**PHỤ LỤC: MÔ TẢ CÔNG VIỆC VÀ TIÊU CHUẨN TUYỂN DỤNG CỤ THỂ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TT** | **Vị trí** | **Số lượng TD** | **Mô tả công việc** | **Tiêu chuẩn tuyển dụng** |
| 1. | Chuyên viên Quản trị mạng truyền thông | **01** | * Thực hiện quản trị các hệ thống, các thiết bị mạng truyền thông phục vụ Chi nhánh BIDV được đặt tại Trung tâm xử lý, các trung tâm miền của BIDV và các Chi nhánh của BIDV.
* Tham gia thiết kế, chuẩn hóa hệ thống mạng truyền thông các đơn vị trực thuộc, Chi nhánh của BIDV.
* Hỗ trợ vận hành hệ thống mạng tại các đơn vị trực thuộc, Chi nhánh của BIDV.
 | * Chịu được áp lực công việc, mức độ đáp ứng thời gian theo yêu cầu công việc (trực giám sát, xử lý sự cố).
* Có tối thiểu 1 năm kinh nghiệm về quản trị hệ thống mạng truyền thông (mạng LAN / WAN / Internet).
* Ưu tiên các ứng viên đã tham gia khoá đào tạo hoặc có chứng chỉ chuyên môn trong lĩnh vực mạng truyền thông: CCNA, CCNP, JNCIA, JNCIP.
* Có kỹ năng làm việc độc lập và làm việc nhóm (với những nhân viên IT, quản trị viên,...khác).
 |
| 2. | Chuyên viên Quản trị hạ tầng khu vực (thiết bị đầu cuối) | **01** | * Thực hiện triển khai, vận hành, giám sát quản trị các hệ thống quản lý các thiết bị đầu cuối (máy trạm, máy in, máy chủ,…) và các TBĐC phục vụ Chi nhánh BIDV được đặt tại Trung tâm xử lý, các trung tâm miền của BIDV và các Chi nhánh của BIDV.
* Thực hiện nghiên cứu, đánh giá đề xuất giải pháp đối với công tác quản lý, vận hành các thiết bị đầu cuối mới phục vụ hoạt động của chi nhánh.
* Nghiên cứu và cập nhật công nghệ - kỹ thuật, cũng như các giải pháp để đảm bảo an toàn và bảo mật cho các thiết bị đầu cuối (quản trị,vận hành, đề xuất giải pháp).
 | * Chịu được áp lực công việc, mức độ đáp ứng thời gian theo yêu cầu công việc (trực giám sát, xử lý sự cố).
* Có tối thiểu 2 năm kinh nghiệm về quản trị hệ thống bảo mật/mạng/máy chủ. Uu tiên ứng viên có khả năng quản trị vận hành thiết bị bảo mật firewall, proxy, các thiết bị bảo mật.
* Có hiểu biết về máy tính, mạng LAN, WAN, Internet, Server, tổng đài, camera, mạng và các phần mềm hệ thống.
* Ưu tiên các ứng viên đã tham gia khoá đào tạo hoặc có chứng chỉ chuyên môn: MCSA, MCSE, CEH, CCNA, CCNP, JNCIA, JNCIP.
* Nhạy bén với những công nghệ và sản phẩm công nghệ mới.
* Có kỹ năng phân tích và tư duy logic và khả năng phát hiện vấn đề và đưa ra giải pháp khắc phục nhanh. Ưu tiên ứng viên có khả năng phân tích, giải quyết các sự cố hệ thống mạng và bảo mật.
 |
| 3. | Chuyên viên Quản trị ứng dụng  | **12** | Quản trị các ứng dụng CNTT trong ngân hàng thương mại | - Có kiến thức về các lĩnh vực xây dựng phần mềm ứng dụng, quản trị, kiểm tra nghiệm thu phần mềm.- Có hiểu biết và nắm bắt, cài đặt, quản trị, sử dụng công nghệ nền tảng như: PL/SQL, IBM COGNOS, IBM Portal và IBM Web, Apache Tomcat, Web Service, API,...- Có hiểu biết và kỹ năng xử lý về cơ sở dữ liệu Oracle, SQL Server, DB2…- Có hiểu biết và nắm bắt, cài đặt về giải pháp sẵn sàng, liên tục cho hoạt động của ứng dụng: HA (High Availability), DR (Disater Recovery), LB (Load Balancing).... - Có khả năng nghiên cứu, nắm bắt, đề xuất và áp dụng công nghệ, đề xuất các biện pháp nhằm tối ưu hoá hệ thống phần mềm ứng dụng được giao quản trị.- Có kỹ năng và kiến thức để đào tạo, phân tích, giải quyết các sự cố xảy ra đối với ứng dụng.- Có hiểu biết về nghiệp vụ ngân hàng và các hệ thống phần mềm của ngân hàng.- Ưu tiên ứng viên có các chứng chỉ về CNTT, ứng viên có kinh nghiệm quản trị các hệ thống quản trị nội bộ, quản trị các phần mềm nền tảng phục vụ triển khai các website, quản trị các hệ thống ứng dụng triển khai trên public cloud. |
| 4. | Chuyên viên Quản trị hệ thống | **04** | * Thực hiện quản trị các hệ thống máy chủ, lưu trữ, sao lưu/phục hồi dữ liệu tại Trung tâm xử lý và Trung tâm dự phòng thảm họa.
* Thực hiện quản trị các loại hệ điều hành Linux, Windows… và các nền tảng ảo hóa Vmware, Microsoft, IBM…
* Tham gia quy hoạch và tối ưu hệ thống.
* Tham gia phân tích thiết kế các chương trình ứng dụng liên quan đến phần hệ hệ thống (máy chủ, lưu trữ, sao lưu/phục hồi dữ liệu).
* Nghiên cứu/Tham gia nghiên cứu, thử nghiệm, triển khai các công cụ quản trị, các giải pháp, công nghệ mới về hệ thống (máy chủ, lưu trữ, sao lưu/phục hồi dữ liệu, cloud…).
 | * Chịu được áp lực công việc cao, chấp nhận trực theo dõi, giám sát hệ thống và xử lý sự cố theo yêu cầu của công việc. Thái độ làm việc nghiêm túc, cẩn thận, nhiệt tình.
* Có khả năng nghiên cứu, học hỏi công nghệ nhanh.
* Có kỹ năng giao tiếp, xử lý tình huống.
* Có khả năng làm việc theo nhóm hoặc độc lập.
* Có kinh nghiệm quản trị hệ thống máy chủ, hệ thống lưu trữ là một lợi thế.
* Có một trong các chứng chỉ MCITP-SA/Oracle Certified Associate/Oracle Solaris 11 System Administrator Certification/Linux Professional Institute LPIC-1 là một lợi thế.
 |
| 5. | Chuyên viên Quản trị CSDL | **03** | - Quản trị hệ thống CSDL bao gồm cài đặt/cấu hình/tối ưu các CSDL sau: Oracle, DB2, Sql Server, Mongodb, Postgresql, Sybase, Netezza, Sailfish,…- Tham gia kiểm tra, nghiệm thu, triển khai, cập nhật CSDL- Giám sát, theo dõi, cảnh báo, xử lý các vấn đề liên quan CSDL- Tham gia phân tích thiết kế các chương trình ứng dụng liên quan đến cấu phần CSDL- Nghiên cứu, thử nghiệm, triển khai các công cụ, giải pháp, công nghệ mới về CSDL. | - Chịu được áp lực công việc cao, theo dõi, giám sát, quản trị CSDL và xử lý sự cố theo yêu cầu công việc.- Thái độ làm việc nghiêm túc, cẩn thận, nhiệt tình.- Ưu tiên các ứng viên:+ Có khả năng nghiên cứu.+ Có kinh nghiệm quản trị các CSDL Oracle, DB2, Sql Server, Mongodb, Postgresql, Sybase, Netezza, Sailfish,…+ Có chứng chỉ quản trị CSDL |
| 6. | Chuyên viên Giám sát vận hành CNTT 24/7 | **03** | * Giám sát hệ thống CNTT 24/7: Theo dõi cảnh báo các hệ thống CNTT, cơ sở hạ tầng theo hướng dẫn; Thông báo lỗi cho các đầu mối xử lý đúng thời gian quy định; Tổng hợp báo cáo ca trực giám sát…
* Thực hiện công tác vận hành cuối ngày (Batchrun) hệ thống Corebanking.
 | * Tốt nghiệp Đại học, chuyên ngành: Máy tính, Công nghệ thông tin
* Ưu tiên các ứng viên: Có kinh nghiệm giám sát/vận hành/hỗ trợ hệ thống CNTT
 |
| 7. | Chuyên viên Quản lý vận hành Trung tâm dữ liệu | **04** | Thực hiện công tác quản lý vận hành Trung tâm dữ liệu (TTDL):* Vận hành và xử lý các lỗi của hệ thống cơ điện lạnh, hệ thống giám sát và hệ thống phụ trợ.
* Giám sát hoạt động hệ thống cơ sở hạ tầng (CSHT) TTDL 24/7.
* Thực hiện công tác bảo trì các hệ thống CSHT.
* Thực hiện các công tác quản lý TTDL như kiểm soát vào ra, quản lý tài sản…
 | * Tốt nghiệp Đại học, chuyên ngành: Máy tính, Công nghệ thông tin, Điện, Tự động hóa
* Ưu tiên các ứng viên: Có kinh nghiệm quản lý vận hành các hệ thống CSHT (điện, điều hòa, hệ thống giám sát...) trong Trung tâm dữ liệu
 |
| 8. | Chuyên viên Triển khai và phát triển ứng dụng | **10** | Thực hiện phát triển các phần mềm nội bộNắm bắt soure code ứng dụng, thực hiện công tác sửa lỗi các ứng dụng phần mềmTiếp nhận triển khai ứng dụng bao gồm front end, back end, cơ sở dữ liệu và source codeTham gia vào quá trình xây dựng yêu cầu người sử dụng, phân tích thiết kế hệ thốngTham gia các dự án CNTT trong lĩnh vực ngân hàng | Tốt nghiệp chuyên ngành CNTT, điện tử viễn thông, công nghệ máy tính, công nghệ phát triển phần mềm.- Có tư duy lập trình, phân tích thiết kế hệ thống tốt, khả năng nghiên cứu nắm bắt công nghệ mới- Tinh thần cầu tiến, chủ động trong mọi công việc và làm việc teamwork cao.- Có kỹ năng giao tiếp, xử lý tình huống.- Thái độ làm việc nghiêm túc, cẩn thận, nhiệt tình.Ưu tiên:* Đã tham gia phát triển, triển khai các dự án phần mềm trong lĩnh vực tài chính, hiểu biết các phần mềm ngân hàng
* Hiểu biết về nghiệp vụ ngân hàng
* Hiểu và nắm bắt được một trong các nền tảng công nghệ sau: Node JS, Angular, Tibco, Websphere, WAS, Oracle, SQL Server, IBM Cognos, IBM Data Stage, Datawarehouse
 |
| 9. | Chuyên viên Quản lý dự án CNTT | **03** | 1. Tham gia vào các giai đoạn của dự án CNTT để phục vụ cho công tác tổ chức, thực hiện:- Giai đoạn khởi tạo trước dự án (tham gia nắm bắt thông tin và xây dựng dự án).- Giai đoạn bắt đầu dự án, ký hợp đồng (tham gia nắm thông tin tổ chức thực hiện).- Giai đoạn triển khai hợp đồng.- Giai đoạn đóng dự án, nghiệm thu, thanh toán.2. Tổ chức quản trị triển khai dự án:- Xác định các bên liên quan trong dự án, đánh giá phạm vi ảnh hưởng để có định hướng phù hợp quản trị công việc.- Lên kế hoạch thời gian thực hiện và phối hợp các bên thống nhất kế hoạch.- Kiểm soát các tiêu chí chất lượng trong dự án.- Trao đổi, báo cáo và đánh giá diễn biến triển khai của dự án để có các đề xuất điều chỉnh hợp lý.- Chủ động phối hợp các bên xác định rủi ro và có các kế hoạch phòng ngừa chủ động.- Phối hợp với các bộ phận nội bộ BIDV để phục vụ triển khai dự án. | - Tốt nghiệp chuyên ngành CNTT, điện tử viễn thông, công nghệ máy tính, công nghệ phát triển phần mềm.- Tinh thần cầu tiến, chủ động trong mọi công việc và làm việc team\_work cao.- Có kỹ năng giao tiếp, xử lý tình huống.- Thái độ làm việc nghiêm túc, cẩn thận, nhiệt tình.Ưu tiên:- Ứng viên có chứng chỉ QTDA quốc tế PMP.- Ứng viên có kinh nghiệm với các giải pháp công nghệ mới ngành tài chính ngân hàng: giải pháp bảo mật ngành ngân hàng, giải pháp thẻ, ngân hàng số, ngân hàng di động … |
| 10. | Chuyên viên Kiểm tra nội bộ | **02** | * Thực hiện công tác kiểm tra đối với các hoạt động của Trung tâm CNTT
* Thực hiện phân tích và quản lý rủi ro đối với các hoạt động của Trung tâm CNTT
 | * Tốt nghiệp đại học chuyên ngành về CNTT (như điện tử viễn thông, công nghệ máy tính, phát triển phần mềm...)
* Có khả năng nghiên cứu, học hỏi công nghệ nhanh
* Có kỹ năng giao tiếp, xử lý tình huống
* Có khả năng làm việc theo nhóm hoặc độc lập
* Thái độ làm việc nghiêm túc, cẩn thận, nhiệt tình, hợp tác
* Có khả năng đọc, nghiên cứu các văn bản, quy định, tài liệu
* Có khả năng quan sát, nắm bắt hoạt động của đơn vị, xác định được các yêu cầu hoạt động theo quy định và logic để kiểm tra, đánh giá

***Ưu tiên:**** Có kinh nghiệm thực hiện kiểm tra, kiểm toán, đánh giá hoạt động của các đơn vị
* Có kinh nghiệm thường xuyên làm việc với các đơn vị kiểm tra, kiểm toán
 |
| 11. | Chuyên viên đánh giá bảo mật ứng dụng | **05** | - Kiểm tra, đánh giá an ninh bảo mật ứng dụng, dịch vụ của BIDV.- Đánh giá, kiểm thử an ninh bảo mật hệ thống CNTT: Máy chủ, ứng dụng, CSDL, …- Nghiên cứu, xây dựng, đề xuất các giải pháp, công cụ an ninh bảo mật.- Đề xuất xây dựng các quy trình, checklist về đánh giá bảo mật ứng dụng.- Tham gia triển khai các giải pháp an ninh bảo mật cho ứng dụng. | - Tốt nghiệp (hoặc chuẩn bị tốt nghiệp) các trường đại học trong nước và quốc tế với chuyên ngành: Công nghệ thông tin, Điện tử viễn thông, An toàn thông tin, Toán tin, … - Có hiểu biết về các lỗ hổng bảo mật ứng dụng (OWASP Top 10, CWE, CVE, …).- Có những chứng chỉ liên quan đến Pentest như CEH/OSCP/OSWE/OSCE/GPEN, … là một lợi thế. |
| 12. | Chuyên viên rà soát, quản lý lỗ hổng | **02** | - Thực hiện rà soát điểm yếu bảo mật, kiểm toán bảo mật các thành phần trong hệ thống CNTT (máy chủ, ứng dụng, CSDL, thiết bị mạng, thiết bị bảo mật, …) để phát hiện các điểm yếu, rủi ro về an toàn bảo mật đang tồn tại.- Đánh giá mức độ ảnh hưởng của các điểm yếu bảo mật đối với hệ thống để đưa ra phương án và khuyến nghị khắc phục.- Cảnh báo, hướng dẫn và phối hợp với các bộ phận khác xử lý các điểm yếu bảo mật được cảnh báo.- Kiểm ra, rà soát kết quả khắc phục các điểm yếu bảo mật. | - Tốt nghiệp (hoặc chuẩn bị tốt nghiệp) các trường đại học trong nước và quốc tế với chuyên ngành: Công nghệ thông tin, Điện tử viễn thông, An toàn thông tin, Toán tin, … - Có hiểu biết về các lỗ hổng bảo mật ứng dụng (OWASP Top 10, CWE, CVE, …).- Có hiểu biết về các tiêu chuẩn bảo mật ví dụ như ISO 27001 (ISO 27005), PCI DSS, CIS, NIST, …- Có những chứng chỉ bảo mật như CEH, CISA, SECURITY+, … là một lợi thế. |
| 13. | Chuyên viên an ninh sản phẩm | **02** | - Xây dựng, hoàn thiện các quy trình bảo mật (quy trình đánh giá bảo mật ứng dụng, quy trình phối hợp theo dõi khắc phục lỗ hổng bảo mật,….), các tiêu chuẩn bảo mật (tiêu chuẩn bảo mật ứng dụng web/mobile/api, tiêu chuẩn OS Hardening/Database Hardening, …) cho các hệ thống ứng dụng.- Nghiên cứu thử nghiệm, đề xuất và tham gia triển khai tích hợp các cấu phần, tính năng, giải pháp về an toàn bảo mật trong phát triển ứng dụng của BIDV.- Tham gia ý kiến đánh giá đề xuất phương án tăng cường an ninh bảo mật đối với các sản phẩm dịch vụ, hệ thống ứng dụng CNTT tại BIDV.- Rà soát, chuẩn hóa các thư viện, cấu phần bảo mật ứng dụng đảm bảo an toàn, đáp ứng kiến trúc bảo mật đang được áp dụng. | - Tốt nghiệp (hoặc chuẩn bị tốt nghiệp) các trường đại học trong nước và quốc tế với chuyên ngành: Công nghệ thông tin, Điện tử viễn thông, An toàn thông tin, Toán tin, … - Có kinh nghiệm 02 năm trong lĩnh vực bảo mật ứng dụng hoặc tương đương.- Có hiểu biết về các lỗ hổng bảo mật ứng dụng (OWASP Top 10, CWE, CVE, …).- Có hiểu biết về các tiêu chuẩn bảo mật ví dụ như ISO 27001 (ISO 27005), PCI DSS, CIS, NIST, …- Có những chứng chỉ bảo mật chuyên sâu như CISSP/GSEC/OSCP/OSWE/OSCE … là một lợi thế. |
| 14 | Chuyên viên Bảo mật (Red Team) | **03** | - Công việc của Red Team tập trung vào việc kiểm thử xâm nhập ở các hệ thống với các mức độ bảo mật phần mềm khác nhau, phát hiện, ngăn chặn và khắc phục các lỗ hổng bảo mật.- Red Team mô phỏng lại các cuộc tấn công có thật, có thể nhắm vào một sản phẩm hoặc một hệ thống/ đơn vị và thực hiện tất cả các các bước cần thiết mà kẻ tấn công có thể sử dụng. Bằng việc đóng vai một kẻ tấn công, Red Team cho thấy được những lỗ hổng bảo mật hoặc các “cửa hậu” có thể bị lợi dụng để đe dọa an ninh mạng.- Nắm rõ về những nguy cơ lợi dụng dữ liệu và ngăn chặn việc rò rỉ trong tương lai bằng việc mô tả các cuộc tấn công mạng và các nguy cơ an minh mạng. | - Tốt nghiệp (hoặc chuẩn bị tốt nghiệp) các trường đại học trong nước và quốc tế với chuyên ngành: Công nghệ thông tin, Điện tử viễn thông, An toàn thông tin, Toán tin, …- Hiểu rõ gốc rễ vấn đề (root-cause) của các lỗ hổng bảo mật (theo OWASP, CWE), cách khai thác lỗ hổng thủ công (manual exploit – không sử dụng các công cụ tự động), cách lập trình an toàn (secure coding) và khắc phục lỗi tương ứng (Bắt buộc).- Hiểu biết về các bước (phase) trong lĩnh vực Red Team. Có kinh nghiệm sử dụng các công cụ hỗ trợ trong quá trình Pentest cũng như các công cụ trong từng Red Team phase.- Có khả năng lập trình một trong những ngôn ngữ kịch bản để viết mã khai thác (Bash, Powershell, Python, Perl, Java, .Net, …), có khả năng sửa, tạo các mã khai thác cho web, OS, …- Có khả năng nghiên cứu chuyên sâu, cách debug trên các ngôn ngữ nhằm xây dựng lại mã khai thác liên quan tới các lỗ hổng bảo mật 1-day hay phát hiện các lỗ hổng 0-day là một lợi thế.- Có hiểu biết về các cơ chế phòng thủ/giám sát của blue-team nhằm tìm cách bypass/ẩn mình trước các cơ chế này là một lợi thế.- Từng tham gia, đạt giải các cuộc thi về ATTT, CTF là một lợi thế.- Tham gia các chương trình bug bounty, có các CVE hay có các bài viết phân tích các lỗ hổng bảo mật chuyên sâu là một lợi thế.- Có khả năng đọc hiểu Tiếng Anh đủ tốt cho các tài liệu chuyên ngành.- Có những chứng chỉ liên quan đến Pentest, Redteam như OSCP/OSWE/OSCE/GPEN, … là một lợi thế.- Có khả năng làm việc độc lập, có tính tự giác, chủ động trong công việc. |
| 15. | Chuyên viên Giám sát an ninh mạng 24/7 (Tier 1) | **05** | - Giám sát trạng thái an ninh của toàn bộ hệ thống công nghệ thông tin theo thời gian thực trên một giao diện quản lí tập trung duy nhất.- Giám sát, phát hiện và cảnh báo bất thường tại từng nút mạng hoặc trên từng thiết bị. - Phân tích và cảnh báo sớm các điểm yếu, nguy cơ an ninh có thể xảy ra.- Hỗ trợ ứng cứu và xử lí các sự cố an ninh mạng.- Xử lý các sự kiện theo qui trình nghiệp vụ, tự động hóa trong công tác vận hành hệ thống. | - Tốt nghiệp (hoặc chuẩn bị tốt nghiệp) các trường đại học trong nước và quốc tế với chuyên ngành: Công nghệ thông tin, Điện tử viễn thông, An toàn thông tin, Toán tin, …- Có kiến thức về hệ thống CNTT, hệ điều hành, phần cứng, mạng truyền thông và bảo mật CNTT.- Nắm vững cơ chế, quy chế, quy trình, quy định của Nhà nước, ngành, BIDV về bảo mật thông tin.- Có kiến thức cơ bản về luật pháp.- Có kỹ năng giải quyết vấn đề.- Có khả năng làm việc theo nhóm.- Nhiệt tình trong công việc. |
| 16. | Chuyên viên Bảo mật (Blue Team) | **01** | - Tiếp nhận và xử lý các sự cố an ninh mạng.- Phân tích, đánh giá ảnh hưởng, mức độ nghiêm trọng của các sự cố an ninh mạng và đưa ra biện pháp xử lý, phản ứng với các sự cố an ninh mạng.- Triển khai các công cụ, giải pháp giám sát an ninh mạng.- Quản trị, vận hành các hệ thống giám sát an ninh mạng như SIEM, SOAR…- Hoàn thiện các quy trình vận hành, giám sát, xử lý sự cố an ninh mạng. | - Tốt nghiệp (hoặc chuẩn bị tốt nghiệp) các trường đại học trong nước và quốc tế với chuyên ngành: Công nghệ thông tin, Điện tử viễn thông, An toàn thông tin, Toán tin, …- Có hiểu biết về các hệ thống giám sát an ninh mạng, hệ thống quản lý và phân tích sự kiện bảo mật như SIEM, SOAR…- Có hiểu biết về các lỗ hổng bảo mật (theo OWASP, CWE), các cách thức tấn công mạng để đưa ra các biện pháp phòng thủ.- Có hiểu biết về quy trình giám sát và xử lý sự cố an ninh mạng. - Có hiểu biết về các cơ chế tấn công mạng nhằm tìm cách phòng thủ trước các cơ chế này là một lợi thế.- Từng tham gia, đạt giải các cuộc thi về ATTT, CTF là một lợi thế.- Có khả năng đọc hiểu Tiếng Anh đủ tốt cho các tài liệu chuyên ngành.- Có các chứng chỉ an ninh bảo mật là một lợi thế.- Có khả năng làm việc độc lập, có tính tự giác, chủ động trong công việc. |
| 17. | Chuyên viên Phân tích sự kiện bảo mật (Forensic Team) | **01** | - Có chức năng chủ động rà quét, săn tìm các sự cố bảo mật.- Phân tích mã độc.- Nghiên cứu, áp dụng các công nghệ mới về an ninh bảo mật.- Phát triển, tối ưu hóa và thực hiện phân tích giải pháp phát hiện nguy cơ, tăng hiệu quả của việc giám sát an ninh mạng và xử lý sự cố.- Tiếp nhận và đưa ra các giải pháp xử lý các sự kiện bảo mật mức độ ảnh hưởng cao/nghiêm trọng. | - Tốt nghiệp (hoặc chuẩn bị tốt nghiệp) các trường đại học trong nước và quốc tế với chuyên ngành: Công nghệ thông tin, Điện tử viễn thông, An toàn thông tin, Toán tin, …- Có tính chủ động, có khả năng tư duy, tự nghiên cứu, đọc hiểu các tài liệu chuyên ngành liên quan tới các giải pháp an ninh bảo mật.- Có tư duy về lập trình, có thể sử dụng ít nhất một trong những ngôn ngữ lập trình như JS, Python, Java, …- Có hiểu biết về các kỹ thuật tấn công, có khả năng xây dựng giả lập các tấn công theo các phase trong cyber kill chain là một lợi thế.- Có khả năng đọc hiểu Tiếng Anh đủ tốt cho các tài liệu chuyên ngành.- Có một trong các chứng chỉ liên quan đến Malware Analysis, Incident response, Forensic như CHFI/GCFA/GCIH/GREM… là một lợi thế.- Có khả năng làm việc độc lập, có tính tự giác, chủ động trong công việc. |
| 18. | Chuyên viên bảo mật dữ liệu cá nhân | **01** | - Xây dựng tiêu chuẩn phân loại, nhận diện và xây dựng quyền chủ thể dữ liệu nhạy cảm quan trọng của cá nhân.- Thực hiện các thủ tục đánh giá rủi ro liên quan tới công tác xử lý dữ liệu cá nhân trong nội bộ.- Rà soát, xây dựng và cập nhật những tài liệu quy trình và hướng dẫn thực hiện tuân thủ với quy định mới của chính phủ và thế giới về bảo mật dữ liêu cá nhân.- Nghiên cứu, đề xuất các giải pháp, công cụ bảo vệ toàn vẹn dữ liệu, giám sát và ngăn chặn các hành vi trộm cắp dữ liệu cá nhân | - Có tối thiểu 02 năm kinh nghiệm trong lĩnh vực an toàn bảo mật- Có hiểu biết về các tiêu chuẩn về an toàn bảo mật hệ thống thông tin ví dụ như: ISO 27001, PCI DSS, CIS, NIST, GDPR … |
| 19 | Chuyên viên quản lý chính sách An toàn thông tin | **01** | - Quản lý các chính sách, quy định, quy trình về an toàn bảo mật hệ thống thông tin.- Lập kế hoạch triển khai thực hiện tuân thủ theo các chính sách, quy định của Nhà Nước và BIDV đối với lĩnh vực an toàn bảo mật CNTT- Nghiên cứu và đề xuất xây dựng các chính sách, quy trình về an toàn bảo mật thông tin tuân thủ theo các quy định của pháp luật, và theo các tiêu chuẩn/thông lệ quốc tế. | - Có tối thiểu 02 năm kinh nghiệm trong lĩnh vực an toàn bảo mật- Có hiểu biết về các tiêu chuẩn về an toàn bảo mật hệ thống thông tin ví dụ như: ISO 27001, PCI DSS, CIS, NIST, … |
|  | **Tổng:** |  **64** |  |  |