

NCS기반 채용직무설명자료 : 정보통신(경력)

채용분야	정보통신	대분류	중분류	소분류	세분류
		20. 정보통신	01.정보기술	02.정보기술개발	06.보안엔지니어링
			01.정보기술	03.정보기술운영	01.IT시스템관리
			01.정보기술	06.정보보호	03.보안사고분석대응
능력단위	<ul style="list-style-type: none"> ○ (보안엔지니어링) 01.보안 구축 계획 수립, 03.보안 구축 요구사항 분석, 04.관리적 보안 구축, 05.물리적 보안 구축 ○ (IT시스템관리) 01.IT시스템 운영 기획, 02.IT시스템 자원획득관리, 03.IT시스템 서비스 수준관리, 08.DB 운영관리 ○ (IT기술지원) 03.기술지원 요청 관리, 04.시스템 장애 대응, 05.시스템 개선 대응, 12.기술지원 품질운영 ○ (보안사고분석대응) 05.침해사고 분석, 06.악성코드 분석, 08.보안사고 대응 				
직무수행내용	<ul style="list-style-type: none"> ○ (보안엔지니어링) 정보 서비스의 보안 요구사항에 따라 정보보안시스템 도입을 위한 설계, 구축, 유지보수 수행 ○ (IT시스템관리) 시스템을 안정적이고 효율적으로 운영하고 관리하기 위하여 하드웨어 및 소프트웨어의 지속적 점검과 모니터링을 통해 제시된 제반 문제점들을 분석하여 사전 예방활동 및 발생된 문제에 대해 적절한 조치를 취함 ○ (IT기술지원) 고객서비스 대상 정보시스템이나 솔루션의 구축 환경에 대한 이해를 바탕으로 전문 기술 지원 체제를 갖추고 고객 요청에 따라 장애 처리, 시스템 개선 및 정기 점검 등을 수행하고 관리함 ○ (보안사고분석대응) 보안사고의 위협정보를 탐지하고, 시스템 복구와 예방 전략을 수립하는 일과 보안사고로 인한 업무 및 서비스에 영향을 준 증거를 확보 후 분석하여 신속하게 대응 				
필요지식	<ul style="list-style-type: none"> ○ 사이버 침해사고에 대한 지식 ○ OS, 시스템, 네트워크, 어플리케이션, DB, 업무 프로세스에 대한 보안지식 ○ 관리적, 물리적, 기술적 특성별 위협과 취약점에 대한 지식 ○ 사이버 공격에 대한 이해 및 공격 유형별 개념 / 사이버 공격 기법 및 활용 도구에 대한 지식 ○ 도출된 취약점 조치를 위한 지식 ○ IT 시스템별 취약점 및 대응방안에 대한 지식 ○ IT 운영환경 및 업무에 대한 지식 ○ 발견된 취약점에 대한 대응 및 보안 통제에 대한 지식 ○ 보안 통제의 Best Practice에 대한 지식 ○ 네트워크와 시스템 이론 / 모의해킹 유형 관련 지식 / 스크립트 코딩 관련 지식 ○ 침입대응, 분석 실무에 필요한 정보 수집 및 활용 방법 ○ 네트워크와 시스템 보안 설정 지식 ○ 가상환경 및 가상화 프로그램에 대한 지식 ○ 프로그램 컴파일러에 대한 지식 ○ OS, WAS/DB 이벤트 로그 형식 및 저장 방식 ○ 네트워크 패킷 구조 ○ 보안시스템 별 탐지정책 및 이벤트 동작 매커니즘 ○ 웹어플리케이션 동작 매커니즘 및 로그 형식 ○ 웹언어에 대한 코딩 이해 / 인코딩, 디코딩, 난독화에 대한 이해 ○ 통합보안관제시스템 동작 원리 ○ 정규식에 대한 이해 ○ 보안 이벤트 유형/ 보안이벤트 대응 절차 ○ 정보시스템의 정상 운영 상태에 대한 지식 ○ 클라우드 컴퓨팅 서비스 및 보안관리 방안 ○ 해킹 이론 				

<p>필요기술</p>	<ul style="list-style-type: none"> ○ 보안활동에 영향을 미치는 업무 특성 분석 기술 ○ 보안이슈 및 사이버침해사고 조사 활용 능력 ○ 시스템, 네트워크, 어플리케이션, DB 등 정보시스템 구성과 보안적용 분석 능력 ○ 취약점 진단 및 모의해킹 도구 활용 능력 ○ 악성코드 행위 분석 기술 ○ 프로그램 행위에 따른 악성코드 여부 판단에 대한 기술 ○ 루트킷, 스크립트 분석도구 사용법에 대한 기술 ○ 파일, 프로세스, 레지스트리 분석을 위한 다양한 분석도구 사용법에 대한 기술 ○ 자산 식별 및 자산 중요도 평가 능력 ○ 관리적, 물리적, 기술적 통합 차원의 복합적인 아키텍처 설계 능력 ○ 정보 자산에 접근 가능한 시스템, 네트워크, 어플리케이션 사용자 식별 능력 ○ 시스템, 네트워크, 어플리케이션, DB 등 IT운영환경 분석 능력 ○ 정보시스템 운영 및 취약점 판단 능력 ○ 정보시스템별 취약점에 대한 개선사항 및 보호대책 수립 능력 ○ 정보시스템별 취약점에 대한 위험처리 적용 능력 ○ 네트워크, 시스템, 어플리케이션, DB 보안취약점 대응·발견·분석 능력 ○ 네트워크와 시스템 식별 및 탐색 기술 ○ 네트워크와 시스템 로그분석, 보안취약점 분석, 분석도구 사용 기술 ○ 네트워크 취약점 점검 능력 ○ 시스템, 네트워크 어플리케이션 기반 취약점에 대한 대응 기술 ○ 운영체제별 사용법에 대한 기술 ○ 클라우드 컴퓨팅 서비스 보안관리 및 취약점 분석 기술 ○ 해킹 대응 능력
<p>직무수행태도</p>	<ul style="list-style-type: none"> ○ (보안엔지니어링) 목표하는 보안 시스템의 기능과 성능향상을 위한 노력, 보안사고의 근본 원인을 파악하려는 노력 ○ (IT시스템관리) 현재 수준에 대한 개선 의지, 장애처리 후 또 다른 장애여부 확인하는 의식, 주어진 현상의 근본 원인을 식별하려는 탐구심 ○ (IT기술지원) 품질 통제를 적극적으로 수행할 수 있는 적극적인 태도, 다양한 시각으로 장애 처리 방안 접근 노력, 분석적이고 논리적인 사고 ○ (보안사고분석대응) 침해사고 근본원인을 파악하려는 노력, 다양한 분석도구 사용법을 습득하고자 하는 노력, 정보보호 관련 법률 및 정보보호 윤리를 엄수하고자 하는 태도, 신규 보안취약점 및 대응 방법에 대해 지속적으로 연구하는 노력
<p>직업기초능력</p>	<p>의사소통능력, 문제해결능력, 정보능력, 기술능력, 대인관계능력</p>
<p>참고</p>	<p>http://www.ncs.go.kr</p>