Họ tên: _____ Ngày: _____ Điểm: _____

Kiến trúc và bảo mật Zero Trust

Xác minh liên tục, phân đoạn vi mô mạng, Quản lý danh tính và truy cập, đặc quyền tối thiểu và kiểm tra tư thế bảo mật.

TỔNG QUAN HỌC VỀ BẢO MẬT ZERO TRUST

ĐÃ BẢO MẬT
MÃ HÓA DỮ LIỆU
Chuẩn AES 256 bit

TUÂN THỦ
TIÊU CHUẨN TOÀN CẦU
Khung GDPR và CCPA

ZERO TRUST
CHÍNH SÁCH TRUY CẬP
Xác thực đa yếu tố

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về kiến trúc bảo mật Zero Trust. Bạn sẽ tìm hiểu về xác minh liên tục, phân đoạn vi mạng, quản lý danh tính và quyền truy cập (IAM), đặc quyền tối thiểu và kiểm tra phiên.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- [ ] **Phần 1-4: Nắm vững an ninh mạng và phòng chống mối đe dọa.**
- [ ] **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- [ ] **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- [ ] **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- [ ] **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- [ ] **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn an ninh mạng của VPN.com

URL: https://www.vpn.com/vi/an-ninh-mang/bao-mat-mang-zero-trust/

Lộ trình học về chiến lược Zero Trust của bạn

- Hiểu nguyên tắc cốt lõi của xác minh liên tục.
- Triển khai phân đoạn vi mô mạng và truy cập đặc quyền tối thiểu.
- Cấu hình kiểm tra tư thế thiết bị và kiểm toán phiên đang hoạt động.

HƯỚNG DẪN BẢO MẬT ZERO TRUST

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về kiến trúc Zero Trust. Kết thúc với hoạt động thưởng Nghĩ nhanh.

KIẾN TRÚC VÀ BẢO MẬT ZERO TRUST (GIỚI THIỆU)

Bảo mật Zero Trust thay thế các mô hình vành đai mạng cũ bằng chính sách nghiêm ngặt 'không bao giờ tin tưởng, luôn luôn xác minh'. Việc triển khai phân đoạn vi mô, quản lý danh tính và truy cập (IAM), quyền hạn tối thiểu và kiểm tra trạng thái thiết bị sẽ chặn mối đe dọa di chuyển ngang.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG.

Điểm kiểm tra 1: Thử thách trắc nghiệm

1 **1. Nguyên tắc cốt lõi của bảo mật Zero Trust là gì?**

- A. Không bao giờ tin cậy, luôn xác minh mọi yêu cầu truy cập bất kể nguồn nào
- B. Cho rằng mọi lưu lượng bên trong tường lửa doanh nghiệp đều an toàn
- C. Lưu tệp cơ sở dữ liệu không mã hóa để tăng tốc độ
- D. Thực thi xác thực email chỉ bằng bản ghi SPF

2 **2. Vi phân đoạn mạng (network micro-segmentation) là gì?**

- A. Chia mạng thành các vùng nhỏ, biệt lập để hạn chế di chuyển ngang
- B. Mã hóa card mạng khi dữ liệu đang truyền
- C. Kết nối mọi máy chủ cục bộ với một địa chỉ IP công khai duy nhất
- D. Giám sát thao tác gõ phím của người dùng trong phiên trình duyệt

3 **3. Nguyên tắc đặc quyền tối thiểu là gì?**

- A. Hạn chế quyền truy cập của người dùng ở mức cần thiết cho công việc của họ
- B. Mặc định cấp mọi đặc quyền hệ thống cho mọi người dùng
- C. Cho phép đăng nhập ẩn danh vào máy chủ cơ sở dữ liệu doanh nghiệp
- D. Cấu hình router Wi-Fi công cộng không có mật khẩu

4 **4. Quản lý danh tính và quyền truy cập (IAM) là gì?**

- A. Các khung quản lý danh tính số và kiểm soát đặc quyền hệ thống
- B. Tiện ích diệt virus quét các thư mục tệp cục bộ
- C. Hệ thống lưu trữ sao lưu dùng phương tiện cách ly mạng (air-gapped)
- D. Một giao thức cổng email từ chối các tên miền giả mạo

5 **5. Xác thực liên tục nghĩa là gì?**

- A. Liên tục xác minh danh tính người dùng và tình trạng thiết bị trong một phiên đang hoạt động
- B. Đổi mật khẩu chính mỗi 10 phút
- C. Băm bản ghi cơ sở dữ liệu bằng nhiều thuật toán
- D. Mã hóa các gói tin truyền qua mạng bằng khóa TLS

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Zero Trust giả định rằng mọi lưu lượng bên trong tường lửa doanh nghiệp đều an toàn.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Phân đoạn vi mô hạn chế khả năng di chuyển ngang của kẻ tấn công giữa các máy chủ nội bộ.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Đặc quyền tối thiểu cấp quyền truy cập vào mọi tệp cơ sở dữ liệu theo mặc định.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Xác minh liên tục kiểm tra tình trạng thiết bị và thông tin xác thực trong suốt phiên đăng nhập.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Triển khai Zero Trust giảm tác động của các thông tin đăng nhập doanh nghiệp bị xâm phạm.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Yêu cầu thông tin xác thực tại mọi điểm truy cập là việc _____ liên tục.
2. Chia mạng doanh nghiệp thành các vùng rất nhỏ là kỹ thuật vi _____ .
3. Cấu hình danh tính số và kiểm soát truy cập là dùng một hệ thống _____ .
4. Hạn chế quyền của người dùng dựa trên nguyên tắc ít _____ nhất.
5. Đánh giá tình trạng của các thiết bị được kết nối là quét _____ của thiết bị.
6. Ghi nhật ký và xem xét các phiên đang hoạt động là hoạt động _____ bảo mật.

NGÂN HÀNG TỪ VỰNG

BỘ ĐỊNH TUYẾN | ĐẶC QUYỀN | IAM | KIỂM TOÁN | PHÂN ĐOẠN | TƯ THẾ BẢO MẬT | TƯỜNG LỬA | XÁC MINH

Viết câu trả lời của bạn tại đây:

1.
2.
3.
4.
5.
6.

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

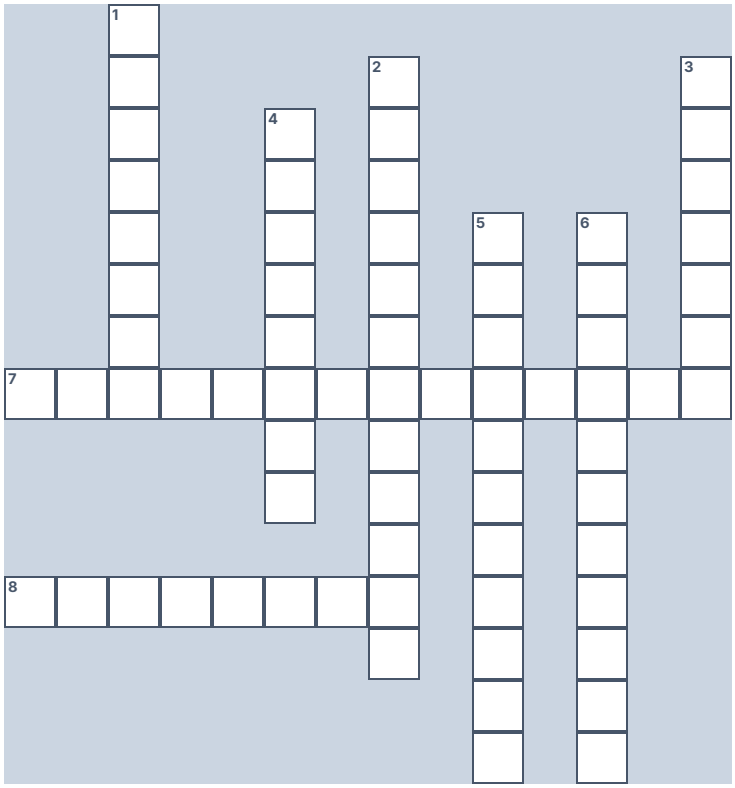
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. XÁC MINH	A	Quản lý quyền truy cập thông tin đăng nhập của người dùng.
☐	2. PHÂN ĐOẠN	B	Nguyên tắc quyền truy cập tối thiểu.
☐	3. IAM	C	Định tuyến lưu lượng gói tin mạng.
☐	4. ĐẶC QUYỀN	D	Bảo vệ rào chắn mạng bên ngoài.
☐	5. TƯ THẾ AN NINH	E	Xem lại các phiên truy cập đã được ghi nhật ký.
☐	6. KIỂM TOÁN	F	Chia các vùng mạng nội bộ.
☐	7. TƯỜNG LỬA	G	Luôn kiểm tra thông tin xác thực của người dùng.
☐	8. ROUTER	H	Đánh giá tình trạng thiết bị.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

7. Quản lý quyền truy cập theo thông tin đăng nhập của người dùng (14)

8. Xem xét các phiên truy cập đã được ghi nhật ký (8)

HÀNG DỌC

1. Bảo vệ bằng hàng rào mạng bên ngoài (8)

2. Chia các vùng mạng nội bộ (12)

3. Luôn kiểm tra thông tin đăng nhập của người dùng (7)

4. Nguyên tắc quyền truy cập tối thiểu (8)

5. Đánh giá tình trạng sức khỏe của thiết bị (11)

6. Định tuyến lưu lượng gói tin mạng (11)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

7 hàng ngang: Quản lý quyền truy cập theo thông tin đăng nhập của người dùng (14 chữ cái):

8 hàng ngang: Xem xét các phiên truy cập đã được ghi nhật ký (8 chữ cái):

HÀNG DỌC

1 hàng dọc: Bảo vệ bằng hàng rào mạng bên ngoài (8 chữ cái):

2 hàng dọc: Chia các vùng mạng nội bộ (12 chữ cái):

3 hàng dọc: Luôn kiểm tra thông tin đăng nhập của người dùng (7 chữ cái):

4 hàng dọc: Nguyên tắc quyền truy cập tối thiểu (8 chữ cái):

5 hàng dọc: Đánh giá tình trạng sức khỏe của thiết bị (11 chữ cái):

6 hàng dọc: Định tuyến lưu lượng gói tin mạng (11 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

G I R Q U P Y D Ê D Q Â A K Ô
N N Ê Y U T H N I Đ Ô B Â T K
A Y L I X A C M I N H U Ư I P
M S A Q Đ Ư H L L E Ê Ơ Ê M Ê
N P Đ K Ă R K P Ư Ê N M Ă S Đ
A X N X C Ư Q Ê R G T V A Ô T
O N N Y Q O G Ô L O R Ê Ô T S
Đ O S S U I A Ư A D O M K Ă N
N T Đ E Y Ô A N Ơ Ư X H I T H
Â X U V Ê Ô I G Y G H M A D G
H Q U A N L Y D A N H T I N H
P Ă R A H D U D I Y I C K Ơ M
H A T Ư T H Ê B A O M Â T Đ O
I N B M Â B Ê G Ă Ă O P L Ô U
S G X Đ X Q E V Ư Ê D P S N S

DANH SÁCH TỪ VỰNG

XACMINH PHÂNĐOANMANG QUANLYDANHTINH ĐĂCQUYÊN TƯTHÊBAOMÂT
KIÊMTOAN TƯƠNGLỬA BÔĐINHTUYÊN

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG
A. XACMINH
B. PHÂNĐOANMANG
C. QUANLYDANHTINH
D. ĐĂCQUYÊN
E. TƯTHÊBAOMÂT
F. KIÊMTOAN
G. TƯƠNGLƯA
H. BÔĐINHTUYÊN

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
1. Bảo vệ bằng hàng rào mạng bên ngoài.
2. Xem xét các phiên truy cập đã được ghi nhật ký.
3. Nguyên tắc quyền truy cập tối thiểu.
4. Chia các vùng mạng nội bộ.
5. Định tuyến lưu lượng gói tin mạng.
6. Đánh giá tình trạng sức khỏe của thiết bị.
7. Quản lý quyền truy cập theo thông tin đăng nhập của người dùng.
8. Luôn kiểm tra thông tin đăng nhập của người dùng.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về an ninh mạng. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. **MNXIHCA** _____

2. **LUYADNQIAH HTNN** _____

3. **TABOTƯÂTÊM H** _____

4. **NƯALGTƯƠ** _____

5. **HANAGÂĐMO PNN** _____

6. **ÊNQYĐUĂC** _____

7. **KNTOAIMÊ** _____

8. **YTNHĐBNÔÊU I** _____

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Những thông tin bạn không bao giờ nên chia sẻ			
2	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
3	Những thứ được kiểm tra trên một thiết bị			
4	Những thứ được ghi nhật ký			
5	Những từ liên quan đến an ninh mạng			
6	Những thứ Zero Trust kiểm tra			
7	Những nơi bạn xuất trình giấy tờ tùy thân trong đời sống hằng ngày			
8	Những cách chứng minh đó thực sự là bạn			
9	Những việc cần làm sau khi dữ liệu bị rò rỉ			
10	Những dấu hiệu máy tính bị nhiễm			
11	Lý do cập nhật phần mềm			
12	Những cấp độ truy cập trong một công ty			
13	Những công cụ bảo mật bạn biết			
14	Những vùng mà một mạng có thể được chia thành			
15	Những câu nói về lòng tin			

Điểm kiểm tra 8: Nghiên cứu tình huống về an ninh mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: CHUYỂN SANG KIẾN TRÚC MẠNG ZERO TRUST

👷

Tình huống: Một doanh nghiệp lớn hiện dùng một mạng nội bộ phẳng, nơi bất kỳ thiết bị nào trên mạng cục bộ đều có thể truy cập mọi máy chủ và cơ sở dữ liệu của công ty.

Câu hỏi thảo luận: Hãy thiết kế một chiến lược phân đoạn vi mô mạng để hạn chế di chuyển ngang.

NGHIÊN CỨU TÌNH HUỐNG 2: TRIỂN KHAI KIỂM SOÁT TRUY CẬP THEO NGUYÊN TẮC ĐẶC QUYỀN TỐI THIỂU

👷

Tình huống: Nhật ký kiểm toán cho thấy những người dùng cơ sở dữ liệu tạm thời và nhân viên cấp thấp nắm giữ quyền đọc và ghi toàn cục đối với các cơ sở dữ liệu kế toán quan trọng.

Câu hỏi thảo luận: Hãy kiểm toán và hạn chế các đặc quyền IAM của cơ sở dữ liệu để thực thi đặc quyền tối thiểu.

Điểm kiểm tra 9: Giải mã mật thư

Chuyên gia an ninh mạng bảo vệ tài sản mạng khỏi các tác nhân đe dọa trực tuyến. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

14 25 18 16 28 1 5 15 12 16 11 27 19 12 13 12 9 16

24 22 25 5 13 11 18 16 10 24 12 16 5 3 29

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q1: Zero Trust là gì?

Zero Trust là một khung bảo mật giả định rằng các mối đe dọa tồn tại cả bên ngoài lẫn bên trong ranh giới mạng, đòi hỏi xác minh cho mọi yêu cầu. [1]

Q2: Quy tắc cốt lõi của Zero Trust là gì?

Không bao giờ tin tưởng, luôn xác minh.

Q3: Vi phân đoạn là gì?

Chia mạng thành các phân đoạn logic nhỏ, an toàn để kiểm soát lưu lượng và ngăn chặn vi phạm lan rộng.

Q4: Đặc quyền tối thiểu là gì?

Chỉ cấp cho người dùng quyền truy cập tối thiểu cần thiết để thực hiện các nhiệm vụ công việc cụ thể của họ. [2]

Q5: IAM là viết tắt của gì?

Quản lý danh tính và truy cập.

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q6: Kiểm tra trạng thái thiết bị giúp ích như thế nào?

Nó xác minh rằng thiết bị đã được vá lỗi, chạy diệt virus đang hoạt động và an toàn trước khi cho phép truy cập.

Q7: Di chuyển ngang là gì?

Quy trình kẻ tấn công dùng để di chuyển trong mạng từ một nút bị xâm nhập ban đầu đến các hệ thống có giá trị cao hơn.

Q8: Zero Trust có thay thế tường lửa không?

Không, nó tăng cường chúng bằng cách bổ sung các kiểm tra lấy danh tính làm trung tâm và tường lửa phân đoạn nội bộ.

Q9: Xác thực liên tục là gì?

Xác minh danh tính người dùng liên tục trong suốt phiên đăng nhập đang hoạt động, chứ không chỉ khi đăng nhập ban đầu.

Q10: Tại sao mạng phẳng (flat network) nguy hiểm?

Trong các mạng phẳng, một nút bị xâm phạm duy nhất cho phép kẻ tấn công dễ dàng truy cập bất kỳ cơ sở dữ liệu nào trên mạng.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q1: Zero Trust giải quyết mô hình vành đai như thế nào?

Nó thay thế mô hình 'lâu đài và hào nước' lỗi thời, chuyển phòng thủ từ các mạng biên sang các danh tính và tài nguyên người dùng cụ thể.

Q2: Điểm quyết định chính sách (PDP) là gì?

Thành phần hệ thống đánh giá các yêu cầu ủy quyền theo các quy tắc bảo mật để quyết định có cấp quyền truy cập hay không.

Q3: Điểm thực thi chính sách (PEP) là gì?

Nút hệ thống (như cổng hoặc proxy) thực sự cho phép hoặc chặn các yêu cầu kết nối dựa trên quyết định của PDP.

Q4: Kiểm soát truy cập dựa trên vai trò (RBAC) hỗ trợ Zero Trust như thế nào?

RBAC nhóm các quyền thành những vai trò cụ thể, giúp ngăn người dùng thừa hưởng quá nhiều đặc quyền quản trị.

Q5: Kiểm soát truy cập theo ngữ cảnh là gì?

Đánh giá các yêu cầu đăng nhập bằng các manh mối thứ cấp như vị trí địa lý, trạng thái thiết bị và thời gian đăng nhập để đánh giá rủi ro.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q6: Vi phân đoạn khác VLAN tiêu chuẩn như thế nào?

VLAN chia mạng thành các phân đoạn logic rộng ở tầng 2, trong khi phân đoạn vi mô dùng chính sách phần mềm để cô lập từng khối lượng công việc riêng lẻ.

Q7: Truy cập đúng lúc (JIT) là gì?

Cấp tạm thời các quyền quản trị nâng cao và tự động thu hồi khi nhiệm vụ hoàn tất.

Q8: Bạn bảo mật API trong khuôn khổ Zero Trust như thế nào?

Bằng cách yêu cầu token OAuth có chữ ký mật mã và kiểm toán chữ ký yêu cầu tại mọi cổng API.

Q9: Ứng dụng khách truy cập mạng zero-trust (ZTNA) là gì?

Tác nhân phần mềm thiết lập các kết nối đi ra được mã hóa, an toàn đến các ứng dụng cụ thể thay vì các mạng con thô.

Q10: Kiểm toán nhật ký hỗ trợ Zero Trust như thế nào?

Ghi nhật ký liên tục cho phép các công cụ phân tích bảo mật tự động phát hiện bất thường và tạm ngưng ngay các lần đăng nhập đáng ngờ.

Phần 11: 10 sự thật và hiểu biết thực tế về an ninh mạng

Xem lại các sự thật thực tế về vi phạm bảo mật, cơ chế phòng thủ và tiêu chuẩn tuân thủ.

1. THÔNG TIN VỀ AN NINH

Kiến trúc Zero Trust thay thế mô hình lâu đài và hào nước cũ bằng các quy tắc xác minh lấy danh tính làm trung tâm.

2. THÔNG TIN VỀ AN NINH

Phân đoạn vi mô mạng thu hẹp phạm vi phần mềm độc hại có thể tiếp cận bằng cách cô lập các khối lượng công việc vào những vùng nhỏ được bảo vệ.

3. THÔNG TIN VỀ AN NINH

Zero Trust tập trung vào việc bảo vệ các tài nguyên như tài sản, dịch vụ và tài khoản thay vì các phân đoạn mạng. [1]

4. THÔNG TIN VỀ AN NINH

Chính sách truy cập đặc quyền tối thiểu giúp giảm rủi ro dữ liệu bị người trong nội bộ đưa ra ngoài từ các cơ sở dữ liệu lõi.

5. THÔNG TIN VỀ AN NINH

Xác thực trạng thái thiết bị kiểm tra mức bản vá hệ điều hành và trạng thái phần mềm diệt virus đang hoạt động theo thời gian thực.

6. THÔNG TIN VỀ AN NINH

Các nhà môi giới Zero Trust Network Access (ZTNA) có thể thay thế hoặc bổ sung VPN doanh nghiệp để hạn chế phạm vi truy cập của người dùng.

7. THÔNG TIN VỀ BẢO MẬT

Ủy quyền đặc quyền quản trị Just-In-Time (JIT) giảm rủi ro đánh cắp thông tin xác thực trên bộ điều khiển miền.

8. THÔNG TIN VỀ BẢO MẬT

Nhật ký xác thực liên tục và kiểm toán hành vi phiên, tạm ngưng người dùng có mẫu thực thi script bất thường.

9. THÔNG TIN VỀ BẢO MẬT

Các biện pháp phòng thủ vành đai truyền thống không chặn được các cuộc tấn công di chuyển ngang một khi thông tin đăng nhập quản trị bị lộ.

10. THÔNG TIN VỀ AN NINH

Ấn phẩm đặc biệt NIST 800-207 (2020) đưa ra định nghĩa trừu tượng về kiến trúc Zero Trust, kèm các mô hình triển khai. [1]

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn toàn cầu của NIST, OWASP và tuân thủ quyền riêng tư dữ liệu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Nguyên tắc cốt lõi của bảo mật Zero Trust là gì? → Không bao giờ tin cậy, luôn xác minh mọi yêu cầu truy cập bất kể nguồn nào [2]

2 Câu hỏi 2 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Vi phân đoạn mạng (network micro-segmentation) là gì? → Chia mạng thành các vùng nhỏ, biệt lập để hạn chế di chuyển ngang

3 Câu hỏi 3 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Nguyên tắc đặc quyền tối thiểu là gì? → Hạn chế quyền truy cập của người dùng ở mức cần thiết cho công việc của họ

4 Câu hỏi 4 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Quản lý danh tính và quyền truy cập (IAM) là gì? → Các khung quản lý danh tính số và kiểm soát đặc quyền hệ thống

5 Câu hỏi 5 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Xác thực liên tục nghĩa là gì? → Liên tục xác minh danh tính người dùng và tình trạng thiết bị trong một phiên đang hoạt động

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: Zero Trust không cấp bất kỳ sự tin cậy ngầm định nào dựa trên vị trí mạng, dù ở bên trong hay bên ngoài.

7 **Câu hỏi 7** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Đúng: các vùng nhỏ bị cô lập hạn chế phạm vi mà kẻ xâm nhập có thể di chuyển giữa các máy chủ.

8 **Câu hỏi 8** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: đặc quyền tối thiểu chỉ cấp mức truy cập tối thiểu mà mỗi vai trò cần.

9 **Câu hỏi 9** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Xác minh liên tục kiểm tra tình trạng thiết bị và thông tin xác thực trong suốt phiên đăng nhập.

10 **Câu hỏi 10** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Triển khai Zero Trust giảm tác động của các thông tin đăng nhập doanh nghiệp bị xâm phạm.

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

G 1. XÁC MINH	F 2. PHÂN ĐOẠN	A 3. IAM	B 4. ĐẶC QUYỀN
H 5. TƯ THẾ AN NINH	E 6. KIỂM TOÁN	D 7. TƯỜNG LỬA	C 8. ROUTER

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 XÁC MINH	2 PHÂN ĐOẠN	3 IAM	4 ĐẶC QUYỀN
5 TƯ THẾ BẢO MẬT	6 KIỂM TOÁN		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 G – TƯƠNGLỬA	2 F – KIỂMTOAN	3 D – ĐẶCQUYÊN	4 B – PHÂNĐOANMẠNG
5 H – BỐĐỊNHTUYÊN	6 E – TƯTHẾBẢOMẬT	7 C – QUẢNLÝDANHTÍNH	8 A – XÁCMINH

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được XÁC MINH, PHÂN ĐOẠN và IAM bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

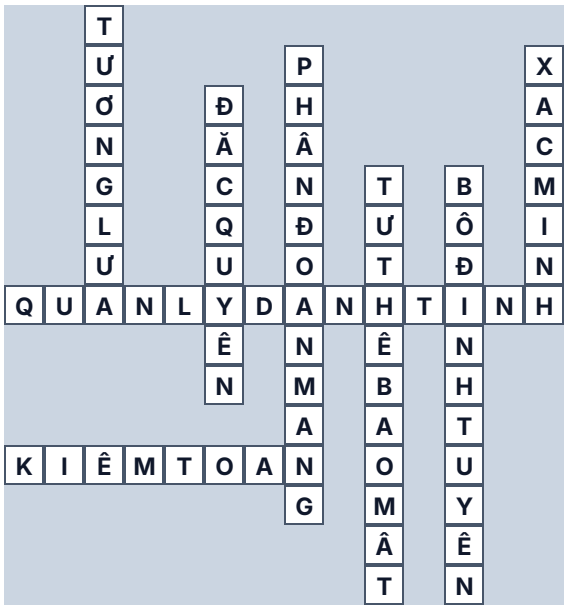
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

G	I	R	Q	U	P	Y	D	Ê	D	Q	Â	A	K	Ô
N	N	Ê	Y	U	T	H	N	I	Đ	Ô	B	Â	T	K
A	Y	L	I	X	A	C	M	I	N	H	U	Ư	I	P
M	S	A	Q	Đ	Ư	H	L	L	E	Ê	Ơ	Ê	M	Ê
N	P	Đ	K	Ă	R	K	P	Ư	Ê	N	M	Ă	S	Đ
A	X	N	X	C	Ư	Q	Ê	R	G	T	V	A	Ô	T
O	N	N	Y	Q	O	G	Ô	L	O	R	Ê	Ô	T	S
Đ	O	S	S	U	I	A	Ư	A	D	O	M	K	Ă	N
N	T	Đ	E	Y	Ô	A	N	Ơ	Ư	X	H	I	T	H
Â	X	U	V	Ê	Ô	I	G	Y	G	H	M	A	D	G
H	Q	U	A	N	L	Y	D	A	N	H	T	I	N	H
P	Ă	R	A	H	D	U	D	I	Y	I	C	K	Ơ	M
H	A	T	Ư	T	H	Ê	B	A	O	M	Â	T	Đ	O
I	N	B	M	Â	B	Ê	G	Ă	Ă	O	P	L	Ô	U
S	G	X	Đ	X	Q	E	V	Ư	Ê	D	P	S	N	S

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

7 hàng ngang: QUANLYDANHTINH Quản lý quyền truy cập theo thông tin đăng nhập của người dùng (14 chữ cái)

8 hàng ngang: KIÊMTOAN Xem xét các phiên truy cập đã được ghi nhật ký (8 chữ cái)

HÀNG DỌC

1 hàng dọc: TƯƠNGLỬA Bảo vệ bằng hàng rào mạng bên ngoài (8 chữ cái)

2 hàng dọc: PHÂNĐOẠNMẠNG Chia các vùng mạng nội bộ (12 chữ cái)

3 hàng dọc: XÁCMINH Luôn kiểm tra thông tin đăng nhập của người dùng (7 chữ cái)

4 hàng dọc: ĐẶCQUYỀN Nguyên tắc quyền truy cập tối thiểu (8 chữ cái)

5 hàng dọc: TỰTHÊBẢOMẬT Đánh giá tình trạng sức khỏe của thiết bị (11 chữ cái)

6 hàng dọc: BỘĐỊNHTUYẾN Định tuyến lưu lượng gói tin mạng (11 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1. MNXIHCA — **XACMINH**
2. LUYADNQIAHHTNN — **QUANLYDANHTINH**
3. TABOTƯÂTÊMH — **TƯTHÊBAOMÂT**
4. NƯALGTƯƠ — **TƯƠNGLƯA**
5. HANAGÂĐMOPNN — **PHÂNĐOANMANG**
6. ÊNQYĐUĂC — **ĐĂCQUYÊN**
7. KNTOAIMÊ — **KIÊMTOAN**
8. YTNHĐBNÔÊUI — **BÔĐINHTUYÊN**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"LUÔN XAC MINH VƠI KIÊN TRUC KHÔNG TIN CÂY"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Chuyển sang kiến trúc mạng zero trust

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một doanh nghiệp lớn hiện dùng mạng nội bộ phẳng, nơi bất kỳ thiết bị nào trên mạng cục bộ đều có thể truy cập mọi máy chủ và cơ sở dữ liệu của công ty.
- Chiến lược và giải pháp đề xuất: Chia mạng phẳng thành các vùng phòng ban cô lập. Cài tường lửa nội bộ để kiểm soát lưu lượng giữa các vùng và bắt buộc xác thực mã thông báo kết nối cho mọi truy cập.

B Nghiên cứu tình huống 2: Triển khai kiểm soát truy cập theo nguyên tắc đặc quyền tối thiểu

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Nhật ký kiểm toán cho thấy người dùng cơ sở dữ liệu tạm thời và nhân viên cấp thấp có quyền đọc và ghi toàn cục đối với các cơ sở dữ liệu kế toán quan trọng.
- Chiến lược và giải pháp đề xuất: Thu hồi mọi đặc quyền quản trị toàn cục. Triển khai kiểm soát truy cập dựa trên vai trò (RBAC) khớp đúng với vai trò công việc, và thiết lập các đợt rà soát quyền tự động hằng tuần.