Deloitte.

사이버 보안 운영 모델의 진화

AI 기반 자율화와 서비스형 리더십(vCISO)의 부상

2026년 5월 | Deloitte Insights

Leader's Message

Deloitte.

백 철 호 파트너
One Cyber & Resilience 리더
한국 딜로이트 그룹

cbaek@deloitte.com

"기업 비즈니스 연속성과 가치 보호를 위한 차세대 보안 전략"

2026년, 사이버 보안 환경은 AI의 급속한 발전, 지정학적 분절화, 공급망 복잡화 속에서 공격 표면이 전방위로 확장되었습니다.

사이버 리스크는 더 이상 특정 시스템이나 보안 조직 내부에 국한되지 않으며, 기업의 관리·통제 범위를 조직 경계 너머로 빠르게 밀어내고 있습니다.

보안은 이제 운영 지속성과 신뢰, 그리고 기업 가치를 좌우하는 핵심 경영 과제입니다.

하지만 많은 기업들의 사이버 보안 운영은 여전히 규제 준수, 사후 대응, 내부 경계 방어라는 기존 모델에 머물러 있습니다. AI 기반 공격이 대량화·자동화·지능화되는 현실 속에서 이러한 방식은 속도와 대응 범위 모두에서 한계를 드러내고 있으며, 운영 비효율과 비용 부담을 동시에 가중시키고 있습니다.

이제 기업은 탐지 후 대응하는 구조를 넘어, AI 기반 자율 운영과 실시간 리스크 통제를 중심으로 보안 운영 모델 자체를 전환해야 합니다.

딜로이트는 AI 기반 자율화 보안과 vCISO를 결합하여, 전략·거버넌스·운영·역량·기술을 하나의 리더십 체계로 통합할 것을 제안합니다.

AI가 실행하고 vCISO가 책임과 의사결정을 수행하는 이 새로운 운영 모델을 통해 기업이 더 빠르고, 더 정교하며, 더 회복탄력적인 사이버 보안 체계를 구축할 수 있도록 지원하겠습니다.

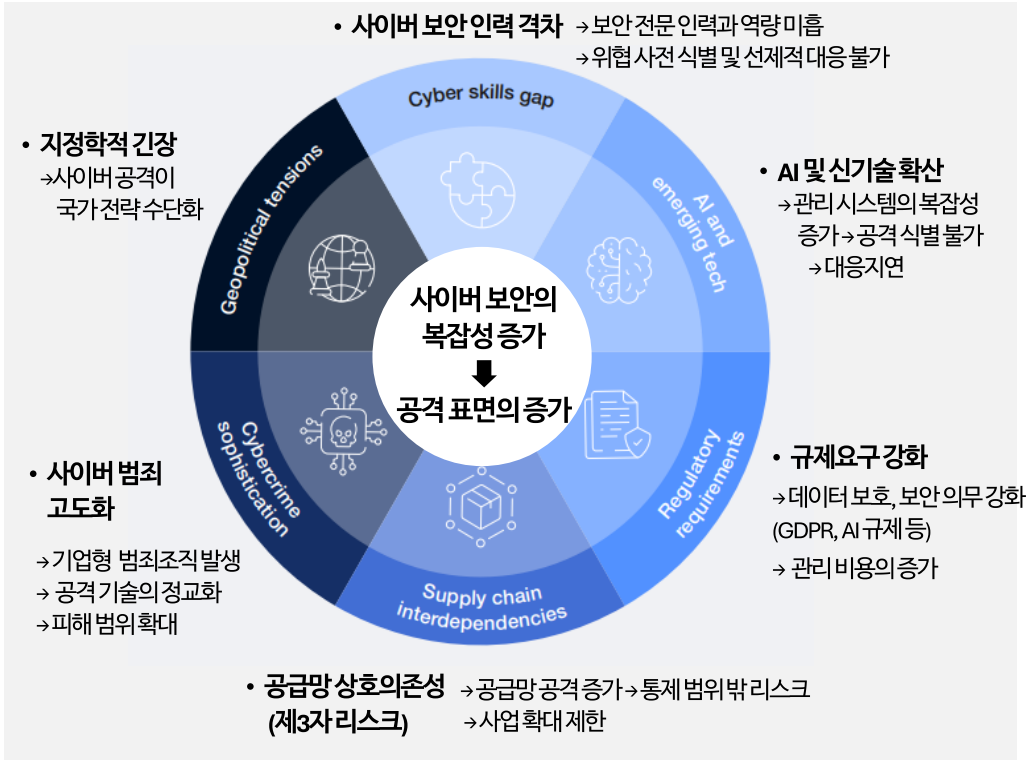
목차

사이버 보안 환경의 변화 - 사이버 공격 표면의 증가

사이버 환경의 복잡성 심화와 공격 표면의 확대는 자산, 신원, 공급망으로 이어지는 관리·통제 범위를 조직 경계 너머로 지속 확장 시키고 있습니다.

사이버 보안의 복잡성 증가 ➡ 공격 표면의 확대

공격 표면의 확장 : 사내(개인 정보) → 클라우드(기업 자산) → 공급망(협력사 신뢰) 등으로 통제 불가능 수준 → 사이버 보안 실패



사이버 보안 관리·통제 범위의 확대

사이버 보안은 계정·내부 중심 통제에서 모든 주체와 공급망 전반의 행위를 실시간 검증하는 Zero Trust 기반으로 전환

공격범위

자산 및 데이터 관리 범위 확대

- **보이지 않는 자산의 폭증 → 실시간 가시성 확보가 통제의 핵심**
  - (기존) PC·서버·네트워크 등 전통적 IT 자산
  - (확장)클라우드·API·AI 모델·학습 데이터·Shadow AI까지

신원 및 접근 통제 범위 확대

- **모든 주체를 매번 검증하는 Zero Trust +, 정적 권한 관리에서 동적·맥락 기반 접근 통제로 이동**
  - (기존) 임직원 계정·권한 중심의 접근 관리 (IAM 기반)
  - (확장) 인간 주체(API·봇·AI 에이전트), 협력사·제3자 계정까지 포함한 Identity Surface 전반으로 확대

공급망 통제 범위 확대

- **조직 경계가 더 이상 통제의 경계가 아님 → 생태계 전반의 지속적 위험 평가**
  - (기존) 내부 사용자의 이상 행위 탐지
  - (확장) SW/AI 공급망·외부 파트너·외주 프로세스까지 생태계 전체

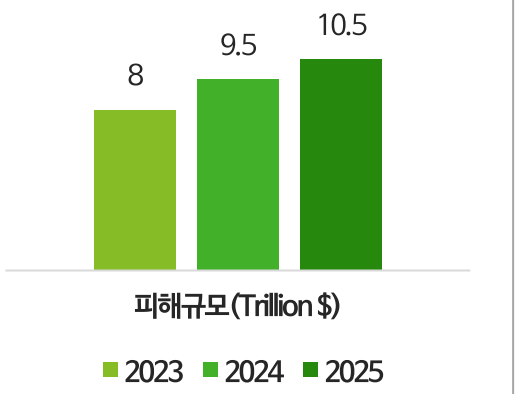
사이버 보안 환경의 변화– 사이버 보안 피해 규모 폭증

전 세계 사이버 범죄 피해가 연간 10조 달러, 국내는 22조원을 넘어서고, AI 기반 공격이 피싱, 딥페이크 및 데이터 탈취 형태로 대량화·자동화·지능화되고 있어, 기존의 보안 운영 모델은 한계점을 드러내고 있습니다.

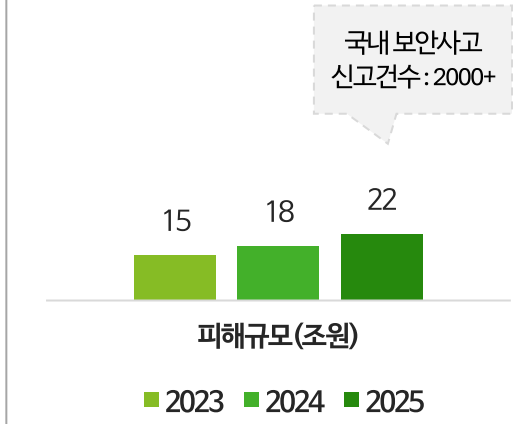
전 세계 사이버 피해 규모[1)]

- 과거 '기술 해킹' 중심에서 현재는 AI로 **'인간의 신뢰와 판단'을 훼손하는 공격**으로 진화
- 랜섬웨어, 사기, 탈취가 동시에 발생하고 사업 중단·규제 대응 등 2차 비용까지 더해져 실제 피해는 통계치를 상회
- 국내 사고 빈도·규모가 동반 증가 했으나, 기업의 사전 투자와 대응 효과는 미흡

글로벌 사이버 범죄 연간 피해액(Trillion $)



국내 사이버 범죄 연간 피해액 (조원)



신종 사이버 공격 유형, 특성 및 기업 위협 수준 : 대량화·자동화·지능화

유형	공격방식	위협 수준[2)]	주요 피해 영역
AI 강화 피싱·스피어피싱	• LLM을 활용한 초정밀 이메일/메시지 생성	매우 높음	• 자격증명 탈취 • 금융사기 • 내부 시스템 침투
딥페이크 기반 소셜 엔지니어링	• 음성·영상 합성을 통한 임원/거래처 사칭 • 실시간 화상회의 기반 공격 등장	높음	• 금융 이체 사기 • 브랜드 신뢰 훼손 • 내부 의사결정 왜곡
LLM 데이터 Poisoning 공격	• 학습 데이터에 악의적 정보 삽입 • AI 의사결정 결과 조작	높음	• AI 의사결정 오류 • 운영 리스크 • 규제/법적 리스크
AI 생성 맞춤형 악성코드	• LLM으로 변종 악성코드 자동 생성 • 보안 탐지 우회 코드 생성	중간~높음	• 시스템 침해 • 랜섬웨어 확산 • 데이터 탈취
AI 기반 취약점 탐색 자동화	• AI를 활용한 시스템 취약점 스캐닝 및 공격 자동화	높음	• 제로데이 공격 • 인프라 침해 • 서비스 중단

1) Global Cybersecurity Outlook 2026, World Economic Forum, January 2026 ;
2) 위협 수준은 "발생가능성(빈도)"과 "비즈니스 영향도"를 종합적으로 고려하여 평가: (매우 높음) 이미 대규모 피해 발생 확산 중, (높음) 빠르게 증가 중이며 주요 리스크로 부상, (중간~높음) 기술적으로 가능하며 확산 초기 단계

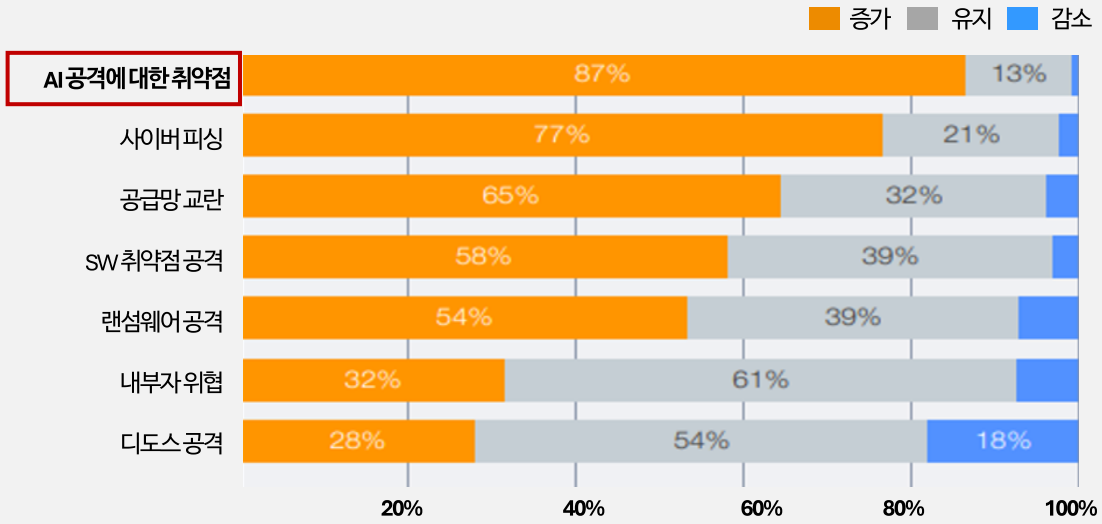
사이버 보안 환경의 변화– 기업 가치를 악화시키는 경영 리스크로 확대

AI 취약성(87%)과 사기·피싱(77%)의 급증은 사이버 리스크를 단순 보안 이슈에서 기업 가치와 신뢰를 결정짓는 경영 리스크로 전환시켰으며, 그 피해는 운영 중단(66%)과 신뢰 붕괴(66%)를 포함해 브랜드·재정·운영 전반에 악영향을 끼칠 수 있습니다.

가장 위협적인 사이버 공격 유형[1)]

- AI 취약성이 가장 빠르게 증가하는 리스크로 부상(87%)
  (AI가 스스로 취약점 스캔 → 공격 도구 개발 → 침투 → AI 공격에 대한 취약점 증가)
- 사기·피싱의 급증(77%)은 기술 해킹보다 인간의 판단과 신뢰를 무너뜨리는 공격의 위험성 인식
- 내부자 위협(32%), DoS(28%)는 기업이 어느 정도 통제력을 갖춘 반면, AI·공급망 등 조직 경계 밖 위협은 통제가 훨씬 어렵다는 인식이 반영

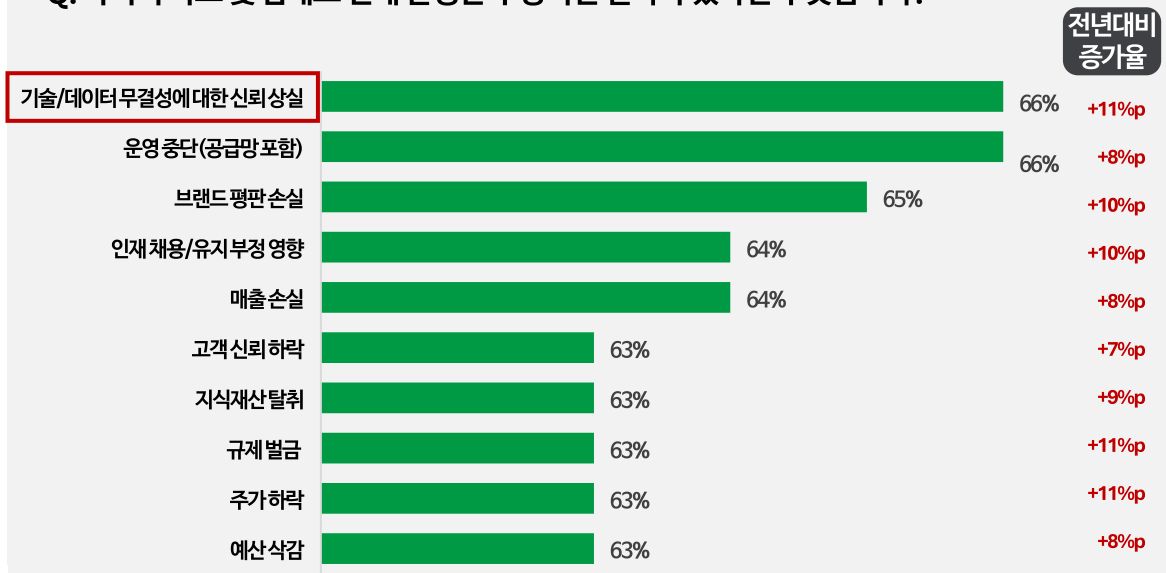
Q: 사이버 리스크의 수준은 어떻게 변화했다고 보십니까?



사이버 공격 시 경영 리스크[2)]

- 회복이 가장 어려운 무형 자산의 손상이 금전적 손실보다 더 크게 인식
  (신뢰상실-66%, 브랜드 평판-66%, 고객신뢰-63%)
- 운영 중단·공급망 차질(66%), 지식재산 탈취(63%), 인재 채용·유지 차질(64%)은 사이버 사고가 기업의 생산 기반과 성장 동력을 동시에 잠식
- 사이버 사고는 즉각적인 재무 손실이 아닌 아닌 장기 재무 리스크로 지속 (e.g. 주가하락-63%, 규제벌금-63%)

Q: 사이버 사고 및 침해로 인해 발생한 부정적인 결과가 있다면 무엇입니까?



1) World Economic Forum, Deloitte Insights 재구성; 2) Deloitte Cyber Survey 4th edition, Deloitte Insights

사이버 보안 환경의 변화– 보안 규제·컴플라이언스 강화

사이버 보안 규제가 강화되면서 경영진의 사고 대응 의무와 책임이 법제화되고 있습니다. 이제 보안은 기술적 선택사항이 아닌, 법적 의무이자, 지배구조와 기업 운영 모델을 근본적으로 재편하는 핵심 경영 과제가 되었습니다.

주요국 보안 규제·컴플라이언스 사항 (AS-IS)		핵심 사안의 강화 방향 (TO-BE)
미국	• CIRCIA[1]: 중요 인프라 사이버 사고 신고 의무화, CISA[2] 주도 체계 구축 • SEC [3]사이버 공시 의무: 상장사 대상 중대 사고 발생 후 4일 이내 공시	• 사고 신고: CISA 체계 내 24~72시간 이내 • 상장사 공시: 중대 사고 4일 이내 • 규제보다 시장 투명성·투자자 보호 중심 통제 모델 추진
EU	• NIS2 Directive: 회원국별 전환 진행 중(2024~2025), 약 2~3만 개 기업으로 적용 확대 • EU AI Act: 2024년 발효, 2026년부터 고위험 AI 의무 단계적 적용	• 공급망 보안 책임 명문화(제3자 리스크 의무화) • 이사회·경영진 책임 직접 부과 • GDPR·NIS2·DORA·AI Act 간 규제 정합성 통합 논의 중
중국	• 사이버보안법(CSL) 개정안: 2026년 1월 1일부터 시행 • 역외 적용(Extraterritorial Enforcement) 확대 • AI 윤리 및 리스크 모니터링 의무 명문화	• 벌금 상한 대폭 상향(최대 1,000만 위안) • CII(Critical Information Infrastructure, 핵심정보인프라) 사업자 규제 강화
한국	• 법·제도 강화: 과징금 상향(최대 매출 10%), 사고 발생 시 과징금 및 24시간 내 신고 의무화 • 임원급 CISO 지정, 이사회 보고 의무, 경영진 법적 책임 명문화	• ISMS-P 확대[4], 서류 → 기술·실증 중심 심사, 사고 시 사후심사·인증 취소 강화 • 상장사 및 인증 기업 대상 공시 의무 확대,투자 수준 → 리스크 관리·대응 체계까지 공개

기업의 직 · 간접 파급 영향

경영진 책임의 법제화

- 사이버보안 책임을 법에 명시
- 보안 사고 발생 시 경영진 개인의 법적·금전적 책임으로 직결

실시간 보고 의무 강화

- 탐지·분석·보고까지 자동화되지 않으면 규제 위반이 확정적
- 대응 체계의 근본적 재설계가 불가피

기업의 보안 범위 공급망까지 확대

- 협력사·클라우드·외주사까지 통제 필요 → 계약 해지·인증 취소·과징금 연쇄 발생
- 기업 단독 보안은 더 이상 의미가 없어짐

1) Cyber Incident Reporting for Critical Infrastructure Act –중요 인프라 사이버사고 보고법; 2) Cybersecurity and Infrastructure Security Agency –사이버보안 및 인프라 보안국; 3)Securities and Exchange Commission– 미국 증권거래위원회 : 4) ISMS-P (Information Security Management System – Privacy)= 정보보호 + 개인정보보호통합인증제도

목차

글로벌 기업의 사이버 보안 투자와 대응 노력 – 사이버 보안의 투자 우선순위 설정 및 예산 증액

글로벌 기업의 사이버 보안 투자는 탐지·대응, 공급망, 서비스화 중심으로 전환되며, 전체 사이버 보안 예산은 확대되는 가운데, 대기업은 비효율을 줄이고 중견기업은 역량을 빠르게 확보하는 방향으로 투자 재편이 진행되고 있습니다.

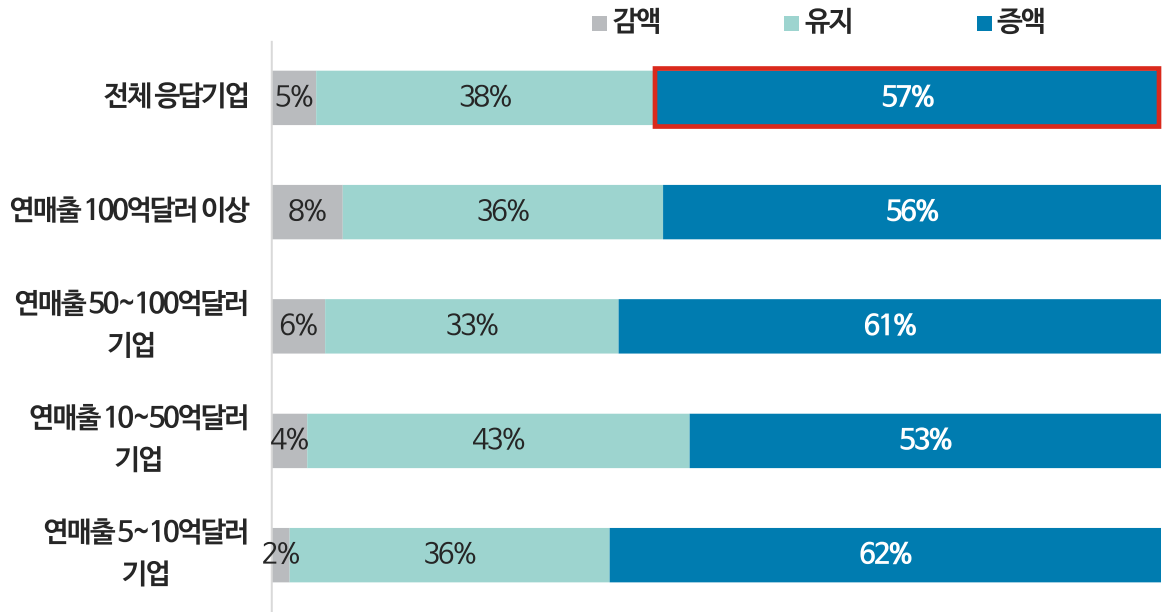
글로벌 기업의 사이버 보안 투자 우선순위[1)]

- 탐지·대응 중심 전환: AI 기반 보안과 클라우드 투자 확대, 예방 → 속도 중심 대응으로 이동
- 통제 범위 확장: 공급망·클라우드 확대로 생태계 단위 보안으로 전환
- 서비스화 가속: MSSP·MXDR 확대, 인력 → 보안 서비스 구매 구조 전환
- ID 보안 강화: Zero Trust 투자 확대, 자격증명 기반 공격 대응

사이버 보안 투자 영역	투자 우선 순위	주요 동인
AI 기반 위협 탐지·대응	★★★★★	• AI가 기업의 공격면 확대 및 침투 증대
클라우드 보안 강화	★★★★★	• 클라우드 침해 35%증가
공급망 보안(TPRM[2)])	★★★★☆	• 대형 조직 54%가 공급망 리스크
사고 대응 및 복구(IR·DR)[3)]	★★★★☆	• 사고 시 복구 역량이 성과에 직접 영향
관리형 보안 서비스 (MSSP·MXDR[4)])	★★★★☆	• 전담 인력 및 스킬 부족 해소 수단
ID·접근 관리 (Zero Trust)	★★★★☆	• 자격증명 탈취 급증

사이버 보안 예산 계획[1)]

- 모든 기업 규모에서 증액 응답이 53~62%로 과반을 차지, 사이버 보안은 경기와 무관한 필수 투자로 정착
- 100억 달러 이상 기업의 감액 비율(8%)이 중견기업(2%)보다 4배 높아, 기존 투자의 비효율을 재평가하고 선택과 집중에 착수



1) Deloitte Cyber Survey 4th edition, Deloitte Insights , 2) TPRM : Third-Party Risk Management, 제3자(협력사·벤더·외주사)의 리스크를 체계적으로 평가·통제·모니터링하는 관리 체계; 3) 사고 대응 및 복구(IR·DR): IR (Incident Response) → 침해사고 대응, DR (Disaster Recovery) → 재해 복구
4) MSSP(Managed Security Service Provider): 관리형 보안 서비스 제공자를 의미 , MXDR(Managed Extended Detection and Response)는 관리형 확장 탐지 및 대응의 약자로, 기존 XDR(확장된 탐지 및 대응) 기술에 '관리형 서비스'를 결합한 차세대 보안 서비스 모델을 의미

글로벌 기업의 사이버 보안 투자와 대응 노력 – 사이버 보안을 전사 과제로 격상

글로벌 두 기업은 사이버 사고 대응을 보안팀의 기술적 과제에서 전 조직이 참여하는 경영 거버넌스로 격상하고, 외부 전문성과 반복적 실전 훈련을 결합하여 사고 이후 더 강한 회복탄력성 체계로 전환했습니다.

사이버 보안 과제 대응 방향 : 전 조직의 경영 과제로 격상

	Pain points	Solution	Impacts
글로벌 미디어 기업	• 보안팀에만 국한된 대응 체계로 전사적 의사결정 불가 • 공격의 예측 가능성 저하	• 전 조직이 참여하는 통합 대응 체계 구축 • 실제 위기 기반 플레이북과 반복 시뮬레이션 훈련으로 실행력 내재화	• 보안팀에 국한된 대응을 전 조직으로 확대하여 부서별 책임과 권한을 명확히 정의 • 전사 차원의 통합된 의사결정 구조로 대응 속도와 정확도 동시 향상 • 고객·임직원·투자자에 대한 부정적 파급 효과를 차단하여 기업 신뢰 보호
글로벌 항공 서비스 기업	• 랜섬웨어로 핵심 항공 시스템 마비 → 기체 운영·고객 서비스 지속성에 심각한 위협 • 통신·스케줄링·운영 계획 등 미션 크리티컬 시스템 전반의 불안정 • 조직 전반의 사이버 준비 수준에 근본적 공백 확인	• 외부 전문 서비스(CIR3)를 활용한 신속한 대응 체계 가동 • 랜섬웨어 확산 차단 및 추가 침해 가능성 탐지·제거 • 핵심 시스템과 데이터 우선순위를 정의하고 단계적 복구 계획 수립 • 미래 위협에 대비한 전사적 사이버 대응 전략과 역량 재설계	• 핵심 운영 시스템 안정화 및 고객 서비스·안전 운영의 신속한 정상화 • 조직 전반의 사이버 회복탄력성 강화 • 미래 위협까지 고려한 지속 가능한 사이버 준비 체계 확보

사이버 보안 대응 방향

보안 과제를 전사적 통합 거버넌스로 격상

- 전 조직이 참여하는 통합 대응 체계를 구축 → 신속하고 일관된 의사결정 구조 확보

실행력 중심의 실전 대응 체계

- 실행력을 내재화하고 우선순위 기반의 단계적 복구 계획을 수립

외부 전문성과 회복탄력성의 결합

- 자체 역량의 공백을 관리형 보안 서비스로 신속히 보완
- 미래 위협에 대비한 전사적 전략을 재설계

글로벌 기업의 사이버 보안 투자와 대응 노력 - 사이버 보안 대응 방향 전환

글로벌 F&B 기업과 국내 통신사는 자체 구축이 아닌 AI 기반 관리형 서비스를 통해 보안 역량을 확보하고, 탐지부터 대응까지 상시 체계로 전환함으로써 비용 효율과 운영 지속성 확보에 집중하고 있습니다.

사이버 보안 과제 대응 방향 : 보안 운영·대응·통제 방식의 전면 전환

	Painpoints	Solution	Impacts
글로벌 F&B 기업 MXDR 도입	• 랜섬웨어로 핵심 시스템 마비 → 비즈니스 연속성 붕괴 • 기존 내부 보안 체계로는 지속 대응에 한계 → 비용 부담	• 내부 보안 시스템 구축 포기 → MXDR 기반 완전 관리형 보안 모델 전환 • 24시간 상시 대응 및 클라우드 기반 통합 환경으로 전환	• 신속한 서비스 정상화 및 중단 최소화 • 상시 모니터링·위협 헌팅 체계 구축 • 보안 운영 비용 절감 및 확장성 확보
국내 통신사	• 대규모 고객 데이터 보유로 이상 활용 리스크 증가 • 규제 강화에 따른 선제적 관리 필요	• AI 기반 이상 탐지 도입→개인정보 보유·활용 패턴 분석 • 상시 모니터링 체계 구축→ 데이터 이력 통합 + 비정상 패턴 자동 탐지 • Human-in-the-loop 운영: AI 선별 → 담당자 검토·판단 • 위험도 기반 대응: 우선순위 체계로 대응 효율성 강화	• 탐지·규제 대응 강화 →위험징후 정확도 향상, 선제적 리스크 식별 • 업무 효율 개선→ 반복 점검 자동화로 부담 감소 • 관리 체계 고도화→데이터 흐름 가시성 확보

사이버 보안 대응 방향

구축 → 운영 (운영 모델 전환)

- 기존: 내부 구축·인력 중심 운영
- 현재: 서비스 기반 자동화 중심 운영

예방 → 대응 (대응 방식 전환)

- 기존: 사고 발생 후 대응
- 현재: 24/7 지속 탐지·모니터링

시스템 → 행위 (통제 대상 전환)

- 기존: 시스템·네트워크 중심 보안
- 현재: 데이터·행위·이상 패턴 중심 통제

1) MXDR (Managed Extended Detection & Response): 외부 전문 조직이 기업의 보안 탐지·대응을 대신 운영해주는 관리형 보안 서비스

목차

사이버 위협에 대한 기존 방식의 한계 – 사이버 보안 강화에 따른 기업 부담의 확대

기존 사이버 위협 대응은 규제·인증의 준수 중심, 사후 대응, 내부 경계 방어에 머물러, 기업에게 운영 비효율, 리스크 확대, 비용 부담을 동시에 가중시키고 있습니다

기존 사이버 위협 대응 방식

정부·인증기관

사후 규제와 준수 점검 강화

- 규제·인증 중심 통제
  - 법·제도(사고 신고, 과징금, 공시)로 최소 기준 강제
  - ISMS-P, ISO 등 정책·절차 기반 인증 운영
- (사후 책임 부과 구조) 사고 발생 후 보고, 감사, 제재 중심
- (정기·정적 평가) 연 1회/주기적 심사, 문서·체계 중심 점검

기업

내부 경계 방어 중심 및 사후 대응

- **내부 자체 SOC[1] 및 보안 인력 직접 채용 운영**
  - SIEM, EDR, 방화벽 등 개별 솔루션을 도입해 자체 보안 스택 구성 운영, 모니터링, 대응까지 내부 조직이 전담
- 내부 네트워크를 신뢰 영역으로 간주하고, 외부와의 경계 보호에 집중
  - IP, 계정, 네트워크 기반의 정적 접근 통제 방식
- 사고 발생 후 탐지 → 분석 → 차단 → 복구의 사후 대응 프로세스 중심
- 서버, 네트워크, 엔드포인트 등 인프라 단위 보호에 집중

기존 사이버 대응 방식의 한계와 기업의 부담

운영

보안 효과 및 운영 한계에 직면

- **CISO[2] 부재 → 전략 없는 단편적 대응, 경영진과 단절 → 의사결정 지연 및 투자 후순위화**
- 투자 대비 실질 방어력 체감 낮음 (사고 반복 발생)
- 분절된 도구·수작업 대응 → 탐지 지연 및 피해 확산

리스크

비즈니스 및 규제 리스크 확대

- **신고·통제 미흡 시 과징금·제재·공시 리스크 즉시 현실화**
- 사고 발생 시 매출 손실·사업 연속성 훼손
- 보안 실패가 경영 리스크로 직접 전이

비용

운영과 비용 구조 비효율 증가

- **인력 부족과 높은 인건비 → 조직 운영의 비용 부담 증가**
- 규제 대응, 보안 운영 비용 이중 부담 구조
- 솔루션 스택 유지·통합 비용 누적 → ROI 압박

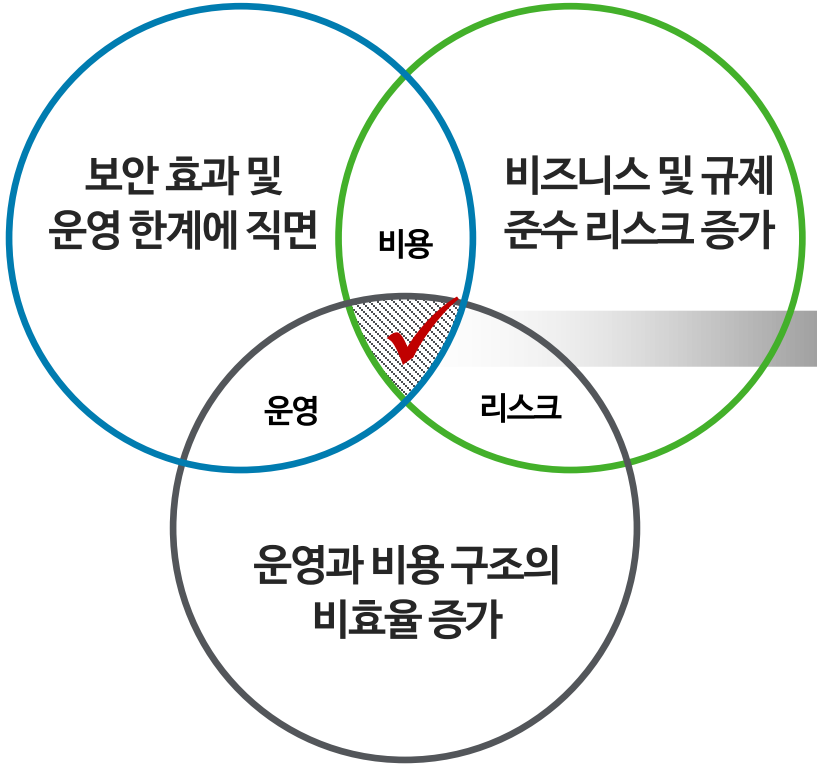
1) SOC (Security Operations Center) : 보안관제 센터 ; 2) * CISO (Chief Information Security Officer) → 최고정보보호책임자

사이버 위협에 대한 기존 방식의 한계 – 사이버 보안 리더십의 필요성 증가

기존 사이버 대응 방식의 한계와 기업의 부담을 해소하기 위해서는 사이버 보안 리더십이 필수적이며, 속도 격차를 해소하고, 사후 대응을 선제적 체계로 전환하며, 비효율적인 운영 모델을 개선하는 핵심 역할을 수행합니다.

사이버 보안 리더십의 필요성

기존 사이버 대응 방식의 한계와 기업의 부담의 해소의 핵심은 사이버 보안 리더십



- CISO 부재 → 보안 예산의 내부 설득 및 투자 집행 지연 → 실질적 방어 실행 미흡

사이버 보안 리더십

- 규제 준수 인증 통과에만 집중 → 보안 전략이 행정 업무로 전락

사이버 보안 리더십의 핵심 역할

속도·환경 불일치 문제 해소

- AI 기반 상시 탐지·자동 대응으로 탐지 – 분석 – 조치 시간 단축
- 클라우드·API·공급망 등 확장된 환경을 통합과 가시성 제고
- 플레이북·SOAR 기반 표준화로 지연 없는 일관된 대응 체계 확보

사후적 규제 준수 → 선제적 대응

- 사고 발생 후 보고 중심에서 이상 징후 사전 탐지·차단 체계로 전환
- 규제 요구사항을 운영 프로세스에 내재화하여 컴플라이언스를 상시 충족
- 리스크 기반 우선순위 관리로 사고 발생 이전에 통제·완화

운영 모델의 비효율 해소

- 인력 중심 관제에서 자동화·서비스 기반 운영으로 전환
- 분절된 보안 도구를 통합하여 중복·비효율 제거 및 운영 단순화
- 인력은 반복 작업이 아닌 전략·고난도 분석에 집중

사이버 위협에 대한 기존 방식의 한계 –사이버 보안 리더십 확보의 현실적 제약

사이버 보안 리더십 확보 시 CISO*는 필수 요건이 되고 있지만, 전문 인력의 공급 부족, 높은 비용 및 채용과 운영의 현실적인 제약으로 인해 대부분의 기업은 이를 상시 확보하기 어려운 상황에 직면해 있습니다.

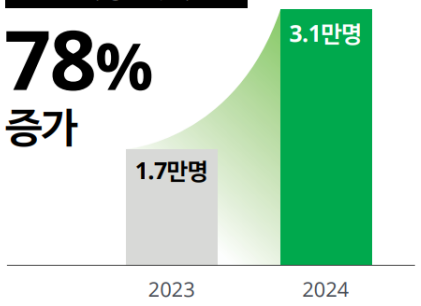
* CISO (Chief Information Security Officer)→ 최고 정보보호 책임자

사이버 보안 전문 인력의 공급 부족

- 필요 인력은 늘었지만 공급이 따라 오지 못하는 구조
  - –국내 보안 인력 약 3.1만 명 부족 (전년 대비 78% 증가)
  - –적합 인재 채용까지 평균 6개월 이상 소요

Talent Gap

보안 인력 공급 부족 GAP



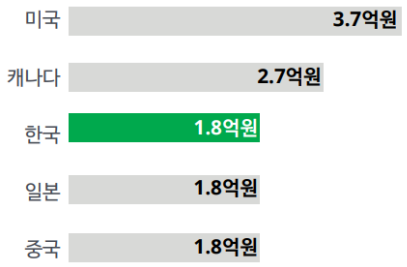
- 리더십 공백 발생
- 전략 없이 솔루션 중심 대응

비용 부담

- 풀타임 CISO 유지 자체가 재무적으로 부담
  - –국내 CISO 평균 연봉 약 1.8억 원
  - –글로벌(미국) 평균 약 3.7억 원 수준

Economic Barrier

글로벌 CISO 평균 연봉



- 투자 우선순위 왜곡
- → 보안이 비용 항목 으로 밀림

CISO 채용과 운영 현실
(채용공백 지속)

- 필요성은 인지하고 있지만 실제 도입은 지연
  - –국내 기업 CISO 임명률 18.1% 수준
  - – 약 30% 기업은 정보보호 투자 우선순위에서 제외

Execution Constraint

기업 규모별 CISO 임명 여부

규모 (근로자 수)	임명함 (%)	임명하지 않음 (%)
10~49명	18.4	81.6
50~249명	6.4	93.6
250명 이상	70.6	29.4

- 의사결정 지연 및 대응력 약화
- → 채용 기간 동안 보안 공백 지속

1) SOC (Security Operations Center): 보안관제 센터

목차

새로운 대안의 모색 – AI 기반 자율화와 vCISO로 완성하는 사이버 보안 리더십

AI 자율화 보안은 운영과 실행을 혁신하고, vCISO는 의사결정과 책임을 확립하여 AI가 실행하고, vCISO가 결정하는 사이버 보안 리더십을 완성합니다.

AI 기반 자율화 보안 센터 구축

기존 방식의 한계	해소 방향
속도 한계 (수동·사후 대응) 해소	AI·SOAR[1]로 탐지 – 분석 – 대응 자동화(분/초 단위)
운영 비효율 (인력 중심·도구 분절) 해소	통합 오케스트레이션으로 표준화·일관 운영
통제 범위 한계 (경계·시스템 중심) 극복	데이터·행위·클라우드·공급망 통합 가시성 확보

기대효과

- 실시간·선제적 리스크 관리 체계로 전환
- 대응 속도 향상과 운영 효율을 동시에 확보

AI 자율화 보안 → 실행(Execution) 혁신

사이버 보안 리더십 확보

vCISO → 의사결정·책임 (Decision & Accountability) 확립

vCISO (Virtual CISO 서비스)

기존 방식의 한계	해소 방향
인력 확보 한계(CISO 부족·고비용·채용 지연)	즉시 투입 가능한 리더십 확보
전략 부재(솔루션 중심 대응)	사업 연계 보안 전략·투자 우선순위 수립
책임·거버넌스 공백 (자문중심 대응)	전략 – 거버넌스 – 운영을 단일 리더십으로 통합

기대효과

- 인력·구축 중심 비용을 줄이고 운영 효율 개선
- 상시 관리 체계로 컴플라이언스 부담 완화

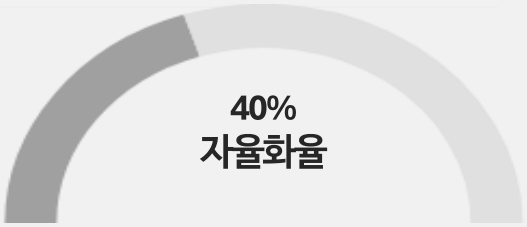
1) SOAR (Security Orchestration, Automation and Response)→보안 오케스트레이션·자동화·대응 플랫폼

AI 기반 자율화 보안 체계 구축

AI 자율화 보안은 AI 기반 이상 탐지, 자동 판단, 즉시 대응을 통해 실시간·선제적 위협 대응을 구현하며, 대응 속도 향상과 운영 효율을 동시에 확보하고 기업 리스크를 효과적으로 통제합니다.

단계적 실행 과제 : AI가 이상 탐지 → 자동 판단 → 즉시 대응

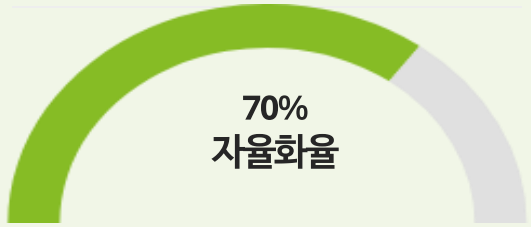
Phase I – 기반 구축
Human-Centric (사람 중심)



- 핵심 보안 솔루션 통합 구축
- 정책·플레이북 설계 및 운영 인력 투입
- 기본 탐지·알람 자동화
- AI 학습용 데이터 수집

인력 비중: 60% AI 비중: 40%

Phase II – 고도화
Semi-Autonomous (반자율)

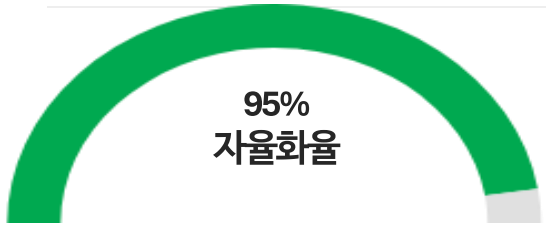


- AI 기반 이상행위 탐지 강화
- SOAR 플레이북 확대(30~50건)
- 자동 대응 시나리오 최적화
- 글로벌 환경으로 적용 확장

인력 비중: 30% AI 비중: 70%

GOAL

완전 자율 운영
Full Autonomy (완전 자율)



- AI 중심 위협 분석·판단 체계 구축
- Self-Learning & Self-Healing 구현
- 예측 기반 사전 차단
- 완전 자율 운영 체계 확

인력 비중: 5% AI 비중: 95%

주요 특성		핵심 성공 요건	
• 핵심 보안 솔루션 통합 구축	• 기본 탐지·알람 자동화	• 조직 역할 재정의 (인력 재배치)	• 보안·IT·데이터 조직 간 통합
• 정책·플레이북 설계 및 운영 인력 투입	• AI 학습용 데이터 수집	• 경영진 지원(리더십)	

AI 기반 자율화 보안 체계 구축 – 기대효과

AI 기반 자율화 보안은 탐지·분석·대응의 의사결정 주체를 사람에서 AI로 전환하고, 리스크 관리 방식을 실시간·자율형 체계로 구현함으로써 보안의 속도, 정확도, 통제 범위를 동시에 확장합니다.

전사적 통합 위험관리 실현 : Deloitte Cyber Managed Service (운영 및 체계 고도화)

보안 운영이 사람 중심 대응에서 시스템 기반 관리 체계로 전환

자동화 기반 구축

- 글로벌 자산·위협 통합 가시성 확보로 보안 사각지대 제거
- 데이터·자산 중심 관리 체계 전환으로 통제 일관성 확보
- SOAR 기반 운영 표준화로 대응 시간(MTTR) 단축 및 인력 의존도 감소
- 정량 KPI 기반 운영으로 보안 성과 측정 및 관리 가능
- 반복 업무 자동화로 운영 비용 절감 및 오류 최소화

보안이 사후 대응에서 선제적 탐지·분석 중심으로 진화

AI 기반 지능화 실현

- AI 기반 이상 탐지로 False Positive 감소 및 탐지 정확도 향상
- 위협 분석 자동화로 대응 의사결정 속도 및 품질 개선
- Zero Trust 확장으로 내부 프로세스에서 공급망까지 통제 범위 확대
- IT·Cloud·AI·OT 통합 가시성 확보로 전사 리스크 통합 관리
- 통합 대시보드 기반으로 실시간 리스크 인지 및 거버넌스 강화

보안이 대응 기능에서 자율적 리스크 통제 시스템으로 전환

완전 자율 보안 체계 확보

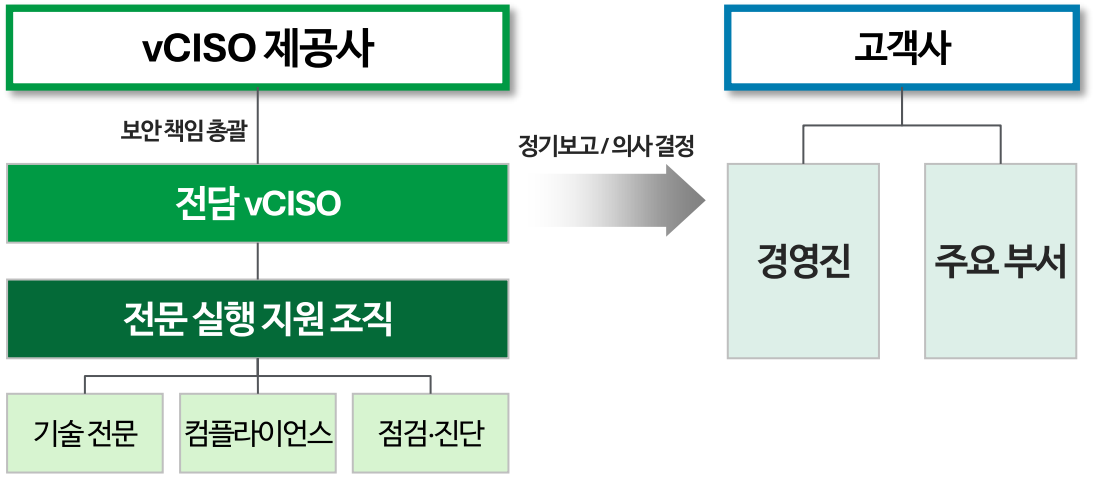
- AI가 위협을 실시간 탐지·판단·자동 차단 (Human-in-the-loop 최소화)
- 공격 패턴 학습 기반으로 선제적 리스크 예측 및 사전 대응
- 대응·운영 데이터 기반으로 자가 학습 및 지속적 최적화
- 보안 인력은 대응이 아닌 전략·정책·감독 중심으로 역할 전환
- 보안 사고 영향 최소화로 비즈니스 연속성 및 신뢰성 확보

vCISO (Virtual CISO 서비스) 도입

Virtual CISO는 외부 보안 리더를 통해 전략–실행–모니터링을 일관되게 지원하여, 기업이 규제·위협 대응 리더십을 신속히 확보하도록 하는 서비스 모델 입니다.

vCISO 수행 조직

일회성 자문이 아닌, vCISO와 전문 실행 조직이 함께 책임지는 서비스



vCISO 서비스의 정의

- **외부의 숙련된 보안 리더가 조직의 정보보호 책임자 역할을 서비스 형태로 수행하는 모델**
  - 상근 임직원이 아닌 외부 보안 리더십, 시간제·계약기반 프로젝트 단위 활용
  - 경영진 수준의 보안 전략 수립 및 의사결정 지원
  - 'Fractional CISO' 또는 'CISO-as-a-Service'

vCISO 서비스 프레임워크

전략 수립부터 실행, 모니터링까지 보안 리더십을 End-to-End로 제공

전략	거버넌스	운영 • 이행	모니터링 • 개선
보안 중장기 전략 • 로드맵 수립	정책 • 조직 • 의사 결정 체계 정립	보안 과제 실행 및 운영 관리	지속적 점검 및 개선
• 현 보안 수준 진단 • 중장기 목표 및 • 실행 과제 정의	• 정책·규정 수립 및 정비 • 경영진 보고 및 • 의사결정 체계 구축	• 보안 과제 관리(PMO) • 기술·관리적 통제 • 이행 지원	• 정기 점검 및 리스크 재평가 • 개선 과제 도출 및 반영

vCISO 도입 필요성

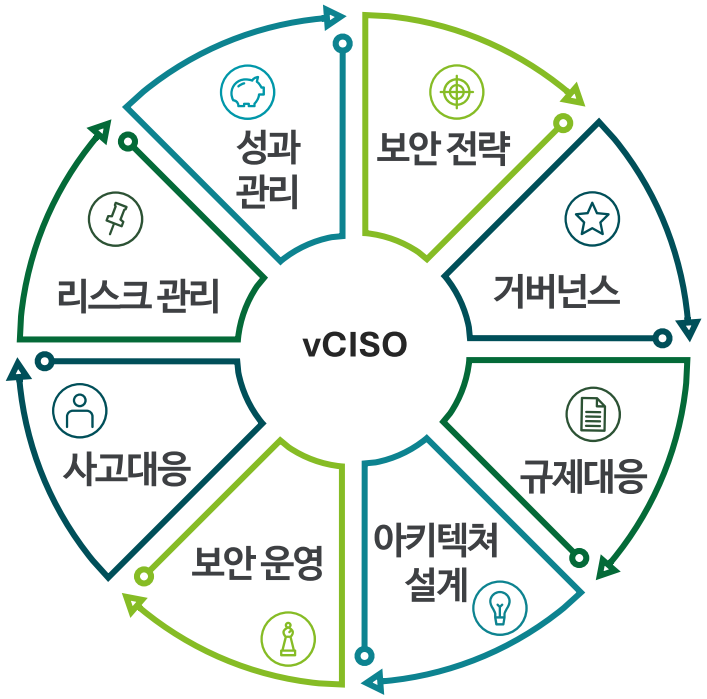
- **CISO의 역할과 책임은 유지하면서 확보 방식만 현실적으로 전환**
  - 책임 일원화: 전담 vCISO가 Single Point of Accountability로서 보안 의사결정·성과 책임 명확화
  - 비용·유연성 최적화: 상근 CISO 대비 비용 절감 + 계약기반 탄력적 활용
  - 운영 효율화: 전략–규제–사고 대응 End-to-End 수행, 내부 인력 핵심 업무 집중

vCISO (Virtual CISO 서비스) 도입 – 기대효과

vCISO 도입을 통해 기업은 비용 부담 없이 전문 보안 리더십을 확보하고, 객관적 진단 기반 전략 수립과 신속한 대응 체계를 구축함으로써 규제와 위협 변화에 선제적으로 대응할 수 있습니다.

vCISO 의 핵심 역할

vCISO는 전략·거버넌스·리스크·운영 전반을 통합 관리하며, 조직의 보안 책임과 실행을 총괄하는 서비스형 보안 리더십



vCISO (Virtual CISO 서비스) 도입 효과

- 책임·리더십 확보: 전담 vCISO 기반 의사결정 일원화 및 규제·위협 대응 역량 강화
- 비용·운영 최적화: 상근 대비 비용 절감, End-to-End 운영으로 효율성과 유연성 동시 확보

비용 효율적인 보안 리더십 확보

- 상근 CISO 채용 대비 고정 인건비 부담 최소화
- 조직 상황에 맞춘 서비스 범위 조정 가능

폭넓은 전문성과 객관적 시각 제공

- 다양한 산업과 환경에서 축적된 실무 기반 경험
- 내부 관성이나 이해관계에서 벗어난 객관적 진단

유연하고 신속한 보안 역량 강화

- 채용 절차 없이 즉시 투입 가능한 보안 리더십
- 규제, 감사, 사고 등 상황 변화에 따른 탄력적 대응

전략 중심의 정보보안 거버넌스 체계 수립

- 단기 대응이 아닌 중장기 보안 전략, 로드맵 수립
- 비즈니스 목표와 연계된 보안 의사결정 체계 정립

목차

딜로이트 사이버 보안 리더십 구축 전략

사이버 보안 리더십은 전략·거버넌스·운영·역량·기술을 단일 책임 체계로 통합하는 문제이며,
딜로이트는 vCISO와 AI 기반 자율 운영을 결합해 이를 실시간·리스크 중심 관리 체계로의 전환을 지원합니다.

사이버 보안 리더십 구축을 위한 5대 전략 질문 및 서비스 오퍼링

"무엇을 지킬 것인가"

- 비즈니스 전략과 연계된 Cyber North Star 정의 (Risk Appetite 포함)
- 자산·데이터 중심 Critical Asset 식별 및 보호 우선순위 설정
- 3~5년 보안 투자·로드맵 및 포트폴리오 전략 수립
- 규제 대응 중심 → Risk-based / Value-based 전략 전환

"누가 책임지는가"

- vCISO 기반 Single Point of Accountability(SPOA) 체계 구축
- 정책·표준·통제 프레임워크 표준화 및 일관성 확보
- Zero Trust 확장 (Human·Non-human·Third-party) 통제 모델 적용

"어떻게 대응하는가"

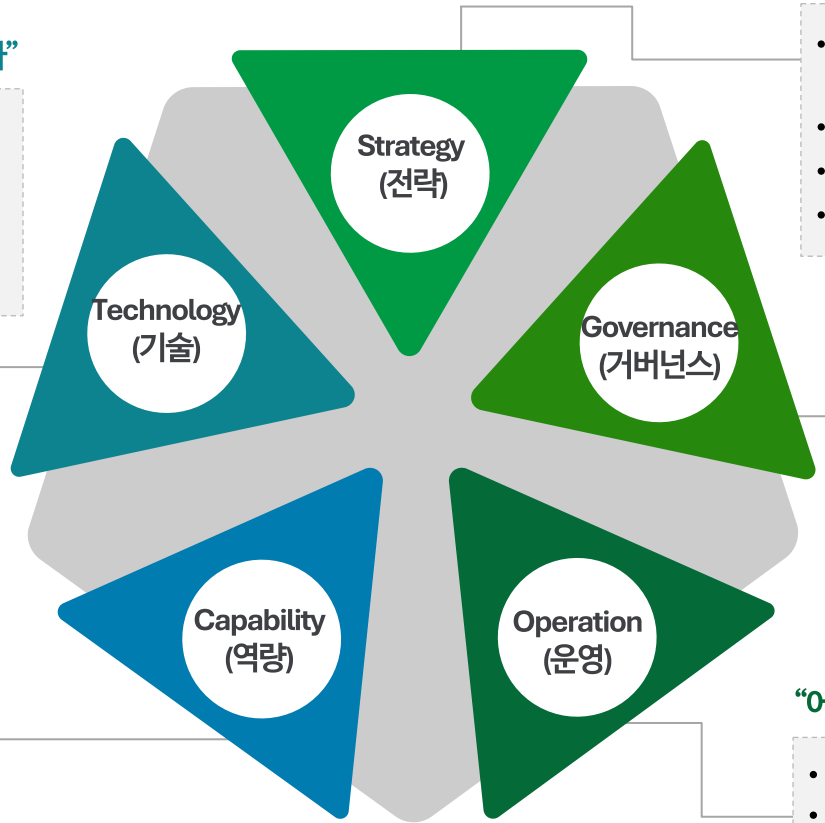
- SOC/MDR/XDR/SOAR 기반 통합 보안 운영 모델 구축
- 탐지–분석–대응 프로세스 표준화 및 자동화
- MTTR, 탐지율 등 KPI 기반 운영 성과 관리 체계 정립

"누가 실행하는가"

- 보안 조직을 전략–아키텍처–운영 3계층 구조로 재설계
- Cyber Talent Upskilling 및 전문 인력 확보 전략
- 부 인력 + vCISO + MDR 하이브리드 운영 모델 구축

"무엇으로 구현하는가"

- Legacy Tool 중심 → 플랫폼 기반 통합 보안 아키텍처 전환
- Data-centric / Identity-centric 보안 구조 강화
- AI 기반 이상 탐지 및 대응 → Autonomous Security 구현
- Cloud·AI·OT 포함 확장형 보안 아키텍처 설계



딜로이트 사이버 보안 리더십 구축 로드맵

사이버 보안 리더십은 Strategy–Governance–Operation–Capability–Technology의 5대 축을 통합해야만 실질적으로 작동하며, 이를 단계적으로 구현하기 위한 로드맵을 통해서만 실행 가능한 자율형 보안 체계로 전환될 수 있습니다.

사이버 보안 구축 로드맵 필요성

5대 전략 설계 없이 보안 리더십 구축 불가능

- Strategy 없이 Technology만 도입 → 투자 대비 효과 미흡
- Governance 없이 Operation 강화 → 책임 분산
- Capability 없이 AI 도입 → 실행 실패

사이버 리더십 구축 로드맵의 필요성

- 전략만 있으면 추상적 → 실행 지연
- 구축 가치만 있으면 이해관계자 설득 불가 → 예산 집행 지연
- 로드맵 마련시 실행 가능성과 현실성 확보 → 실행력과 빠른 예산 확보

AI 자율화와 vCISO 기반 사이버 보안 전환의 로드맵

Phase I	Phase II	Phase III
Foundation (0~6개월) 기반 구축	**Scale (6~18개월) 통합·고도화**	**Autonomous (18개월+) 자율화 완성**
• vCISO 투입 및 SPOA (단일 책임 체계) 확립	• AI 기반 이상 탐지 및 분석 기능 확대	• AI 주도 탐지 – 판단 – 대응 체계 구현
• 자산·위협 가시성 확보 (현황 진단 및 Gap 분석)	• Cloud·OT·공급망 포함 통합 보안 운영 체계 구축	• 보안 운영 자동화 (70~90%) 달성
• 보안 운영 표준화 및 초기 자동화 (SOAR Lite)	• Zero Trust 및 데이터 중심 통제 체계 정립	• 리스크 예측 기반 선제적 대응 체계 전환
• 핵심 리스크 영역 중심 Quick Win 실행	• KPI 기반 정량적 보안 성과 관리 체계 구축	• 보안 인력 → 전략·감독 중심 역할 재편

Endnotes

1) Global Cybersecurity Outlook 2026, World Economic Forum, January 2026.
2) 2025 Official Cybercrime Report, Steve Morgan, Cybersecurity Ventures, 2025. https://cybersecurityventures.com/official-cybercrime-report-2025/
3) 사이버범죄동향보고서
4) 한국인터넷진흥원(KISA), 통계청
5) Deloitte Global Future of Cyber Survey 2024, Deloitte
6) Global Cybersecurity Outlook 2025, World Economic Forum, January 2025.
7) Deloitte Cyber Threat Trends Report 2025, Deloitte, 2025.03, https://www.deloitte.com/us/en/services/consulting/articles/cybersecurity-report-2025.html
8) Virtual CISO 서비스, 한국 딜로이트 그룹 One Cyber & Resilience, 2026
9) Preparedness can flip the script on cybersecurity events, Deloitte Global, https://www.deloitte.com/global/en/Industries/tmt/case-studies/preparedness-can-flip-the-script-on-cybersecurity-events.html?utm_source=chatgpt.com
10) Taking flight as a more cyber-ready organization, Deloitte Global, https://www.deloitte.com/ce/en/services/consulting-risk/case-studies/taking-flight-more-cyber-ready-organization.html?utm_source=chatgpt.com
11) A recipe for greater cyber confidence, Deloitte Global, https://www.deloitte.com/an/en/services/risk-advisory/perspectives/recipe-for-greater-cyber-confidence.html

한국 딜로이트 그룹 전문가

사이버 보안 및 리스크

한국 딜로이트 그룹은 사이버 리스크 대응을 위한 정보보호 및 개인정보보호 자문, 정보보안 인증, 기술적 취약점 진단 및 대책 수립, 정보보호 전략 수립, Cyber Incident 대응 등의 서비스를 제공하고 있습니다. 또한, 수많은 유형의 사이버 리스크를 사전에 방지해 기업 운영의 든든한 조력자 역할을 수행합니다. 리스크 최소화를 통한 안정적인 기업 경영을 딜로이트가 함께 합니다.

백철호 Partner
One Cyber & Resilience 리더

02 6676 2250
cbaek@deloitte.com

서영수 Partner
One Cyber & Resilience

02 6676 1929
youngseo@deloitte.com

이창성 Partner
One Cyber & Resilience

02 6099 4888
changsulee@deloitte.com

Deloitte.

딜로이트 인사이트 카카오 채널 & 앱

전 세계 경제·산업·경영 트렌드와 인사이트를

실시간으로 확인하세요!

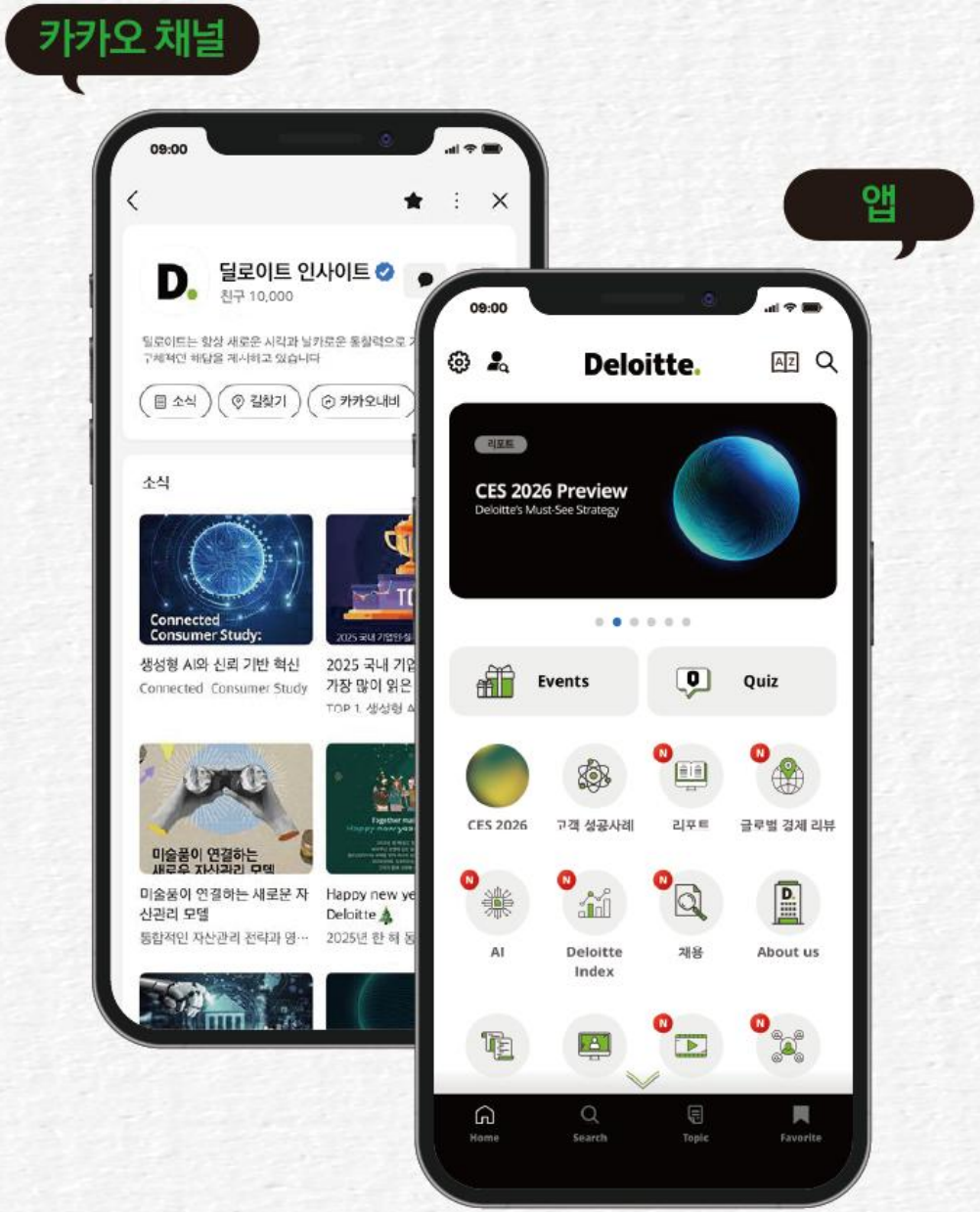
- AI 시대의 전략과 리스크, 산업별 핵심 이슈를 다룬 **분석 리포트**
- 소비심리지수·자동차 구매의향 등 실물경제의 향방을 보여주는 **Deloitte Index**
- 딜로이트 전문가의 인사이트와 글로벌 행사의 현장을 담은 **영상 콘텐츠**
- 글로벌 프로젝트에서 검증된 실행 인사이트를 담은 **고객 성공 사례**

카카오채널

앱

Download on the App Store

GET IT ON Google Play



앱스토어, 구글플레이/카카오톡에서 '딜로이트 인사이트' 를 검색해보세요.
더욱 다양한 소식을 만나보실 수 있습니다.

Deloitte. Insights

성장전략부문 대표	딜로이트 인사이트 편집장	연구원	Contact us
손재호 Partner	박경은 Director	배순한 Director	krinsightsend@deloitte.com
jaehoson@deloitte.com	kyungepark@deloitte.com	soobae@deloitte.com	