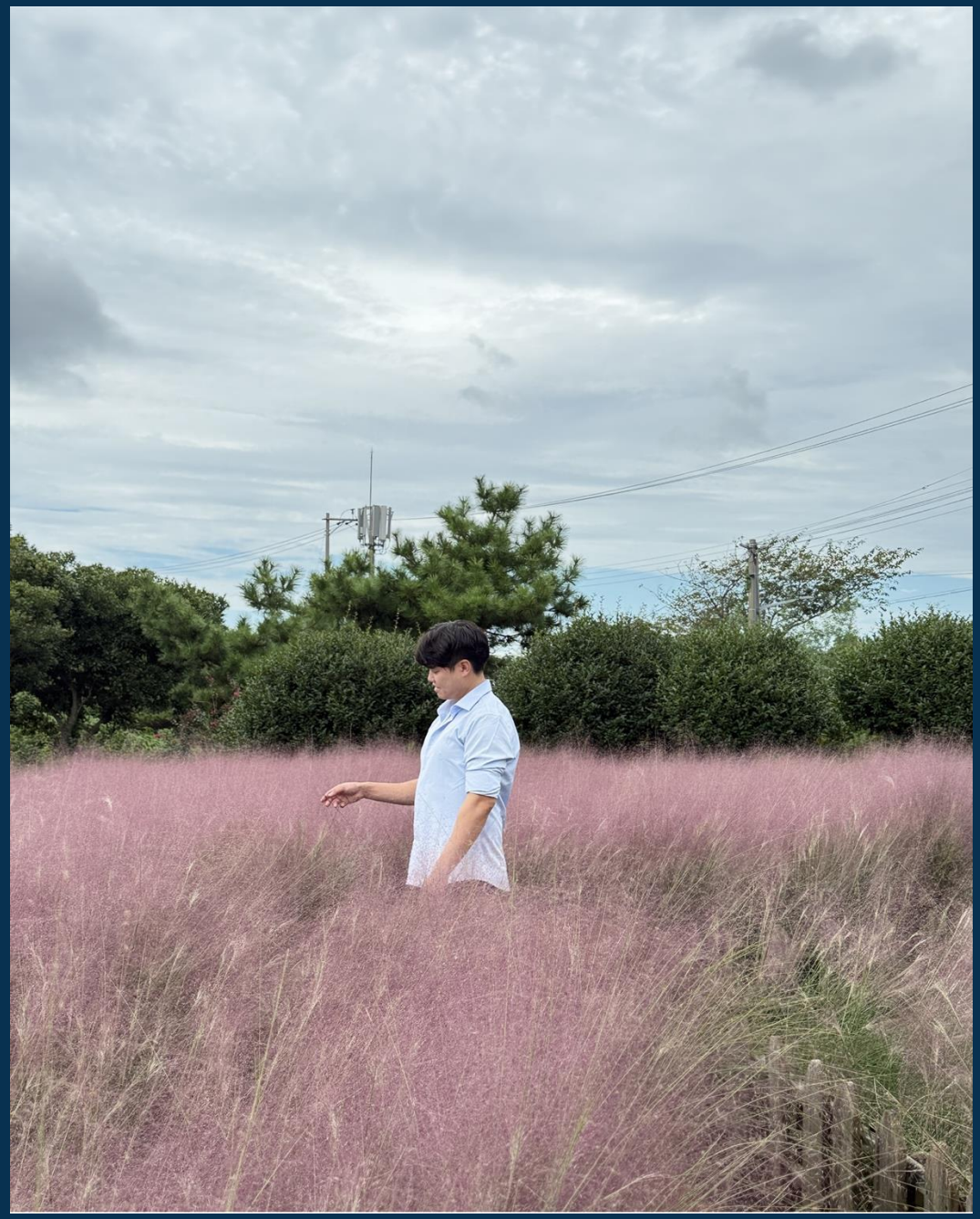
사이버 위협 대응을 위한 Incident Response와 다크웹 활용 전략

효과적인 IR 프로세스와 다크웹 인텔리전스 실무 적용 방안

컴투스플랫폼 | 이진욱

2025. 9. 30



이진욱 | 컴투스플랫폼 기술보안 담당자

안녕하세요.

컴투스플랫폼에서 기술보안(Technical Security) 업무를 담당하고 있는 이진욱입니다.

저는 게임 서비스 및 플랫폼 환경에서 발생할 수 있는 보안 위협 탐지 및 침해사고 대응 체계 구축을 주요 업무로 수행하고 있으며,특히 다크웹 기반의 위협 인텔리전스 수집 및 분석, 취약점 관리, 보안 정책 수립, 사고 대응 프로세스 고도화 등 다양한 영역에서 실무 경험을 쌓아오고 있습니다.

최근에는 빠르게 변화하는 사이버 위협 환경 속에서,
조직이 보다 선제적으로 공격을 탐지하고 대응할 수 있는 체계적인 IR(Incident Response) 프로세스와다크웹 인텔리전스 활용 방안을 중심으로 연구 및 적용을 진행하고 있습니다.

이번 세미나에서는 실제 현장에서 경험한 침해사고 대응 과정과
다크웹 위협 인텔리전스의 실질적 활용 사례를 바탕으로,
보안 담당자들이 직면하는 현실적인 문제와 이를 해결하기 위한 대응 전략을 공유드리고자 합니다.
오늘 발표가 여러분의 보안 대응 체계 강화에 작은 인사이트가 되길 바라며,
함께 발전적인 논의를 이어갈 수 있기를 기대합니다.

감사합니다.

목차 CONTENTS

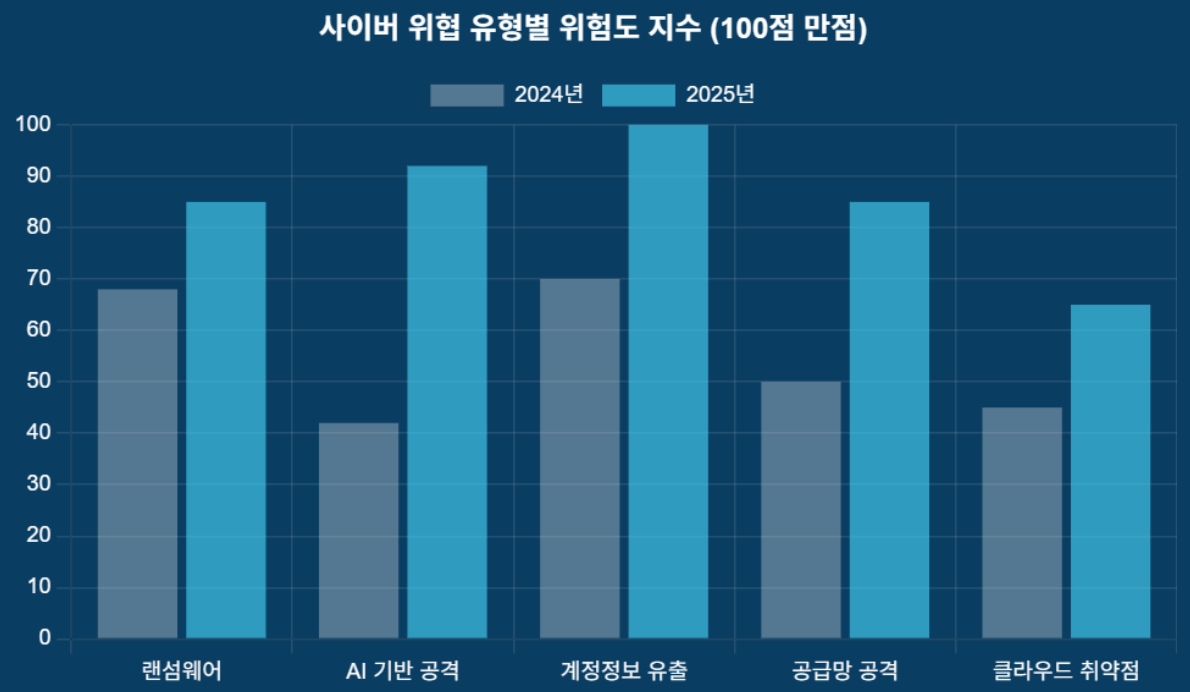
사이버 위협 동향과 과제 (2025)

진화하는 사이버 공격과 효과적인 대응을 위한 과제

- AI 기반 고도화된 공격 증가: 2025년 1분기 AI 활용 피싱·랜섬웨어 122% 증가, 자동화된 취약점 탐색 확산
- 계정 정보 유출 대규모화: 다크웹에 유출된 개인정보·계정정보 1000억 건 돌파 (전년대비 42% 급증)
- 랜섬웨어 전략 변화: 데이터 암호화에서 탈취 ·유출 협박으로 전환, 중소기업 타깃 증가
- 공급망 공격 고도화 : 보안 취약 제 3자 업체 통한 대규모 침투 시도 70% 증가

2025 주요 과제

- 신속한 탐지 · 대응 체계 구축
- 실시간 위협 인텔리전스 확보 · 활용
- 전사적 보안 리더십 강화



자료 출처: 포티넷 글로벌 위협 환경 보고서 2025

Incident Reponse(IR)
개요 및 최신 프로세스

침해사고 대응을 위한 체계적인 6단계 프로세스

인시던트 대응(IR) 이란
사이버 보안 침해사고를 식별, 분석, 억제, 제거 및 복구하기 위한 조직화된
접근 방식으로 사고 발생 시 신속하고 효과적으로 대응하여 비즈니스 영향을
최소화 하는것을 목표로 함.

- NIST 기반 IR 프레임워크를 국내 환경에 맞게 최적화 하여 체계적 대응 가능
- 효과적인 IR 운영을 위한 핵심요소: 명확한 프로세스 정의, 역할과 책임 분배, 의사소통 체계 수립, 정기적 훈련과 개선
- IR팀 구성: CISO, 보안 분석가, IT 담당자 등 다양한 전문가 참여 필요

IR 준비 상태 체크리스트

- 사고대응 플레이북 및 문서화
- 명확한 에스컬레이션 경로
- 정기적인 시뮬레이션 훈련
- 임원진 참여 및 지원

자료 출처: NIST IR 자동화 프레임워크 및 Gartner 2025 보안 자동화 리포트

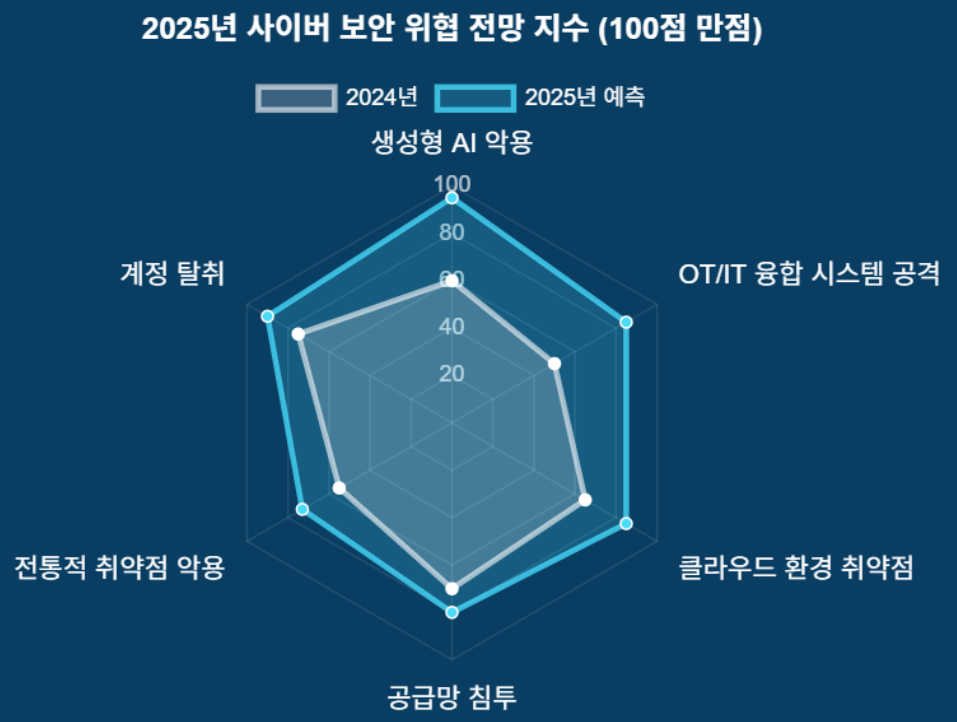
2025년 보안이슈 및 위협 트랜드 심층 분석

진화하는 AI 위협과 융합 환경에서의 새로운 방어 전략

- 생성형 AI오용 위협 급증: AI 기반 피싱 공격 152%증가, 딥페이크를 활용한 CEO 사칭 공격 3배 증가(2024년 대비)
- AI 방어에 집중한 틈을 노린 전통적 위협: 생성형 AI에 대한 과도한 집중으로 기본 보안 통제 미흡, 기존 취약점 악용 공격 32% 증가
- 클라우드 환경 확장에 따른 취약점: 멀티/하이브리드 클라우드 환경 내 자격증명 관리 실패로 인한 침해사고 44% 증가
- OT/IT 융합 환경 공격: 스마트 팩토리, 중요 인프라 등 OT와 IT 융합 시스템 공격 70% 증가, 랜섬웨어 그룹의 주요 타깃화

방어 전략 전환 필요성

- AI 위협 인텔리전스 + 기본 보안 강화
- 융합 환경(IT+OT) 통합 보안 체계 구축



자료 출처: 2025 사이버 보안 위협 전망 보고서 (KISA, Gartner, S-RM)

실무 중심 IR 체계와 커뮤니케이션 전략

효과적인 침해사고 대응을 위한 조직 구성과 의사소통 프로세스

- 전략 CSIRT 구성: CISO 리드, IT·보안 ·인프라 등 전문가로 구성된 다기능팀 (지휘체계 명확화)
- 역할 명확화: 최초 대응, 분석 ·조사, 상황 보고, 외부 소통 등 담당자 사전 지정
- 핫라인 구축: 24시간 비상연락망 및 에스컬레이션 프로세스 수립
- 의사결정 권한: 시스템 격리, 서비스 중단 등 결정권자 사전 지정

효과적 커뮤니케이션 원칙

- 단일 정보 창구 유지
- 사전 준비된 템플릿 활용
- 시간별 상황 업데이트 정례화
- 객관적 사실 기반 투명한 소통

침해사고 커뮤니케이션 흐름

01 탐지·인지 > 02 초기보고 > 03 분석·조사 > 04 대응 ·통제 > 05 최종보고

다크웹 기반 위협 인텔리전스란?

사이버 공격 대응을 위한 위협 정보 수집과 분석 체계

- 개념 정의: 다크웹/딥웹을 포함한 다양한 소스에서 위협 관련 정보를 수집·분석하여 실행 가능한 인사이트로 가공하는 프로세스
- 특정과 가치: 잠재적 위협 행위자의 TTP(전술·기법·절차) 사전 파악 가능, 위협 탐지와 대응 능력 향상
- 다크웹 인텔리전스: 일반 검색엔진으로 접근 불가능한 다크웹·딥웹에서 유출 계정정보, 취약점 판매, 공격 준비 징후 등 사전 탐지

다크웹 모니터링 주요 대상

- 유출 계정 ·개인정보 판매글
- 해킹 도구 · 제로데이 취약점 거래
- 위협 행위자 커뮤니케이션팀
- 기업 · 기관 타깃 공격 논의

01. 전략적 인텔리전스 : 장기적 계획/의사결정 지원

02. 전술적 인텔리전스 : 위협 행위자의 TTP 분석

03. 운영적 인텔리전스 : 현재 진행/임박한 위협 탐지

04. 기술적 인텔리전스 : IoC(침해지표) 기반 탐지/대응

위협 인텔리전스 효과: 공격 예방 65% 향상, 탐지 시간 47% 단축 (Recorded Future 2025)

다크웹 모니터링·계정 유출 실제 사례

2024-2025년 주요 유출 사례 분석과 실질적 대응 방안

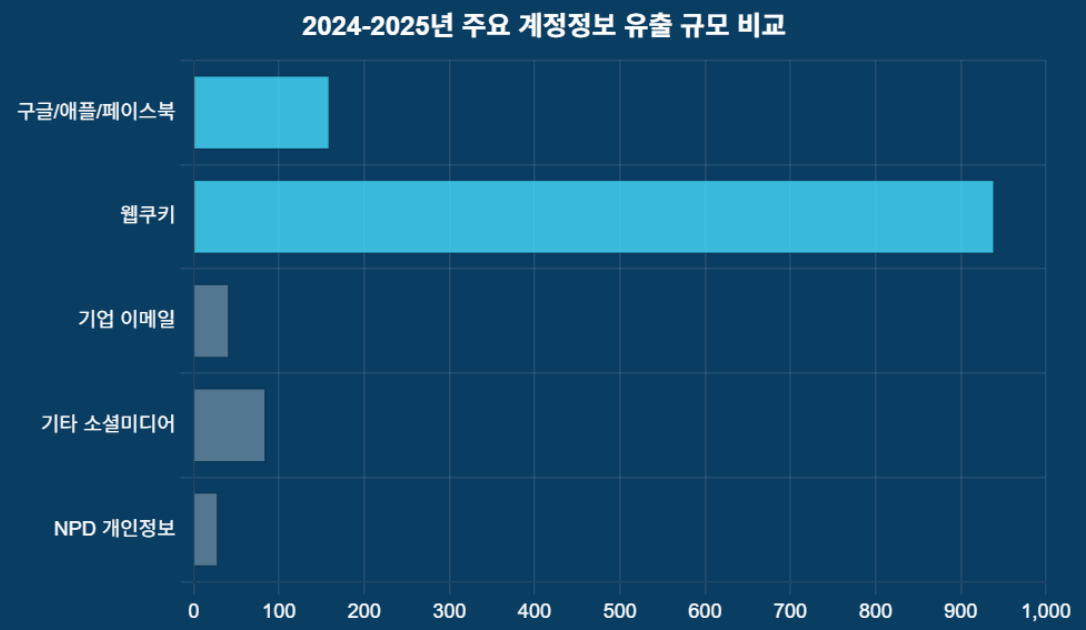
구글·애플 ·페이스북 계정정보 160억건 유출
2025년 6월, 30개 대형 데이터셋에서 발견된 대규모 유출.
사용자 ID, 이메일 등 개인정보 포함

웹 쿠키 정보 940억개 유출
전 세계적으로 약 940억개 웹 쿠키가 다크웹에 노출,
한국에서만 5.7억개 확인. 개인 인증정보 및 세션 탈취에 활용 가능

- 주요 공격 벡터: 인포스틸러 멀웨어를 통한 브라우저 저장 정보 대량 탈취
- 공격 목적: 크리덴션 스터핑을 통한 계정 탈취, 기업 내부 시스템 침투, 개인정보 유출 및 금융 피해
- 다크웹 판매가: 대량 계정 묶음 10만 ~350만 달러에 거래 중

조기 감지 및 대응 전략

- 조직에 맞는IR플레이북 작성 및 주기적인 업데이트
- CSIRT 구성원 간 명확한 역할 정의와 원활한 소통 체계 확립
- AI 기반 자동화 도구 적극 활용(효율성 증대)



자료 출처: 제로다크웹 분석 보고서 2025, 노드VPN 연구보고서

랜섬웨어 침입 사례와 IR 적용 전략

2025년 급증하는 랜섬웨어 동향과 효과적인 IR 대응 방안

- 2025년 급증 추세: 1분기 전 세계 랜섬웨어 피해 2,575건(전년 동기 대비 122% 증가), 중소기업 표적 확대
- 공격 패턴 변화: 데이터 암호화 → 탈취 및 유출 협박 →디도스 공격 병행 (다중 협박 전략)
- 주요 침입 벡터: 이메일 피싱(41%), VPN/RDP 취약점(32%), 제 3자 공급망(18%)

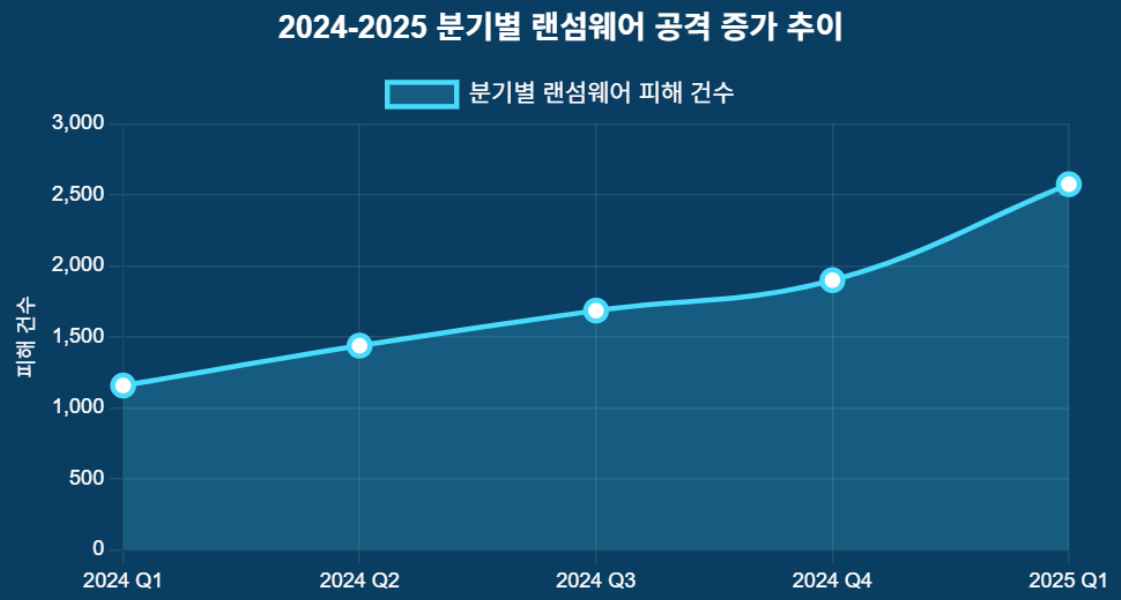
랜섬웨어 IR 실무 적용 전략

초기 탐지 & 격리
의심 시스템 즉시 네트워크
분리, 공유폴더 접근 차단

로그 보존 & 조사
시스템 종료 지양,
로그/IoC 확보, 감염 경로 추적

회복 & 재발방지
클린 백업 복구, 취약점 패치, 교육 강화

공격자 협상 (최후 수단)
법률 자문, 협상 대리인 활용, 증거 보존



자료 출처: S2W 위협 인텔리전스 센터, 2025 상반기

조직 보안체계 강화 및 사전예방 전략

표준 프레임워크와 제로트러스트 기반 통합 보안 체계 구현

- NIST CSF 2.0 기반 보안 체계 수립: 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover), 거버넌스(Govern) 6대 핵심
  기능 구현
- 제로트러스트 아키텍쳐 도입: 모든 접근 시도를 잠재적 위협으로 간주,
  접근 통제 최소화 및 지속적 검증 체계 구현
- 취약점 관리 체계 고도화: 위험기반 우선순위 관리로 실질적 위협 완화에 집중, 자동화된 지속적 취약점 모니터링

통합 모니터링 핵심 요소

- 실시간 위협 인텔리전스 기반 대응
- 클라우드 – 온프레미스 통합 가시성
- 자산 인벤토리 실시간 관리

거버넌스
전략·정책 수립
과 리더십

식별
자산·위험·취약
점
파악

보호
접근통제·교육·
데이터보안

복구
정상화 및 복원
력 강화

대응
침해사고
분석 및 대응

탐지
이상징후
모니터링

제로트러스트 아키텍처

사용자
다중인증(MFA)
및 권한 최소화

디바이스
상태 모니터링
및 검증

네트워크
마이크로
세그멘테이션

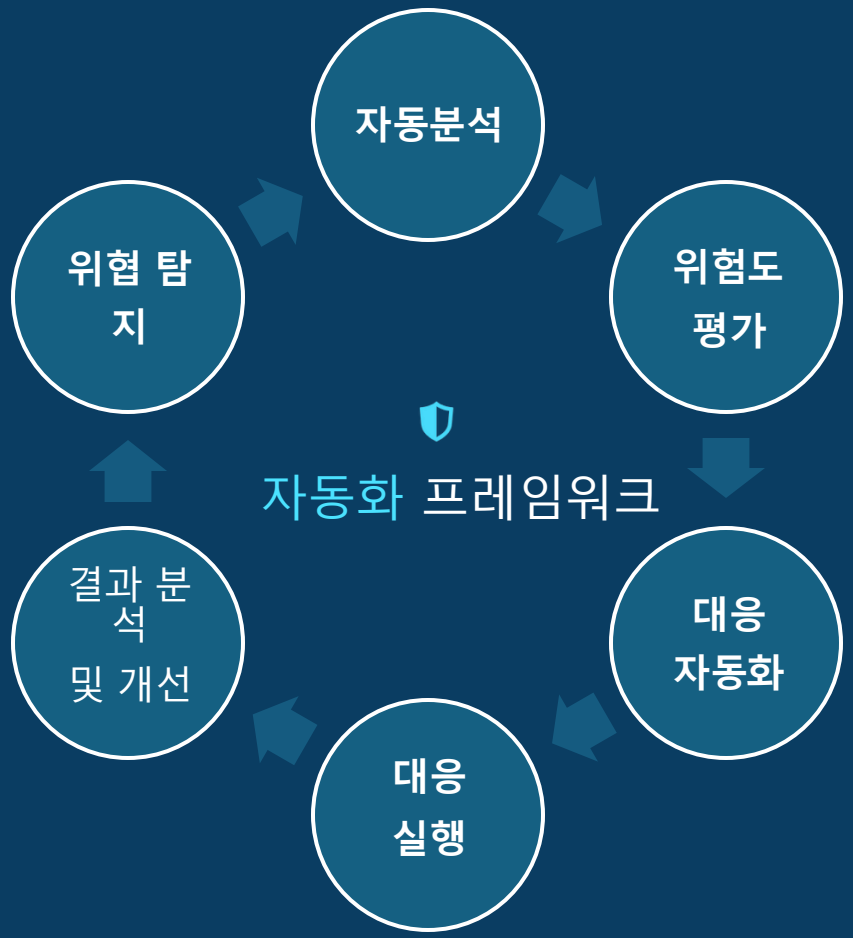
IR 자동화와 AI·신기술 활용

위협 헌팅부터 대응까지 자동화된 프로세스 구축으로 인시던트 대응 효율화

- AI 기반 위협 탐지 : 머신러닝 기반 이상 행위 탐지로 95% 이상의 위협을 24시간 이내에 식별, 오탐율 70% 감소 효과
- 자동 트리아지 및 분류: 위협 유형과 위험도에 따라 자동 분류, 우선순위 지정으로 대응 시간 60% 단축
- SOAR 솔루션 활용: Security Orchestration, Automation and Response 도구로 반복 작업 자동화, 대응 일관성 확보
- 자동화된 포렌식 데이터 수집: 관련 로그·아티팩트 자동 수집으로 분석 시간 단축, 초기 대응 신속화

AI·자동화 도입 성공 요소

- 자동화 니즈에 대한 자동화 업무 정의 및 프로세스 수립
- 자동화 시나리오의 지속적 업데이트 및 검증
- A조직 환경에 맞는 커스터마이징



자료 출처: NIST IR 자동화 프레임워크 및 Gartner 2025 보안 자동화 리포트

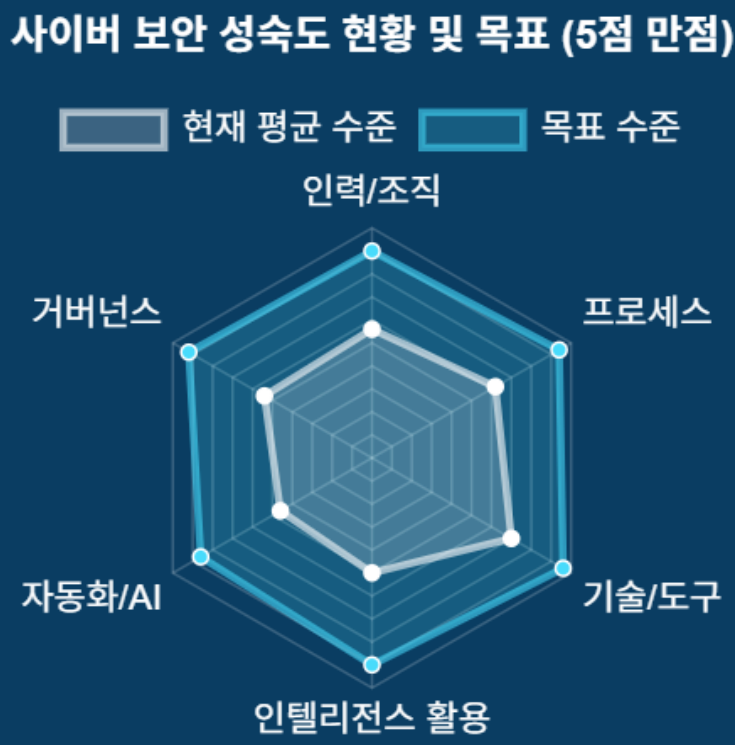
종합 결론 및 실무 적용 가이드

보안 문화 내재화와 지속적인 개선을 위한 조언

- 통합적 보안 관점 수립: 사이버 위협 대응은 기술적 문제를 넘어 경영 리스크 관점에서 접근 필요. 경영진의 적극적 참여와 리더십이 성공적인IR의 "핵심"
- 선순환 구조 확립: 다크웹 모니터링 → 위협 정보 확보 → 신속한 IR 적용 → 조직 학습 → 보안 강화로 이어지는 선순환 구조 확립
- 사전 준비와 훈련: 사고 발생 이후가 아닌, 발생 전부터 IR 프로세스와 담당자를 명확히 정의하고 정기적인 모의훈련 실시 필요
- OT/IT 융합 환경 공격: 전략·전술 ·운영 ·기술 영역에서 다크웹 기반 인텔리전스를 적재적소에 활용하여 선제적 방어 체계 구축

실무자를 위한 3가지 핵심 "팁"

- 다크웹 전문 모니터링 도구 활용
- 주기적 계정정보 유출 확인 및 시스템 구축
- 다중인증(MFA) 의무화 및 패스워드 정책 강화



Q&A