##### **Phụ lục 2**

##### **Danh sách Nhóm kiến thức, kỹ năng kỹ thuật chuyên sâu**

##### **về an toàn thông tin mạng**

*(Ban hành kèm theo thông tư số /2021/TT-BTTTT ngày / /2021 của*

*Bộ trưởng Bộ Thông tin và Truyền thông)*

| **STT** | **Nội dung/Yêu cầu cần đạt** | **Yêu cầu cần đạt theo hạng** |
| --- | --- | --- |
| **Kiến thức** | **Kỹ năng** | **IV** | **III** | **II** | **I** |
| **1** | **Tiếp nhận và phân loại sự cố** | **X** | **X** |  |  |
|  | - Kiến thức về các mối đe dọa và lỗ hổng không gian mạng.- Kiến thức về các công cụ đánh giá tính dễ bị tổn thương và phòng thủ không gian mạng và khả năng của chúng.- Kiến thức về các khả năng và chức năng liên quan đến công nghệ sáng tạo nội dung - Kiến thức về các khả năng và chức năng của các công nghệ khi tích hợp với nhau.- Kiến thức về công nghệ điện toán đám mây, trung tâm dữ liệu và các khái niệm liên quan đến bảo mật, quản trị.- Kiến thức về các tiêu chuẩn và phương pháp phân loại dữ liệu dựa trên độ nhạy và các yếu tố rủi ro khác.- Kiến thức về lý thuyết phân loại.- Kiến thức về các tiêu chuẩn bảo mật dữ liệu Thông tin Nhận dạng Cá nhân (PII).- Kiến thức về các tiêu chuẩn bảo mật dữ liệu.- Kiến thức về các trường hợp sử dụng liên quan đến kết hợp và đồng bộ hóa nội dung trên các nền tảng (ví dụ: Di động, PC, Đám mây).- Kiến thức về phân loại thông tin của một tổ chức và các thủ tục để xâm phạm thông tin.- Kiến thức về các phương pháp, thủ tục và kỹ thuật chính của việc thu thập thông tin và sản xuất, báo cáo và chia sẻ thông tin.- Kiến thức về kỹ thuật khai phá dữ liệu.- Kiến thức về cơ sở dữ liệu. | - Có kỹ năng thực hiện tìm kiếm thông tin.- Kỹ năng tổng hợp các kiến thức liên quan đến sự cố ATTTT- Kỹ năng phân tích, tổng hợp dự đoán và đưa ra các trưởng hợp, các loại sự cố.- Kỹ năng ứng dụng công nghệ để quản lý tài nguyên thông tin- Kỹ năng nghiên cứu, tìm tòi để phục vụ việc phân loại sự cố ATTT |
| **2** | **Ứng cứu sự cố** |  | **X** | **X** | **X** |
|  | - Kiến thức về các khái niệm và giao thức mạng.- Kiến thức về các quy trình quản lý rủi ro.- Kiến thức về luật, quy định, chính sách.- Kiến thức về các mối đe dọa và lỗ hổng không gian mạng.- Kiến thức về hậu quả của việc mất an toàn thông tin mạng.- Kiến thức về sao lưu và phục hồi dữ liệu.- Kiến thức về bảo đảm tính liên tục sau khi ứng cứu sự cố.- Kiến thức về cơ chế kiểm soát truy cập máy chủ/máy trạm.- Kiến thức về ứng phó sự cố và quá trình phục hổi.- Kiến thức về phương pháp ứng phó và xử lý sự cố.- Kiến thức về phương pháp và kỹ thuật phát hiện xâm nhập.- Kiến thức về các phương pháp phân tích lưu lượng mạng.- Kiến thức về các mối đe dọa và lỗ hổng bảo mật hệ thống và ứng dụng.- Kiến thức về các loại tấn công khác nhau.- Kiến thức về các khái niệm và phương pháp phân tích phần mềm độc hại.- Kiến thức về Rủi ro Bảo mật Ứng dụng. | - Kỹ năng thu thập thông tin về sự cố an toàn thông tin một cách liên tục.- Kỹ năng sử dụng các phương pháp xử lý sự cố.- Kỹ năng xử lý sự cố và chẩn đoán các bất thường về cơ sở hạ tầng phòng thủ mạng.- Kỹ năng điều tra phân tích các cuộc tấn công mạng.- Có kỹ năng khắc phục các sự cố vật lý và kỹ thuật ảnh hưởng đến hiệu suất của hệ thống / máy chủ.- Lựa chọn và thực hiện các biện pháp thích hợp sau khi xem xét nguyên nhân sự cố.- Kỹ năng phát hiện, khắc phục về các lỗ hổng bảo mật không gian mạng tiềm ẩn.- Kỹ năng bảo quản tính toàn vẹn theo quy trình thao tác tiêu chuẩn hoặc tiêu chuẩn quốc gia.- Kỹ năng nhận biết và phân loại các loại lỗ hổng và các cuộc tấn công liên quan.- Kỹ năng bảo vệ mạng khỏi phần mềm độc hại. - Kỹ năng thực hiện đánh giá thiệt hại.- Kỹ năng sử dụng các công cụ tương quan sự kiện bảo mật.- Kỹ năng thiết kế ứng phó sự cố cho các mô hình dịch vụ đám mây, trung tâm dữ liệu. |
| **3** | **Kiểm soát và đánh giá điểm yếu** |  | **X** | **X** | **X** |
|  | - Kiến thức về lỗ hổng ứng dụng.- Kiến thức về mật mã và các khái niệm quản lý khóa mật mã- Kiến thức về cơ chế kiểm soát truy cập máy chủ/mạng (ví dụ: danh sách kiểm soát truy cập, danh sách khả năng).- Kiến thức về truy cập mạng, danh tính và quản lý truy cập (ví dụ: cơ sở hạ tầng khóa công khai, Oauth, OpenID, SAML, SPML).- Kiến thức về lưu lượng mạng. - Kiến thức về cấu trúc ngôn ngữ lập trình và logic.- Kiến thức về các mối đe dọa và lỗ hổng bảo mật hệ thống và ứng dụng.- Kiến thức về các công cụ quản lý hệ thống và kỹ thuật xác định lỗi.- Kiến thức về các cấu thành một cuộc tấn công mạng và mối quan hệ của cuộc tấn công mạng đối với cả các mối đe dọa và lỗ hổng bảo mật.- Kiến thức về ngôn ngữ máy tính thông dịch và biên dịch.- Kiến thức về các loại tấn công khác nhau (ví dụ: tấn công thụ động, chủ động, nội gián, cận cảnh, phân phối).- Kiến thức về những kẻ tấn công mạng (ví dụ: kẻ giả mạo kịch bản, mối đe dọa nội gián, nhà nước phi quốc gia bảo trợ và quốc gia bảo trợ).- Kiến thức về quản trị hệ thống, mạng, phần cứng, phần mềm. - Kiến thức về các giai đoạn tấn công mạng (ví dụ: trinh sát, quét, liệt kê, giành quyền truy cập, nâng cấp đặc quyền, duy trì quyền truy cập, khai thác mạng, theo dõi).- Kiến thức về các khái niệm kiến ​​trúc an toàn mạng bao gồm cấu trúc liên kết, giao thức, thành phần và nguyên tắc (ví dụ: ứng dụng chuyên sâu về phòng thủ).- Kiến thức về các mô hình bảo mật (ví dụ: mô hình Bell-LaPadula, mô hình toàn vẹn Biba, mô hình toàn vẹn Clark-Wilson).- Kiến thức về các nguyên tắc và kỹ thuật hack.- Kiến thức về chương trình phân loại thông tin của một tổ chức và các thủ tục để xâm phạm thông tin.- Kiến thức về phân tích mức gói bằng các công cụ thích hợp (ví dụ: Wireshark, tcpdump).- Kiến thức về mật mã học.- Kiến thức về các nguyên tắc, công cụ và kỹ thuật kiểm tra thâm nhập.- Kiến thức về môi trường đe dọa của tổ chức. | - Kỹ năng tiến hành quét lỗ hổng bảo mật và nhận diện lỗ hổng trong hệ thống bảo mật.- Kỹ năng đánh giá mức độ an toàn của thiết kế và hệ thống an ninh.- Kỹ năng phát hiện xâm nhập dựa trên máy chủ và mạng thông qua công nghệ phát hiện xâm nhập (ví dụ: Snort).- Kỹ năng bắt chước hành vi đe dọa.- Kỹ năng sử dụng các công cụ và kỹ thuật kiểm tra thâm nhập.- Kỹ năng sử dụng các kỹ thuật xây dựng xã hội. (ví dụ: lừa đảo, lừa bịp, lừa đảo, v.v.).- Kỹ năng sử dụng các công cụ phân tích mạng để xác định các lỗ hổng. (ví dụ: fuzzing, nmap, v.v.).- Kỹ năng xem lại nhật ký để xác định bằng chứng về các vụ xâm nhập trong quá khứ.- Kỹ năng thực hiện đánh giá lỗ hổng ứng dụng.- Kỹ năng thực hiện đánh giá tác động / rủi ro.- Kỹ năng phát triển về bối cảnh môi trường đe dọa của tổ chức- Kỹ năng áp dụng các nguyên tắc an ninh mạng và quyền riêng tư cho các yêu cầu của tổ chức (liên quan đến tính bảo mật, tính toàn vẹn, tính khả dụng, xác thực, không từ chối).  |
| 4 | **Phân tích/giám sát ATTT** |  | **X** | **X** | **X** |
|  | - Kiến thức về thuật toán máy tính.- Kiến thức về thuật toán mã hóa.- Kiến thức về mật mã và các khái niệm quản lý khóa mật mã.- Kiến thức về hệ thống cơ sở dữ liệu.- Kiến thức về cài đặt, tích hợp và tối ưu hóa các thành phần hệ thống.- Kiến thức về nguyên lý tương tác giữa con người và máy tính.- Kiến thức về các nguồn phổ biến về lỗ hổng bảo mật.- Kiến thức về truy cập mạng, danh tính và quản lý truy cập- Kiến thức về cách lưu lượng truy cập qua mạng- Có kiến thức về các công cụ, phương pháp và kỹ thuật thiết kế hệ thống bảo mật.- Có kiến thức về kỹ thuật phần mềm.- Kiến thức về quy trình kỹ thuật hệ thống.- Kiến thức về các khái niệm kiến trúc an ninh mạng bao gồm cấu trúc liên kết, giao thức, các thành phần và nguyên tắc.- Kiến thức về các nguyên tắc, mô hình, phương pháp quản lý hệ thống mạng.- Kiến thức về các khái niệm quản lý dịch vụ cho mạng và các tiêu chuẩn liên quan.- Kiến thức về các mô hình bảo mật.- Có kiến thức về các loại kiến trúc máy tính.- Kiến thức về kỹ thuật quản lý cấu hình.- Kiến thức về quản lý bảo mật.- Có kiến thức về các phương pháp kiểm tra và đánh giá bảo mật hệ thống.- Kiến thức về thiết kế biện pháp đối phó với các rủi ro bảo mật đã xác định. | - Có kỹ năng thiết kế tích hợp các giải pháp phần cứng và phần mềm.- Kỹ năng xác định cách thức hoạt động của hệ thống bảo mật (bao gồm khả năng phục hồi và khả năng kiểm tra) và những thay đổi như thế nào trong điều kiện, hoạt động hoặc môi trường.- Có kỹ năng phát triển và áp dụng các kiểm soát truy cập hệ thống an ninh.- Kỹ năng đánh giá tính đầy đủ của các thiết kế bảo mật.- Kỹ năng viết mã bằng ngôn ngữ lập trình hiện được hỗ trợ (ví dụ: Java, C ++).- Kỹ năng đánh giá thiết kế hệ thống an ninh.- Có kỹ năng đánh giá các biện pháp kiểm soát an ninh dựa trên các nguyên tắc an ninh mạng- Có kỹ năng nhận biết lỗ hổng trong hệ thống bảo mật.- Kỹ năng áp dụng các nguyên tắc an ninh mạng và quyền riêng tư cho các yêu cầu của tổ chức. |
| 5 | **An toàn cơ sở hạ tầng thông tin** |  | **X** | **X** | **X** |
|  | - Có kiến thức về sao lưu và phục hồi dữ liệu.- Kiến thức về cơ chế kiểm soát truy cập máy chủ/mạng.- Kiến thức về phương pháp ứng phó và xử lý sự cố.- Kiến thức về an ninh mạng và các nguyên tắc riêng tư và các yêu cầu của tổ chức.- Kiến thức về các phương pháp phân tích lưu lượng mạng.- Kiến thức về cách lưu lượng truy cập qua mạng.- Kiến thức về bảo mật Mạng riêng ảo (VPN).- Có kiến thức về các chính sách, thủ tục và quy định về quốc phòng và an toàn thông tin mạng.- Kiến thức về các khái niệm kiến trúc an ninh mạng bao gồm cấu trúc liên kết, giao thức, các thành phần và nguyên tắc.- Kiến thức cơ bản về hệ thống, mạng và kỹ thuật tăng cường hệ điều hành.- Kiến thức về các thủ tục, nguyên tắc và phương pháp kiểm tra.- Kiến thức về các giao thức mạng như TCP/IP, Cấu hình Máy chủ Động, Tên miền, Hệ thống tên (DNS).- Kiến thức về phân tích lưu lượng mạng (công cụ, phương pháp, quy trình). | - Có kỹ năng áp dụng các điều khiển truy cập máy chủ/mạng (ví dụ: danh sách điều khiển truy cập).- Kỹ năng điều chỉnh cảm biến.- Kỹ năng sử dụng các phương pháp xử lý sự cố.- Kỹ năng sử dụng thiết bị Mạng riêng ảo (VPN) và mã hóa.- Kỹ năng bảo mật thông tin liên lạc mạng.-Kỹ năng bảo vệ mạng chống lại phần mềm độc hại.- Có kỹ năng về kỹ thuật tăng cường hệ thống, mạng và hệ điều hành.- Kỹ năng xử lý sự cố và chẩn đoán các bất thường về cơ sở hạ tầng phòng thủ mạng và công việc thông qua độ phân giải.- Kỹ năng áp dụng các nguyên tắc an ninh mạng và quyền riêng tư cho các yêu cầu của tổ chức |
| 6 | **Phân tích nguy cơ/tình báo ATTT** |  |  | **X** | **X** |
|  | - Kiến thức về các khái niệm, thuật ngữ và hoạt động của nhiều loại hình thông tin liên lạc phương tiện truyền thông (máy tính và mạng điện thoại, vệ tinh, cáp quang, không dây).- Kiến thức về các thành phần và kiến trúc máy tính vật lý, bao gồm các chức năng của các thành phần và thiết bị ngoại vi khác nhau.- Kiến thức về các giai đoạn tấn công mạng.- Kiến thức về các loại trang web, quản trị, chức năng và hệ thống quản lý nội dung (CMS).- Có kiến thức về các phương pháp và kỹ thuật tấn công.- Có kiến thức về tiêu chuẩn, chính sách và thủ tục đánh dấu phân loại và kiểm soát.- Kiến thức về khả năng thu thập thông tin/trí tuệ mạng và kho lưu trữ.- Kiến thức về hệ thống kiểm soát giám sát và thu thập dữ liệu.- Kiến thức về cách trích xuất, phân tích và sử dụng siêu dữ liệu.- Kiến thức về các chiến thuật nội bộ để dự đoán và/hoặc mô phỏng các khả năng và hành động của mối đe dọa.- Kiến thức về phần mềm độc hại.- Kiến thức về bảo mật hoạt động.- Kiến thức về các thiết bị mạng vật lý và logic và cơ sở hạ tầng để bao gồm các trung tâm, thiết bị chuyển mạch, bộ định tuyến, tường lửa, v.v.- Kiến thức về các giao thức mạng và định tuyến phổ biến và cách chúng tương tác để cung cấp thông tin liên lạc qua mạng.- Có kiến thức về các sản phẩm ảo hóa (VMware, Virtual PC). | - Có kỹ năng thực hiện nghiên cứu bằng cách sử dụng .- Có kỹ năng xác định và mô tả tất cả các khía cạnh thích hợp của môi trường hoạt động.- Kỹ năng phát triển hoặc đề xuất các phương pháp tiếp cận hoặc giải pháp phân tích cho các vấn đề.- Kỹ năng đánh giá thông tin về độ tin cậy, tính hợp lệ và mức độ liên quan.- Kỹ năng xác định các diễn giải phân tích thay thế để giảm thiểu điều không lường trước được kết quả.- Kỹ năng xác định các yếu tố mục tiêu quan trọng, bao gồm các yếu tố mục tiêu quan trọng cho không gian mạng.- Có kỹ năng chuẩn bị và trình bày các cuộc họp giao ban theo yêu cầu.- Kỹ năng cung cấp hiểu biết về các hệ thống mục tiêu hoặc mối đe dọa thông qua việc xác định và liên kết phân tích các mối quan hệ vật lý, chức năng hoặc hành vi.- Có kỹ năng sử dụng nhiều công cụ phân tích, cơ sở dữ liệu và kỹ thuật.- Kỹ năng sử dụng nhiều công cụ tìm kiếm (ví dụ: Google, Yahoo, LexisNexis, DataStar) và các công cụ trong việc thực hiện tìm kiếm mã nguồn mở.- Kỹ năng sử dụng không gian làm việc ảo và/hoặc các công cụ.- Kỹ năng viết, đánh giá và chỉnh sửa các sản phẩm trí tuệ liên quan đến không gian mạng. |
| 7 | **Tư vấn ATTT** |  | **X** | **X** | **X** |
|  | - Kiến thức về các mối đe dọa và lỗ hổng không gian mạng.- Kiến thức về các tác động hoạt động cụ thể của việc mất kiểm soát an toàn thông tin mạng.- Kiến thức về các khái niệm và thực hành xử lý dữ liệu kỹ thuật số.- Kiến thức về công nghệ thông tin (CNTT) và công nghệ an toàn thông tin và các xu hướng mới.- Kiến thức về điều tra, báo cáo, công cụ điều tra và luật/quy định về bảo mật.- Kiến thức về các chính sách, thủ tục và quy định về quốc phòng, an ninh mạng và an toàn thông tin.- Kiến thức về các tiêu chuẩn bảo mật dữ liệu. - Kiến thức về luật, chính sách, thủ tục hoặc quản trị liên quan đến an toàn, an ninh mạng cho các cơ sở hạ tầng quan trọng.- Kiến thức về các nguyên tắc, chính sách và thủ tục thu thập thông tin tình báo.- Kiến thức về kế hoạch hoạt động kinh doanh hoặc quân sự, kế hoạch hoạt động khái niệm, chính sách và quy tắc giao kết thường trực.- Kiến thức về chính sách công bố thông tin nước ngoài và các quy định kiểm soát xuất nhập khẩu liên quan đến an toàn thông tin mạng.- Kiến thức về thông tin cá nhân dựa trên văn bản quy phạm pháp luật. | - Có kỹ năng giao tiếp giữa các cá nhân, khả năng tiếp cận, kỹ năng lắng nghe, sử dụng ngôn ngữ phù hợp với đối tác.- Kỹ năng lập kế hoạch về khảo sát hệ thống mạng, bảo mật theo yêu cầu.- Kỹ năng nghiên cứu, tìm hiểu các văn bản quy phạm pháp luật, quy định, tiêu chuẩn kỹ thuật về đảm bảo an toàn thông tin.- Kỹ năng nghiên cứu, tìm tòi, tự đào tạo, nâng cao kiến thức đến các nhiệm vụ được giao.- Kỹ năng sử dụng từ ngữ chuyên môn để xây dựng các chính sách, quy trình sử dụng hệ thống mạng.- Kỹ năng tư vấn, giải thích các giải pháp bảo mật, bảo đảm ATTT cho các cơ quan, đơn vị.- Kỹ năng lập báo cáo từ thực tế tổ chức để kiến nghị những biện pháp, giải pháp bảo đảm ATTT cho cơ quan, đơn vị. |
| 8 | **Đào tạo, huấn luyện an toàn thông tin** |  |  | **X** | **X** |
|  | - Kiến thức về các nguyên tắc và kỹ thuật quản lý tài nguyên.- Kiến thức về các mục tiêu và công nghệ thông tin doanh nghiệp (CNTT) của tổ chức.- Kiến thức về bản chất và chức năng của cấu trúc thông tin liên quan (ví dụ: Cơ sở hạ tầng thông tin quốc gia).- Kiến thức về các quy trình kinh doanh/sứ mệnh cốt lõi của tổ chức.- Kiến thức về các vấn đề, rủi ro và lỗ hổng bảo mật mới.- Kiến thức về văn bản quy phạm pháp luật, quy chế hiện hành. - Kiến thức về công nghệ thông tin (CNTT) bảo mật chuỗi cung ứng và các chính sách, yêu cầu và thủ tục quản lý rủi ro chuỗi cung ứng.- Kiến thức về các kỹ thuật đánh giá học tập (phiếu đánh giá, kế hoạch đánh giá, bài kiểm tra, câu đố).- Kiến thức về chính sách đào tạo của tổ chức.- Kiến thức về Khung năng lực an toàn thông tin mạng quốc gia, vai trò công việc và các nhiệm vụ liên quan, kiến ​​thức, kỹ năng và khả năng.- Kiến thức về quản lý, vận hành mạng (ví dụ: phòng thủ, tấn công, khai thác).- Kiến thức về các chính sách, quy trình và thủ tục nguồn nhân lực của tổ chức.- Kiến thức về các chính sách, quy trình và thủ tục đào tạo và giáo dục của tổ chức.- Kiến thức về các công nghệ mới có tiềm năng khai thác.- Kiến thức về các chỉ số ngành hữu ích cho việc xác định xu hướng công nghệ.- Kiến thức về các tổ chức bên ngoài và các tổ chức học thuật tập trung vào mạng (ví dụ: chương trình đào tạo/đào tạo và Nghiên cứu & Phát triển không gian mạng).- Kiến thức về các công nghệ mạng hiện tại và xu hướng mới. | - Có kỹ năng phát triển lực lượng lao động và tiêu chuẩn trình độ vị trí.- Có kỹ năng sử dụng nhân lực và hệ thống CNTT.- Có kỹ năng sư phạm, diễn đạt và thực hành tốt.- Có kỹ năng xây dựng và thực hiện các chương trình và giáo trình đào tạo kỹ thuật.- Kỹ năng xây dựng đề cương dựa trên đối tượng đào tạo về an toàn thông tin.- Có kỹ năng tự nghiên cứu, tìm tòi, tự đào tạo liên quan đến công tác đào tạo, huấn luyện, bồi dưỡng.- Có kỹ năng thực tế để xây dựng các bài thực hành các kỹ năng đảm bảo an toàn thông tin cho người dùng. |
| 9 | **Điều tra số** |  |  | **X** | **X** |
|  | - Kiến thức về các công rà quét và kỹ thuật xác định lỗi.- Kiến thức về các thành phần và kiến ​​trúc máy tính, bao gồm chức năng của các thành phần và thiết bị ngoại vi khác nhau (ví dụ: CPU, Thẻ giao diện mạng, lưu trữ dữ liệu).- Kiến thức về triển khai hệ thống tệp (ví dụ: Hệ thống tệp công nghệ mới [NTFS], Bảng phân bổ tệp [FAT], Phần mở rộng tệp [EXT]).- Kiến thức về quy trình thu giữ và bảo quản bằng chứng số.- Kiến thức về phương pháp hack.- Kiến thức về điều tra giám sát phần cứng, Hệ điều hành và công nghệ mạng.- Kiến thức về lưu dữ liệu log (ví dụ: Quy tắc về bằng chứng).- Kiến thức về các quy trình thu thập, đóng gói, vận chuyển và lưu trữ bằng chứng điện tử.- Kiến thức về các dạng dữ liệu liên tục.- Kiến thức về tệp hệ thống. (ví dụ: tệp nhật ký, tệp đăng ký, tệp cấu hình) chứa thông tin liên quan và nơi tìm các tệp hệ thống đó.- Kiến thức về các loại dữ liệu điều tra số và cách nhận biết chúng.- Kiến thức về điều tra số triển khai.- Kiến thức về các công cụ tương quan sự kiện bảo mật.- Kiến thức về kỹ thuật quản trị hệ thống, mạng, hệ điều hành.- Kiến thức về các khái niệm kiến ​​trúc an toàn, an ninh mạng bao gồm cấu trúc liên kết, giao thức, thành phần và nguyên tắc (ví dụ: ứng dụng chuyên sâu về phòng thủ).- Kiến thức về các công cụ và kỹ thuật lưu dữ liệu.- Kiến thức về chiến thuật, kỹ thuật và quy trình chống điều tra số.- Kiến thức về cấu hình thiết kế phòng thí nghiệm pháp y và các ứng dụng hỗ trợ (ví dụ: VMWare, Wireshark).- Kiến thức về các thủ tục và công cụ gỡ lỗi.- Kiến thức về việc lạm dụng loại tệp của đối thủ vì hành vi bất thường.- Kiến thức về các công cụ phân tích phần mềm độc hại (ví dụ: Oily Debug, Ida Pro).- Kiến thức về phần mềm độc hại có tính năng phát hiện máy ảo.- Kiến thức về các khái niệm quản trị hệ thống cho các hệ điều hành như hệ điều hành Unix/Linux, IOS, Android và Windows.- Kiến thức về phân tích nhị phân.- Kiến thức về các khái niệm kiến ​​trúc mạng bao gồm cấu trúc liên kết, giao thức và các thành phần.- Kiến thức về các khái niệm và thực hành xử lý dữ liệu điều tra số. - Có kiến ​​thức và hiểu biết về thiết kế vận hành.- Kiến thức về Rủi ro Bảo mật Ứng dụng | - Có kỹ năng phát triển, kiểm tra và thực hiện các kế hoạch dự phòng và khôi phục cơ sở hạ tầng mạng.- Kỹ năng bảo quản tính toàn vẹn của bằng chứng theo quy trình thao tác tiêu chuẩn hoặc tiêu chuẩn quốc gia.- Kỹ năng phân tích kết xuất bộ nhớ để trích xuất thông tin.- Kỹ năng xác định và trích xuất dữ liệu quan tâm của điều tra số trong các phương tiện truyền thông đa dạng.- Kỹ năng xác định, sửa đổi và thao tác các thành phần hệ thống áp dụng trong Windows, Unix hoặc Linux (ví dụ: mật khẩu, tài khoản người dùng, tệp).- Kỹ năng thu thập, xử lý, đóng gói, vận chuyển và lưu trữ bằng chứng điện tử để tránh thay đổi, mất mát, hư hỏng vật lý hoặc phá hủy dữ liệu.- Kỹ năng sử dụng các bộ công cụ điều tra số (ví dụ: EnCase, Sleuthkit, FTK).- Kỹ năng sử dụng máy ảo. (ví dụ: Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop / Server, Amazon Elastic Compute Cloud, v.v.).- Kỹ năng thực hiện phân tích điều tra số cho hệ điều hành (ví dụ: hệ thống thiết bị di động).- Kỹ năng phân tích sâu về mã độc (ví dụ: pháp y về phần mềm độc hại).- Kỹ năng sử dụng các công cụ phân tích nhị phân (ví dụ: Hexedit, mã lệnh xxd, hexdump).- Kỹ năng trong các hàm băm một chiều.- Kỹ năng phân tích mã bất thường là độc hại hay không độc hại.- Kỹ năng phân tích dữ liệu biến động.- Kỹ năng xác định các kỹ thuật xáo trộn.- Kỹ năng diễn giải kết quả của trình gỡ lỗi để xác định kỹ thuật và quy trình.- Kỹ năng phân tích phần mềm độc hại.- Kỹ năng xử lý bằng chứng điều tra số, bao gồm việc bảo vệ và tạo bản sao hợp pháp của bằng chứng.- Kỹ năng thực hiện phân tích mức gói. |
| 10 | **Quản trị, tổng hợp an toàn thông tin** | **X** | **X** | **X** | **X** |
|  | - Kiến thức về an ninh mạng và các nguyên tắc riêng tư được sử dụng để quản lý rủi ro liên quan đến việc sử dụng, xử lý, lưu trữ và truyền thông tin hoặc dữ liệu.- Kiến thức về các nguyên tắc phân tích tiêu chuẩn ngành và được tổ chức chấp nhận và các phương pháp.- Kiến thức về các yêu cầu của Khung quản lý rủi ro (RMF).- Kiến thức về các biện pháp hoặc chỉ số về hiệu suất và tính khả dụng của hệ thống.- Kiến thức về các phương pháp hiện tại của ngành để đánh giá, thực hiện và phổ biến đánh giá, giám sát, phát hiện và khắc phục bảo mật công nghệ thông tin.- Kiến thức về các phương pháp phân tích lưu lượng mạng.- Có kiến ​​thức về các nguyên tắc và kỹ thuật quản lý tài nguyên.- Kiến thức về quản trị máy chủ và các lý thuyết, khái niệm về kỹ thuật hệ thống và các phương pháp.- Kiến thức về các nguyên tắc quản lý vòng đời hệ thống, bao gồm bảo mật phần mềm và khả năng sử dụng.- Kiến thức về khả năng chấp nhận rủi ro và/hoặc cách tiếp cận quản lý rủi ro của tổ chức.- Kiến thức về chương trình ứng phó sự cố doanh nghiệp, vai trò và trách nhiệm.- Có kiến ​​thức về các yêu cầu mua sắm công nghệ thông tin (CNTT) quan trọng.- Kiến thức về các nguyên tắc, mô hình, phương pháp quản lý hệ thống mạng- Kiến thức về luật pháp, chính sách, thủ tục hoặc quản trị có liên quan đến an ninh mạng. | - Kỹ năng tạo chính sách phản ánh các mục tiêu bảo mật hệ thống.- Kỹ năng xác định cách thức hoạt động của hệ thống bảo mật (bao gồm khả năng phục hồi và khả năng đáng tin cậy) và những thay đổi như thế nào trong điều kiện, hoạt động của môi trường sẽ ảnh hưởng đến những kết quả này.- Kỹ năng đánh giá mức độ tin cậy của nhà cung cấp và/hoặc sản phẩm.- Có kỹ năng quản trị hệ điều hành.- Có kỹ năng giám sát và tối ưu hóa hiệu suất hệ thống/máy chủ.- Kỹ năng hỗ trợ trong công tác quản lý và điều hành việc tổ chức, hoạt động Đội Ứng cứu sự cố và duy trì công việc đảm bảo an toàn thông tin trong toàn bộ tổ chức.- Kỹ năng chẩn đoán sự cố kết nối.- Kỹ năng tham mưu, đề xuất các phương hướng liên quan đến công tác quản trị, tổng hợp.- Kỹ năng tổng hợp thông tin để kịp thời báo cáo về các sự cố, duy trì hệ thống bảo mật, ngăn chặn phá hoại.  |