미래창조과학부 KISA 한국인터넷진흥원 Korea Internet & Security Agency

정보보호 진로 가이드 북

정보보호 직업의 종류, 교육 · 훈련 로드 맵

정보보호 경력 개발을 위한 '교육 · 훈련' 안내서

보안 컨설턴트
진단/평가 분야 Analyze

침해사고 대응 전문가
사전 침투/방어 Protect and Defend

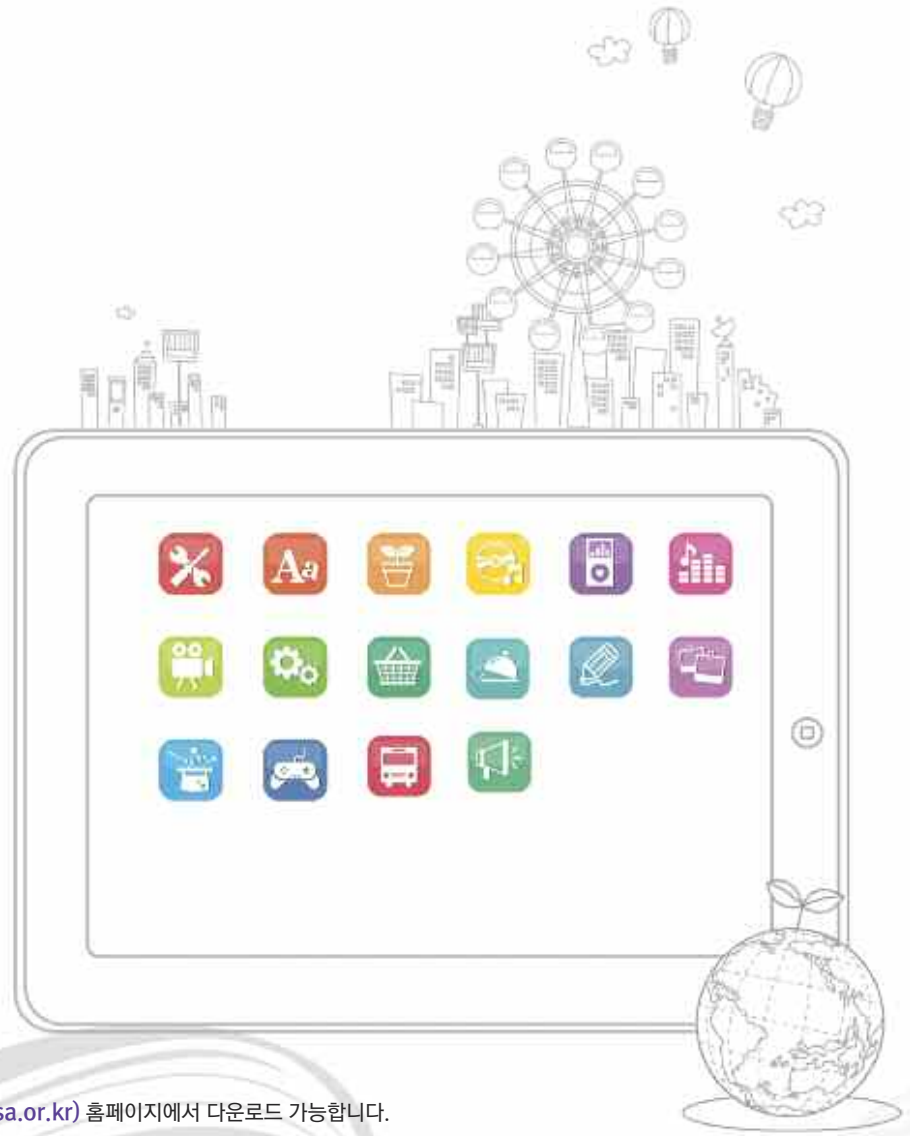
디지털 포렌식 전문가
사후조사 분야 Investigate

보안 관리자
관리 분야 Operate and Maintain

악성코드 분석 전문가
수집/해독 분야 Collect and Operate

보안제품 개발자
개발 분야 Securely Provision

최고 보안 관리자
감독/총괄 분야 Oversight and Development

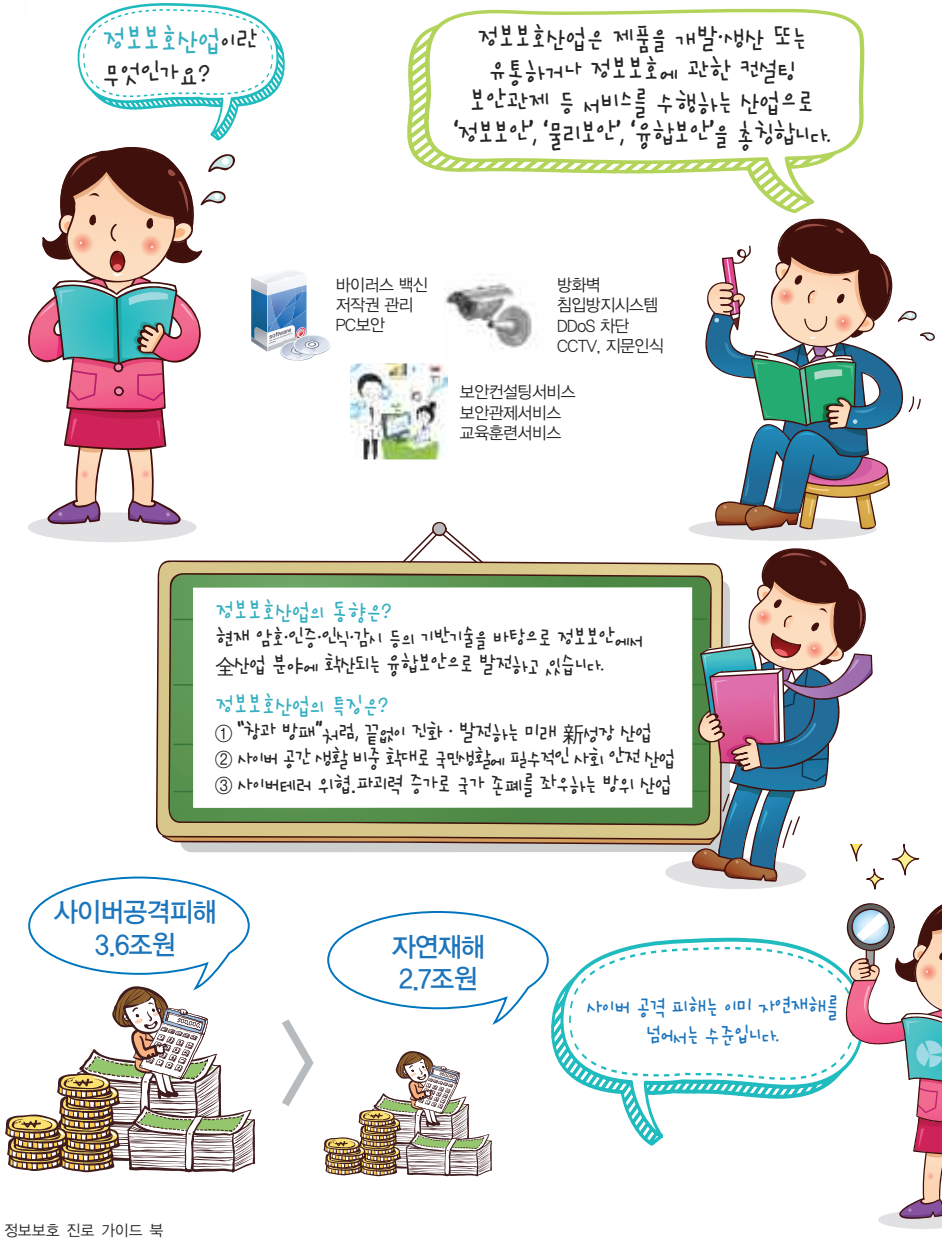


2014
정보보호 진로 가이드 북

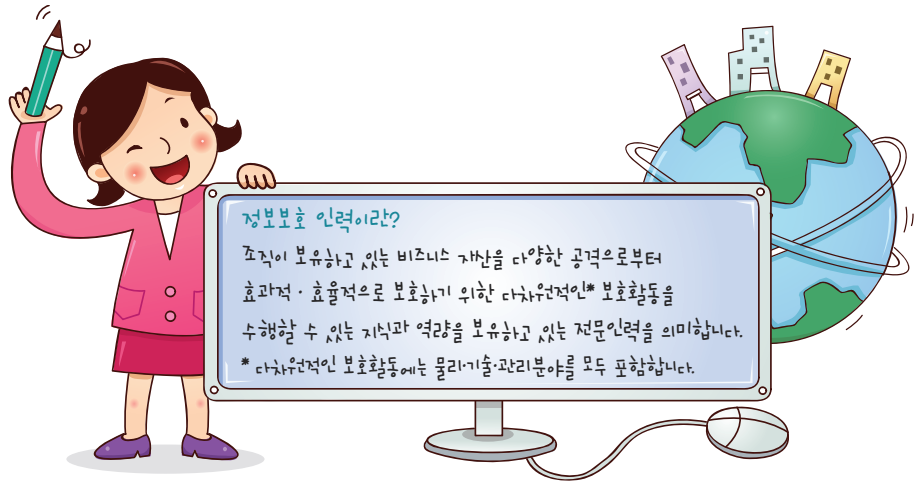
C · O · N · T · E · N · T · S

정보보호 진로 가이드 북은
한국인터넷진흥원 KISA 아카데미(academy.kisa.or.kr) 홈페이지에서 다운로드 가능합니다.

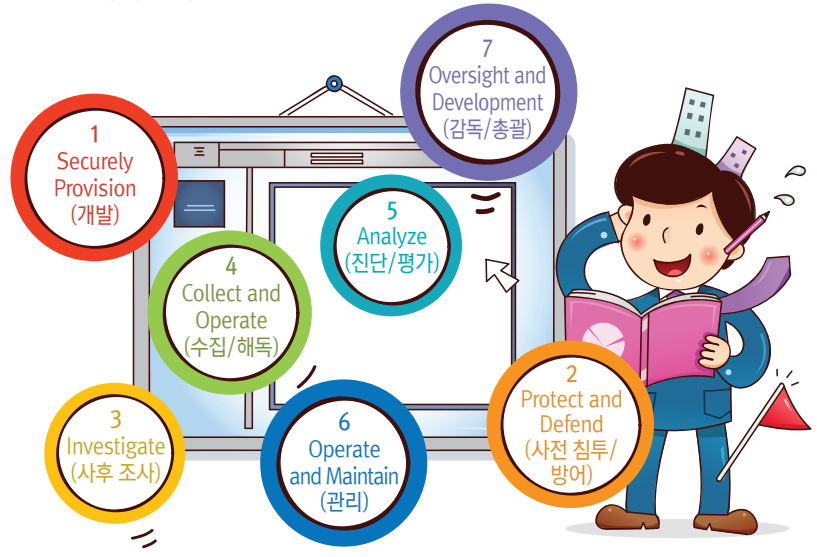
정보보호 산업



정보보호 인력



정보보호 인력의 분류



보안제품 개발자 개발
Security System Developer

정보보호 관련 사고를 미연에 방지하기 위해서 보안이 필요한 분야에서 요구되는 소프트웨어 프로그램을 개발하는 전문가를 말합니다.

SW 분석/설계 전문가, SW 개발자, 보안제품 기술자, SW 테스트 기술자(품질 관리자), 보안제품 기술영업

수집/해독 악성코드 분석 전문가
Malicious Code Analysis Specialist

새로운 악성코드를 분석하여 감염 경로나 방법–증산–치료 방법 등을 개발하고 치료할 수 있는 백신프로그램을 제작하는 일을 하는 전문가를 이야기 합니다.

암호/해독 전문가

사전침투/방어 침해사고 대응 전문가
Incident Handling Specialist

보안사고가 발생했을 때 피해규모를 최소화하기 위해 사고를 보고하고 시스템을 복구하고 예방전략을 수립하는 일을 하는 전문가를 이야기합니다.

사이버 보안 관제사(보안관제요원), 취약성 분석 전문가, 모의 해킹 전문가

보안 컨설턴트 진단/평가
Security Consultant

고객의 정보자산과 비즈니스 프로세스에 따른위협 및 취약점을 분석하여 보안 수준을 파악하고, 요구수준에 맞는 통합적인(기술 + 관리) 보안 해결책을 설계하는 전문가를 이야기합니다.

정보시스템 감리사, 정보시스템 보안감사, 보안제품 인증 전문가, 보안관리 인증 전문가, 보안기술 컨설턴트, 사이버 보안 관제사(보안관제요원)

디지털 포렌식 전문가 사후 조사
Digital Forensic Specialist

정보자산을 위협하여 보안사고를 발생시키는 요인에 대하여 증거를 수집하여 복구하고 추적하는 활동을 수행하는 일을 합니다.

사이버 범죄 수사관

관리 보안관리자
Security Manager

조직관점에서 보안이라는 목적을 달성하기 위하여 보안과 관련된 정책–관리체계–시스템 구축–운영(관리)업무를 실제적으로 수행하는 전문가를 이야기합니다.

지식 관리자, DB 보안 관리자, 정보시스템(네트워크) 관리자, 보안시스템 관리자, 개인정보보호 관리자

최고 보안 관리자(보안전략전문가) 감독/총괄
Chief Security Manager(Security Strategy Specialist)

조직의 경영 관점에서 전체적인 보안전략을 총괄적–통합적으로 수립하고 운영하며 조정하는 전문가를 이야기합니다.

보안관리 기획자, 준법 감시자, 보안 교육 전문가(변화관리전문가), 보안전문 검사/변호사, 개인정보보호 전문가, 보안전문 교수/기자, 국제 보안 전문가

1 보안제품 개발자

개발 분야 Securely Provision

정보보호 관련 사고를 미연에 방지하기 위해서 보안이 필요한 분야에서 요구되는 소프트웨어 프로그램을 개발하는 전문가를 말합니다.

1 보안제품 개발자는 무엇인가요?

정보보호 관련 사고를 미연에 방지하기 위해서 보안이 필요한 분야에서 요구되는 소프트웨어 프로그램을 개발하는 전문가를 말합니다.

K
- 현재 또는 향후 발생 가능할 보안위협에 대한 지식

S
- 보안 시스템 품질검증(성능측정/보정) 기술

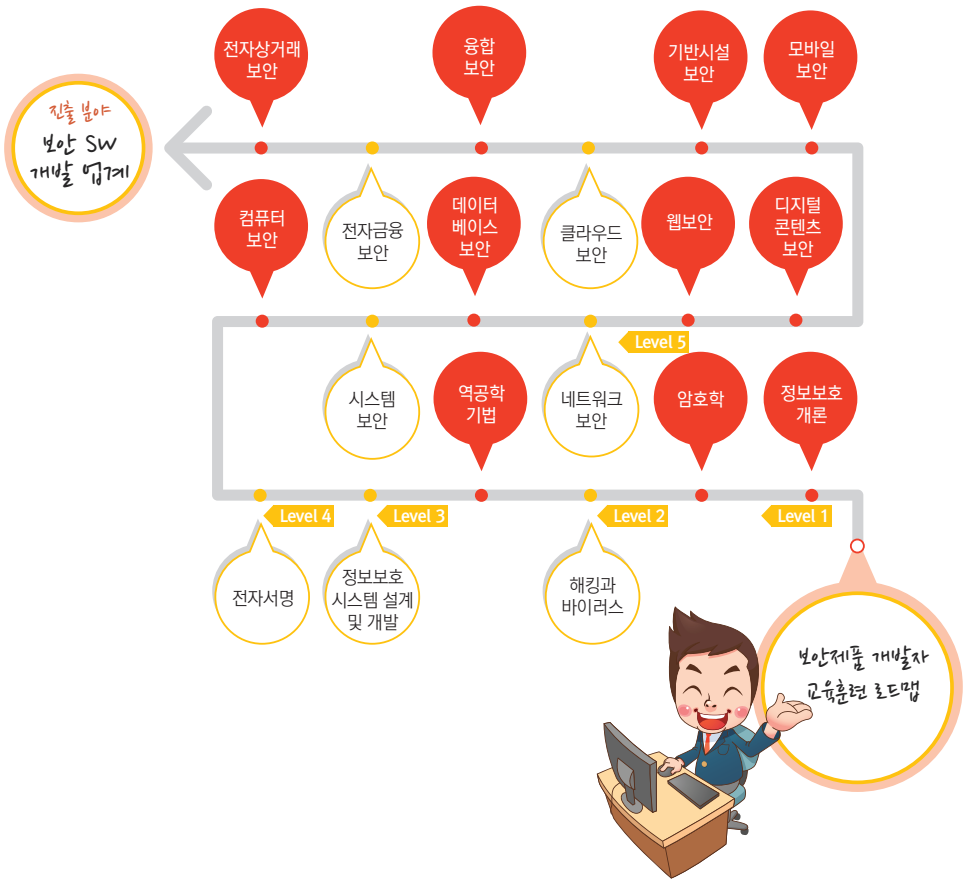
A
- 보안시스템 가용성/신뢰성 확보를 위한 생명주기관리 능력
- 보안시스템 설계/기술/개발에 대한 능력
- 개발된 보안시스템을 고객환경에 적응할 수 있는 능력
- 네트워크 트래픽 수집/필터링/분석 능력

2 관련 직업은 어떤 것들이 있나요?

- **보안 SW 분석/설계 전문가**
  보안SW 시스템 개발을 위한 요구사항을 분석하고 이를 해결하기 위한 계획과정을 수행하는 전문가입니다.
- **보안 SW 개발자**
  보안SW 시스템 구현과 함께 이와 연관된 프로젝트를 관리하는 전문가입니다.
- **보안제품 기술자**
  개발된 정보보호 시스템에 대해 품질을 보증하면서 고객맞춤화를 위해 기술지원을 수행하는 전문가입니다.
- **보안제품 기술영업**
  정보보호 시장분석을 통해 잠재적인 시장(고객)을 발굴하고, 요구사항 분석을 통해 최적의 정보보호 시스템 구축방안을 제시하는 전문가입니다.

3 보안제품 개발자는 무엇을 하나요?

정보보호 산업의 동향을 파악하고, 고객이 요구하는 수준에 맞는 보안제품을 기획합니다. 기획에 따른 정보보호 제품을 설계하고 동시에 암호화 알고리즘을 개발합니다. 또한, 외부로부터 불법 침입을 탐지하기 위한 시스템과 방화벽, 백신 프로그램을 개발합니다.



보안제품 개발자 인터뷰

"100% 완벽한 보안은 불가능 하다고 합니다만,
그렇기에 늘 도전이 필요하고,
새로움을 창조할 수 있는 직업"

이상준 전무 | 유넷

직업의 역할	정보보호 제품에 대한 기획, 개발, 유지보수
기 본 능 력	이해력, 끈기, 논리적 사고능력, 프로그래밍 기술
준 비 사 항	컴퓨터 공학 전공 또는 C/C++, JAVA, HTML 등의 프로그래밍 기술

Q 보안제품개발 환경은 SW 개발환경과 어떤 차별성이 있나요?

A 장애 발생에 따른 리스크가 보안 이외 SW 제품보다 높습니다. 그 만큼 패치/재가동 등을 위해 주어지는 시간이 많지 않을뿐더러, 시시 각각으로 변화하는 보안 환경에 대한 대응을 위한 기능 고도화를 늘 염두에 두어야 합니다.

Q 현재 어떤 일을 하고 있나요?

A 저는 무선보안연구소 소장을 맡고 있습니다.

대내적으로는 보안제품의 라이프사이클(기획 → 개발 → 구축 → 유지보수) 전반에 대한 관리 감독 역할을 수행하고 있으며, 임원으로서 회사의 전반적인 의사 결정에 참여하고 있습니다. 대외적으로는 연구소장 모임, 각종 포럼 참석, 자문, 기고, 강연, 평가 등등의 활동을 합니다.

유넷시스템은 2003년 창업했으며, 현재 임직원은 95명, 매출은 대략 100억 정도하는 정보보호 전문 중소기업입니다.

사업은 보안제품 개발 및 공급, 보안관제 서비스로 크게 나누어 볼 수 있으며, 개발 및 공급하고 있는 보안제품으로는 무선랜 침입 방지 시스템(WIPS), 빅데이터 로그 분석, 유/무선 통합 인증, PKI 등이 있습니다.

Q&A 01

보안제품 개발자

Q 어떤 과정을 거쳐 이 직업을 갖게 되었나요? (관심분야, 직업경로 등)

A 대학 때 전자계산학을 전공하여 SW 개발자로 10여년을 근무했으며, 2000년부터 보안제품 개발을 했습니다.

관심 분야는 현재 주력 제품인 PKI, 로그분석, 무선랜 보안 등이 되겠습니다. 물론 회사의 임원으로서 영업 및 전반적인 회사의 경영에도 많은 관심이 있습니다.

Q 관련 업무 수행 시 필요한 기본능력은 무엇인가요?

A 기본적으로 보안 기술 및 개발에 대한 이해력이 있어야 할 것입니다. 물론 개발 경험이 있으면 더 좋겠지만, 연구소장은 관리적인 역할이 더 많기 때문에 조직 및 인력에 대한 관리 역량 또한 중요한 능력이 됩니다.

더불어 보안 기술 및 시장 동향에 대한 통찰력이 있어야 새로운 제품을 개발하거나 현재 제품에 대한 업그레이드를 경쟁사에 뒤지지 않고 이루어 갈 수 있을 것입니다.

Q 일하면서 힘들거나 어려움을 느낄 때는 언제인가요? 어떻게 극복하셨나요? (직업의 단점 등)

A 장애 발생에 따른 리스크가 보안 이외 SW 제품보다 높습니다. 그 만큼 패치/재가동 등을 위해 주어지는 시간이 많지 않을뿐더러, 시시 각각으로 변화하는 보안 환경에 대한 대응을 위한 기능 고도화를 늘 염두에 두어야 합니다.

Q 해당 직업 관련 단체 및 기관은 무엇이 있을까요?

A KISA(한국인터넷진흥원), KISIA(지식정보보안산업협회), KOSA(한국 SW 산업협회), CONCERT(한국침해사고대응팀협의회), ETRI, KEIT, NIPA, IITP, 중소기업청, 기술 보증 기금, CC 평가 기관, CC 인증 기관(국정원, 국보연), 특허청, 특허 사무소, CISO 포럼 등이 관련 단체 입니다.

2 침해사고 대응 전문가

사전 침투/방어 분야 Protect and Defend

보안사고가 발생했을 때 피해규모를 최소화하기 위해 사고를 보고하고
시스템을 복구하고 예방전략을 수립하는 일을 하는 전문가를 이야기합니다.

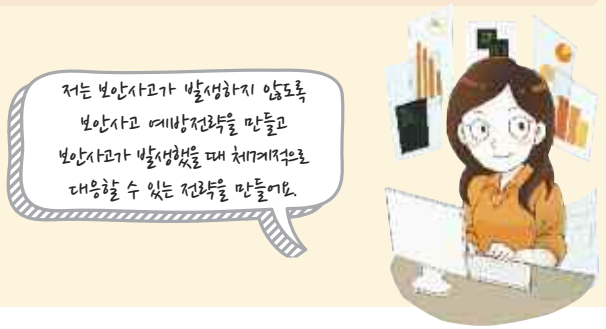
1 침해사고 대응 전문가는 무엇인가요?

보안사고가 발생했을 때 피해규모를 최소화하기 위해 사고를 보고하고 시스템을 복구하고 예방전략을 수립하는 일을 하는 전문가를 이야기합니다.

K
- 정보수집/생성/보고/공유 등에 관한 방법/절차/기술에 대한 지식
- 다양한 사이버 공격(전술/기술/절차)에 대한 지식

S
- 모의 침투 원칙/도구/기술에 대한 활용 기술

A
- 시스템/네트워크 보안위협(취약점) 식별/도출(인지/분류) 능력
- 시스템/네트워크 비상계획 수립/보안사고(재해) 복구(구현) 능력

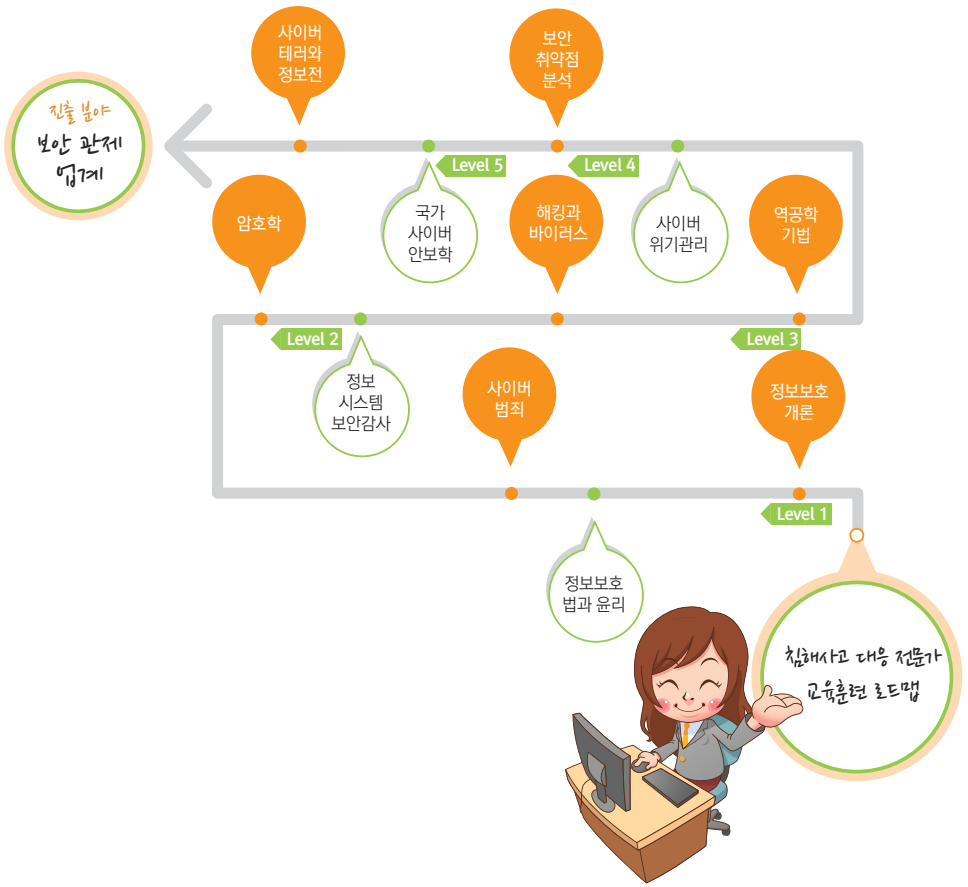


2 관련 직업은 어떤 것들이 있나요?

- **사이버 보안 관제사(보안관제요원)**
  정보자산 위협요소를 실시간으로 탐지하여, 시스템 취약점을 분석하고, 해킹/웜/바이러스 발생 시 대응팀과 협조하여 빠르게 보안위협에 대응하는 전문가입니다.
- **취약성 분석 전문가**
  정보자산에 피해를 끼칠 수 있는 보안위협을 확인하고, 정보자산 취약성에 따라 발생할 수 있는 위험정도와 피해규모를 평가하고, 이를 감소시킬 수 있는 통제방법을 도출하는 전문가입니다.
- **모의 해킹 전문가**
  정보자산에 대해 다양한 해킹 도구/기법을 활용하여 시스템 침투가능성을 진단하는 전문가입니다.

3 침해사고 대응 전문가는 무엇을 하나요?

보안사고 조사를 위한 도구를 준비하고, 사고 보고 문서양식을 정형화합니다. 사고에 대한 대응 전략 수행을 위해 적절한 정책과 운영 과정을 수립합니다. 사고로 인한 업무 및 서비스에 영향을 준 증거를 확보하고, 사고에 대한 데이터를 수집합니다. 수집한 데이터를 분석하고, 분석 내용을 문서양식으로 보고합니다.



침해사고 대응 전문가 인터뷰

"최신 보안공격기술과 맞서 싸우는
어둠을 밝히는 등불 같은 존재"

손동식 상무 | 윈스

직업의 역할	침해사고 대응을 위한 보안관제, 취약성 연구 등
기 본 능 력	윤리의식, 강한 의지, 긍정적 마인드
준 비 사 항	네트워크, 시스템, 어플리케이션(서비스)등 기반 기술에 관한 완벽한 이해

Q 관련 업무 수행 시 필요한 기본능력은 무엇인가요?

A 네트워크, 시스템, 어플리케이션(서비스)등의 기반 기술에 관한 완벽한 이해라고 봅니다.
어설픈 이해는 실제 ICT 운영자에게 혼란을 초래할 뿐이고 잘못된 업무 수행은 더 큰 보안상의 홀을 만들기 때문입니다.

Q 현재 어떤 일을 하고 있나요?

A 저는 보안 솔루션 제조사(Vendor)의 침해사고 대응센터장을 맞고 있습니다. 일반적인 기업의 CSO와는 조금 다른 성격을 가진 직군으로 설명됩니다. 역할은 보안관제 기술 총괄, 모의해킹 취약성 분석 및 설계 기술 총괄, 악성코드 수집/분석/패턴/패치 기술 총괄, 취약성 연구(Bug hunting)을 맡고 있습니다. 정보보안 기술분야에서 수집된 정보를 바탕으로 벤더(제조사) 특성상 당사에서 판매되는 모든 L7기반에서의 보안장비의 침입탐지를 위한 탐지 패턴(Signature) 업데이트 총괄을 겸하고 있습니다.

Q&A 02

침해사고 대응 전문가

Q 어떤 과정을 거쳐 이 직업을 갖게 되었나요? (관심분야, 직업경로 등)

A 통신사에서 네트워크 설계자 (백본/IDC 설계) 역할을 수행하며, 네트워크 인프라와 광대역 인터넷 서버 팜 및 센터 구축을 통한 ICT 기반기술을 습득하였습니다. 해당 업무 수행 중 우연히 설계한 대형 프로젝트가 해킹 사고로 인하여 문제가 발생하였고, 해당 문제를 해결하기 위하여 보안에 매진하다 보니 보안 기술에 매료되어 현재에 이르렀습니다.

Q 직업에서 필요로 하는 사람의 적성, 흥미 및 소질은 어떤 것들이 있나요? (신입채용 시 필요한 인성 등)

A 보안을 다루는 보안전문가의 本質은 '윤리의식' 입니다. 다루는 모든 것들이 불법, 악성 이라는 소프트웨어 중에서도 민감한 부분을 다루기에 본질을 다루는 마인드의 시작이 매우 중요하다 말할 수 있습니다.

Q 직업에 종사하시면서 느끼는 보람이나 매력은 무엇인가요? (직업의 장점 등)

A 단언컨대, 최신 공격기술에 대한 최전선에서의 정보습득이고 진화하는 기술에 대하여 손에 쥐고 있다는 것이 매력입니다. 더불어 그러한 공격기술을 분석하여 더 큰 위협과 위험을 방지하는데 보람을 느낍니다. 이는 화이트 해커로서의 윤리의식이 기반이 된다고 봐야 할 듯 합니다. 어둠을 밝히는 등불 같은 존재 멋지지 않나요?

Q 이 직업을 꿈꾸는 취업준비생들에게 조언해주고 싶은 말이 있다면 말씀부탁드립니다.

A 악성코드, 악의적 해커와 경쟁한다는 것은 생각보다 힘들고 어려운 일입니다. 그들은 매니아적 성향을 가지고 있어 절대적으로 정보기기를 즐기지 않으면 대응할 수 없습니다. 독창적 아이디어와 변칙적인 매커니즘은 분석가들로 하여금 혀를 내두르게 할 정도입니다. 코드는 진화합니다. 기술도 진화합니다. 사람도 진화합니다. 진화의 발판아래 반드시 윤리를 밟고 계시길 바라며, 개인의 잔기술 보다는 가능성과 유연함을 두고 정보보호 업무에 임해 주시길 간절히 부탁드립니다.

3 디지털 포렌식 전문가

사후조사 분야 Investigate

정보자산을 위협하여 보안사고를 발생시키는 요인에 대하여
증거를 수집하여 복구하고 추적하는 활동을 수행하는 일을 합니다.

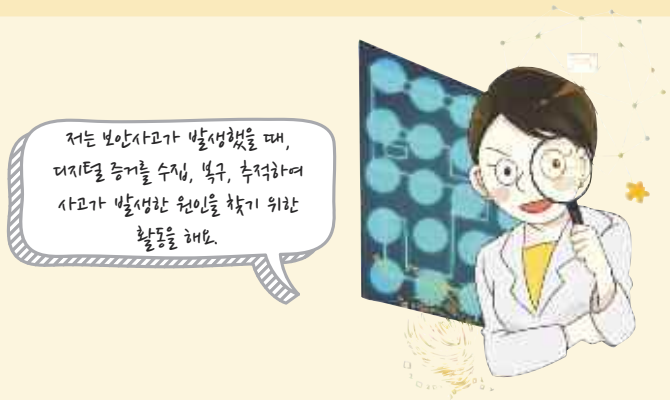
1 디지털 포렌식 전문가는 무엇인가요?

정보자산을 위협하여 보안사고를 발생시키는 요인에 대하여 증거를 수집하여 복구하고 추적하는 활동을 수행하는 일을 합니다.

K
- 정보이론/디지털 저작권 관리에 대한 지식

S
- 정보 유형에 따른 비정상적인 행위에 대한 식별/확인 기술

A
- 정보 추출을 위한 메모리덤프(디버거 결과) 추출/분석/활용능력
- 디지털 포렌식 도구 구성/지원 프로그램 활용 능력
- 다양한 매체로부터 법의학적 관점의 정보를 식별/추출하는 능력
- 정보 변경/손실과 물리적 손상/파괴 등을 방지하기 위한 전자적 증거 수집/포장/운반/저장 능력



2 관련 직업은 어떤 것들이 있나요?

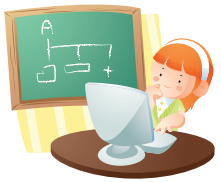
- **사이버 범죄 수사관**
  사이버범죄에 대한 증적자료 확보를 통해 법적인 수사업무를 집행하는 전문가입니다.

3 디지털 포렌식 전문가는 무엇을 하나요?

보안사고가 발생하는 경우, 저장된 데이터를 그대로 운반하여 범죄 단서가 될 만한 디지털 자료를 수집합니다. 범죄자가 악의적으로 숨기거나 변형-훼손한 데이터를 찾아서 복구합니다.
또한, 확보한 디지털 자료에 대해 철저한 분석을 통해 법적 증거자료로 사용가능한지 파악하고, 증거로서의 생명력을 잃지 않도록 유지 –보관 -인계합니다. 마지막으로, 분석한 자료를 법적 증거자료로 작성하고 제출합니다.

디지털 포렌식 전문가 인터뷰

"사이버 탐정
디지털포렌식 전문가"



사이버조사관 | 경찰청 사이버안전국

직업의 역할	법의학을 기반으로 전자적 증거획득을 위한 디지털 자료 분석
기 본 능 력	국가관, 사명감, 분석력
준 비 사 항	기본적 포렌식 도구 이해와 활용 및 수사/경찰학과 형법 및 형사 소송법에 대한 이해

Q 디지털 포렌식 전문가가 되기 위해서는 무엇부터 시작해야하나요?

A 나를 생각하기 보다는 '타인'을 배려하는 마음이 무엇보다 중요하며, 생각했던 것보다 훨씬 일이 힘들수도 있다는 점을 알아야 합니다.

또한, 재미있을 것 같아서 시작했다가 후회하는 사람들이 많으며, 따라서 각자 자신이 본 사이버범죄 수사라는 직업에 대한 적성과 소질이 있는지부터 아는것이 중요하겠습니다.

Q 현재 어떤 일을 하고 있나요?

A 저는 현재 경찰청 사이버안전국에서 사이버범죄 관련 수사 및 분석(데이터베이스 등) 업무를 수행하고 있습니다. 현재 사이버테러형 범죄 중 개인정보 대량 해킹, 사회이목을 집중시키는 사이버범죄 등을 사이버안전국에서 집중적으로 처리하고 있으며, 문제 발생시 사후조치는 물론, 예비단계에서도 적극적으로 대응하여 사고를 미연에 방지하는 업무 또한 병행하고 있습니다.

Q&A 03

디지털 포렌식 전문가

Q 관련 업무 수행 시 필요한 기본능력은 무엇인가요?

A 일반적으로 범죄수사는 법을 다루어야 하기 때문에 Legal Mind 확립이 무엇보다 중요합니다.

또한, 사이버범죄수사는 기술적 요소로써 컴퓨터 전반에 대한 이해가 있어야 하며, 이를 바탕으로 형사소송법과 같은 절차적 요소를 반드시 숙지, 준수하여야 합니다.

Q 직업에 종사하시면서 느끼는 보람이나 매력은 무엇인가요? (직업의 장점 등)

A 사회적으로 이슈가 되는 범죄행위에 대해 범인검거 및 증거 수집하였을 때, 사건을 해결하였다는 기쁨과 국가의 위기관리에 기여하였다는 자부심을 느낄 수 있습니다.

Q 일하면서 힘들거나 어려움을 느낄때는 언제인가요? 어떻게 극복하셨나요? (직업의 단점 등)

A 사건의 양이 방대하여 처리가 너무 어렵고 힘들 수 있습니다. 그러나 언제나 자기가 맡은 일에만 묵묵히 일하면 결국 모든 것들이 자기발전에 크게 도움이 될 것입니다. 특히 사건을 많이 처리할수록 본인의 노하우가 그만큼 많이 쌓이게 되는 것이며, 결국 그것이 본인의 발전에 크게 도움이 되는 것입니다.

Q 이 직업의 향후전망에 대해 말씀부탁드립니다.

A 모 언론기관에서는 향후 10년내 가장 인기직종이 사이버범죄수사관이 될 것이라고 보도한 바 있습니다. 그만큼 사회적으로도 관심을 받는 직종이며, 특히 정보화사회로 되면서 더욱 그 가치가 높아지고 있는 것이 사실입니다. 현재는 채용인원이 점점 많아져서 매년 정기적으로 채용하고 있으며, 지금도 많은 사람들이 해당시험에 응시준비를 하고 있습니다.
특히, 앞으로 민간조사업이 활성화 될 것이고, 로펌에 이어 포렌식펌도 생길 것으로 예상되는 등, 민간분야에서도 정보보안은 더욱 활성화 될 것으로 기대되고 있습니다.
따라서 향후, 민관이 협력하여 정보보호 관련 분야는 앞으로 훨씬 더 많이 발전하게 될 것으로 예상되는 만큼, 이 분야의 미래도 밝다고 생각됩니다.

4 악성코드 분석 전문가

수집/해독 분야 Collect and Operate

새로운 악성코드를 분석하여 감염 경로나 방법–증산–치료 방법 등을 개발하고 치료할 수 있는 백신프로그램을 제작하는 일을 하는 전문가를 이야기 합니다.

1 악성코드 분석 전문가는 무엇인가요?

새로운 악성코드를 분석하여 감염 경로나 방법 – 증산 – 치료 방법 등을 개발하고 치료할 수 있는 백신 프로그램을 제작하는 일을 하는 전문가를 이야기 합니다.

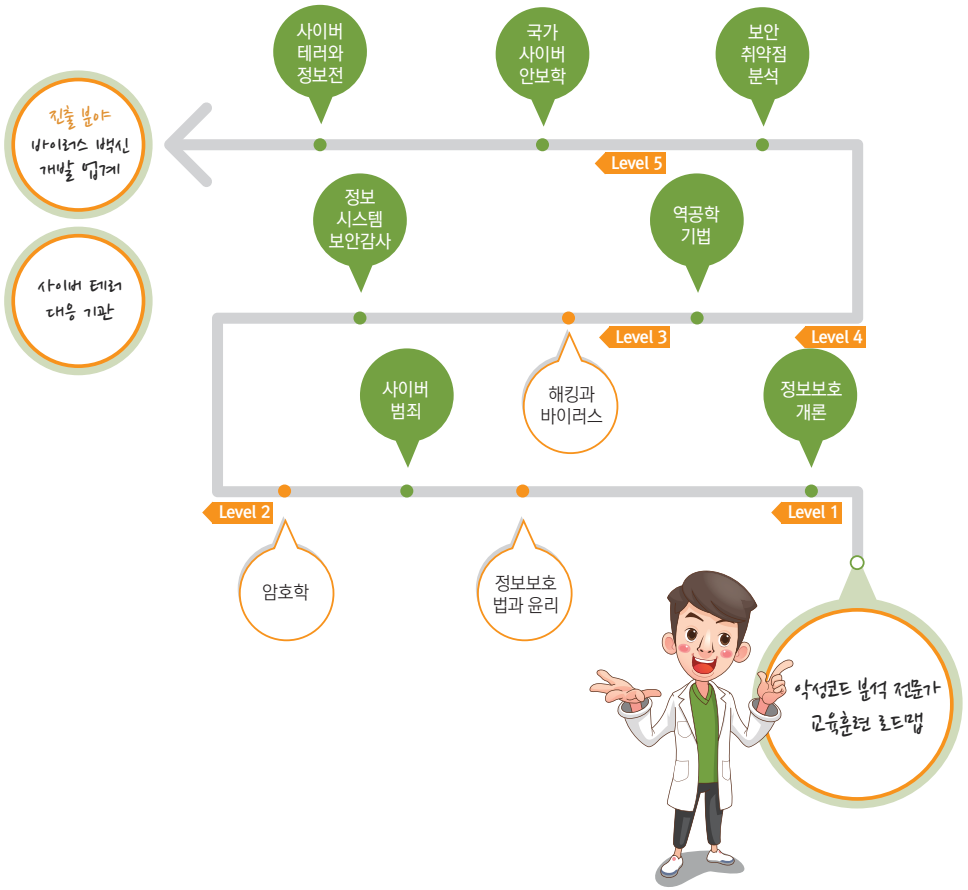
- **K** 다양한 운영체제 환경에서의 해킹방법에 대한 지식
- **S** 사이버 활동에 영향을 미칠 수 있는 법적/기술적 동향을 추적/분석하는 기술
- **A**
  - 다양한 보안 (이벤트)도구를 활용하여 관련정보를 수집 / 통합 / 해석 할 수 있는 능력
  - 전자서명/악성코드 / 휘발성 데이터 등에 관한 해독 / 분석 / 해석할 수 있는 능력
  - 암호학/암호화알고리즘 지식 / 구현 능력
  - 역공학/난독화 기술 인지 / 활용능력

2 관련 직업은 어떤 것들이 있나요?

- **암호해독 전문가**
  중요정보에 대한 높은 수준(고강도)의 암호화 또는 높은 수준으로 암호화된 정보에 대해 해석하는 전문가입니다.

3 악성코드 분석 전문가는 무엇을 하나요?

악성코드 분석 툴을 이용하여 악성코드의 종류 및 특징을 분석합니다. 이에 따라 악성코드에 대한 치료 데이터를 만들고, 기존 백신프로그램에 악성코드를 치료하기 위한 데이터를 추가합니다. 그리고, 악성코드 분석에 대한 결과를 사용자에게 알리고 백신프로그램을 배포하는 일을 합니다.



악성코드 분석 전문가 인터뷰

"보안에서 반드시 필요한 직종이지만
아무나 할수 없는 전문직종"

권석철 대표 | 큐브피아

직업의 역할	새로운 방식의 악성코드 및 해킹기법에 대한 정확한 분석
기 본 능 력	분석력, 꼼꼼함, 강한 의지
준 비 사 항	역공학에 활용되는 각종 디버깅 기법 및 툴 사용법 숙지. 운영체제 동작원리, 프로그램 개발 능력 등

Q 이 직업을 가지게 되면 나쁜 유혹도 많을 것 같은데, 어떻게 이러한 부분을 극복하고 계신가요?

A 악성코드 전문가가 되게 되면 나름대로 금전적 유혹이 많이 들어오는 것은 사실입니다. 그러나, 처음부터 이 분야는 화이트 해커(보안전문가)의 영역이기 때문에 관심조차 없었으며, 가볍게 치부하면 됩니다. 이러한 유혹은 당신을 범죄자로 만들수가 있기 때문입니다.

Q 어떤 과정을 거쳐 이 직업을 갖게 되었나요? (관심분야, 직업경로 등)

A 대학교 1학년 전자계산과에 입학을 하면서 프로그램으로 바이러스가 있다는 것을 알게 되어 호기심을 가지게 되었으며, 졸업 후 정부출연기관에서 일하게 되었고 그 후 퇴사하여 백신 프로그램 개발회사를 창업하게 되었습니다. 기술의 진화와 함께 바이러스와 해킹기술을 파악하기 위해 지금은 해킹전문업체를 운영하고 있습니다.

Q&A 04

악성코드 분석 전문가

Q 관련 업무 수행 시 필요한 기본능력은 무엇인가요?

A 해킹전문가(해커)등이 되기 위해서는 시스템 공부에 대한 것을 반드시 알아야 합니다. 특히 운영체제를 이해하는 것이 반드시 필요하고 이 또한 바이러스분석가처럼 프로그램의 취약점을 찾거나, 막을 수 있기 위한 기술도 필요합니다.

Q 직업에 종사하는데 어떤 공부 (학교 교과목, 자격증 등)이 필요하나요? (관심 있게 공부했던 과목, 신입채용 시 필요한 자격증 등)

A 저는 시스템 프로그래밍, OS 커널 분석, 바이러스 제작, 및 백신 제작, 그리고 컴퓨터 범죄 예방 관련 책, 등을 주로 보았으며 특히, 전자신문, 디지털 타임즈등의 전문매체, 그리고 마이크로소프트웨어같은 잡지 등을 가지고 주로 공부했습니다. 지금은 각종 전문가들의 포럼, 블로그 등의 자료를 참고하는 방법으로 공부를 하는 것이 어떨까 합니다.

신입채용 시 자격증은 있으면 좋지만 그것이 반드시 입사조건은 아니기 때문에 학력, 자격증 보다는 현재 자신이 가지고 있는 기술, 열정, 등을 어떻게 잘 표현하느냐가 더 중요합니다.

Q 직업에 종사하시면서 느끼는 보람이나 매력은 무엇인가요? (직업의 장점 등)

A 바이러스 분석 전문가 및 보안전문가는 많은 사람들이 하고 싶은 직종이지만, 그만큼 어렵고 힘들기 때문에 그 직업을 가진다는 것은 대단한 자부심도 느낄 수가 있습니다. 또한, 주변사람들이 바이러스나 해킹 때문에 고민을 가지고 있을 때 이를 해결하기 위한 해결사(?)등도 될 수 있으므로 인기가 좋습니다.
또한 보안은 국가 산업 발전에 필수적인 부분이라 국가발전에 이바지 한다는 자부심 또한 가질 수 있는 매력 있는 직업이기도 합니다.

Q 이 직업을 꿈꾸는 취업준비생들에게 조언해주고 싶은 말이 있다면 말씀부탁드립니다.

A 남들이 하지 않는 그러한 직업은 선택하는 것은 스스로 어려운 길을 가는 것이지만 해냈을 때의 성취감은 대단히 높으며 남들보다 훨씬 빨리 앞으로 나갈수 있는 통로가 될수 있다고 하고 싶습니다.
따라서 이 보안분석전문가 타이틀은 여러분의 새로운 꿈을 만들어 줄 것임을 확신합니다.

5 보안 컨설턴트

진단/평가 분야 Analyze

고객의 정보자산과 비즈니스 프로세스에 따른위협 및 취약점을 분석하여 보안 수준을 파악하고, 요구수준에 맞는 통합적인(기술 + 관리) 보안 해결책을 설계하는 전문가를 이야기합니다.

1 보안 컨설턴트는 무엇인가요?

고객의 정보자산과 비즈니스 프로세스에 따른 위협 및 취약점을 분석하여 보안 수준을 파악하고, 요구수준에 맞는 통합적인(기술 + 관리) 보안 해결책을 설계하는 전문가를 이야기합니다.

K
- 보안시스템 신뢰성/성능 등과 연관된 표준 지식(절차)
- 보안관리 프로세스/체계 등과 연관된 표준 지식(절차)
- 보안시스템 탐지/보급 등에 관한 최신 산업동향 지식

S
- 비즈니스 프로세스와 연관된 위험관리(평가) 기술

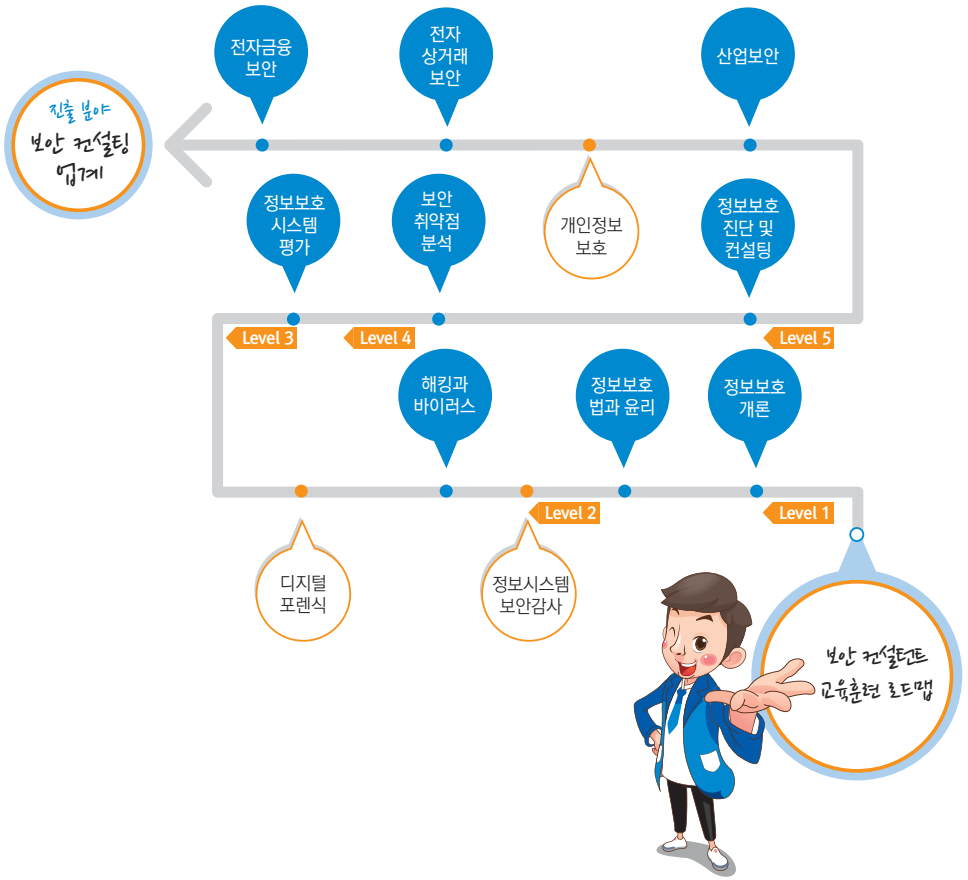
A
- 보안시스템 적합성/견고성/무결성 등을 평가할 수 있는 능력

2 관련 직업은 어떤 것들이 있나요?

- **정보시스템 감리사**
  사전에 설계된 객관적인 기준에 따라 시스템에 대한 효과성/효율성/안전성 등을 평가하는 전문가입니다.
- **보안관리 컨설턴트**
  정보자산과 비즈니스 프로세스 대상의 위협/취약점에 대응되는 보안수준을 비교하여 관리적인 보안 해결책을 제시하는 전문가입니다.
- **정보시스템 보안감사**
  시스템 보안 상태를 사전에 정의된 보안 요구사항과 비교하여 객관적인 충족여부를 검증하는 전문가입니다.
- **보안기술 컨설턴트**
  정보자산과 비즈니스 프로세스 대상의 위협/취약점에 대응되는 보안 수준을 비교하여 기술적인 보안 해결책을 제시하는 전문가입니다.
- **보안제품 인증 전문가**
  보안시장에 출시된(출시예정인) 보안제품에 대해 사전에 정의된 보안 적합성(보안 프로파일)에 충족하는지 평가하는 전문가입니다.
- **보안관리 인증 전문가**
  조직수준의 정보보호 관리체계가 통제항목을 충족하는지 평가하는 전문가입니다.

3 보안 컨설턴트는 무엇을 하나요?

고객의 업무와 요구사항을 분석하고, 정보자산에 대한 위험과 취약점을 진단하여, 보안 관점에서 최적화할 수 있는 개선방안을 도출합니다. 개선방안을 바탕으로 하여 고객의 보안성을 향상시킬 수 있도록 관리 - 기술 - 인적 관점에서 체계를 설계합니다. 고객의 구축 비용 등 제반 사항을 고려하여 일정에 따라 구체적으로 실행하는 일을 합니다.



보안 컨설턴트 인터뷰

"보안분야 종합예술의 시작
보안컨설턴트"

이준택 소장 | 한국정보경영연구소

직업의 역할	경영, 컨설팅기획, 교육, 구축, 정책개발
기 본 능 력	논리력, 분석력
준 비 사 항	인문학적 접근력, 심도깊은 관련분야 경험, 프로세스 알고리즘 분석력

Q 보안컨설턴트의 첫 걸음을 위한 준비는 어떻게 해야 하나요?

A 보안컨설턴트는 종합 예술을 시행하는 위치입니다. 이에 따라, 실무의 경험을 가질 수 있도록 현장에 참여한 이력을 만드는 것이 중요합니다. 자신만의 "보안관련 포트폴리오"를 작성해보세요.

Q 어떤 과정을 거쳐 이 직업을 갖게 되었나요? (관심분야, 직업경로 등)

A Application Programmer로 시작해서 IT Communication Hardware Management(IT시스템 관리) 및 정보보안경영 관리시스템(ISMS) 구축 및 심사원 활동했었으며, 현재는 국제표준 심사원으로 활동하고 있습니다.

Q 관련 업무 수행 시 필요한 기본능력은 무엇인가요?

A – '정보보안 컨설턴트'로써의 업무 수행 자질은 크게 4단계로 나눌수 있으며, 다음과 같습니다.

[1단계]
: 인문학적(철학, 법, 경제학, 심리학) 접근이 가능한 기초소양
: 정보시스템(Information System) 설계(Analysis) 및 소프트웨어개발 방법론
: 국제표준(ISO) Standard 요구사항

[2단계]
: Computer Program Language–JAVA, C++, JSP, PHP
: 아래한글, MS Word, Presentation 능력
: IS Communication Analysys, Network Control
: Secure Coding

[3단계]
: IMS(Information Management System, 경영관리시스템) 아키텍쳐 실무
: IT Technical(Mobile, Computer Network, Server Management 등)
: ISMS(Information Security Management System) 설계 및 구축방법

[4단계]
: SA(Security Architecture) 구축 및 운영, 관리
: IT Device Configuration Setting & 위험분석(자산분석, 위협–취약성분석)
: 통제항목 대응 정책수립

Q&A 05

보안 컨설턴트

Q 직업에서 필요로하는 사람의 적성, 흥미 및 소질은 어떤 것들이 있나요?

A 인문학적(산업심리학, 경제학, 철학) 접근이 가능해야하며, 관련분야(보안: 기술적–관리적)의 Capability 및 경험이 필요합니다. 또한, 프로세스의 알고리즘 분석방법에 대한 이해 및 응용이 가능해야 합니다.

Q 직업에 종사하시면서 느끼는 보람이나 매력은 무엇인가요?

A "정보시스템 보안감사" 영역이 전사적으로 중요성을 인정 받고 있으며, 조직내 회계 및 정보보안사건/사고에 대한 효과적인 대응이 강화되고 있습니다. 또한, 국제 사회에서 "정보의 상호제공"에 대한 보안관리를 강조하고 있고, 증가하고 있는 기술유출 및 보안사고의 증가로 법적대응, 기업이미지 관리에 필요성 증가하고 있습니다. 이러한 상황에서 체계적이고 종합적으로 관리할 수 있는 "정보보호관리체계(ISMS)"의 중요성이 증가하고 있으며, 이에 ISMS 구축 컨설턴트의 역할로 조직의 정보자산을 파악하고 위험분석을 체계적으로 진단함으로써, 조직이 대응해야 할 보안요구사항을 표준(법률, 국제표준 등)에 따라 구축할 수 있는 전문인력이 부족함으로, 정보보안컨설턴트에 대한 희소가치가 높다 할 수 있습니다.
이처럼, 직업의 전문성을 인정 받을 수 있으며, 조직에 경제적/관리적 효과를 직간접적으로 성과를 얻을 수 있습니다.

Q 이 직업의 향후전망에 대해 말씀부탁드립니다.

A 2014년도 ICT 10대 전망에 보안분야가 1위~4위 안에 고루 분포되어 있습니다. 특히, 사물인터넷, 모바일(스마트) 오피스의 미래 기술의 발전에 따른 "보안분야"의 동방성장이 예상되므로 관련 기술 및 보안에 인력 부족으로 인력 양성의 강조되고 있습니다. 따라서, 정보보안 기술인력(Revers Engine, Secure Coding, 위험분석전문가, 정보보안컨설팅 등)의 부족으로 정보보호 컨설턴트의 전문가로써의 입지가 매우 커질것으로 기대하고 있습니다.

6 보안 관리자

관리 분야 Operate and Maintain

조직관점에서 보안이라는 목적을 달성하기 위하여 보안과 관련된 정책–관리체계–시스템 구축–운영(관리)업무를 실제적으로 수행하는 전문가를 이야기합니다.

1 보안 관리자는 무엇인가요?

조직관점에서 보안이라는 목적을 달성하기 위하여 보안과 관련된 정책–관리체계–시스템 구축–운영(관리)업무를 실제적으로 수행하는 전문가를 이야기합니다.

K
- 위험허용/관리 절차(방법)에 대한 지식
- 보안시스템 구축원칙과 대응방법에 대한 지식
- 조직의 정보보증 원칙과 보안 요구사항(기밀성, 무결성, 가용성, 인증, 부인방지 등)에 대한 지식

S
- 보안정책에 기반한 위험수용 통제 기술

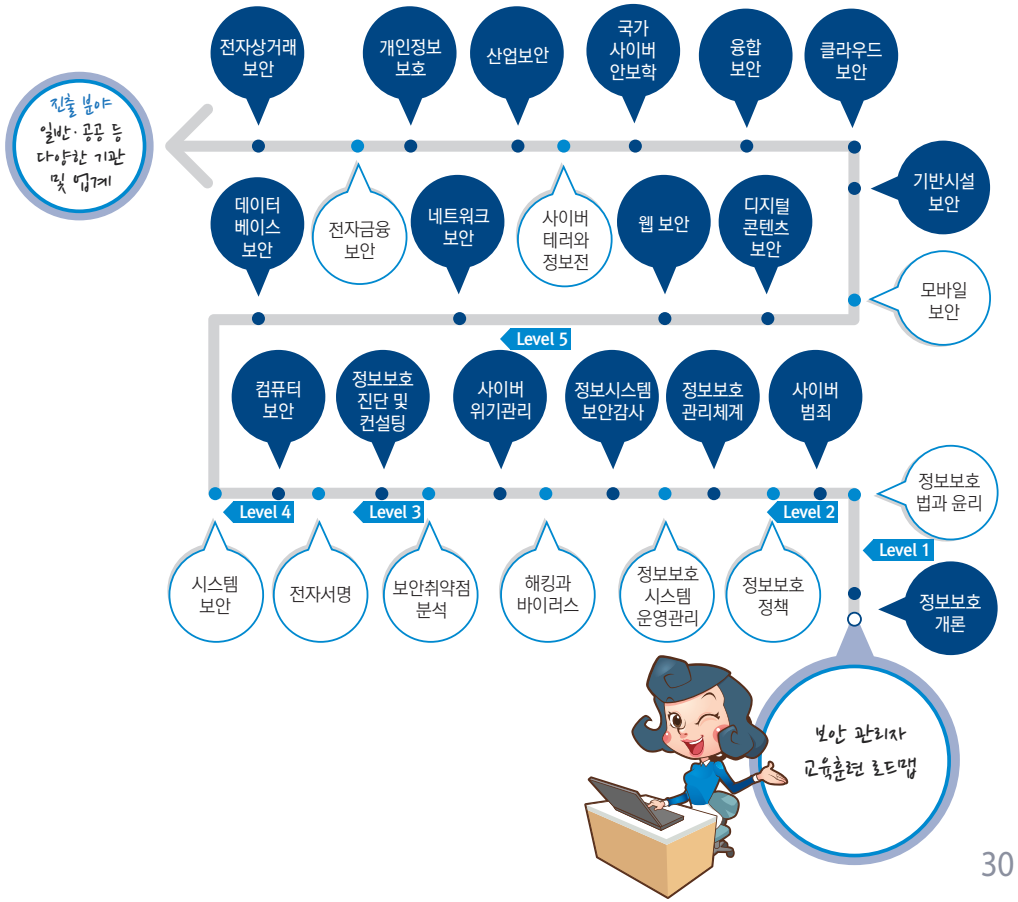
A
- 취약점 식별을 위한 분석도구 활용능력
- 보안사고 발생에 따른 대응절차 이행능력
- 보안시스템 구축(구성)/운영(활용) 능력
- 조직의 보안목적을 반영한 정책을 설계하는 능력

2 관련 직업은 어떤 것들이 있나요?

- **보안시스템 관리자**
  정보자산을 보호하는 보안시스템을 고장 없이 안정적으로 구축/운영/유지보수하는 전문가입니다.
- **정보시스템(네트워크) 관리자**
  시스템/네트워크 운영/관리 업무를 진행하는 전문가입니다.
- **개인정보보호 관리자**
  개인정보 보호를 위한 정책을 개발하고 법제도를 준수하고 보안관리 활동을 수행하고 책임지는 전문가입니다.
- **DB 관리자**
  조직의 비즈니스 프로세스 흐름 속에서 발생된 모든 정보를 대상으로 통합적인 보안통제를 수행하는 전문가입니다.
- **(보안) 지식 관리자**
  조직의 비즈니스 프로세스 흐름 속에서 발생되는 정보의 생성/활용/폐기 등에 관한 통합적인 정보 생애주기를 관리하는 전문가입니다.

3 보안 관리자는 무엇을 하나요?

정보자산에 대한 보안정책을 수립하고 심의하며, 보안성을 검토합니다. 시스템 및 네트워크에 대한 취약성을 진단하고 모의해킹을 실시합니다. 또한, 관리자와 사용자의 사용기록을 추출하고 분석하며, 조직의 구성원들에게 보안 교육을 실시합니다.



보안 관리자 인터뷰

"기업의 보안을 관리하는 창의적 전문인"

이병권 실장 | 현대오토에버

직업의 역할	직원 보안수준 향상을 위한 교육과정 운영 및 평가체계 운영 및 각종 기술적인 보안가이드 및 지침, 프로세스 수립 및 관리
기 본 능 력	꼼꼼함, 창의적 사고, 관찰력
준 비 사 항	IT 기본 지식, 보안 솔루션 지식, 보안관리 및 보안법률에 대한 지식

Q 미래 보안 인력의 수요는 어떻게 될까요?

A IoT 등 IT기술이 발전함에 따라 기기들의 스마트화, 자동화 등으로 보안에 대한 중요성은 더더욱 커지고 있어 인력수요는 더욱 급증할 것입니다. 지금까지는 고객정보, 금융정보 위주의 보안이었다면, 앞으로는 의료기기, 차량, 제어기기 등의 개발과정부터 보안을 고려해야 할 것이기 때문입니다.

Q 현재 어떤 일을 하고 있나요?

A 저는 자동차그룹의 IT회사에서 정보보안실장(최고 보안관리자)으로 재직 중 입니다. 업무의 범위는 매우 다양합니다. 첫째, 그룹 보안관제센터 운영을 통한 침해사고 대응 및 악성코드 분석, 둘째, FW, WAF, IDS, IPS, DRM, NAC 등 도입된 정보보안시스템 관리 운영, 셋째, FW, WAF, IDS, IPS, DRM, NAC 등 그룹내 보안시스템 구축, 넷째, 서버, 네트워크, DB의 보안취약점 관리, 다섯째, 업무시스템/SCDA/차량의 취약점 점검 및 개선관리, 여섯째, 직원 보안수준 향상을 위한 교육과정 운영 및 평가체계 운영, 일곱째, 각종 기술적인 보안가이드 및 지침, 프로세스 수립 및 관리, 여덟째, 신규 위협에 대한 보안 강화 대책 수립 및 기술적 대응책 연구, 아홉째, 유관기관과의 협력 등 우리 그룹과 제품을 대내외로부터 보호하기 위해 다양한 업무를 수행하고 있습니다.

Q&A 06

보안 관리자

Q 직업에서 필요로 하는 사람의 적성, 흥미 및 소질은 어떤 것들이 있나요? (신입채용 시 필요한 인성 등)

A 성공적인 보안관리자가 되기 위해서는 신기술에 대한 적극적인 습득 노력, 꼼꼼한 설계 및 점검 능력, 전체적인 관점에서 보고 판단할 수 있는 시야, 창의적인 생각을 할 수 있는 소질이 요구됩니다.

Q 직업에 종사하는데 어떤 공부 (학교 교과목, 자격증 등)이 필요하나요? (관심 있게 공부했던 과목, 신입채용 시 필요한 자격증 등)

A 저는 운영체제, 통신 & 네트워크, 데이터베이스, 컴파일러, C언어, 어셈블리언어, 임베디드 개발, 정보보호개론, 시스템/네트워크 보안 등과 관련한 자격증을 관심 있게 공부하였습니다. 신입채용 시 우대되는 자격증은 CCNA, SIS, CISA 입니다.

Q 일하면서 힘들거나 어려움을 느낄 때는 언제인가요? 어떻게 극복하셨나요? (직업의 단점 등)

A 보안의 특성상 사고가 발생하지 않는 한 평상시에 보안에 대한 필요성이 과소평가되고 보안에 대한 투자가 비용으로 인식되면서 투자를 받아내기 어려운 경우가 많습니다. 또한, 새로운 해킹 기술들이 개발되면 그에 따른 신규 보안 위협이 발생할 뿐만 아니라 이에 대한 대책은 상대적으로 늦게 제시되기 때문에 보안사고 발생을 완벽하게 막기 위한 고차원적인 노력이 필요합니다.

Q 이 직업의 향후전망에 대해 말씀부탁드립니다.

A 이제 기업에서는 실력 있는 보안인력을 얼마나 많이 보유하고 있느냐가 기업의 경쟁력 지표로 언급해도 될 정도입니다. 시장의 우수인력은 부족하고 이를 채용하고자 하는 기업은 많아 대우도 높아지고 있는 실정입니다. 또한, IoT 등 IT기술이 발전함에 따라 기기들의 스마트화, 자동화 등으로 보안에 대한 중요성은 지속적으로 커지고 있어 인력수요는 더욱 급증할 것입니다.

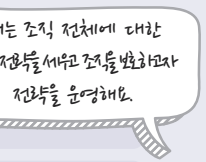
7 최고 보안 관리자

감독/총괄 분야 Oversight and Development

조직의 경영 관점에서 전체적인 보안전략을 총괄적-통합적으로 수립하고 운영하며 조정하는 전문가를 이야기합니다.

1 최고 보안 관리자는 무엇인가요?

조직의 경영 관점에서 전체적인 보안전략을 총괄적-통합적으로 수립하고 운영하며 조정하는 전문가를 이야기합니다.



K
- 새로운 정보기술/보안기술(위험/시스템)에 대한 지식
- 사이버 보안문제를 다루는 외부조직(학술기관)에 대한 지식
- 국제적인 사이버 정보보호 동향 지식

S
- 비즈니스와 연관된 법적인 Governance에 이행 기술

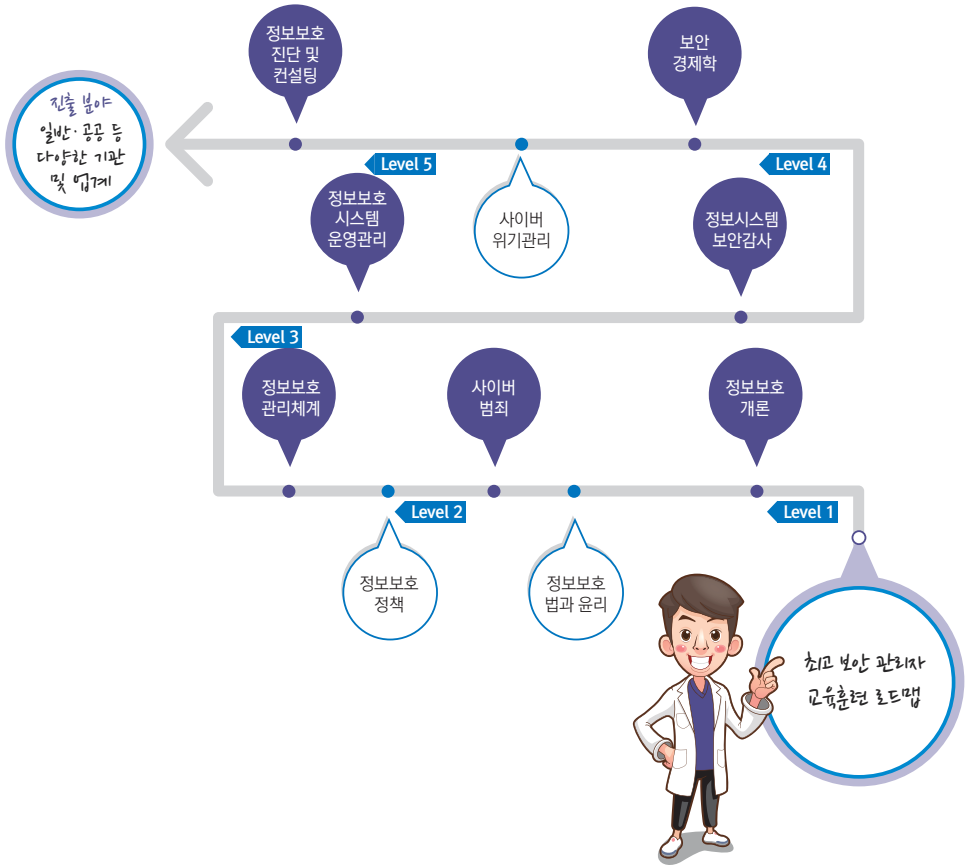
A
- 조직 보안사고 대응체계 구축 능력

2 관련 직업은 어떤 것들이 있나요?

- **보안관리 기획자**
  조직 경영목표에 부합된 보안정책과 단계별 추진전략을 수립하는 전문가입니다.
- **개인정보보호 전문가**
  조직의 개인정보보호 수준을 평가하고, 이에 부합하는 보안 대책 구축 방안을 제시하는 전문가입니다.
- **보안전문 교수**
  보안 분야에 특화된 학문적 지식과 역량을 보유한 전문가입니다.
- **보안 교육 전문가(변화관리전문가)**
  정보보호 인식제고/지식/역량 향상을 위해 사용자/전문가 대상의 교육 프로그램을 설계/운영하는 전문가입니다.
- **보안전문 기자**
  보안 분야에 특화된 기사를 조사하고 보도하는 전문가입니다.
- **보안전문 검사/변호사**
  보안 분야(사이버 범죄 등)에 특화된 법률적 지식을 보유한 법조인입니다.
- **국제 보안 전문가**
  국가간 상호 운영성이 확보될 수 있는 보안기술/보안 관리체계 표준화 업무를 수행하는 전문가입니다.
- **준법 감시자**
  책임 있는 비즈니스 업무수행을 위해 지켜야 할 관련법규 준수활동을 설계/운영/평가하는 전문가입니다.

3 최고 보안 관리자는 무엇을 하나요?

경영자와 협력하여 위험을 완화하고, 사고에 대처하며, 보안과정과 정책을 기획-개발-실시-관리합니다. 또한 국내외 최고 수준의 법집행 기관들과 관계를 형성하며, 하위 관리자를 통하여 최적의 인적 자원과 장비를 사용하여 자산을 보장하기 위해 보안활동을 조정하고 수행합니다.



최고 보안 관리자 인터뷰

"기업의 정보보호관리의 총 책임역할"

신수정 CISO | KT

직업의 역할	기업정보보호 총괄
기 본 능 력	리더십, 논리력
준 비 사 항	정보보호 컨설팅, 논리적 사고 훈련, 다양한 정보보호 기술과 관리 경험

Q 어떤 과정을 거쳐 이 직업을 갖게 되었나요? (관심분야, 직업경로 등)

A 저는 IT기업인 한국HP에서 시스템 엔지니어로 출발하여, 삼성SDS에서 IT컨설턴트로서의 경험을 가지고 있습니다. 이후 인포섹에서 보안 컨설턴트로 일하며 보안 컨설팅 사업본부를 맡게 되었고 이후 대표이사를 역임하였습니다. 이후 현재 KT의 CISO를 맡게 되었습니다.

Q 업무 수행시 필요한 기본능력은 무엇인가요?

A 정보보안의 전체적인 영역에서의 이해와 설계능력이 필요합니다.
첫째, IT 전반의 기술적 보안을 이해해야 합니다.
둘째, 관리적 보안 설계를 할 수 있어야 합니다.
셋째, 기업의 비즈니스를 이해할 수 있어야 합니다.

Q&A 07

최고 보안 관리자

Q 직업에 종사하시면서 느끼는 보람이나 매력은 무엇인가요? (직업의 장점 등)

A 기업의 보안체계를 설계하고 이행함으로써 고객의 정보를 보호하고, 기업의 경쟁력을 강화한다는 보람과 매력이 있습니다.

Q 일하면서 힘들거나 어려움을 느낄 때는 언제인가요? 어떻게 극복하셨나요? (직업의 단점 등)

A 보안의 취약성은 엄청나게 많습니다. 이를 모두 해결하는 것은 거의 불가능합니다. 이러한 문제는 위험 중심으로 해결하고 있습니다. 즉, 높은 위험의 문제부터 우선순위를 두어 해결합니다

Q 이 직업을 꿈꾸는 취업준비생들에게 조언해주고 싶은 말이 있다면 말씀부탁드립니다.

A 최고 보안 관리자는 보안전문가의 최종 목표 중 하나입니다. 초기 5년간 정도는 한 가지 전문영역을 정해서 그 분야에 집중해서 최고가 되어야 합니다. 이후 다양한 영역들을 다루는 것이 좋습니다.

Q 최고 보안관리자의 향후 전망은 어떻게 될까요?

A 해외의 경우 정보보호최고임원은 가장 높은 연봉을 받는 유망직업중 하나입니다. 국내에도 대기업과 금융권을 중심으로 전담 정보보호최고임원직이 등장하고 있습니다. 향후 이 직책의 수요가 더 확대될 것이고 전문가들의 진출이 더 가속화 될 것입니다.

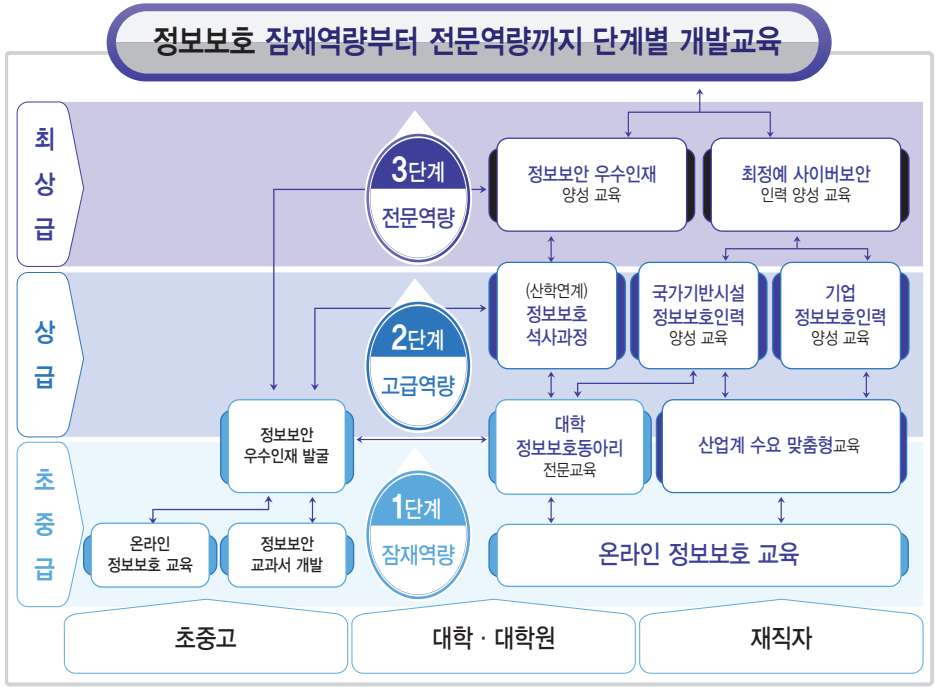
C · O · N · T · E · N · T · S

KISA아카데미 교육과정

한국인터넷진흥원 KISA아카데미 소개

최근 고도화된 정보보호 침해사고로 인한 보안취약성 우려가 확대되면서 정보보호 전문인력에 대한 사회적 수요가 증가하고 있습니다. 이에 따라 KISA아카데미는 최고의 정보보호 교육 서비스 제공을 목표로 수년간 다부처 수요맞춤형 교육과정을 운영하는 등 분야별 정보보호 인력의 수급해소에 기여하고 있습니다.

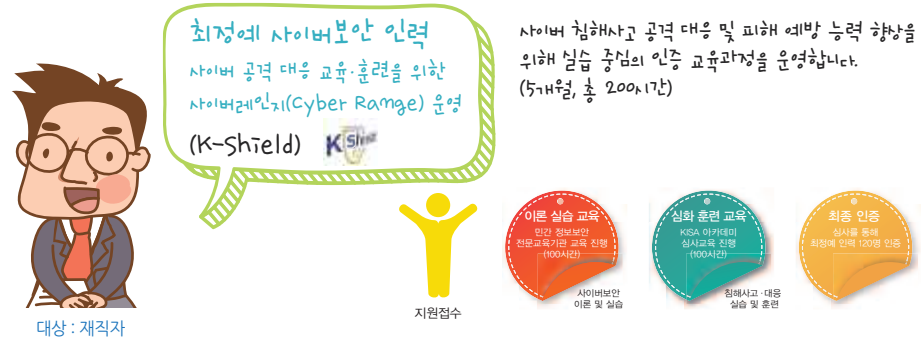
분야별 정보보호 교육 현황



정보보안 우수두뇌 양성 프로그램

국가 사이버보안의 방패 역할을 합니다.

대한민국이 인증하는 최고 사이버보안 인력양성 프로그램

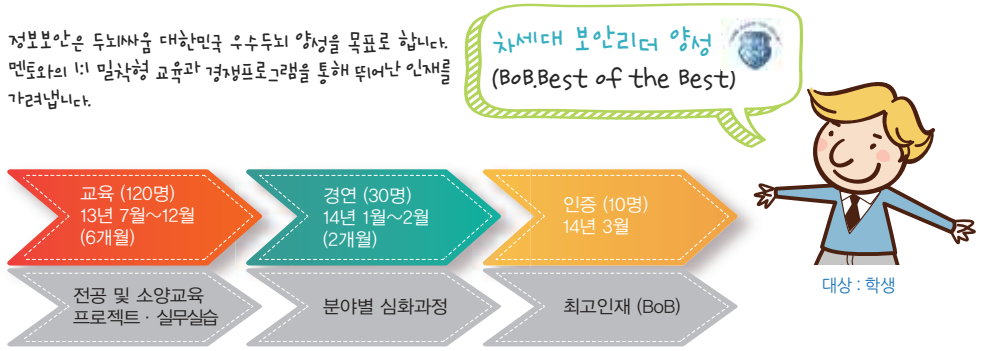


최종 인증된 최정예 보안인력은 국가사이버위기 시 정보보호 전문가로 참여하여 사회적 피해를 최소화하고 유사사고를 예방하는 등 국가정보보호 역량강화에 기여할 수 있습니다.

최고 중의 최고!

대한민국 보안 기술·산업의 미래를 이끌어나갈 우수두뇌를 양성합니다.

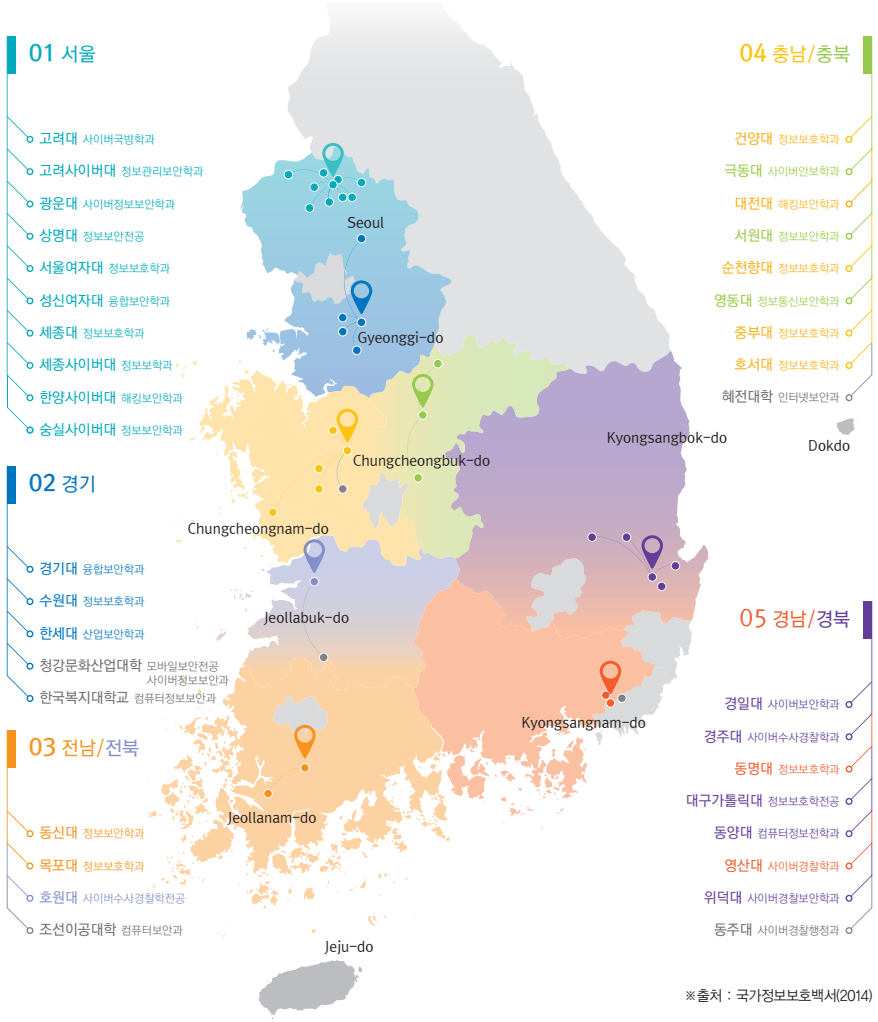
정보보안은 두뇌싸움 대한민국 우수두뇌 양성을 목표로 합니다. 멘토와의 1:1 밀착형 교육과 경쟁프로그램을 통해 뛰어난 인재를 가려냅니다.



향후 정보보호 난제를 해결하는 브레인이자 국가 안보에 대한 윤리적가치, 사명감을 가진 화이트해커로서 국가사이버역량 강화에 기여할 수 있습니다.

대학·전문대학 정보보호 관련 학과 현황

대학 · 전문대학 정보보호 관련 학과 현황



※출처 : 국가정보보호백서(2014)

대학 정보보호동아리 지원

대학 정보보호동아리 학생이라면 꼭 참여해보세요.
무료 교육, 세미나, 연구 활동 지원 등 다양한 혜택이 기다리고 있습니다.
대학정보보호동아리 : www.kucis.org

"건전한 윤리관을 함양한 미래 정보보호 전문인력을 양성시킵니다"

- 전국의 대학생을 대상으로 정보보호의 올바른 가치관을 인식시키고 관련 활동 시 갖추어야 할 윤리 의식을 함양할 수 있도록 지원합니다.
- 다양한 정보보호 교육 및 세미나, 연구 활동 지원 등을 통해 기술력과 전문성을 향상시키고 미래 정보보호 전문가로서 양성시키고자 합니다.

매년 40개 이상의 대학 정보보호동아리가 선정되며, 하계 워크샵 이외에도 4개 권역별(서울/경기/강원권역, 충청권역, 영남권역, 호남권역)로 정보보호 교육 및 컨퍼런스가 활발히 진행됩니다. 연말에는 활동 실적을 평가하여 우수 동아리와 우수 기술문서 시상을 합니다.

"교육, 세미나 등을 통해서 전문기술을 함양할 수 있습니다"

- 정보보호 실습교육(웹해킹대응, 악성코드 탐지 및 분석 등), 전문가 강연/멘토링, 세미나 등을 통해서 실무 중심의 전문기술을 습득할 수 있습니다.

"동아리간 기술 교류 및 경진을 통해 기량을 향상시킬 수 있습니다"

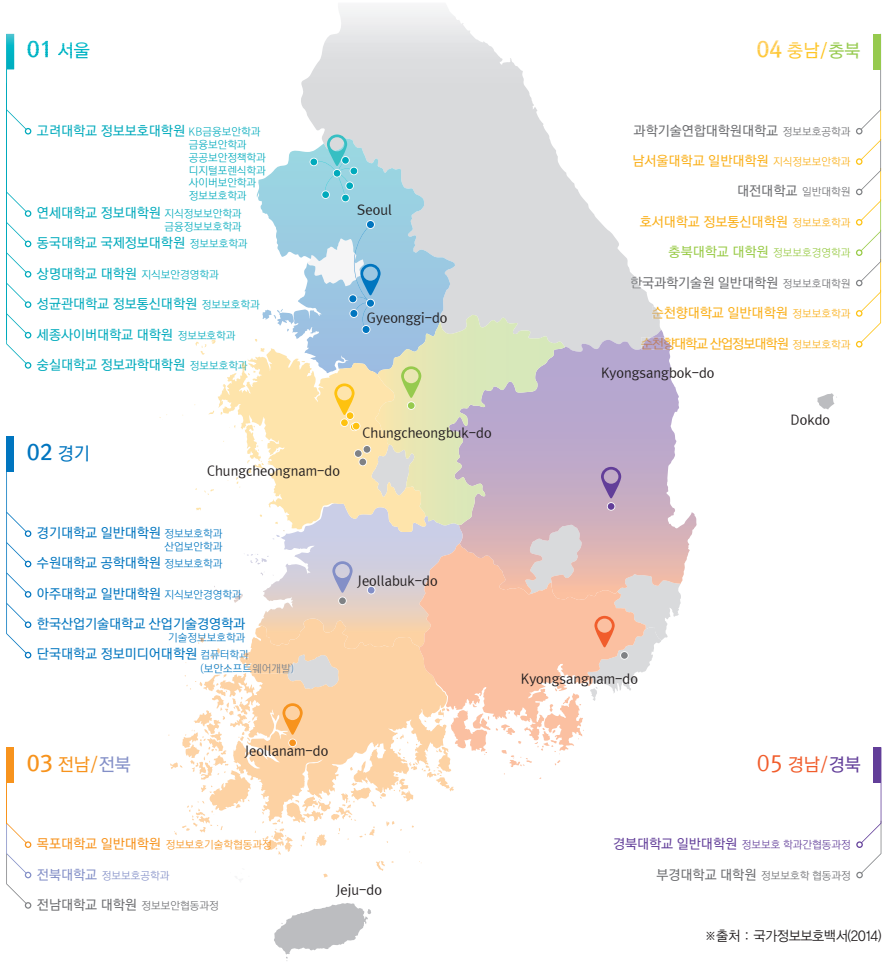
- 동아리별 특화 정보보호 프로젝트 수행, 기술문서 발표, 권역별 세미나 개최 등을 통해 동아리 및 개인의 기량을 향상시킬 수 있습니다.
- 동아리간 활발한 정보교류와 폭 넓은 인적 네트워크 형성을 위해 하계 워크숍을 개최하며, 대학 정보보호동아리연합회 전용 웹사이트도 운영합니다.

"산업과 학계의 교류를 통해 현장성을 높이고 재능기부를 통해 사회공헌에 기여합니다"

- 산·학 연계를 통해서 정보보호 전문 기관 및 업체 현장 학습을 지원하고, 중소기업 정보보호지원 등의 지역봉사 활동을 장려합니다.

대학원 정보보호 관련 학과 현황

대학원 정보보호 관련 학과 현황



※출처 : 국가정보보호백서(2014)

고용계약형 정보보호 석사과정

많은 기업에서 정보보호 고급인력을 필요로 합니다.
여러분이 그 주인공이 될 수 있습니다.

고용계약형 석사과정 : 자세한 사항은 각 대학 홈페이지 참조

"기업 연계 고용계약형 정보보호 석사과정의 2년간 학비를 전액 무료 지원합니다"

- 지식정보보호 전문 인재를 양성하기 위해 기업체와 대학이 컨소시엄을 이뤄 함께 커리큘럼을 개발하고 교육을 진행합니다.
- 정부는 기업과의 공동 출자로 2년 과정의 학비를 무상으로 지원하며, 고용계약 조건을 통해 정보보호 산업 일자리 창출을 돕습니다.
- 참여 학생은 졸업 후 연계된 일터에 바로 투입되어 일할 수 있는 역량을 갖추게 됩니다.

"지식정보보호 분야의 전문성과 기술력을 갖춘 고급 인력으로 성장할 수 있습니다"

금융보안, 모바일보안, 지식서비스보안, 산업보안, 융합서비스보안 등 각 대학별 특성화 교육과정은 지식정보보호 분야의 전문성과 기술력을 집중적으로 키워줍니다.

※ '14년 현재 6개 분야, 8개 대학(고려대, 단국대, 동국대, 상명대, 순천향대, 아주대, 연세대, 충북대) 참여 중

"현직 전문가 강의와 참여 기업 인턴쉽을 통해 현장감을 높일 수 있습니다"

- 전문성과 숙련도를 갖춘 현장 중심 인재로 키우기 위해 현직 연구자/개발자의 강의가 교육 과정에 포함되며, 방학 중 참여 기업 인턴쉽도 필수로 수행합니다.
- 세미나 및 해외 컨퍼런스 참석, 논문 발표 등의 기회도 제공합니다.

"졸업 후 현장에 바로 투입되어 일 할 수 있는 기회가 주어집니다"

- 졸업 후 최소 2년간 참여 기업 의무 근무를 통해 실무 경험을 쌓고 정보보호 산업 분야로 커리어를 이어갈 수 있습니다.
- 대기업을 포함한 여러 정보보호 업체들의 컨소시엄 참여는 졸업 이후 취업과 연계되는 다양한 기업 맞춤형 인력 양성을 가능하게 합니다.

민간 교육기관

민간 정보보호 교육 기관 현황

기 관 명	교육과정명	홈페이지
와이즈로드	CISSP, CISA, CISM, CPPG 자격증 과정 등	www.wiseroad.co.kr
라이지움	CISSP, CPPG, CIA 자격증 과정 등	www.lyzeum.com
삼성SDS	CISSP, CISA, CCNA, 보안실무 과정 등	www.multicampus.co.kr
솔데스크	기업해킹 보안전문가 과정, 정보보안기사 과정 등	www.soldesk.com
아이티뱅크	네트워크·시스템 해킹 보안전문가 과정, 웹해킹, 포렌식(침해대응) 과정 등	www.itbankstar.com
금융보안교육센터 (FSA)	직무강화 및 정보시스템에 대한 해킹원리 및 대응방안 등의 실습교육 과정	www.edu.fsa.or.kr
LAWnB	개인정보보호관리사 과정	www.lawnbedu.com
ITECH	네트워크·시스템 보안과정 및 CISSP, CISA 과정 등	www.itech.ac.kr
올에듀넷	정보보안기사·산업기사 과정 등	www.ks.alledu.net
한국정보보호 평생교육원	정보보안기사·산업기사 과정 등	www.kisle.co.kr
이지스원	보안(해킹) 실무, 리버스엔지니어링 실무, CISSP 시스템 보안전문가, CISA 정보보호전문가 과정 등	www.hackerscollege.co.kr
인섹 시큐리티	모바일포렌식, 컴퓨터포렌식, 사이버보안 포렌식, Malware·Memory 포렌식 등	www.insec-security.co.kr
인포레버컨설팅	정보시스템감리사 자격증 과정	www.infoever.co.kr
케이씨에이(KCA)	정보시스템감리사 자격증 과정	www.kca21.com
패스트레인	정보보호 실무, 웹 해킹·대응 실무, 정보보호 컨설팅, 리버스엔지니어링 등	www.flane.co.kr
한국정보보호교육센터(KISEC)	정보보호전문가 과정, 모의해킹 전문가 과정 등	www.kisec.com
지안에듀	정보보안기사·산업기사 자격증 과정	www.sec.zianedu.com
국제정보보안 교육센터(I2SEC)	정보보안전문가 과정, 정보보안자격증 (SIS, CISA, CISSP) 과정 등	www.i2sec.co.kr
한국HP교육센터	보안개발자 과정, 보안전문가 자격증 과정 등	www.hpeducation.co.kr
KH정보교육원	웹 해킹 보안 등 취업 전문가 과정	www.iei.or.kr
한국첨단기술 경영진흥원	정보보호전문가 양성과정 등	www.kemdec.or.kr
코어 시큐리티	리버스코드 엔지니어링, 모의해킹·취약점 분석 과정 등	www.coresec.co.kr
라온 시큐어	사이버보안 전문가 과정	www.raonsecure.com
이즈러닝 by 씨드젠	보안일반 과정, CISSP, CISA, CPPG 등 자격증 과정	www.islearning.co.kr
테크데이터 웹타임 교육센터	정보보안 자격증, 보안실무, 모의해킹 등	www.webtime.co.kr

※출처 : 국가정보보호백서(2014)

정보보안기사 및 산업기사

정보보안기사 및 산업기사 자격소개

정보보안 자격제도(자격검정센터) : www.kisq.or.kr

국가공인 민간자격이었던 정보보호전문가(SIS, Specialist for Information Security) 자격이 국가기술자격으로 전환하여 정보보안기사·산업기사 자격증이 되었습니다.

정보보안기사·산업기사 시험은 2013년부터 현재까지 필기 및 실기 각 3회씩 시행하여 총 21,613명의 응시자 중 기사 296명, 산업기사 198명의 합격자를 배출하였습니다.

정보보안자격증은 기사, 산업기사로 분류됩니다.

[기사 필기시험]
시스템 보안, 네트워크 보안, 애플리케이션 보안, 정보보안 일반, 정보보안 관리 및 법규 등 5개 과목으로 구성

[산업기사 필기시험]
정보보안 관리 및 법규 과목을 제외한 4개 과목으로 구성

[실기시험]
2종목 공통으로 단답형, 서술형, 실무형의 3가지 형태로 구성되고, 정보보안 실무에 적합한 지식 및 기술력을 검증 할 수 있도록 출제

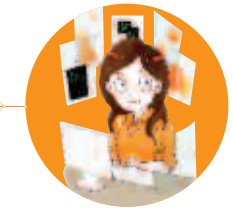
구 분	필기시험			실기시험		
	원서접수	시험일자	합격(예정자) 발표	원서접수	시험일자	최종 합격자 발표
2014 – 1회	3.3~3.7	4월 5일	4월 25일	4.28~5.2	5월 31일	6월 23일
2014 – 2회	8.25~8.29	9월 27일	10월 17일	10.20~24	11월 22일	12월 15일

개발 보안제품 개발자
Security System Developer

- SW 분석/설계 전문가
- SW 개발자
- 보안제품 기술자
- SW 테스트 기술자(품질 관리자)
- 보안제품 기술영업

사전침투/방어 침해사고 대응 전문가
Incident Handling Specialist

- 사이버 보안 관제사(보안관제요원)
- 취약성 분석 전문가
- 모의 해킹 전문가



사후 조사 디지털 포렌식 전문가
Digital Forensic Specialist

- 사이버 범죄 수사관

- 암호/해독 전문가

수집/해독 악성코드 분석 전문가
Malicious Code Analysis Specialist

최고 보안 관리자(보안전략전문가) 감독/총괄
Chief Security Manager(Security Strategy Specialist)

- 보안관리 기획자
- 준법 감시자
- 보안 교육 전문가(변화관리전문가)
- 보안전문 검사/변호사
- 개인정보보호 전문가
- 보안전문 교수/기자
- 국제 보안 전문가

보안관리자 관리
Security Manager

- 지식 관리자
- DB 보안 관리자
- 정보시스템(네트워크) 관리자
- 보안시스템 관리자
- 개인정보보호 관리자

- 정보시스템 감리사
- 정보시스템 보안감사
- 보안제품 인증 전문가
- 보안관리 인증 전문가
- 보안기술 컨설턴트
- 사이버 보안 관제사(보안관제요원)

보안 컨설턴트 진단/평가
Security Consultant

정보보호 진로 가이드 북

KISA 한국인터넷진흥원 Korea Internet & Security Agency 서울시 송파구 중대로 109 (가락동 79-3) 대동빌딩 TEL.405-4118 www.kisa.or.kr