보안담당자 대응 방안

(1) 예방 조치

- **접근통제 및 계정 관리**
  - 개발자 단말과 서버 계정에 대해 **다중인증(MFA)PAM(Privileged Access Management)**적용.
  - 권한 최소화, 인증키/비밀번호 정기적 교체.

네트워크 및 시스템 보안

- 방화벽(FW), 침입방지시스템(IPS), 위협관리시스템(TMS)을 통해 외부 침투 차단 및 탐지.
- NAC 도입으로 단말 무결성 검증 및 비인가 장비 접속 차단.

데이터 보안

- 내부자료 암호화(DRM, DB 암호화), 파일 전송 시 DLP(Data Loss Prevention) 솔루션 도입.
- 중요 자료는 망분리 환경에서만 접근 가능하도록 정책 강화.

애플리케이션/코드 보안

- 정적/동적 분석(SAST/DAST) 및 오픈소스 취약점 점검 툴 활용.
- 소스코드 저장소 접근 로그 모니터링 및 무결성 검증 체계 마련.

(2) 탐지 및 모니터링

- **통합로그·SIEM/XDR**
  - 서버·클라이언트·네트워크 전 구간 로그를 수집·분석, 이상행위 탐지.
  - 내부자 이상 행위(User Behavior Analytics, UBA) 기반 탐지 강화.

위변조/침입 탐지

- 홈페이지 위변조 감시 시스템, 무선 침입 차단(WIPS) 적용.
- 실시간 공격 및 악성코드 탐지 체계 운영.

(3) 대응

- **사고 대응 프로세스 가동**
  - 침해 사실 인지 즉시 **시스템 격리 → 로그 분석 → 증거 보존**수행.
  - 유출 자료 범위 파악 및 고객·규제기관 통보 체계 마련.
  - 공격자 금전 요구에 대한 법률/경영진 협의 및 공식 입장 수립.

포렌식 및 원인분석

- 개발자 단말 및 서버 포렌식 조사로 침투 경로 확인.
- 취약점 패치 및 동일 경로 재발 방지 조치.

(4) 회복 및 사후 조치

- **백업/복구 체계**
  - 중요 시스템/코드 저장소의 오프라인 백업 검증.
  - 주기적 복구 훈련으로 랜섬웨어 상황 대비.

정책·교육 강화

- 보안 정책 재정립: 자료 접근/반출 프로세스, 문서 취급 절차.
- 전 직원 대상 피싱·랜섬웨어 대응 교육.
- 정기 침투테스트 및 보안 훈련(Tabletop Exercise) 실시.