INSIDER THREAT PROTECTION
WIZNOTE AI

정보보안 위협평가

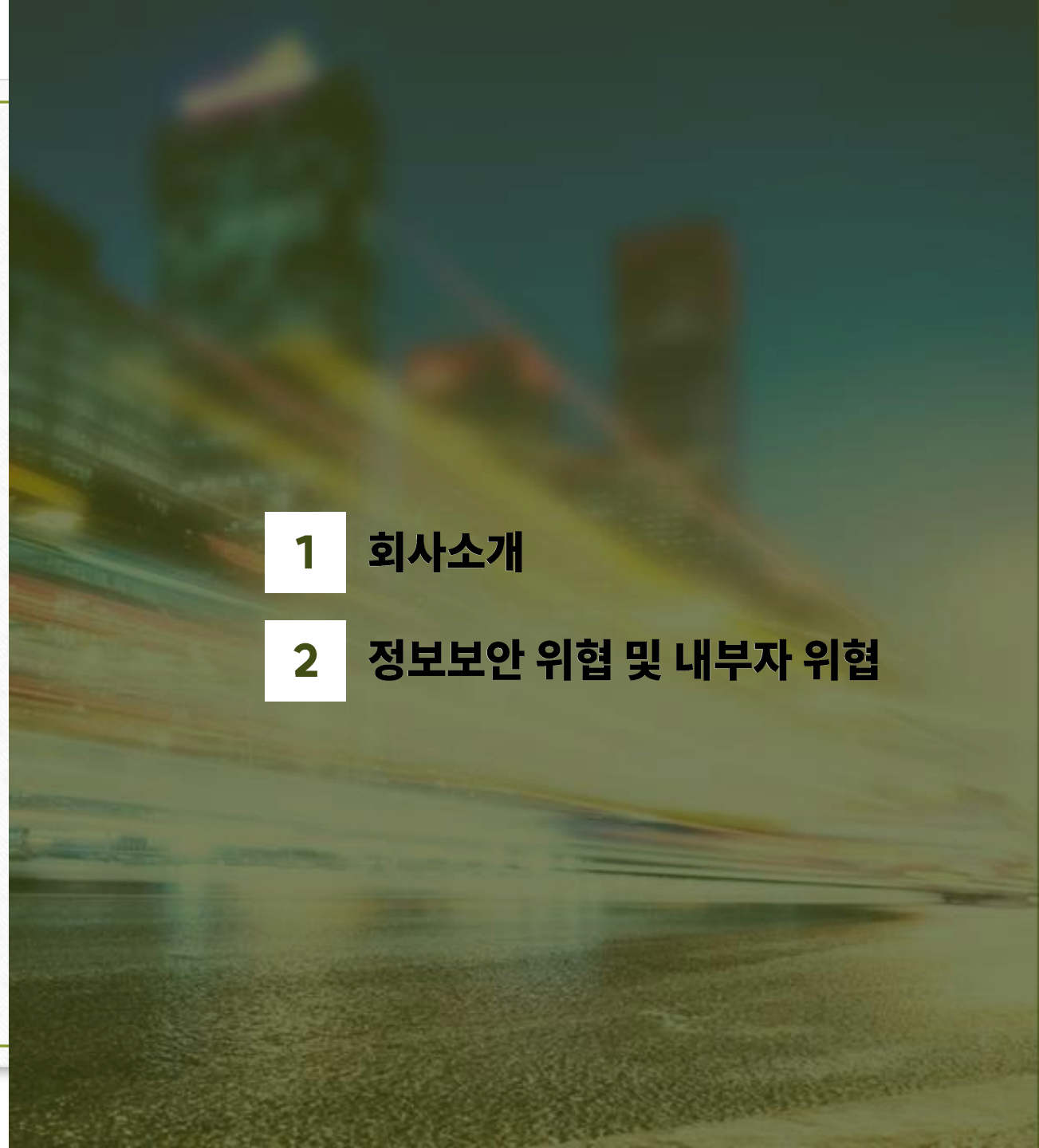
서비스소개자료

위즈노트에이아이(주)

Contents

Chapter 01

회사소개



1 회사소개

2 정보보안 위협 및 내부자 위협

INSIDER THREAT PROTECTION
WIZNOTE AI

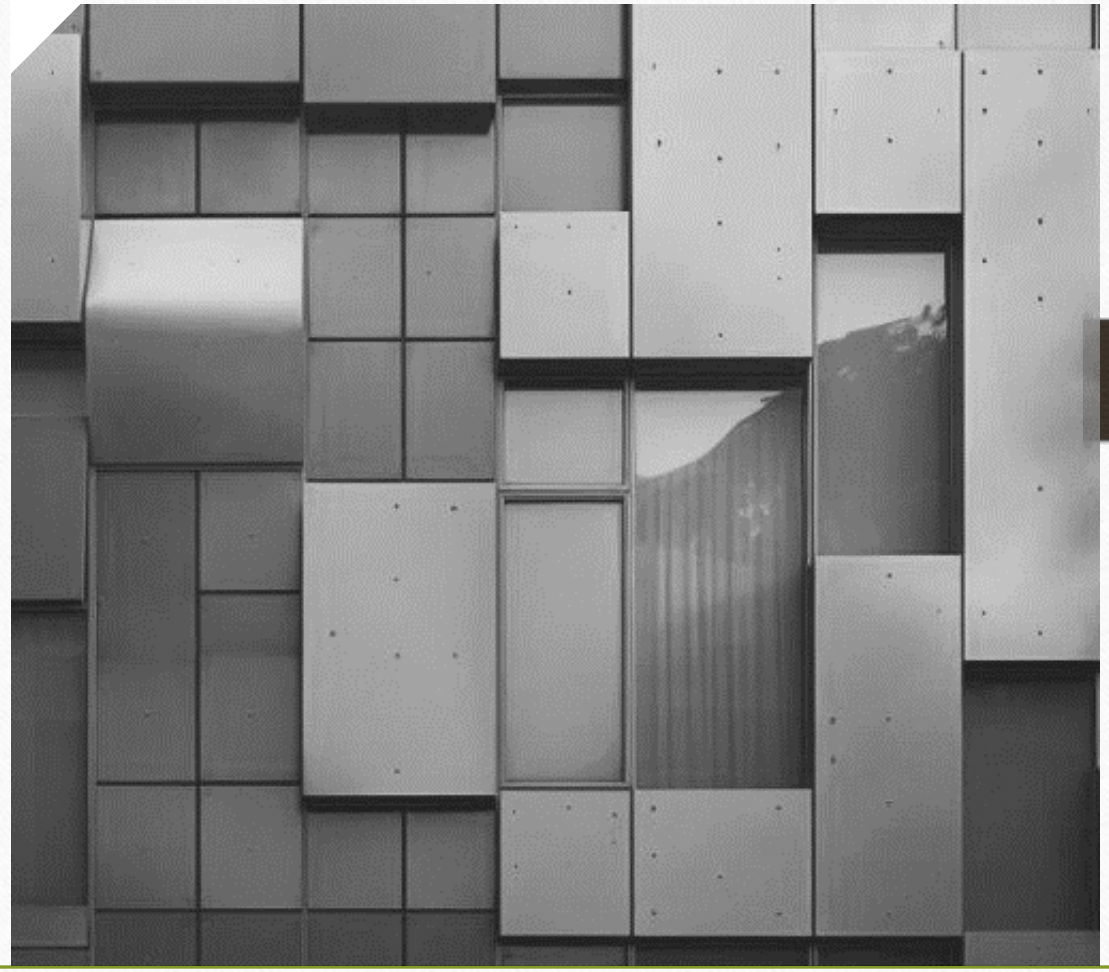
회사소개

정보보안 위협 분석 및 평가 전문기업입니다

국정원 출신 전문가들이 고객사의 기술 등 주요정보를 보호합니다

위즈노트에이아이(주)는 대표이사를 포함, 국정원 출신 정보보안 전문가들을 주축으로 구성된
정보보안 위협 평가 전문 법인으로 기업의 전현직 직원에 의한 기술 및 주요정보 유출을 대응합니다

회사명	위즈노트에이아이(주)
주요사업	정보보안 위협 평가, 컨설팅, 정보보안 교육
대표이사	한경운
설립일	2020년 8월 3일
주소	경기도 성남시 분당구(본사), 경북 구미시 대학로(연구소)
홈페이지	www.wiznoteai.com
이메일	contact@wiznoteai.com



연혁

위즈노트(유) 설립
2020년 8월

정보보안위협 평가서비스 개시

위즈노트 AI(주) 분사
2024년 1월

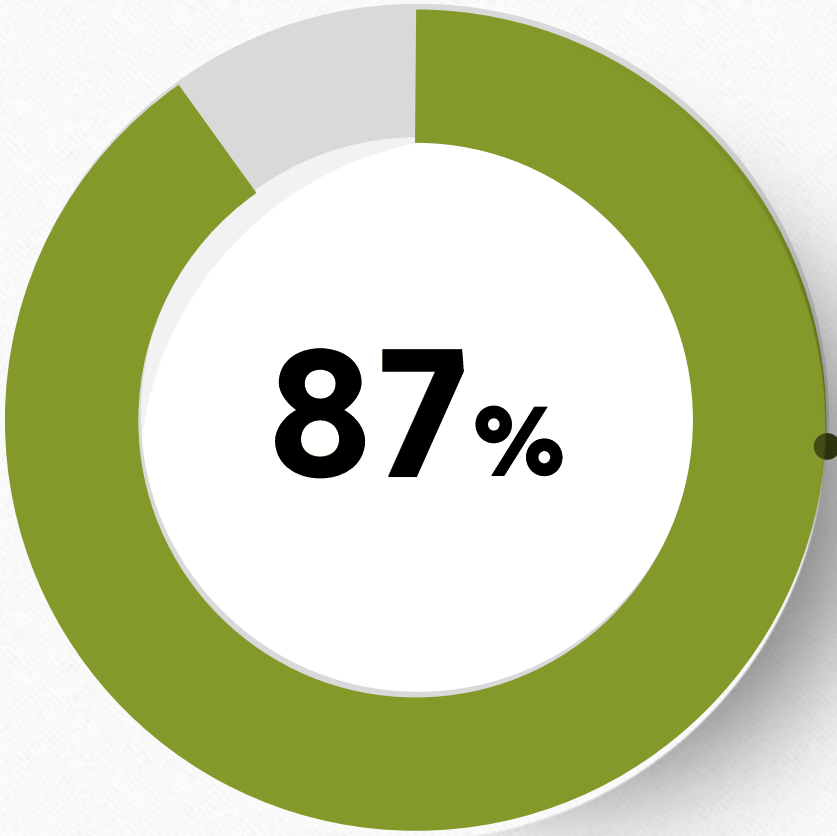
연구소기업 승인
2024년 1월

정보보안위협 평가 솔루션 개발착수
2024년 2월

과기정통부 중소기업벤처부 R&D 과제수행
2024년 6월

벤처기업 등록
2024.11

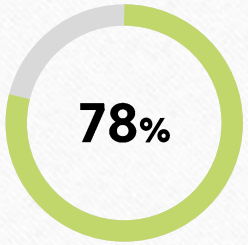
정보보안 위협 평가



정보유출의 87%는 내부자

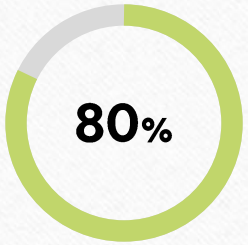
의도를 가진 악의적 내부자와 실수에 의한 부주의한 내부자에 의해
대부분의 정보는 유출됩니다

유출주체



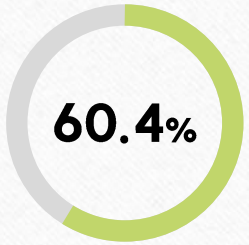
전/현직직원

피해산업군



반도체. 디스플레이,
이차전지 등

피해규모



국가 총연구개발비의
60.4% 수준

Insider Threat Protection

Insider Threat

'Insider Threat(내부자 위협)' 이란

주요 정보와 엑세스 권한 등을 부여받은 '내부자'(직원 등)가 조직에 해를 입힐 수 있는 잠재 가능성을 의미합니다*

기술보호관점에서 '내부자 위협'은 직원 등 주요자료 접근권한을 가진 사람이 자신의 권한을 이용하여 의도적으로 또는 실수로 회사의 주요 기술정보를 외부로 유출하는 행위라고 정의할 수 있습니다

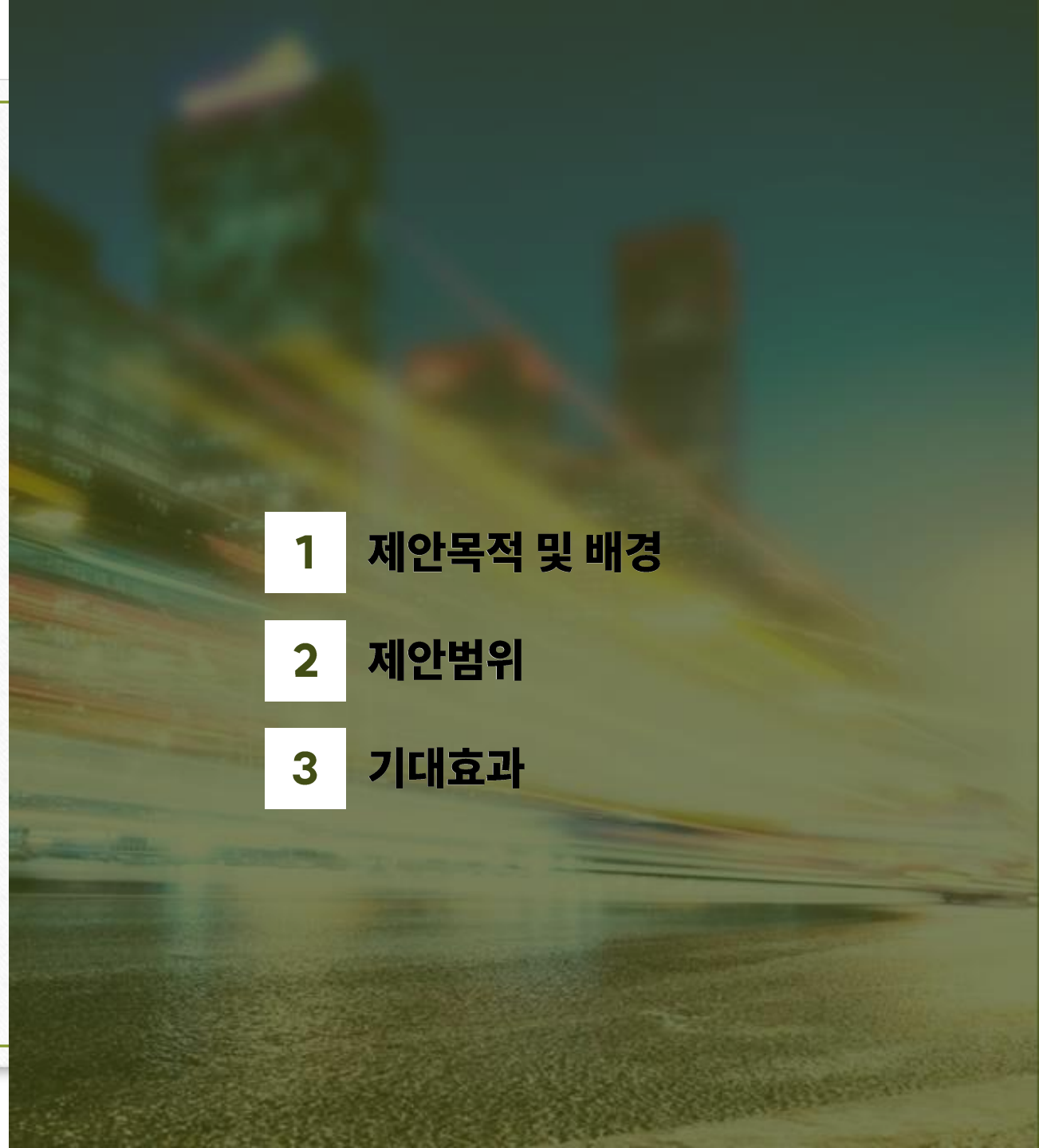
Insider Threat Protection

내부자 위협의 유형은 ① 의도되지 않은 위협(부주의 또는 우발적)과 ② 의도적인 위협으로 구분됩니다. 위즈노트AI는 국가정보원의 HUMINT 전문가와 분석 전문가 등으로 구성되어 두가지 위협 모두에 대한 탐지와 분석, 대응 서비스를 제공합니다.

* 美 Cybersecurity&Infrastructure Security Agency(CISA)

Chapter 02

서비스 제안



1 제안목적 및 배경

2 제안범위

3 기대효과

INSIDER THREAT PROTECTION
WIZNOTE AI

제안목적 및 배경

기업을 '정보보안위협'으로부터 보호합니다

정보보안위협 평가 및 분석/대응

- 기업의 경쟁력인 독보적인 기술이 이직 등 이슈와 함께전현직 직원을 통해 경쟁사 등으로 흘러 들어갑니다
- 기업이 가장 위험한 상황은 "무엇이 유출되었는지도 모르고 있는 경우"이며, 유출인원, 유출내용 등을 확보하면 얼마든지 대응할 수 있습니다
- 위즈노트에아이이는 이러한 내부자의 정보유출 관련 파일유출, 출력물 유출 등 모든 상황을 분석하고 평가하며 대응방안을 제시합니다

정보보호체계 진단

- 정보보안위협과 관련된 업무는 기업의 정보보안, 감사, 법무, 인사의 전영역에 있기 때문에 사각지대가 발생할 수 있습니다
- 관련법의 보호를 받기 위한 관리적 보안부터 물리보안, 기술적 보안부분까지 종합적으로 진단평가합니다
- 이직 등 이슈에서 주로 발생되는 정보유출 통제를 위한 인사조직, 감사조직, 정보보안조직의 협업 프로세스에 있어 사각지대 가 없는지 평가합니다

관리체계 및 이행전략 수립

- 정보보안위협에 대응할 수 있는 관리적, 기술적 보안 분야의 중장기 추진전략을 수립해 드립니다
- 관련법 보호를 받기 위해 필요한 규정 지침 등 미흡 분야에 대한 개선 보완을 지원합니다
- 비용효과적이면서 현장의 요구사항을 반영한 이행과제와 상세 추진방안을 제시해 드립니다

제안범위

내부자 정보유출 위협분석 및 평가

정보보호체계 진단

관리체계 및 이행전략 수립

조각정보를 모아 내부자에 의한 정보보안 위협을 찾아냅니다

- 내부자 위협은 사람의 행동에서 비롯되므로 항상 이유가 있습니다. 야근을 안하던 직원이 야근하고 평소 열람하지 않던 파일을 단시간에 많은 양을 열람하고…"왜 " 라는 의문에서 시작합니다.
- 인간의 행동은 단순 규칙만으로는 분석과 평가가 어렵습니다. 내부자위협 행위의 앞과 뒤, 흘러가는 맥락을 쫓아야 합니다. 자기소개서가 왜 작성되었는지, 연봉자료를 왜 출력했는지…맥락을 봅니다
- 내부자위협은 맥락이 있는 스토리입니다. 현장에 대한 이해, '왜'라는 의문, 조각 정보, 조직과 사람의 특성을 반영해야 내부자 위협을 식별할 수 있습니다. 데이터분석만으로는 절대 찾을 수 없습니다

수행과제

- 사용자별 정보유출 현황 분석
- 해사행위 식별

결과물

- 정보유출현황 및 대응전략 보고서

제안범위

내부자 정보유출
위협분석 및 평가

정보보호체계 진단

관리체계 및
이행전략 수립

정보보호업무 프로세스의 전영역을 살핍니다

- 정보보호 업무 프로세스의 사각지대가 없는지 관리적 보안분야를 진단하고, 특히 관련법의 보호를 받기 위해 필수적으로 수행되어야 할 업무 중 누락된 부분은 없는지 꼼꼼하게 평가합니다
- 기술적 보안분야는 해킹방지 등 네트워크 보안 분야에 치중된 경우가 많습니다. 내부자위협 대응을 위해서는 별도의 정보통제체계가 가동되어야 하는데, 국내최고전문가 그룹이 설계부터 운영까지의 전영역을 진단해 드립니다

수행과제

- 업무용툴 및 보안솔루션 취약점 진단
- 관리적보안 분야 미비점 진단

결과물

- 진단평가 보고서

제안범위

내부자 정보유출 위협분석 및 평가

정보보호체계 진단

관리체계 및 이행전략 수립

현장에 적용가능하고 비용 효과적인 전략 수립

- 기술적 보안분야의 보완을 위해서는 시간과 비용이 들어갑니다. 현장의 목소리를 반영한 중장기 전략을 수립해 드립니다
- 제도적인 보완이 필요한 부분에 대해서는 신속히 보완될 수 있도록 이행과제를 지원합니다

수행과제

- 관리적보안 분야 보완 방안 도출
- 보안솔루션 취약점 보완 방안 도출

결과물

- 개선 로드맵
  (제도정비, 운영절차, 보안솔루션 보완 이행 과제)

기대효과

정보유출 식별 및 예방

- 전현직 직원에 의해 독자기술 등 주요정보의 유출행위가 발생하였는지, 발생중인지 식별
- 내부직원에 의한 각종 해사(害社)행위 식별
- 정보유출 가능성이 높은 내부직원에 대한 사전 대응으로 예방효과 기대

최고수준 정보통제체계 확보

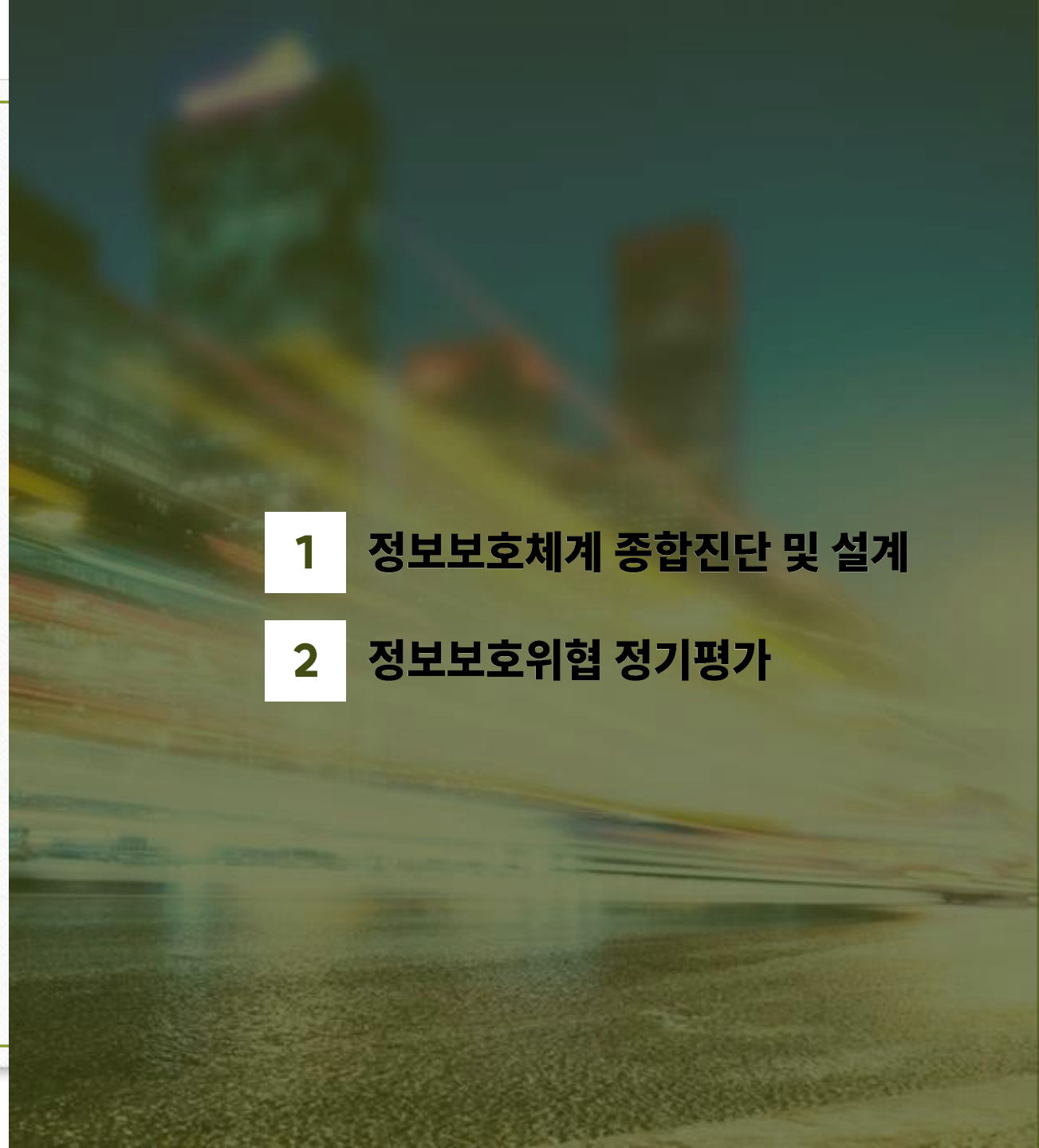
- 인사, 감사, 정보보안 부서 등 효율적인 정보통제 협업을 위한 체계 설계 및 구축
- 국내 최고 전문가가 고객사 특성을 잘 반영한 '맞춤형 정보통제 체계'를 제공하므로, 현장적용 시간 단축

최소비용 최대효과 세부추진안 수립

- 현실성있는 세부추진안의 수립과 진행지원을 통해 비용은 낮추고 효과는 극대화
- 고객사에 이상적인 정보통제체계가 안착할 수 있도록 내재화 지원

Chapter 03

상품소개



1 정보보호체계 종합진단 및 설계

2 정보보호위협 정기평가

INSIDER THREAT PROTECTION
WIZNOTE AI

상품소개

정보보호체계 종합평가 및 설계 (최초 1회)

필요에 따라 선택하세요

정보보호위협 정기평가

Chapter 3-1

정보보호체계 종합평가 및 설계

정보보호체계 종합 평가 및 설계

01 정보보호체계 진단 및 평가

고객사의 업무흐름과 호흡을 같이하며 정보유통 현황을 종합적으로 평가합니다

02 보안체계 설계/구축 지원

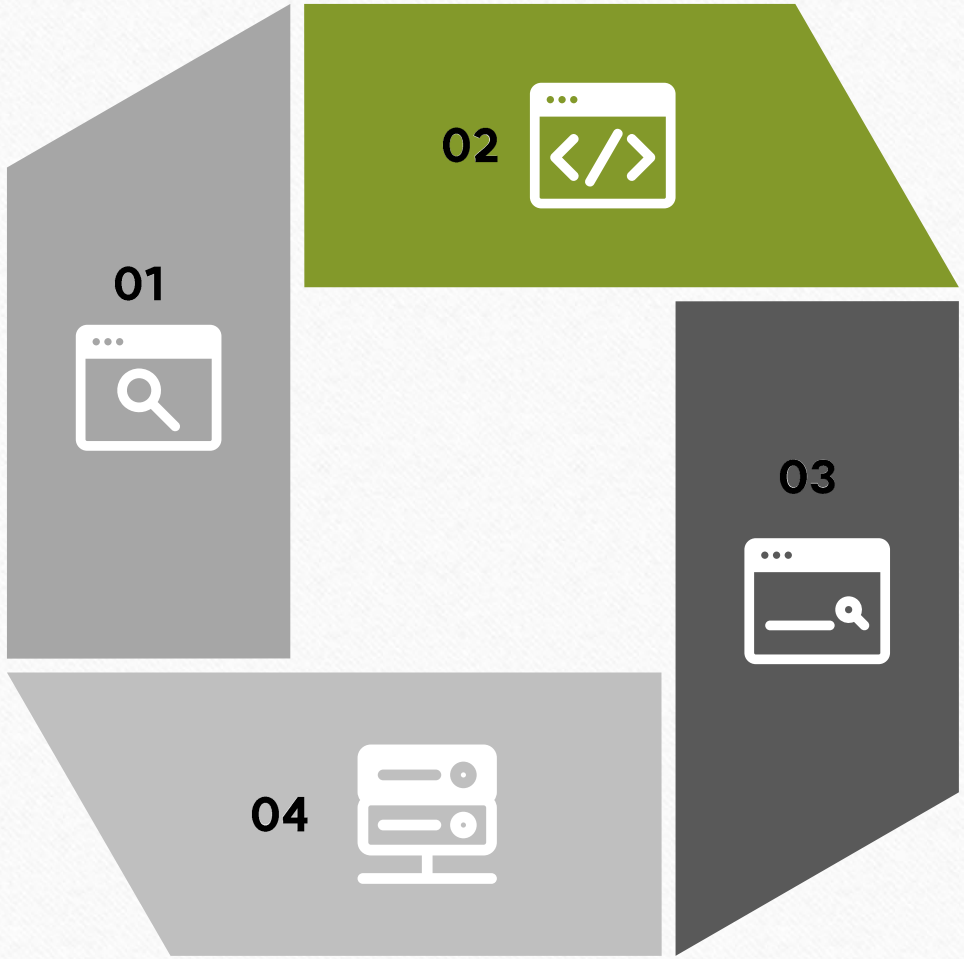
고객사 특성에 맞춘 보안체계를 설계하고 운영중 또는 도입예정 보안솔루션에 설계내용을 반영

03 네트워크 보안 취약점 진단

해킹 등 외부공격 방어에 대한 우리회사의 실태를 진단하고 고객사 실정에 맞춘 대안을 제시

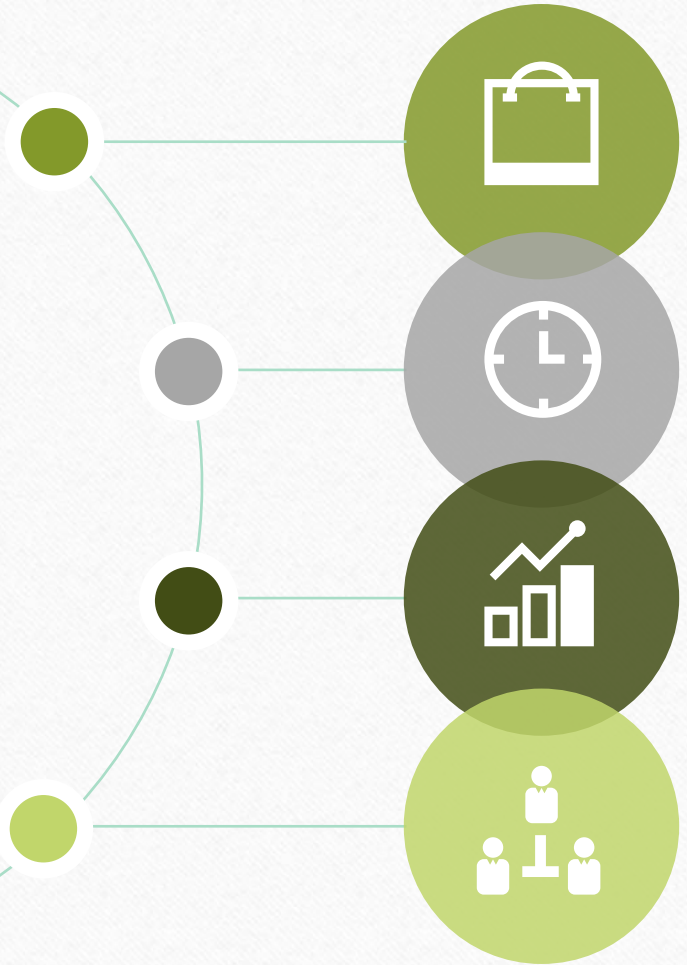
04 유출분석 및 회수

최근 6개월 이내 내부 직원에 의한 주요 자료의 유출가능성을 평가하고 회수를 지원합니다



업무 프로세스

이렇게 진행됩니다



01 고객사 미팅
- 기업이 체감하고 있는 정보보안 위협에 대해 무엇이 필요한지, 요청사항은 무엇인지 파악

02 고객사 업무 현장 진단
- 고객사가 평소 업무를 수행함에 있어 사용하는 프로그램/프로세스를 분석, 정보보안 위협요소 도출

03 효과적인 정보보안체계 설계
- 고객사의 업무 프로세스에 맞추고, 직원들의 현업에 불편함이 없는 맞춤형 정보보안체계 설계

04 구축 및 내재화 지원
- 설계된 정보보안체계를 도입되는 또는 운영중인 솔루션 등에 적용하는 구축단계 지원
- 정보보안체계의 내재화를 위한 안내자료 등 지원

기대효과

최고 보안전문가가 평가하고 설계합니다

- 회사의 특성을 반영하여 업무효율을 저해하지 않습니다
- 기업규모 및 형황에 맞춘 맞춤형 정보보안체계를 만들어 드립니다
- 관리적 보안분야 부터 물리적 보안분야까지 모든 분야를 포함합니다

중복투자 방지

- 기업에 필요한 정보보안체계를 기초부터 평가하고 설계하므로, 향후 중복투자의 위험을 줄일 수 있습니다
- 정보보안에 대한 부서별 업무 사각지대에 대한 보완도 기대할 수 있습니다

평가/설계/구축을 한번에

- 평가부터 설계와 구축지원을 모두 지원합니다
- 국내외 솔루션의 보안성검토 및 비용비교 등을 포함합니다

Chapter 3-2

정보보안위협 정기평가

정보보안위협 정기평가

우리회사는 과연 안전할까

모든 조직에는 악의적 내부자가 존재합니다. 우리회사의 주요 기술자료 등이 유출되지는 않고 있는지 평가하고 관련법 적용을 위한 증거도 확보합니다

주요 임직원의 퇴직이슈

오랜기간 우리회사 기술을 다뤘던 임직원, 회계처리를 했던 직원 등은 어떤 경우에는 잠재적 위협이 되기도 합니다. 퇴직예정자에 대한 정보유출 위협을 집중 평가해 드립니다

회사정보 보호

임직원에 의해 외부로 유출된 정보가 파악되면, 삭제/회수를 직접 수행하거나 필요시 법적조치를 위한 증거를 확보하고 지원합니다

필요한 만큼만 이용하세요

주요 임직원 퇴사시 일회성 점검을 비롯, 필요한 경우 연간, 분기별로 평가를 할 수 있으며 월간 구독형 서비스도 있습니다

기대 효과

정보 보안 위협 대응

우리회사에서 어떤 자료나 정보가 외부로 유출되었는지도 알지 못하는 상황이 가장 위험합니다. 임직원에 의한 정보보안위협을 정확히 탐지/평가하고 대응방안을 제시합니다

정보보안 사각지대 극복

정보보안 관련 부서가 있는 경우에도 인사, 감사 등과의 협업이 힘들면 사각지대가 발생합니다. 국정원 전문가 집단을 대표님 직속의 참모조직처럼 운영하실 수 있으며, 이 경우 업무사각지대 극복 및 전문가 집단의 조언을 활용할 수 있습니다

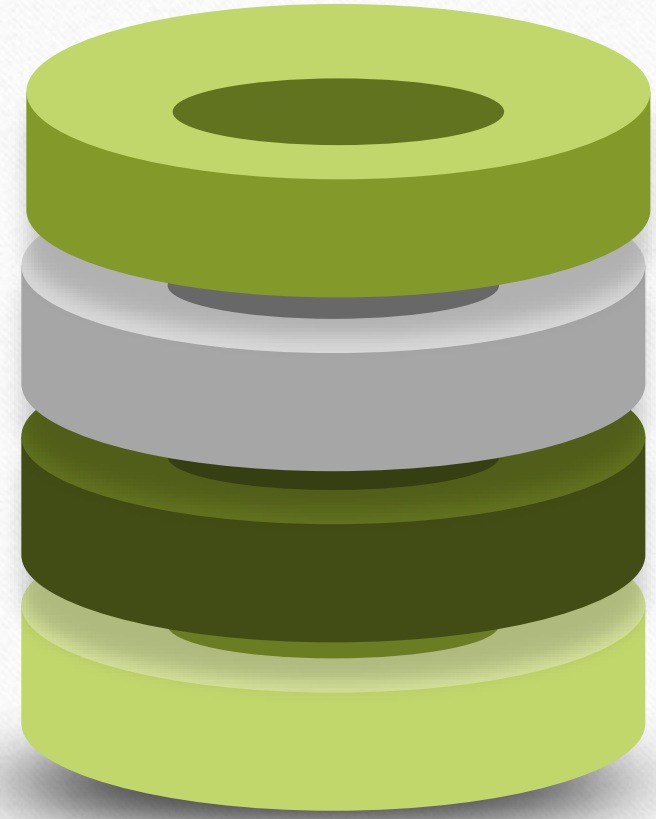
해킹/랜섬 등 걱정도 그만

내부자에 의한 정보보안 위협 뿐만이 아니라 필요한 경우 외부 공격에 의한 해킹이나 랜섬에 대한 위협평가와 대응방안도 전문가 집단이 제시해 드립니다

비용절감

정보보안 전문조직을 회사내 운영하기 위해서는 상당한 인건비가 소요됩니다. 위즈노트에이아이에 맡김으로써 엄청난 비용절감이 가능해 집니다

업무 프로세스



이렇게 진행됩니다

01 고객사 요청사항 파악
- 회사에서 걱정되는 부분이 무엇인지, 어떤 부분을 확인하고 싶은지 등에 대한 고객사 요청사항을 파악합니다

02 필요한 로그데이터 수령
- 분석에 필요한 로그데이터를 고객사에 요청하고 수령합니다

  보안솔루션 데이터 및 이메일 아카이빙 데이터 등입니다

03 정보보안위협 평가
- 임직원에 의한 기술 및 정보유출 흔적을 찾아내고, 해당 사안의 위협정도를 평가하여 REPORT 합니다

04 대응방안 제시
- 확인된 위협에 대해 회사가 할 수 있는 대응방안들을 제시하고 자료삭제나 회수가 필요한 경우 전문가집단이 직접 대행해 드립니다

보고서 내용

정보보안위협 정기평가 보고서에는 이런 내용이 담깁니다

임직원 위협평가

어떤 임직원이 어떤 자료를 유출했는지, 유출수단은 무엇이었는지, 유출시기나 주기는 어떻게 되었는지 등에 대해 직관적으로 확인 가능한 데이터를 담아 보고합니다

위협 평가 근거

임직원에 대한 위협평가시 평가 근거도 제시합니다. A라는 기업에는 정보보안 위협이 되지 않는 행위가 B라는 기업에는 치명적일 수 있습니다

기업의 특성을 반영한 정보보안위협 평가의 근거를 제시합니다

대응방안

실제 임직원에 의한 주요 기술자료 등 정보유출의 흔적이 있는 경우 가능한 대응방안을 제시합니다

위즈노트에이아이가 직접 수행 가능한 대응방안부터 법적조치가 필요한 경우 증거지원까지 회사의 경영 판단에 따라 요구되는 대응수준을 제시합니다

철저한 비밀유지

정보보안위협평가와 관련된 모든 프로세스는 비밀유지 됩니다. 필요한 경우 대표님을 비롯한 최소한의 인원만 인지하는 상황에서 진행할 수도 있습니다

정보역류 위험(관련 임직원이 인지하여 증거인멸 시도 등)을 방지합니다

상품구성

필요한 만큼만 이용하세요

정기 구독형

월간/분기별/반기별

특정기간별 정보보안위협 평가를 하고, 대표이사 보고 후 필요한 대응방안을 **직접 수행**해 드립니다

일회성

퇴직자 등 현안발생시

회사의 기술유출 우려, 각종 해사(害社) 행위 등 발생시 일회성으로 정보보안위협 평가를 진행합니다

내부자 또는 외부 공격자에 의한 정보보안위협으로부터 우리기업을 보호합니다

contact@wiznoteai.com