bảo mật cần được thực hiện trong suốt vòng đời ứng dụng web:
 - Trong giai đoạn phát triển & triển khai
 - Phân tích
 - Thiết kế
 - Lập trình
 - Kiểm thử
 - Triển khai
 - Bảo trì
 - Trong quá trình hoạt động
 - Giám sát
 - Vá lỗi
 - Nâng cấp,...

Đặt vấn đề

- ❖ Các giải pháp bảo mật được thực hiện ở các giai đoạn sớm của vòng đời ứng dụng web cho hiệu quả càng cao và tiết kiệm chi phí.



Bảo mật trong phát triển ứng dụng web

- ❖ Các hướng tiếp cận bảo mật ứng dụng web
 - Hướng “Thâm nhập và vá” (penetrate and patch)
 - Hướng tiếp cận toàn diện
- ❖ Các mô hình phát triển ứng dụng web an toàn
 - MSDL
 - CLASP
 - SAMM
 - BSIMM

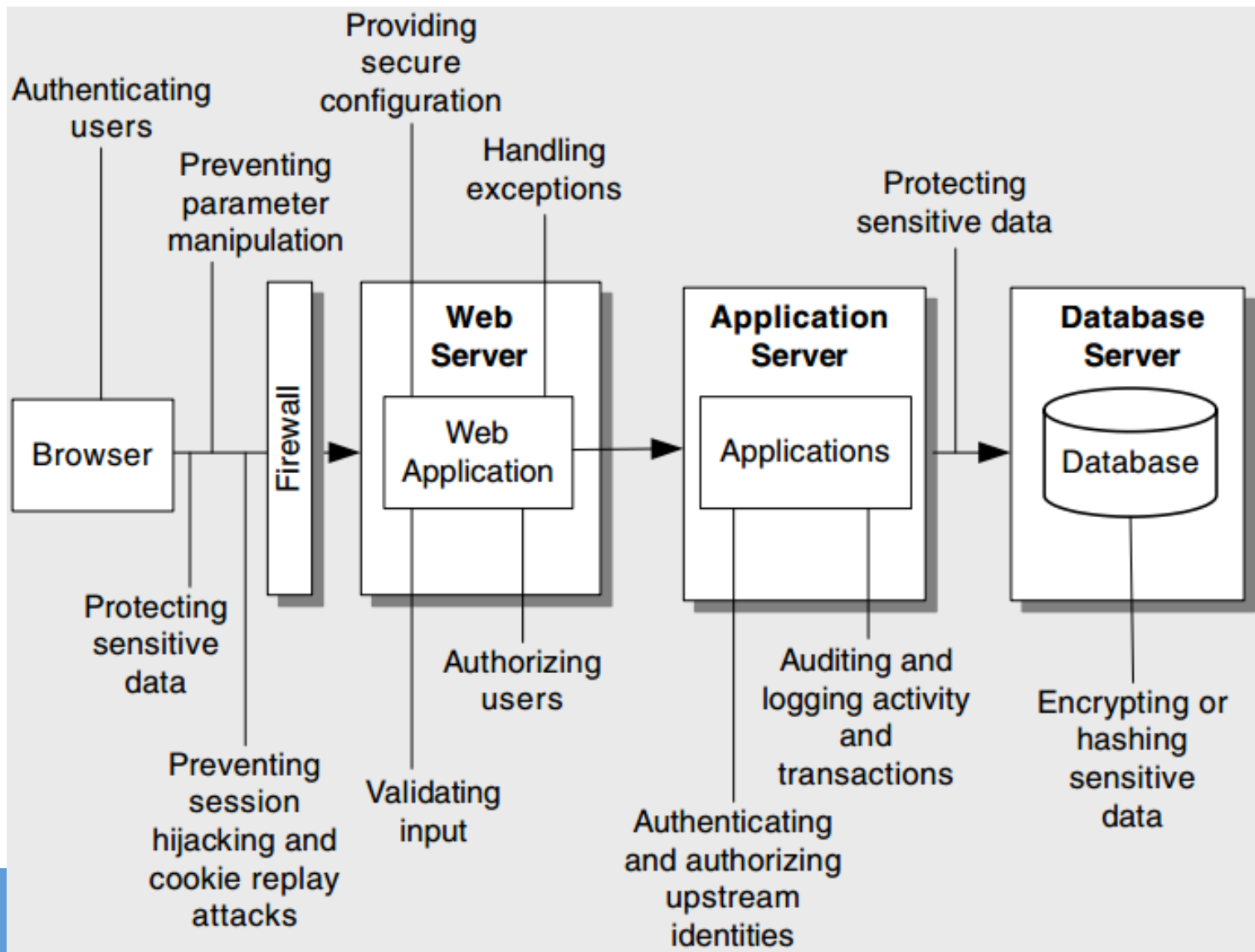
Thiết kế ứng dụng web an toàn

- ❖ Các định hướng thiết kế ứng dụng web an toàn
- ❖ Đánh giá kiến trúc và thiết kế ứng dụng web an toàn

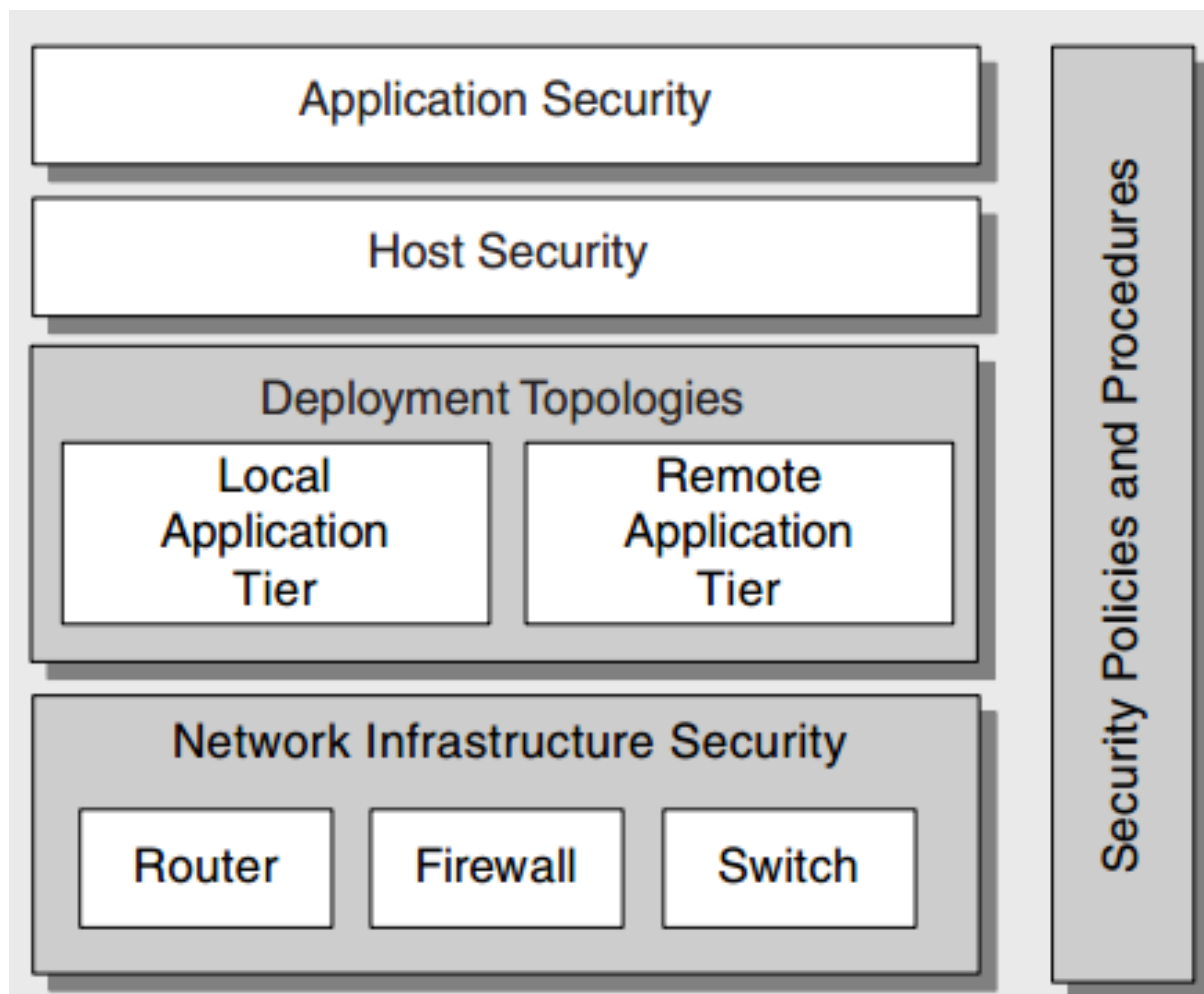
Các định hướng thiết kế ứng dụng web an toàn

- ❖ Các vấn đề đối với kiến trúc và thiết kế ứng dụng web
- ❖ Các vấn đề bảo mật khi triển khai
- ❖ Các định hướng thiết kế ứng dụng web an toàn

Các vấn đề đối với kiến trúc và thiết kế ứng dụng web



Các vấn đề bảo mật khi triển khai



Các định hướng thiết kế ứng dụng web an toàn

- ❖ Vấn đề kiểm tra đầu vào
- ❖ Vấn đề xác thực
- ❖ Trao quyền
- ❖ Quản lý cấu hình
- ❖ Các dữ liệu nhạy cảm
- ❖ Quản lý phiên
- ❖ Xử lý các tham số
- ❖ Mã hóa
- ❖ Quản lý các ngoại lệ
- ❖ Kiểm toán và ghi logs

Các định hướng thiết kế ứng dụng web an toàn

❖ Vấn đề kiểm tra đầu vào

- Không tin tưởng đầu vào từ người dùng
- Xem xét thực hiện kiểm tra tập trung
- Không chỉ dựa vào việc kiểm tra ở client side
- Tối thiểu cần kiểm tra kiểu, kích thước, định dạng và phạm vi

❖ Xác thực

- Chia website thành các phần theo quyền truy nhập (khách, thành viên và quản trị,...)
- Sử dụng mật khẩu mạnh
- Không lưu mật khẩu ở dạng rõ
- Sử dụng SSL/TLS

Các định hướng thiết kế ứng dụng web an toàn

❖ Trao quyền

- Cấp quyền tối thiểu cho tài khoản người dùng
- Xem xét cấp quyền ở mức chi tiết
- Thực hiện tách các đặc quyền
- Hạn chế người dùng truy cập đến tài nguyên hệ thống cấp.

❖ Quản lý cấu hình

- Sử dụng các tài khoản với quyền tối thiểu chạy các dịch vụ và tiến trình
- Không lưu thông tin tài khoản ở dạng rõ
- Sử dụng các biện pháp xác thực và cấp quyền “mạnh” ở phần quản trị
- Sử dụng kênh truyền thông bảo mật cho phần quản trị
- Tránh lưu các thông tin nhạy cảm trong không gian web.

Các định hướng thiết kế ứng dụng web an toàn

❖ Các dữ liệu nhạy cảm

- Tránh lưu trữ các khóa
- Mã hóa các dữ liệu nhạy cảm cần truyền
- Sử dụng kênh truyền thông bảo mật
- Sử dụng các biện pháp kiểm soát truy nhập mạnh với các dữ liệu nhạy cảm
- Không lưu các dữ liệu nhạy cảm trong các cookie cố định
- Tránh gửi dữ liệu nhạy cảm sử dụng HTTP-GET

Các định hướng thiết kế ứng dụng web an toàn

❖ Quản lý phiên

- Đặt thời gian làm việc cho phiên
- Sử dụng kênh truyền thông bảo mật
- Mã hóa nội dung của các cookie dùng cho xác thực
- Bảo vệ trạng thái phiên chống truy nhập trái phép

❖ Xử lý các tham số

- Mã hóa các cookie nhạy cảm
- Không tin tưởng các trường mà người dùng có thể xử lý
- Kiểm tra tất cả các dữ liệu từ người dùng

Các định hướng thiết kế ứng dụng web an toàn

❖ Mã hóa

- Không nên sử dụng các mô đun mã hóa tự phát triển. Nên sử dụng các mô đun có sẵn trên các nền tảng đã được test kỹ
- Sử dụng thuật toán và khóa phù hợp
- Nên thay đổi khóa định kỳ
- Lưu khóa ở các vị trí an toàn

❖ Quản lý các ngoại lệ

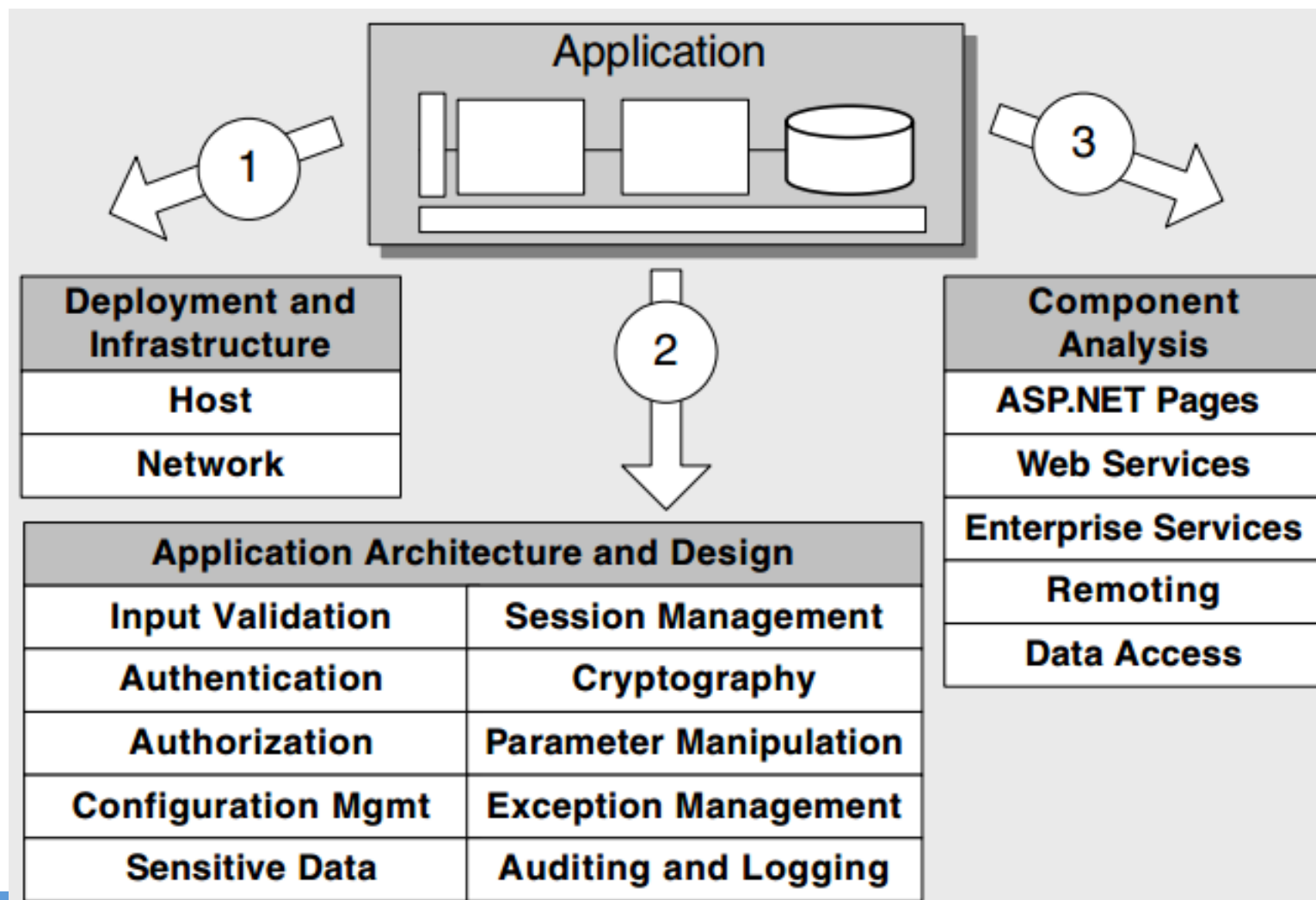
- Sử dụng kỹ thuật xử lý ngoại lệ có cấu trúc
- Không tiết lộ các chi tiết nhạy cảm về ứng dụng
- Không ghi logs các dữ liệu nhạy cảm như mật khẩu
- Xem xét sử dụng khung quản lý ngoại lệ tập trung

Các định hướng thiết kế ứng dụng web an toàn

❖ Kiểm toán và ghi logs

- Nhận dạng các hành vi đáng ngờ
- Cần xác định mẫu lưu lượng bình thường
- Kiểm toán và ghi logs ở tất cả các lớp của ứng dụng
- Cần giới hạn truy nhập đến file log
- Sao lưu và phân tích thường xuyên các file logs.

Đánh giá kiến trúc và thiết kế ứng dụng web an toàn



Đánh giá bảo mật ứng dụng

- ❖ Xem xét/đánh giá mã nguồn
- ❖ Xem xét/đánh giá việc triển khai

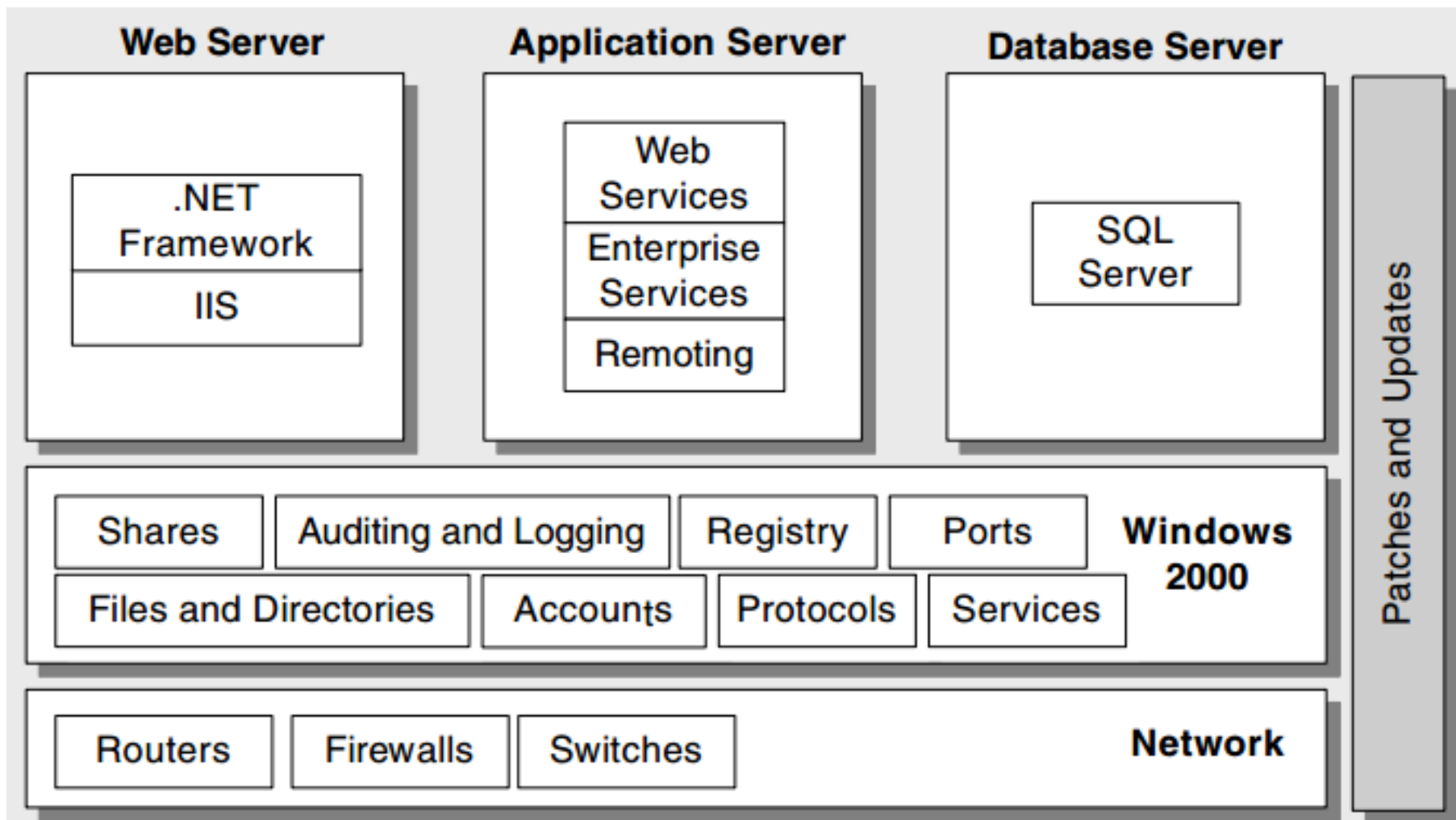
Xem xét/đánh giá mã nguồn

- ❖ Thực hiện tìm kiếm các chuỗi trong mã nguồn
 - Tìm các chuỗi được hard-coded
 - Sử dụng các công cụ
- ❖ Tìm kiếm lỗ hổng XSS
- ❖ Tìm kiếm lỗ hổng chèn mã SQL
- ❖ Tìm kiếm lỗ hổng tràn bộ đệm
- ❖ Xem xét mã truy cập dữ liệu

Xem xét/đánh giá việc triển khai

- ❖ Xem xét cấu hình máy chủ nền
- ❖ Xem xét cấu hình máy chủ web
- ❖ Xem xét cấu hình ứng dụng web
- ❖ Xem xét cấu hình máy chủ CSDL
- ❖ Xem xét cấu hình mạng.

Xem xét/đánh giá việc triển khai



10 lời khuyên cho thiết kế, phát triển & triển khai ứng dụng web an toàn (MS Platform)

1. Không bao giờ tin tưởng các đầu vào trực tiếp từ người dùng
2. Các dịch vụ không nên được cấp quyền hệ thống hoặc quản trị
3. Thực hiện các thực tế tốt nhất về máy chủ SQL
4. Cần có biện pháp bảo vệ các tài nguyên
5. Có các tính năng Kiểm toán, Ghi logs và Báo cáo
6. Phân tích mã nguồn
7. Triển khai các thành phần theo nguyên tắc “Phòng vệ nhiều lớp”
8. Tắt các thông báo lỗi chi tiết đến người dùng
9. Nắm được 10 quy tắc quản trị bảo mật
10. Có kế hoạch phản ứng với sự cố mất ATTT

Không bao giờ tin tưởng các đầu vào trực tiếp từ người dùng

- ❖ Tất cả các dữ liệu đầu vào từ người dùng cần được kiểm tra cẩn thận
 - Tối thiểu phải kiểm tra kích thước, kiểu, định dạng và phạm vi
- ❖ Một số lưu ý:
 - Xem xét vấn đề an toàn khi thiết kế ứng dụng
 - Phân tích/đánh giá các rủi ro, nguy cơ đối với ứng dụng
 - Đưa ra các biện pháp phòng chống từ khâu thiết kế.
 - Không chỉ dựa vào việc kiểm tra các dữ liệu đầu vào từ người dùng ở phía client
 - Cần kiểm tra lại dữ liệu tại mỗi lớp/mỗi thành phần của ứng dụng
 - Không giả thiết không xuất hiện tấn công từ bên trong.

Các dịch vụ không nên được cấp quyền hệ thống hoặc quản trị

- ❖ Sử dụng các tài khoản quản trị hoặc hệ thống để chạy các dịch vụ có thể dẫn đến các hậu quả nghiêm trọng;
 - Tin tặc có thể chiếm quyền điều khiển hệ thống khi khai thác thành công lỗi của ứng dụng/dịch vụ.
- ❖ Các lưu ý:
 - Các dịch vụ & UD web chỉ được chạy với người dùng có quyền tối thiểu;
 - Sử dụng Domain User Account cho các truy nhập giữa các máy
 - Không cho phép các tài khoản dịch vụ được đăng nhập trực tiếp trên console hoặc từ xa.
 - Thay đổi mật khẩu định kỳ.

Thực hiện các thực tế tốt nhất về máy chủ MS SQL

- ❖ Máy chủ CSDL là một thành phần rất quan trọng của ứng dụng web.
- ❖ Một số lưu ý:
 - Không sử dụng tài khoản ngầm định SA
 - Sử dụng Roles và Logins để điều khiển truy nhập vào SQL Server
 - Cấm các tài khoản dịch vụ (service account) truy nhập trực tiếp các bảng dữ liệu
 - Sử dụng thủ tục với các câu truy vấn tham số hóa
 - Sử dụng Microsoft SQL Server Best Practices Analyzer để kiểm tra kép.

Cần có biện pháp bảo vệ các tài nguyên

- ❖ Cần có các biện pháp bảo vệ các tài nguyên một cách phù hợp (CPU time, băng thông, dữ liệu người dùng,...)
- ❖ Lưu ý:
 - Bảo vệ các khóa mật mã
 - Cần có các biện pháp bảo vệ các khóa mật mã, như sử dụng các hệ thống phần cứng (Hardware Security Module), hay mô đun phần mềm như Data Protection API,...
 - Bảo vệ các thông tin tài khoản dịch vụ
 - Bảo vệ dữ liệu cá nhân của người dùng

Có các tính năng Kiểm toán, Ghi logs và Báo cáo

- ❖ Các tính năng Kiểm toán, Ghi logs và Báo cáo không chỉ cung cấp thông tin để phân tích và đo kiểm ứng dụng web, mà chúng cũng rất cần thiết cho vận hành và cho đội phản ứng sự cố.
- ❖ Lưu ý:
 - Giữ cho dữ liệu logs an toàn
 - Lưu bản ghi lịch sử
 - Ký dữ liệu logs, đảm bảo cho chúng ko bị sửa đổi
 - Thu thập và tập trung hóa dữ liệu

Phân tích mã nguồn

- ❖ Mã nguồn cần được phân tích, đánh giá về an ninh để tìm các nguy cơ và các lỗ hổng tiềm tàng.
 - Có thể thực hiện thủ công hoặc sử dụng các công cụ tự động.
- ❖ Lưu ý:
 - Cần phân tích mã nguồn và sửa các lỗi phát hiện được
 - Kiểm tra khả năng xuất hiện lỗi tràn bộ đệm, tràn số nguyên
 - Kiểm tra khả năng xuất hiện lỗi XSS
 - Tìm và kiểm tra các hàm nguy hiểm/rủi ro cao
 - Sử dụng các công cụ quét tự động

Triển khai các thành phần theo nguyên tắc “Phòng vệ nhiều lớp”

- ❖ Nguyên tắc “Phòng vệ nhiều lớp” không chỉ được áp dụng cho toàn hệ thống mà nên được áp dụng cho cả các thành phần.
- ❖ Lưu ý:
 - Nên sử dụng kiến trúc 2 lớp hoặc 3 lớp cho các ứng dụng web
 - VD: CSDL không nên được kết nối trực tiếp từ Internet
 - Sử dụng SSL/TLS
 - Sử dụng tường lửa, phân đoạn mạng và danh sách kiểm soát truy nhập ở những vị trí có thể
 - Xem xét mã hóa lưu lượng mạng back-end.

Tất các thông báo lỗi chi tiết đến người dùng

- ❖ Các thông báo lỗi chi tiết có thể cung cấp nhiều thông tin hữu ích cho tin tặc.
 - Ngoài ra, việc hiển thị lỗi chi tiết có thể gây hoang mang, mất tin tưởng ở dịch vụ.
- ❖ Lưu ý:
 - Thiết lập ứng dụng web chỉ thông báo lỗi chi tiết cho hệ thống cục bộ
 - Không hiển thị báo lỗi chi tiết khi ứng dụng đã được triển khai
 - Gửi thông báo lỗi đến back-end (ghi logs,...)
 - Sử dụng các cơ chế báo lỗi thân thiện với người dùng, nhưng không cung cấp thông tin cho tin tặc
 - Giám sát các dấu hiệu của tấn công.

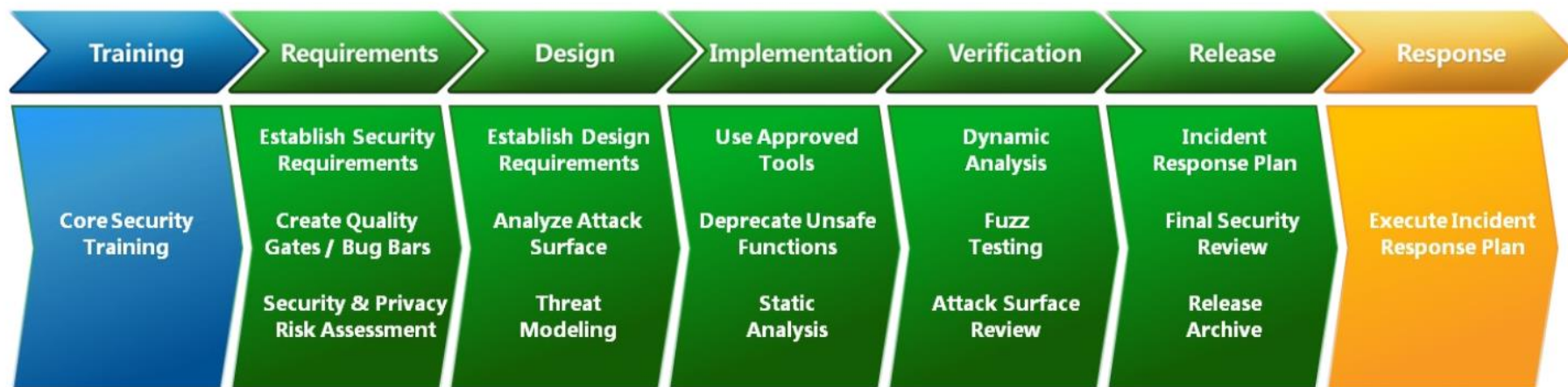
Nắm được 10 quy tắc quản trị bảo mật

1. Không ai biết được điều xấu xảy ra cho đến khi nó xảy ra
2. Các biện pháp bảo mật chỉ hiệu quả nếu dễ sử dụng/áp dụng
3. Nếu bạn không luôn cập nhật các bản vá, mạng của bạn sẽ không thuộc về bạn lâu dài
4. Việc cập nhật các bản vá an ninh cho một máy tính sẽ không hiệu quả nếu nó không được quản trị an toàn từ đầu
 - Sử dụng mật khẩu quản trị yếu, cho phép tài khoản guest,...
5. Luôn cảnh giác là cái giá của an ninh (luôn cần giám sát,...)
6. Có ai đó bên ngoài cố gắng đoán mật khẩu của bạn
7. Mạng an toàn nhất là mạng được quản trị tốt
8. Mạng khó quản trị khi càng phức tạp
9. An ninh không phải là tránh rủi ro mà nó là quản lý rủi ro
10. Công nghệ/kỹ thuật không phải là thuốc chữa bách bệnh.

Có kế hoạch phản ứng với sự cố mất ATTT

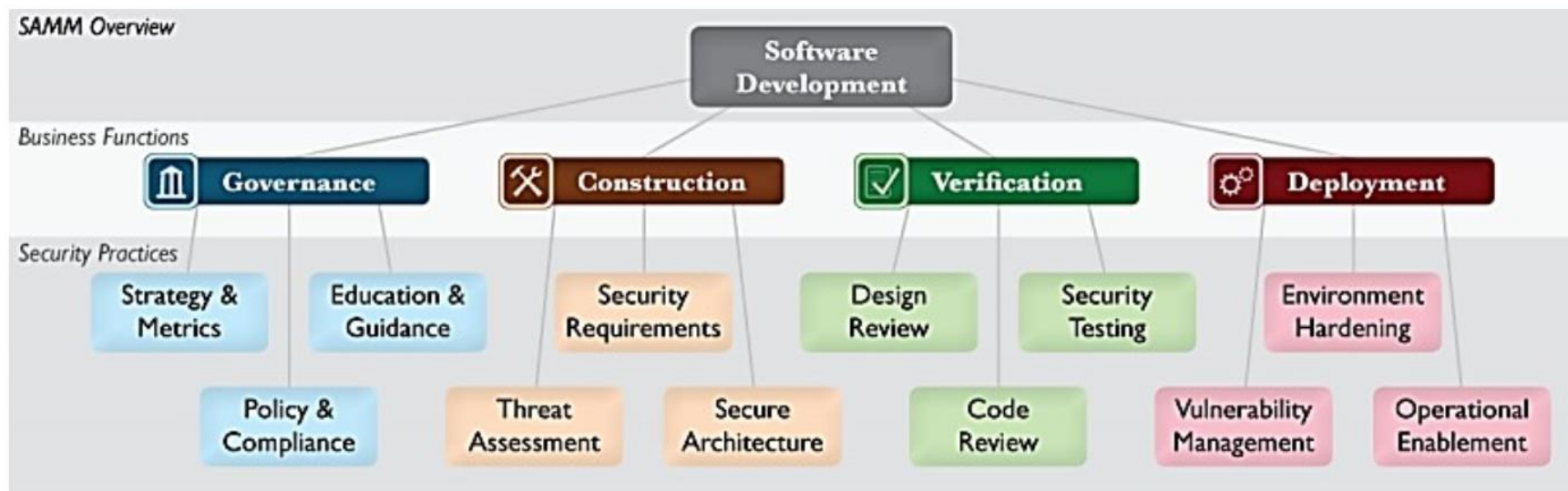
- ❖ Cần có kế hoạch cụ thể cho phản ứng với sự cố mất ATTT:
 - Mỗi sự cố có cần có một kế hoạch phản ứng cụ thể.
- ❖ Lưu ý:
 - Cần biết phải gọi điện cho ai?
 - Hy vọng cho điều tốt nhất, chuẩn bị cho điều xấu nhất
 - Thực hiện xử lý sự cố theo kế hoạch đã đề ra
 - Phân tích/đánh giá sau sự cố
 - Kết hợp các phản hồi và bài học kinh nghiệm từ sự cố và xử lý sự cố.

Các mô hình và phương pháp phát triển phần mềm an toàn



Các pha của Microsoft Security Development Lifecycle

Các mô hình và phương pháp phát triển phần mềm an toàn



Hình 4.5. Cấu trúc của mô hình OWASP SAMM

Governance

Assessment worksheet

Strategy & Metrics

SCORE

0.0

0.2

0.5




1.0

♦ Is there a software security assurance program in place?	No	<1 YR	>1 YR	MATURE
♦ Are development staff aware of future plans for the assurance program?	No	SOME	HALF	MOST
♦ Do the business stakeholders understand your organization's risk profile?	No	SOME	HALF	MOST
♦ Are many of your applications and resources categorized by risk?	No	SOME	HALF	MOST
♦ Are risk ratings used to tailor the required assurance activities?	No	SOME	HALF	MOST
♦ Does the organization know about what's required based on risk ratings?	No	SOME	HALF	MOST
♦ Is per-project data for the cost of assurance activities collected?	No	SOME	HALF	MOST
♦ Does your organization regularly compare your security spend with that of other organizations?	No	ONCE	EVERY 2-3 YRS	ANNUALLY

 SM 1

 SM 2

 SM 3

Policy & Compliance	SCORE	0.0	0.2	0.5	1.0
♦ Do project stakeholders know their project's compliance status?	No	SOME	HALF	MOST	
♦ Are compliance requirements specifically considered by project teams?	No	NOT APPLY	AD-HOC	YES	
♦ Does the organization utilize a set of policies and standards to control software development?	No	PER TEAM	ORG WIDE	INTEGRATED PROCESS	
♦ Are project teams able to request an audit for compliance with policies and standards?	No	SOME	HALF	MOST	
♦ Are projects periodically audited to ensure a baseline of compliance with policies and standards?	No	SOME	HALF	MOST	
♦ Does the organization systematically use audits to collect and control compliance evidence?	No	BUS AREA	ORG WIDE	ORG WIDE & REQUIRED	

Education & Guidance	SCORE	0.0	0.2	0.5	1.0	
◆ Have developers been given high-level security awareness training?	No	ONCE	EVERY 2-3 YRS	ANNUALLY		
◆ Does each project team understand where to find secure development best-practices and guidance?	No	SOME	HALF	MOST		EG 1
◆ Are those involved in the development process given role-specific security training and guidance?	No	SOME	HALF	MOST		
◆ Are stakeholders able to pull in security coaches for use on projects?	No	SOME	HALF	MOST		EG 2
◆ Is security-related guidance centrally controlled and consistently distributed throughout the organization?	No	PER TEAM	ORG WIDE	INTEGRATED PROCESS		
◆ Are developers tested to ensure a baseline skill-set for secure development practices?	No	ONCE	EVERY 2-3 YRS	ANNUALLY		EG 3

Construction

Assessment worksheet

Threat Assessment

SCORE

0.0

0.2

0.5

1.0

◆ Do projects in your organization consider and document likely threats?

No

SOME

HALF

MOST

◆ Does your organization understand and document the types of attackers it faces?

No

SOME

HALF

MOST

◆ Do project teams regularly analyze functional requirements for likely abuses?

No

SOME

HALF

MOST

◆ Do project teams use a method of rating threats for relative comparison?

No

SOME

HALF

MOST

◆ Are stakeholders aware of relevant threats and ratings?

No

SOME

HALF

MOST

◆ Do project teams specifically consider risk from external software?

No

SOME

HALF

MOST

◆ Are the majority of the protection mechanisms and controls captured and mapped back to threats?


No

SOME




HALF




MOST

 TA 1

 TA 2

 TA 3

Security Requirements	SCORE	0.0	0.2	0.5	1.0	
♦ Do project teams specify security requirements during development?	No	SOME	HALF	MOST		
♦ Do project teams pull requirements from best practices and compliance guidance?	No	PER TEAM	ORG WIDE	INTEGRATED PROCESS		
♦ Do stakeholders review access control matrices for relevant projects?	No	SOME	HALF	MOST		 SR 1
♦ Do project teams specify requirements based on feedback from other security activities?	No	SOME	HALF	MOST		
♦ Do stakeholders review vendor agreements for security requirements?	No	SOME	HALF	MOST		 SR 2
♦ Are audits performed against the security requirements specified by project teams?	No	ONCE	EVERY 2-3 YRS	ANNUALLY		 SR 3

Secure Architecture	SCORE	0.0	0.2	0.5	1.0
♦ Are project teams provided with a list of recommended third-party components?	No	PER TEAM	ORG WIDE	INTEGRATED PROCESS	
♦ Are project teams aware of secure design principles and do they apply them consistently?	No	SOME	HALF	MOST	
♦ Do you advertise shared security services with guidance for project teams?	No	BUS AREA	ORG WIDE	ORG WIDE & REQUIRED	
♦ Are project teams provided with prescriptive design patterns based on their application architecture?	No	PER TEAM	ORG WIDE	INTEGRATED PROCESS	
♦ Do project teams build software from centrally-controlled platforms and frameworks?	No	SOME	HALF	MOST	
♦ Are project teams audited for the use of secure architecture components?	No	ONCE	EVERY 2-3 YRS	ANNUALLY	

Verification

Assessment worksheet

Design Review

SCORE

0.0

0.2

0.5

1.0

◆ Do project teams document the attack perimeter of software designs?

No

SOME

HALF

MOST

◆ Do project teams check software designs against known security risks?

No

SOME

HALF

MOST

◆ Do project teams specifically analyze design elements for security mechanisms?

No

SOME

HALF

MOST

◆ Are project stakeholders aware of how to obtain a formal secure design review?

No

SOME

HALF

MOST

◆ Does the secure design review process incorporate detailed data-level analysis?

No

SOME

HALF

MOST

◆ Does a minimum security baseline exist for secure design review results?

No

PER TEAM

ORG WIDE

INTEGRATED
PROCESS






DR 1



DR 2



DR 3

Implementation Review	SCORE	0.0	0.2	0.5	1.0
◆ Do project teams have review checklists based on common security related problems?	No	BUS AREA	ORG WIDE	ORG WIDE & REQUIRED	 IR 1
◆ Do project teams review selected high-risk code?	No	SOME	HALF	MOST	
◆ Can project teams access automated code analysis tools to find security problems?	No	PER TEAM	ORG WIDE	INTEGRATED PROCESS	
◆ Do stakeholders consistently review results from code reviews?	No	SOME	HALF	MOST	 IR 2
◆ Do project teams utilize automation to check code against application-specific coding standards?	No	BUS AREA	ORG WIDE	ORG WIDE & REQUIRED	
◆ Does a minimum security baseline exist for code review results?	No	PER TEAM	ORG WIDE	INTEGRATED PROCESS	 IR 3

Security Testing

SCORE

0.0

0.2

0.5

1.0

◆ Do projects specify security testing based on defined security requirements?

No

SOME

HALF

MOST

◆ Is penetration testing performed on high risk projects prior to release?

No

SOME

HALF

MOST

◆ Are stakeholders aware of the security test status prior to release?

No

SOME

HALF

MOST

◆ Do projects use automation to evaluate security test cases?

No

SOME

HALF

MOST

◆ Do projects follow a consistent process to evaluate and report on security tests to stakeholders?

No

SOME

HALF

MOST

◆ Are security test cases comprehensively generated for application-specific logic?

No

SOME

HALF

MOST

◆ Does a minimum security baseline exist for security testing?

No

PER TEAM

ORG WIDE

INTEGRATED
PROCESS

✓ ST 1

✓ ST 2

✓ ST 3

Operations

Assessment worksheet

Issue Management

SCORE

0.0

0.2

0.5

1.0

♦ Do projects have a point of contact for security issues or incidents?	No	SOME	HALF	MOST
♦ Does your organization have an assigned security response team?	No	<1 YR	>1 YR	MATURE
♦ Are project teams aware of their security point(s) of contact and response team(s)?	No	SOME	HALF	MOST
♦ Does the organization utilize a consistent process for incident reporting and handling?	No	BUS AREA	ORG WIDE	ORG WIDE & REQUIRED
♦ Are project stakeholders aware of relevant security disclosures related to their software projects?	No	SOME	HALF	MOST
♦ Are incidents inspected for root causes to generate further recommendations?	No	SOME	HALF	MOST
♦ Do projects consistently collect and report data and metrics related to incidents?	No	SOME	HALF	MOST



Environment Hardening

SCORE

0.0

0.2

0.5

1.0

◆ Do projects document operational environment security requirements?

No

SOME

HALF

MOST

◆ Do projects check for security updates to third-party software components?

No

SOME

HALF

MOST

◆ Is a consistent process used to apply upgrades and patches to critical dependencies?

No

BUS AREA

ORG WIDE

ORG WIDE
& REQUIRED

 EH 1

◆ Do projects leverage automation to check application and environment health?

No

SOME

HALF

MOST

 EH 2

◆ Are stakeholders aware of options for additional tools to protect software while running in operations?

No

PER TEAM

ORG WIDE

INTEGRATED
PROCESS

◆ Does a minimum security baseline exist for environment health (versioning, patching, etc)?

No

BUS AREA

ORG WIDE

ORG WIDE
& REQUIRED

 EH 3

Operational Enablement

SCORE

0.0

0.2

0.5

1.0

♦ Are security notes delivered with each software release?

No

SOME

HALF

MOST

♦ Are security-related alerts and error conditions documented on a per-project basis?

No

SOME

HALF

MOST

♦ Do projects utilize a change management process that's well understood?

No

SOME

HALF

MOST

♦ Do project teams deliver an operational security guide with each product release?

No

SOME

HALF

MOST

♦ Are project releases audited for appropriate operational security information?

No

ONCE

EVERY 2-3 YRS

ANNUALLY

♦ Is code signing routinely performed on software components using a consistent process?


No


NOT APPLY

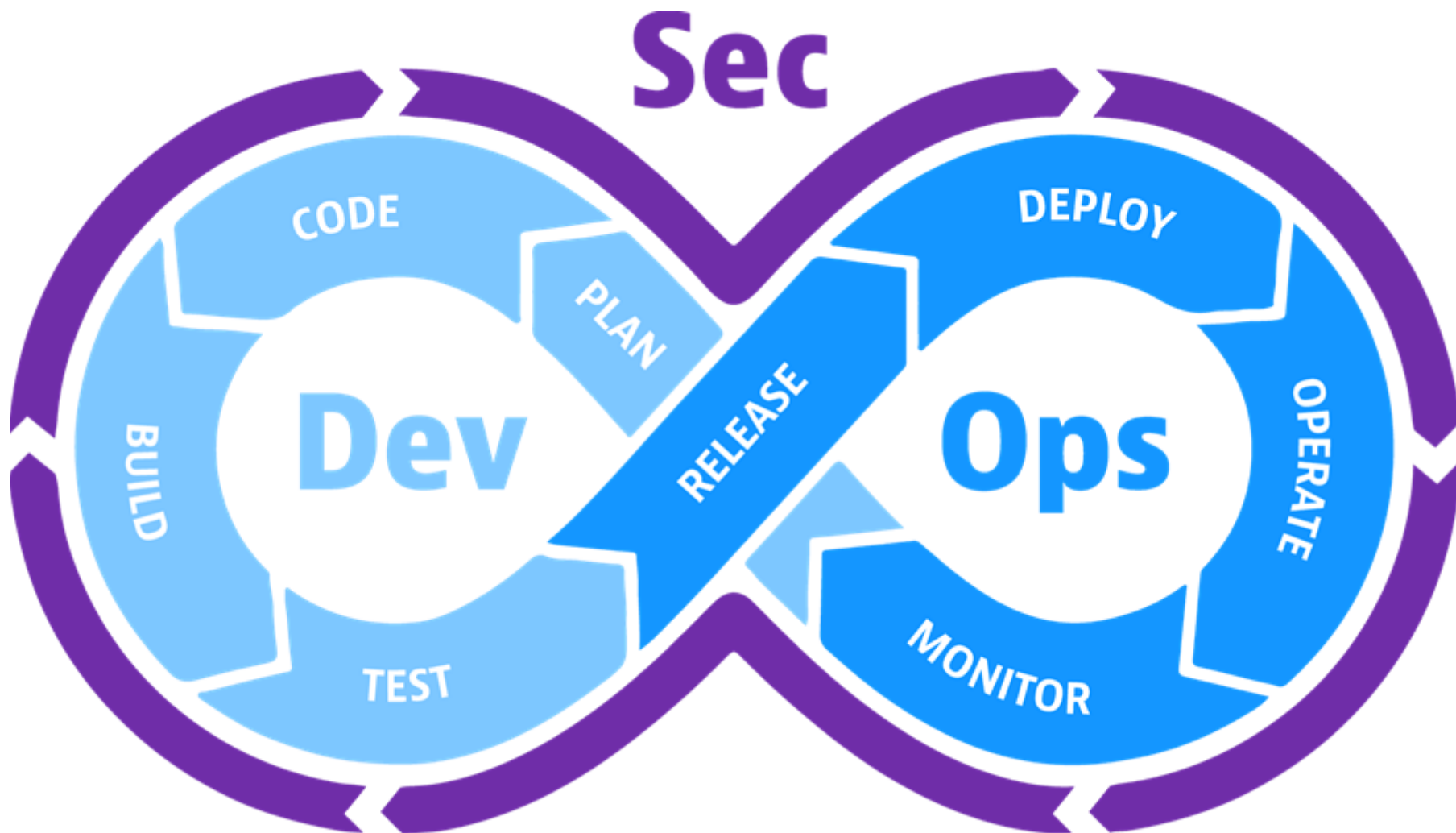
AD-HOC

YES

 OE 1

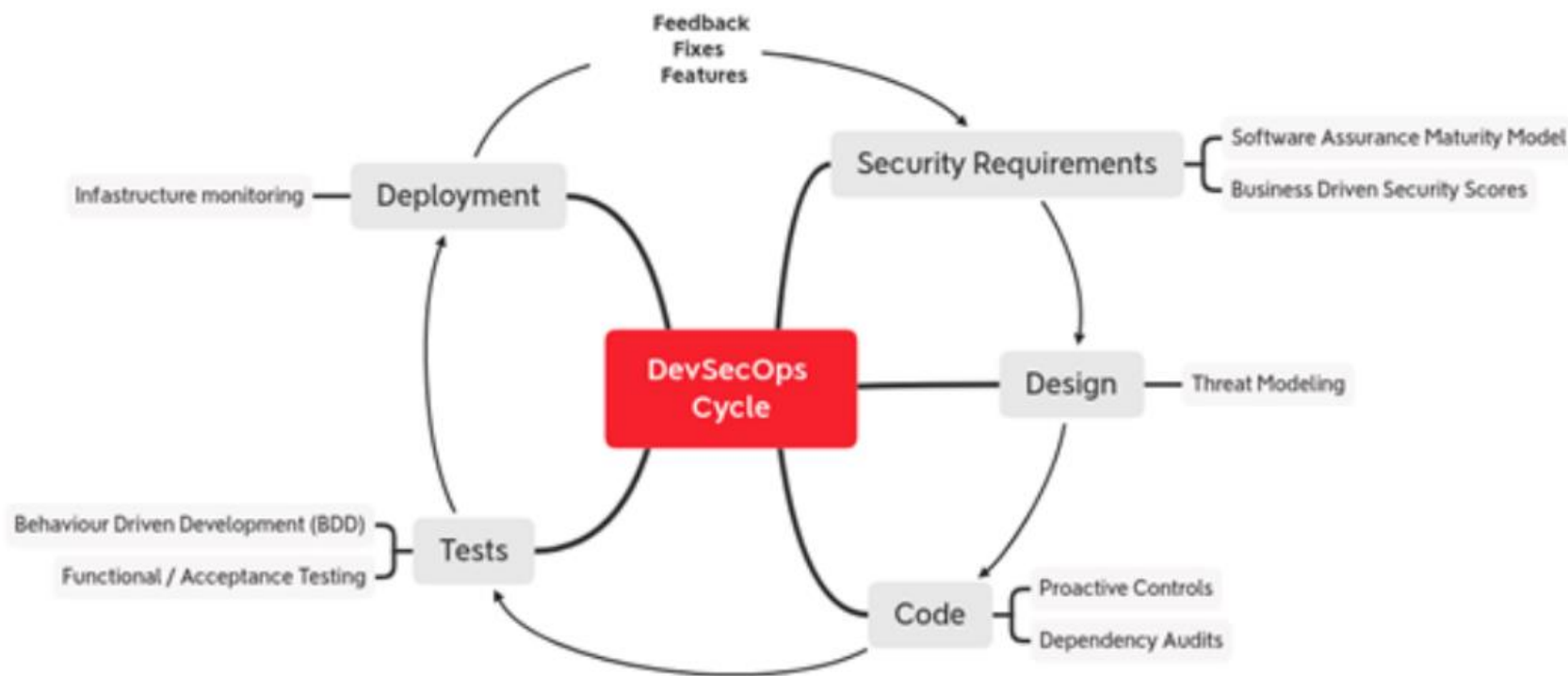
 OE 2

 OE 3



DevSecOps

Các mô hình và phương pháp phát triển phần mềm an toàn



DevSecOps

Các mô hình và phương pháp phát triển phần mềm an toàn



Quy trình dịch chuyển bảo mật sang trái