



# 채용 공고

## 악성코드 분석

이다영

01 . *ESTsecurity*



SOMANSA .02

03 . *winS*



.04

05 . AhnLab

# 1. ESTsecurity - 보안 인텔리전스 / 악성코드 분석 및 대응 (2020년 9월 채용 마감)

인기순 | 다운로드순 | 업데이트순

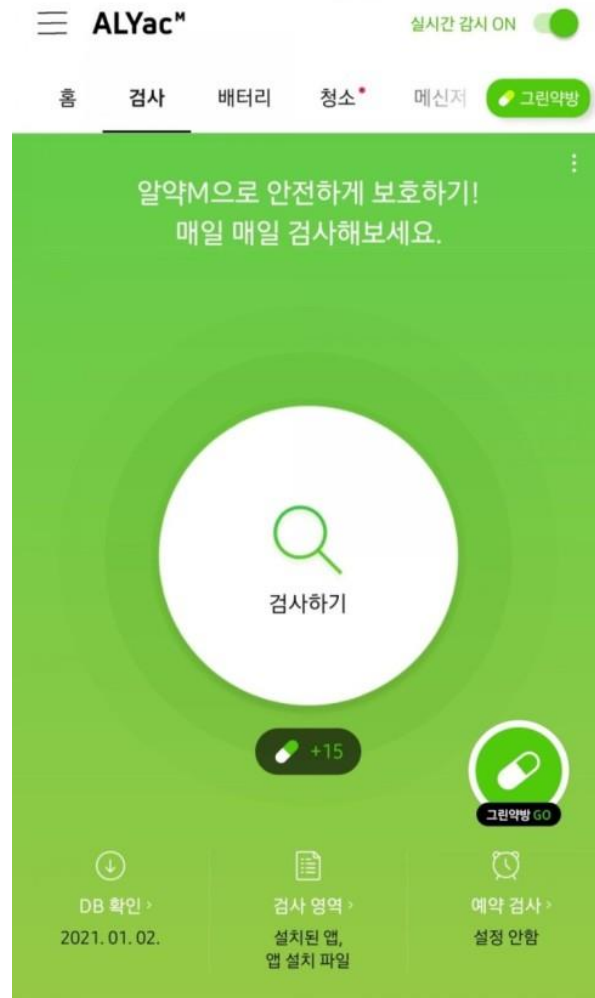
라이선스 전체 ▼

OS 전체 ▼

총 76건

 <b>알약</b> 이스트소프트의 가볍고 강력한 무료 백신	업데이트일 2020.12.28. 인기  프리 	다운로드수 16,590,745 최근7일 56,650	 <b>3.5</b> 3,052명 참여
 <b>안랩 V3 Lite</b> AhnLab의 가볍고 빠른 무료백신	업데이트일 2020.10.20. 인기  프리 	다운로드수 13,442,732 최근7일 8,161	 <b>3.6</b> 3,361명 참여
 <b>말웨어 제로</b> 설치가 필요 없는 무료 악성코드 제거 도구	업데이트일 2019.06.06. 인기  프리 	클릭수 1,037,022 최근7일 8,038	 <b>4.6</b> 480명 참여
 <b>네이버 백신</b> 사용자의 PC를 보호하는 다기능 백신 프로그램	업데이트일 2020.12.01. 인기  프리 	다운로드수 4,907,254 최근7일 6,854	 <b>3.8</b> 2,600명 참여
 <b>다잡아</b> 악성코드, 랜섬웨어 예방, 광고창 치료프로그램	업데이트일 2020.07.03. 인기  세어 	다운로드수 311,527 최근7일 756	 <b>3.4</b> 379명 참여

# 1. ESTsecurity - 보안 인텔리전스 / 악성코드 분석 및 대응 (2020년 9월 채용 마감)



## 보안 인텔리전스 / 악성코드 분석 및 대응

업무	자격요건	우대사항
보안 인텔리전스 분석 및 대응	보안 인텔리전스 분석 경험 (윈도우, 맥)	리버스 엔지니어링 가능 (OllyDBG, WinDBG, IDA 등)
최신 동향 악성코드 분석 및 대응	운영체제, 네트워크 관련 기본 지식 보유자	보안 관련 프로젝트 참여 경험
	Python, C/C++ 등 개발 언어 가능	기술관련 github나 블로그 보유자
	원활한 커뮤니케이션 가능	

## 2. SOMANSA — 악성코드 보안 솔루션 연구 / 개발 엔지니어 (2020년 12월 채용 마감)

22년간 시장1위, SSL/TLS 가시성 확보 및 복호화  
네트워크DLP 솔루션 Mail-i

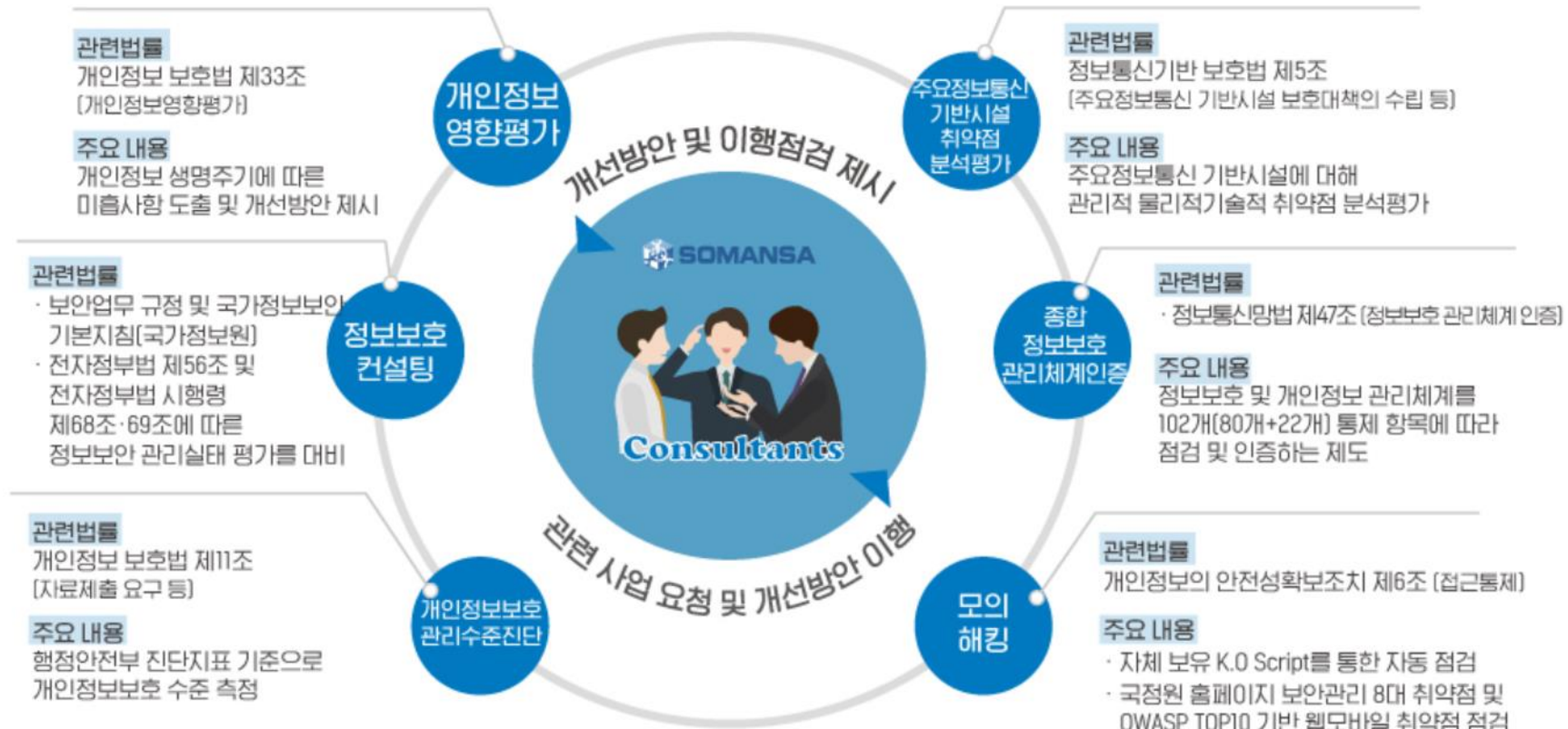


시장 1위, 개인정보유출방지  
엔드포인트DLP 솔루션 Privacy-i



## 2. SOMANSA — 악성코드 보안 솔루션 연구 / 개발 엔지니어 (2020년 12월 채용 마감)

### 개인정보 법규정에 최적화된 프라이버시 컨설팅 서비스



## 악성코드 보안 솔루션 연구 / 개발 엔지니어

업무	자격요건	우대사항
악성코드 보안 솔루션 연구 / 개발	C++에 대한 기초적인 이해	악성 코드의 트렌드에 대한 지식
	객체지향 패러다임에 대한 이해	악성 코드 분석 경험
	자료구조 및 알고리즘에 대한 이해	Kerner, Driver 등 시스템 개발에 대한 지식 및 경험
	악성코드의 동작 원리에 대한 이해	C++ 11/C++14/C++20, Boost 등에 대한 지식 및 경험
		리버스 엔지니어링 경험
		클라우드에 대한 이해 및 운영 능력
		Rust/Go 등의 언어에 대한 경험



### 3. WINS - 분석 (채용 진행중)



Sniper ONE-i



Sniper NGFW

### 3. WINS - 분석 (채용 진행중)

#### 벤더에서 제작한 시그니처로 관제

- 16년간 침입탐지 개발로 인한 다량의 탐지패턴 보유
- CERT요원들의 직접 보안관제 수행에 따른 침입탐지 대응 및 분석
- 이벤트에 대한 정확한 분석
- Raw Data 분석 및 대응

#### 지능화된 통합관제 시스템 적용

- ESM과 TMS의 진화된 통합 보안 관제 시스템인 Sniper TSMA 적용
- 이벤트에 대해 즉각적으로 대응가능한 능동적인 위협 관리 시스템



#### 타사와 차별화된 특화 서비스 제공

- SecureCAST 서비스 제공 (빠른 정보 제공과 정확한 위협예측)
- DDoS 모의훈련 서비스 제공 (DDoS공격 전용 장비 이용)
- 보안클리닉 서비스 제공
- 홈페이지 위변조 감시서비스 제공
- 웹로그 침해사고 실시간 분석
- 모의해킹 서비스 제공

#### 네트워크 보안 No.1

- 인터넷 망의 트래픽을 보호하는 네트워크 보안업체 1위
- IDS, IPS 등 국내 시장 점유율 1위
- 공공기관 관제센터, 금융권 ISAC 등 다수의 보안관제 경험 보유

## 분석

업무	자격요건	우대사항
취약점/악성코드 분석	네트워크패킷 분석 경험자	정보보호 자격증 보유자
탐지 시그니처 개발	탐지 이벤트 분석 경험자	Bug Hunting 경험자
최신 해킹 트렌드 연구		



## 4. SECULETTER - 기술연구소 분석팀 (2020년 6월 채용 마감)



SLE(SecuLetter Email) / SLF(SecuLetter Filesever)

## 4. SECULETTER - 기술연구소 분석팀 (2020년 6월 채용 마감)



MARS SLE(지능형 이메일 악성코드 위협 대응) 솔루션 도입

## 기술연구소 분석팀

업무	자격요건	우대사항
Non-PE 기반 취약점 분석 및 탐지 알고리즘 연구 개발 - 문서 파일, HTML 파일, 스크립트 파일 등	역공학 기술을 활용한 악성코드 (Non-PE, PE) 분석가능한 분	악성코드 분석 경력 1년 이상
악성 Non-PE 파일 탐지 알고리즘 연구 개발 - 문서내 악성 매크로 및 자바 스크립트 등	취약점에 대한 지식(BOF, UAF, OOB Write 등)이 있는 분	취약점 발생 원인을 분석해본 경험이 있는 분
취약점 관련 기술 리서치	취약점을 찾고 연구하는 것을 즐기는 분	취약점 상세 분석 포트폴리오를 갖고 계신 분
	기존 CVE 취약점에 대한 발생 원인을 분석할 수 있는 능력이 있는 분	

## 5. AhnLab — 보안위협 / 악성코드 분석 및 대응 (2020년 11월 채용 마감)

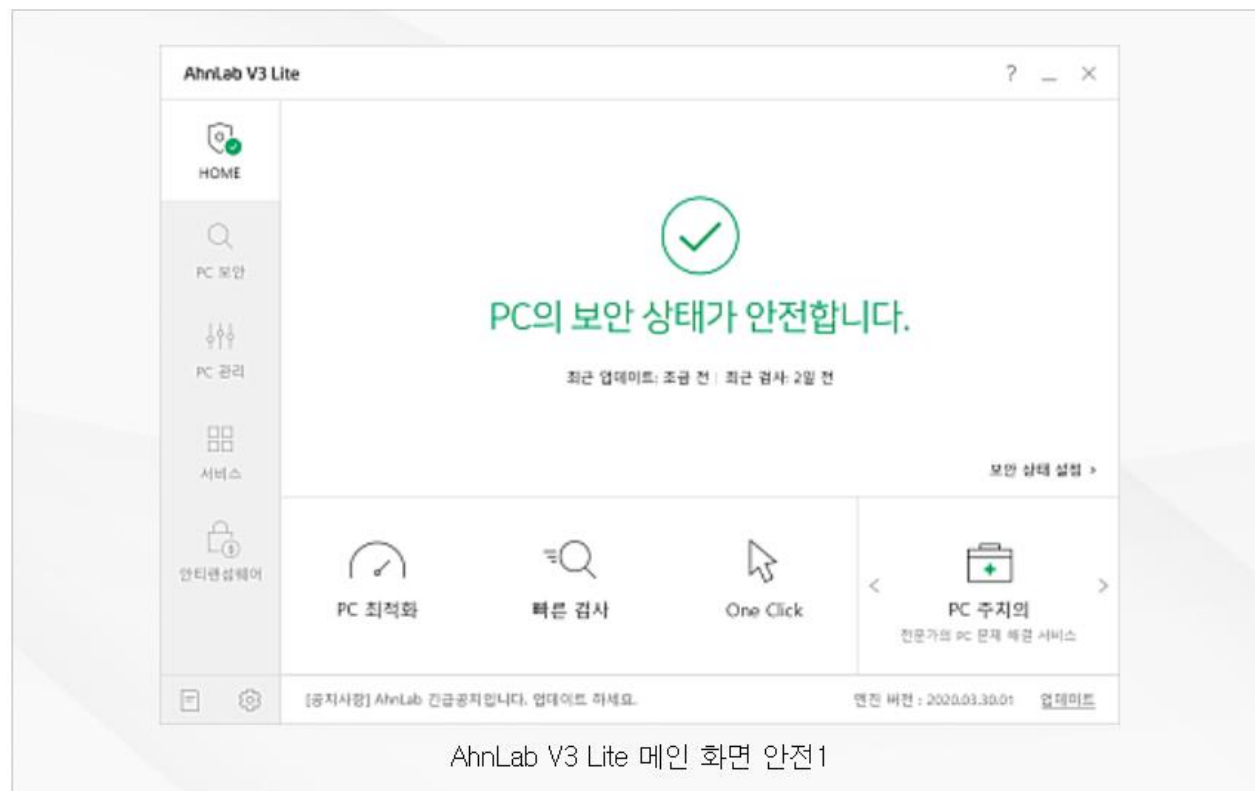


안랩 V3 Lite V3 Lite

인기도

백신 2위

다운로드수 13,444,992 (최근 7일:8,075)



AhnLab V3 Lite 메인 화면 안전1

## 보안위협 / 악성코드 분석 및 대응

업무	자격요건	우대사항
보안위협 분석 및 대응	악성코드 또는 보안위협 분석 경험(PC, Mobile 등)	리버싱 가능 (OllyDBG, WinDBG, IDA 등)
PC/서버용 악성코드 분석 및 대응	시스템 및 파일 구조에 대한 이해	어셈블리 언어 이해 및 활용 가능
실시간 악성코드 대응 서비스	C/C++, Java, Python 등 개발 언어 가능	보안 사고 추적/분석 경험





## 느낀점 & 계획

- 내가 찾는 직무가 생각보다 많지 않다
- 개발 언어는 다양하게 익힐수록 유리하다  
→ C, C++, JAVA를 주로 공부하되, 이외 언어도 가볍게라도 익혀두기
- 네트워크 지식도 쌓아야 한다  
→ TCP, IP 먼저 공부하고 이후 네트워크 장비와 라우터 등의 내용 순차적 학습
- 리버싱 공부 더 열심히 하자  
→ 겨울방학 스터디 계획 이행(리버싱 핵심원리 학습)



“본인과 맞는 직원을 구하는 회사는 어디에서나 분명히 있기때문에 절대 좌절하지 마시고 실망하지 않으셨으면 좋겠습니다. 항상 본인에 대해 자신감을 가지고 구직을 하셨으면 좋겠고 당연히 조급하시겠지만 절대 조급한 마음을 갖지 않으셨으면 좋겠습니다.”

NIT Service – IT·솔루션·기술영업 신입  
최종합격자