Mục Tiêu Của Kỳ Thi Cấp Chứng Chỉ CompTIA Cybersecurity Analyst (CySA+)

KỲ THI SỐ: CS0-002

CompTIA

Giới Thiệu về Kỳ Thi

Ứng viên nên sử dụng tài liệu này để chuẩn bị cho kỳ thi cấp chứng chỉ CompTIA Cybersecurity Analyst (CySA+) CS0-002. Với mục tiêu cuối cùng là chủ động bảo vệ và không ngừng nâng cao tính bảo mật của một tổ chức, CySA+ sẽ xác minh rằng ứng viên thành công sẽ có kiến thức và kỹ năng cần thiết để:

- Sử dụng các kỹ thuật phát hiện thông tin và mối đe dọa
- Phân tích và diễn giải dữ liệu
- Xác định và giải quyết các lỗ hổng bảo mật
- Đề xuất các biện pháp phòng ngừa
- Ứng phó hiệu quả và khôi phục sau sự cố

Điều này tương đương với 4 năm kinh nghiệm thực hành trong vai trò kỹ thuật an ninh mạng.

Các ví dụ về nội dung này nhằm nêu bật các mục tiêu của kỳ thi và không nên được hiểu là danh sách hoàn chỉnh về tất cả các nội dung trong kỳ thi này.

XÂY DỰNG KỲ THI

Các kỳ thi CompTIA là kết quả của các hội thảo chuyên gia về chủ đề và kết quả khảo sát toàn ngành về các kỹ năng cũng như kiến thức cần thiết của một chuyên gia CNTT.

CHÍNH SÁCH VỀ SỬ DỤNG TÀI LIỆU ĐƯỢC PHÉP CỦA CompTIA

CompTIA Certifications, LLC không liên kết và không cho phép, xác nhận hoặc dung túng cho việc sử dụng bất kỳ nội dung nào do các trang web đào tạo bên thứ ba trái phép cung cấp (hay còn gọi là "ngân hàng câu hỏi thực tế trái phép"). Các cá nhân sử dụng những tài liệu này để chuẩn bị cho bất kỳ kỳ thi CompTIA nào sẽ bị thu hồi chứng chỉ và bị đình chỉ thi trong tương lai theo các Thỏa Thuận Dành Cho Ứng Viên CompTIA. Với nỗ lực truyền đạt rõ ràng hơn các chính sách của kỳ thi CompTIA liên quan đến việc sử dụng tài liệu nghiên cứu trái phép, CompTIA hướng dẫn tất cả các ứng viên tham gia lấy chứng chỉ tham khảo Các Chính Sách của Kỳ Thi Cấp Chứng Chỉ CompTIA. Vui lòng xem xét tất cả các chính sách CompTIA trước khi bắt đầu quá trình nghiên cứu cho bất kỳ kỳ thi CompTIA nào. Các ứng viên sẽ phải tuân theo Thỏa Thuận Dành Cho Ứng Viên CompTIA. Nếu ứng viên có câu hỏi về việc liệu tài liệu nghiên cứu có bị coi là trái phép (hay còn gọi là "ngân hàng câu hỏi thực tế trái phép") hay không, thì họ nên liên hệ với CompTIA tại examsecurity@comptia.org để xác nhận.

XIN LƯU Ý

Danh sách các ví dụ được cung cấp ở định dạng gạch đầu dòng không phải là danh sách đầy đủ. Các ví dụ khác về công nghệ, quy trình hoặc nhiệm vụ liên quan đến từng mục tiêu cũng có thể được đưa vào kỳ thi mặc dù không được liệt kê hoặc đề cập trong tài liệu mục tiêu này. CompTIA liên tục xem xét nội dung các kỳ thi của chúng tôi và cập nhật các câu hỏi kiểm tra để đảm bảo các kỳ thi của chúng tôi là mới nhất và tính bảo mật của các câu hỏi được bảo vệ. Khi cần thiết, chúng tôi sẽ công bố các kỳ thi cập nhật dựa trên mục tiêu của kỳ thi thử nghiệm. Xin lưu ý rằng tất cả các tài liệu luyện thi liên quan sẽ vẫn có giá trị.

THÔNG TIN CHI TIẾT VỀ KỲ THI

Kỳ thi bắt buộc	CS0-002
Số câu hỏi	Tối thiểu là 85
Loại câu hỏi	Trắc nghiệm và tự luận
Thời gian thi	165 phút
Kinh nghiệm được đề xuất	• 4 năm kinh nghiệm thực hành trong vai trò kỹ thuật an ninh mạng • Security+ và Network+ hoặc kiến thức và kinh nghiệm tương đương
Điểm đạt	750

MỤC TIÊU CỦA KỲ THI (CÁC LĨNH VỰC)

Bảng dưới đây liệt kê các lĩnh vực được đánh giá theo kỳ thi này và mức độ mà các lĩnh vực đó được thể hiện.

LĨNH VỰC	PHẦN TRĂM KIỂM TRA
1.0 Quản Lý Mối Đe Dọa và Lỗ Hổng Bảo Mật	22%
2.0 Bảo Mật Phần Mềm và Hệ Thống	18%
3.0 Hoạt Động và Giám Sát Bảo Mật	25%
4.0 Ứng Phó Với Sự Cố	22%
5.0 Tuân Thủ và Đánh Giá	13%
Tổng	**100%**

1.0 Quản Lý Mối Đe Dọa và Lỗ Hổng Bảo Mật

1.1 Giải thích tầm quan trọng của dữ liệu và thông tin về mối đe dọa an ninh mạng.

- **Nguồn thông tin**
  - Thông tin nguồn mở
  - Thông tin nguồn đóng/độc quyền
  - Kịp thời
  - Mức độ liên quan
  - Tính chính xác
- **Mức độ tin cậy**
- **Quản lý chỉ báo**
  - Biểu Thức Thông Tin Về Mối Đe Dọa Có Cấu Trúc (STIX)
  - Trao Đổi Thông Tin Chỉ Báo Tự Động Điện Tử Đáng Tin Cậy (TAXII)
  - OpenIoC
- **Phân loại mối đe dọa**
  - Mối đe dọa xác định và mối đe dọa chưa xác định
  - Lỗ hổng chưa được công bố hoặc khắc phục
  - Mối đe dọa dai dẳng
- **Tác nhân đe dọa**
  - Quốc gia-nhà nước
  - Tin tặc
  - Tội phạm có tổ chức
  - Mối đe dọa nội gián
    - Có chủ định
    - Không có chủ định
- **Chu kỳ thông tin**
  - Yêu cầu
  - Thu thập
  - Phân tích
  - Phổ biến
  - Phản hồi
- **Phần mềm độc hại hàng hóa**
- **Cộng đồng phân tích và chia sẻ thông tin**
  - Chăm sóc sức khỏe
  - Tài chính
  - Hàng không
  - Chính phủ
  - Cơ sở hạ tầng quan trọng

1.2 Đưa ra một tình huống, sử dụng thông tin về mối đe dọa an ninh mạng để hỗ trợ bảo mật cho tổ chức.

- **Các khuôn khổ tấn công**
  - MITRE ATT&CK
  - Mô Hình Kim Cương về Phân Tích Xâm Nhập
  - Mô hình Kill chain
- **Tìm kiếm mối đe dọa**
  - Danh tiếng
  - Hành vi
  - Chỉ báo xâm nhập (IoC)
  - Hệ thống chấm điểm lỗ hổng bảo mật phổ biến (CVSS)
- **Phương pháp mô hình hóa mối đe dọa**
  - Khả năng của đối thủ
  - Tổng bề mặt tấn công
  - Vectơ tấn công lừa đảo
  - Tác động
  - Khả năng
- **Chia sẻ thông tin về mối đe dọa với các chức năng được hỗ trợ**
  - Ứng phó với sự cố
  - Quản lý lỗ hổng bảo mật
  - Quản lý rủi ro
  - Kỹ thuật bảo mật
  - Phát hiện và giám sát

1.3 Đưa ra một tình huống, thực hiện các hoạt động quản lý lỗ hổng bảo mật.

- **Xác định lỗ hổng bảo mật**
  - Tầm quan trọng của tài sản
  - Quét chủ động và thụ động
  - Lập bản đồ/liệt kê
- **Thẩm định**
  - Dương tính thật
  - Dương tính giả
  - Âm tính thật
  - Âm tính giả
- **Khắc phục/giảm thiểu**
  - Đường cơ sở cấu hình
  - Vá lỗi
  - Làm cứng
  - Kiểm soát bù trừ
  - Chấp nhận rủi ro
  - Xác minh giảm thiểu
- **Thông số và tiêu chí quét**
  - Rủi ro liên quan đến các hoạt động quét
  - Nguồn cấp dữ liệu về lỗ hổng bảo mật
  - Phạm vi
  - Đã được xác thực và chưa được xác thực
  - Dựa trên máy chủ và dựa trên đại lý
  - Nội bộ và bên ngoài
  - Lưu ý đặc biệt
    - Loại dữ liệu
    - Ràng buộc kỹ thuật
    - Quy trình làm việc
    - Mức độ nhạy cảm
    - Yêu cầu theo quy định
    - Phân đoạn
    - Hệ thống ngăn chặn xâm nhập (IPS), hệ thống phát hiện xâm nhập (IDS) và cài đặt tường lửa
- **Yếu tố hạn chế khả năng khắc phục**
  - Biên bản ghi nhớ (MOU)
  - Thỏa thuận cam kết chất lượng dịch vụ (SLA)
  - Quản trị tổ chức
  - Can thiệp vào quy trình kinh doanh
  - Giáng cấp chức năng
  - Hệ thống cũ
  - Hệ thống độc quyền

1.4 Đưa ra một tình huống, phân tích kết quả từ các công cụ đánh giá lỗ hổng bảo mật thường dùng.

- **Trình quét ứng dụng web**
  - OWASP Zed Attack Proxy (ZAP)
  - Burp suite
  - Nikto
  - Arachni
- **Trình quét lỗ hổng bảo mật của cơ sở hạ tầng**
  - Nessus
  - OpenVAS
  - Qualys
- **Công cụ và kỹ thuật đánh giá phần mềm**
  - Phân tích tĩnh
  - Phân tích động
  - Kỹ thuật đảo ngược
  - Kiểm thử Fuzzing
- **Liệt kê**
  - Nmap
  - hping
  - Chủ động và thụ động
  - Người phản hồi
- **Công cụ đánh giá không dây**
  - Aircrack-ng
  - Reaver
  - oclHashcat
- **Công cụ đánh giá cơ sở hạ tầng đám mây**
  - ScoutSuite
  - Prowler
  - Pacu

1.5 Giải thích các mối đe dọa và lỗ hổng bảo mật liên quan đến công nghệ chuyên biệt.

- **Di động**
- **Internet vạn vật (IoT)**
- **Nhúng**
- **Hệ điều hành theo thời gian thực (RTOS)**
- **Hệ thống trên Chip (SoC)**
- **Mảng phần tử logic có thể tái lập trình (FPGA)**
- **Kiểm soát truy cập vật lý**
- **Xây dựng các hệ thống tự động**
- **Xe cộ và máy bay không người lái**
  - CAN bus
- **Hệ thống tự động hóa quy trình và quy trình làm việc**
- **Hệ thống kiểm soát công nghiệp**
- **Kiểm soát giám sát và thu thập dữ liệu (SCADA)**
  - Modbus

1.6 Giải thích các mối đe dọa và lỗ hổng bảo mật liên quan đến hoạt động trên nền tảng đám mây.

- **Mô hình dịch vụ đám mây**
  - Phần Mềm dạng Dịch Vụ (SaaS)
  - Nền Tảng dạng Dịch Vụ (PaaS)
  - Cơ Sở Hạ Tầng dạng Dịch Vụ (IaaS)
- **Mô hình triển khai đám mây**
  - Công khai
  - Riêng tư
  - Cộng đồng
  - Kết hợp
- **Chức Năng dạng Dịch Vụ (FaaS)/ kiến trúc không máy chủ**
- **Cơ sở hạ tầng dạng mã (IaC)**
- **Giao diện lập trình ứng dụng (API) không bảo mật**
- **Quản lý mã khóa không phù hợp**
- **Bộ nhớ không được bảo vệ**
- **Ghi nhật ký và giám sát**
  - Ghi nhật ký và giám sát không đầy đủ
  - Không thể truy cập

1.7 Đưa ra một tình huống, triển khai các biện pháp kiểm soát để giảm thiểu các cuộc tấn công và lỗ hổng bảo mật phần mềm.

- **Các hình thức tấn công**
  - Tấn công bằng ngôn ngữ đánh dấu có thể mở rộng (XML)
  - Ngôn ngữ truy xuất có cấu trúc (SQL) injection
  - Tấn công Tràn
    - Bộ nhớ đệm
    - Số nguyên
    - Khối xếp
  - Thực thi mã từ xa
  - Tấn công bằng cách truy cập vào thư mục
  - Tăng đặc quyền
  - Thử một mật khẩu trên nhiều tài khoản
  - Nhồi thông tin đăng nhập
  - Mạo danh
  - Tấn công xen giữa (Man-in-the-middle)
  - Chiếm quyền điều khiển phiên truy cập
  - Rootkit
  - Thực thi tập lệnh trên nhiều trang web
    - Phản chiếu
    - Dai dẳng
    - Mô hình đối tượng tài liệu (DOM)
- **Lỗ hổng bảo mật**
  - Xử lý lỗi không đúng cách
  - Tham chiếu
  - Đối tượng tham chiếu thiếu an toàn
  - Tranh chấp dữ liệu
  - Xác thực bị hỏng
  - Rò rỉ dữ liệu nhạy cảm
  - Thành phần không an toàn
  - Ghi nhật ký và giám sát không đầy đủ
  - Cấu hình yếu hoặc mặc định
  - Sử dụng chức năng không an toàn
    - strcpy

2.0 Bảo Mật Phần Mềm và Hệ Thống

2.1 Đưa ra một tình huống, áp dụng các giải pháp bảo mật để quản lý cơ sở hạ tầng.

- **Đám mây và tại cơ sở**
- **Quản lý tài sản**
  - Gắn thẻ tài sản
- **Phân đoạn**
  - Vật lý
  - Ảo
  - Jumpbox
  - Cô lập hệ thống
    - Khoảng hở
- **Cấu trúc mạng**
  - Vật lý
  - Do phần mềm xác định
  - Đám mây riêng ảo (VPC)
  - Mạng riêng ảo (VPN)
  - Không có máy chủ
- **Quản lý thay đổi**
- **Ảo hóa**
  - Cơ sở hạ tầng máy tính ảo (VDI)
- **Công nghệ ảo hóa**
- **Quản lý danh tính và quyền truy cập**
  - Quản lý đặc quyền
  - Xác thực đa yếu tố (MFA)
  - Đăng nhập một lần (SSO)
  - Liên kết
  - Dựa vào vai trò
  - Dựa vào thuộc tính
  - Bắt buộc
  - Xem lại theo cách thủ công
- **Nhà môi giới bảo mật truy cập đám mây (CASB)**
- **Honeypot**
- **Giám sát và ghi nhật ký**
- **Mã hóa**
- **Quản lý chứng chỉ**
- **Chủ động bảo vệ**

2.2 Giải thích các biện pháp thực hành tốt nhất để đảm bảo bảo mật phần mềm.

- **Nền tảng**
  - Di động
  - Ứng dụng web
  - Máy khách/máy chủ
  - Nhúng
  - Hệ thống trên chip (SoC)
  - Firmware
- **Tích hợp chu trình phát triển phần mềm (SDLC)**
- **DevSecOps**
- **Phương pháp đánh giá phần mềm**
  - Kiểm tra sự phù hợp với người dùng
  - Ứng dụng kiểm thử khả năng chịu tải
  - Kiểm tra hồi quy bảo mật
  - Xem lại mã
- **Biện pháp mã hóa bảo mật tốt nhất**
  - Xác thực đầu vào
  - Mã hóa đầu ra
  - Quản lý phiên
  - Xác thực
  - Bảo vệ dữ liệu
  - Các truy vấn được tham số hóa
- **Công cụ phân tích tĩnh**
- **Công cụ phân tích động**
- **Các phương pháp chính thức để xác minh phần mềm quan trọng**
- **Cấu trúc định hướng dịch vụ**
  - Ngôn Ngữ Đánh Dấu Xác Nhận Bảo Mật (SAML)
  - Giao Thức Truy Cập Đối Tượng Đơn Giản (SOAP)
  - Chuyển Đổi Trạng Thái Đại Diện (REST)
  - Microservices

2.3 Giải thích các biện pháp thực hành tốt nhất để đảm bảo bảo mật phần cứng.

- **Bảo mật ngay từ phần cứng**
  - Mô-đun nền tảng đáng tin cậy (TPM)
  - Mô-đun bảo mật phần cứng (HSM)
- **eFuse**
- **Giao Diện Chương Trình Cơ Sở Mở Rộng Hợp Nhất (UEFI)**
- **Giả mạo đáng tin cậy**
- **Xử lý an toàn**
  - Thực thi tin cậy
  - Secure enclave
  - Tiện ích mở rộng bảo mật bộ vi xử lý
  - Thực thi không thể phân chia
- **Chống làm giả**
- **Ổ đĩa tự mã hóa**
- **Cập nhật chương trình cơ sở tin cậy**
- **Khởi động được bảo vệ và chứng thực**
- **Mã hóa bus**

3.0 Hoạt Động và Giám Sát Bảo Mật

3.1 Đưa ra một tình huống, phân tích dữ liệu như một phần của hoạt động giám sát bảo mật.

- **Kinh nghiệm**
- **Phân tích xu thế**
- **Điểm cuối**
  - Mã độc
    - Kỹ thuật đảo ngược
  - Bộ nhớ
  - Hành vi của hệ thống và ứng dụng
    - Hành vi tốt xác định
    - Hành vi bất thường
    - Kỹ thuật khai thác
  - Hệ thống tệp
  - Phân tích hành vi của người dùng và thực thể (UEBA)
- **Mạng**
  - Phân tích đường dẫn Uniform Resource Locator (URL) và hệ thống tên miền (DNS)
    - Thuật toán tạo tên miền
  - Phân tích luồng
  - Phân tích giao thức và gói tin
    - Mã độc
- **Xem xét nhật ký**
  - Nhật ký sự kiện
  - Nhật ký hệ thống
  - Nhật ký tường lửa
  - Tường lửa ứng dụng web (WAF)
  - Proxy
  - Hệ thống phát hiện xâm nhập (IDS)/ Hệ thống ngăn chặn xâm nhập (IPS)
- **Phân tích tác động**
  - Tác động đến tổ chức và tác động cục bộ
  - Tức thời và tổng thể
- **Xem lại quản lý sự kiện và thông tin bảo mật (SIEM)**
  - Ghi quy tắc
  - Giao thức Internet xấu được biết đến (IP)
  - Trang tổng quan
- **Ghi truy vấn**
  - Tìm kiếm dòng
  - Tệp lệnh
  - Piping
- **Phân tích email**
  - Tair độc hại
  - Thư Được Xác Định Bằng Khóa Miền (DKIM)
  - Xác Thực, Báo Cáo và Tuân Thủ Thông Báo Dự Trên Miền (DMARC)
  - Khung Chính Sách Người Gửi (SPF)
  - Tấn công giả mạo
  - Chuyển tiếp
  - Chữ ký số
  - Chặn chữ ký email
  - Liên kết nhúng
  - Mạo danh
  - Header

3.2 Đưa ra một tình huống, thực hiện thay đổi cấu hình đối với các biện pháp kiểm soát hiện có để cải thiện tính bảo mật.

- **Quyền**
- **Lập danh cho phép**
- **Lập danh sách bị chặn**
- **Tường lửa**
- **Quy tắc hệ thống ngăn chặn xâm nhập (IPS)**
- **Ngăn chặn mất dữ liệu (DLP)**
- **Phát hiện và phản hồi điểm cuối (EDR)**
- **Kiểm soát truy cập mạng (NAC)**
- **Sinkholing**
- **Chữ ký phần mềm độc hại**
  - Ghi quy tắc/phát triển
- **Hộp cát**
- **Bảo mật cổng**

3.3 Giải thích tầm quan trọng của việc chủ động tìm kiếm mối đe dọa.

- **Thiết lập giả thuyết**
- **Lập hồ sơ các tác nhân và hoạt động đe dọa**
- **Chiến thuật tìm kiếm mối đe dọa**
  - Phân tích quy trình có thể thực thi
- **Giảm bề mặt tấn công**
- **Nhóm các nội dung quan trọng**
- **Vectơ tấn công lừa đảo**
- **Thông tin tích hợp**
- **Cải thiện khả năng phát hiện**

3.4 So sánh và đối chiếu các khái niệm và công nghệ tự động hóa.

- **Điều phối quy trình làm việc**
  - Điều Phối, Tự Động Hóa và Phản Hồi Bảo Mật (SOAR)
- **Tệp lệnh**
- **Tích hợp giao diện lập trình ứng dụng (API)**
- **Tự động tạo chữ ký phần mềm độc hại**
- **Làm giàu dữ liệu**
- **Kết hợp nguồn cấp dữ liệu về mối đe dọa**
- **Máy học**
- **Sử dụng giao thức và tiêu chuẩn tự động**
  - Giao Thức Tự Động Hóa Nội Dung Bảo Mật (SCAP)
- **Tích hợp liên tục**
- **Triển khai/phân phối liên tục**

4.0 Ứng Phó Với Sự Cố

4.1 Giải thích tầm quan trọng của quy trình ứng phó với sự cố.

- **Kế hoạch trao đổi thông tin**
  - Giới hạn trao đổi thông tin với các bên tin cậy
  - Tiết lộ thông tin dựa trên các yêu cầu pháp lý/theo quy định
  - Ngăn ngừa khả năng vô tình tiết lộ thông tin
  - Sử dụng phương pháp trao đổi thông tin an toàn
  - Yêu cầu báo cáo
- **Hợp tác ứng phó với các thực thể có liên quan**
  - Pháp lý
  - Nhân sự
  - Quan hệ công chúng
  - Nội bộ và bên ngoài
  - Bộ phận thực thi pháp luật
  - Lãnh đạo cấp cao
  - Cơ quan quản lý
- **Các yếu tố góp phần vào tầm quan trọng của dữ liệu**
  - Thông tin nhận dạng cá nhân (PII)
  - Thông tin sức khỏe cá nhân (PHI)
  - Thông tin cá nhân nhạy cảm (SPI)
  - Tài sản có giá trị cao
  - Thông tin tài chính
  - Tài sản trí tuệ
  - Thông tin doanh nghiệp

4.2 Đưa ra một tình huống, áp dụng quy trình ứng phó với sự cố phù hợp.

- **Chuẩn bị**
  - Đào tạo
  - Kiểm thử
  - Tài liệu về quy trình
- **Phát hiện và phân tích**
  - Các đặc điểm góp phần vào việc phân loại mức độ nghiêm trọng
  - Thời gian ngừng hoạt động
  - Thời gian khôi phục
  - Toàn vẹn dữ liệu
  - Kinh tế
  - Tầm quan trọng của quy trình hệ thống
  - Kỹ thuật đảo ngược
  - Tương quan dữ liệu
- **Ngăn chặn**
  - Phân đoạn
  - Tách biệt
- **Xoá bỏ và khôi phục**
  - Giảm thiểu lỗ hổng bảo mật
  - Vệ sinh
  - Tái cấu trúc/tái nhân bản
  - Tiêu hủy an toàn
  - Vá lỗi
  - Khôi phục quyền
  - Tái tạo tài nguyên
  - Khôi phục các tính năng và dịch vụ
  - Xác minh ghi nhật ký/trao đổi thông tin với giám sát bảo mật
- **Các hoạt động sau sự cố**
  - Lưu giữ bằng chứng
  - Báo cáo rút ra bài học kinh nghiệm
  - Quy trình kiểm soát thay đổi
  - Cập nhật kế hoạch ứng phó với sự cố
  - Báo cáo tóm tắt sự cố
  - Tạo IoC
  - Giám sát

4.3 Đưa ra một sự cố, phân tích các dấu hiệu chỉ báo sự xâm phạm tiềm ẩn.

- **Liên quan đến mạng**
  - Tiêu thụ băng thông
  - Báo hiệu
  - Trao đổi thông tin ngang hàng không thường xuyên
  - Thiết bị giả trên mạng
  - Quét
  - Tăng đột biến lưu lượng truy cập bất thường
  - Giao thức chung qua cổng không tiêu chuẩn
- **Liên quan đến máy chủ**
  - Sử dụng bộ xử lý
  - Sử dụng bộ nhớ
  - Sử dụng dung lượng ổ đĩa
  - Phần mềm trái phép
  - Quy trình độc hại
  - Thay đổi trái phép
  - Đặc quyền trái phép
  - Lọc dữ liệu
  - Hành vi xử lý bất thường của hệ điều hành
  - Thay đổi hoặc bất thường của hệ thống tệp
  - Thay đổi hoặc bất thường của trang đăng ký
  - Nhiệm vụ theo lịch trái phép
- **Liên quan đến ứng dụng**
  - Hoạt động bất thường
  - Giới thiệu tài khoản mới
  - Kết quả không mong muốn
  - Trao đổi thông tin ra bên ngoài không mong muốn
  - Can thiệp vào dịch vụ
  - Nhật ký ứng dụng

4.4 Đưa ra một tình huống, sử dụng các kỹ thuật pháp lý kỹ thuật số cơ bản.

- **Mạng**
  - Wireshark
  - tcpdump
- **Điểm cuối**
  - Ổ đĩa
  - Bộ nhớ
- **Di động**
- **Đám mây**
- **Ảo hóa**
- **Lưu giữ pháp lý**
- **Quy trình**
- **Băm**
  - Thay đổi đối với mã nhị phân
- **Carving**
- **Thu thập dữ liệu**

5.0 Tuân Thủ và Đánh Giá

5.1 Hiểu rõ tầm quan trọng của việc bảo mật và bảo vệ dữ liệu.

- **Riêng tư và bảo mật**
- **Biện pháp kiểm soát phi kỹ thuật**
  - Phân loại
  - Quyền sở hữu
  - Lưu giữ
  - Loại dữ liệu
  - Tiêu chuẩn lưu giữ
  - Bảo mật
  - Yêu cầu pháp lý
  - Chủ quyền dữ liệu
  - Tối thiểu hóa dữ liệu
  - Giới hạn mục đích
  - Thỏa thuận không tiết lộ thông tin (NDA)
- **Kiểm soát kỹ thuật**
  - Mã hóa
  - Ngăn chặn mất dữ liệu (DLP)
  - Che dấu dữ liệu
  - Hủy xác định danh tính
  - Mã hóa
  - Quản lý quyền kỹ thuật số (DRM)
    - Dấu nước
  - Yêu cầu quyền truy cập theo khu vực địa lý
  - Kiểm soát quyền truy cập

5.2 Đưa ra một tình huống, áp dụng các khái niệm bảo mật để hỗ trợ giảm thiểu rủi ro cho tổ chức.

- **Phân tích tác động kinh doanh**
- **Quy trình xác định rủi ro**
- **Tính toán rủi ro**
  - Xác suất
  - Tầm quan trọng
- **Thông báo các yếu tố rủi ro**
- **Xác định mức độ ưu tiên về rủi ro**
  - Kiểm soát bảo mật
  - Cân bằng kỹ thuật
- **Đánh giá hệ thống**
- **Kiểm soát bù trừ tài liệu**
- **Đào tạo và diễn tập**
  - Đội Đỏ
  - Đội Xanh
  - Đội Trắng
  - Diễn tập trong phòng họp
- **Đánh giá chuỗi cung ứng**
  - Thẩm định nhà cung cấp
  - Xác thực nguồn phần cứng

5.3 Giải thích tầm quan trọng của các chương trình khung, chính sách và quy trình, và các biện pháp kiểm soát.

- **Khung chương trình**
  - Dựa trên rủi ro
  - Theo quy định
- **Chính sách và quy trình**
  - Bộ quy tắc ứng xử/đạo đức
  - Chính sách sử dụng được chấp nhận (AUP)
  - Chính sách về mật khẩu
  - Quyền sở hữu dữ liệu
  - Lưu giữ dữ liệu
  - Quản lý tài khoản
  - Giám sát liên tục
  - Lưu giữ sản phẩm công việc
- **Loại kiểm soát**
  - Quản lý
  - Vận hành
  - Kỹ thuật
  - Phòng ngừa
  - Phát hiện
  - Ứng phó
  - Sửa chữa
- **Kiểm tra và đánh giá**
  - Quy định
  - Tuân thủ

Danh Sách Các Từ Viết Tắt Trong Kỳ Thi Cấp Chứng Chỉ CompTIA Cybersecurity Analyst (CySA+)

Sau đây là danh sách các từ viết tắt xuất hiện trong kỳ thi CompTIA CySA+. Khuyến khích các ứng viên xem danh sách đầy đủ và hiểu rõ tất cả các từ viết tắt được liệt kê như một phần của chương trình luyện thi toàn diện.

TỪ VIẾT TẮT	GIẢI THÍCH
3DES	Triple Data Encryption Algorithm
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
BEC	Business Email Compromise
BYOD	Bring Your Own Device
CA	Certificate Authority
CAN	Controller Area Network
CASB	Cloud Access Security Broker
CI/CD	Continuous Integration/Continuous Delivery
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPU	Central Processing Unit
CRM	Customer Relations Management
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DGA	Domain Generation Algorithm
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOM	Document Object Model
DRM	Digital Rights Management
EDR	Endpoint Detection and Response

TỪ VIẾT TẮT	GIẢI THÍCH
ELK	Elasticsearch, Logstash, Kibana
ERP	Enterprise Resource Planning
FaaS	Function as a Service
FPGA	Field-programmable Gate Array
FTK	Forensic Toolkit
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MaaS	Monitoring as a Service
MAC	Mandatory Access Control
MD5	Message Digest 5
MDM	Mobile Device Management
MFA	Multifactor Authentication
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRTG	Multi Router Traffic Grapher
NAC	Network Access Control
NAS	Network-attached Storage

TỪ VIẾT TẮT	GIẢI THÍCH
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NIC	Network Interface Card
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OSSIM	Open Source Security Information Management
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Pluggable Authentication Module
PCAP	Packet Capture
PCI	Payment Card Industry
PHI	Personal Health Information
PID	Process Identification Number
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-in User Service
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RTOS	Real-time Operating System
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDLC	Software Development Life Cycle
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMB	Server Message Block
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SoC	System on Chip
SPF	Sender Policy Framework
SPI	Sensitive Personal Information
SQL	Structured Query Language
SSH	Secure Shell
SSHD	Solid-state Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
TACACS+	Terminal Access Controller Access Control System Plus
TAXII	Trusted Automated eXchange of Intelligence Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross-site Scripting
ZAP	Zed Attack Proxy

Danh Sách Phần Mềm và Phần Cứng Đề Xuất của CySA+

CompTIA đưa vào danh sách mẫu phần cứng và phần mềm này để hỗ trợ ứng viên khi họ chuẩn bị cho kỳ thi CySA+. Danh sách này cũng có thể hữu ích cho các công ty đào tạo muốn tạo ra một bài lab để cung cấp cho dịch vụ đào tạo của họ. Danh sách gạch đầu dòng bên dưới mỗi chủ đề đều là tượng trưng đại diện và không phải là danh sách đầy đủ.

PHẦN CỨNG CNTT

- Máy trạm (hoặc máy tính xách tay) có thể chạy VM
- Bộ chuyển đổi có quản lý
- Tường lửa
- Điện thoại di động
- Điện thoại VoIP
- WAP
- IDS/ IPS
- Thiết bị IoT
- Máy chủ

PHẦN MỀM

- File ảnh máy ảo (VM) cho các mục tiêu tấn công
- Máy Chủ Windows
- Máy Khách Windows
  - Commando VM
- Linux
  - Kali
  - ParrotOS
  - Security Onion
- Chrome OS
- UTM Appliance
- pfSense
- Metasploitable
- Access to cloud instances
  - Azure
  - AWS
  - GCP
- SIEM
  - Graylog
  - ELK
  - Splunk
- Trình quét lỗ hổng bảo mật
  - OpenVAS
  - Nessus