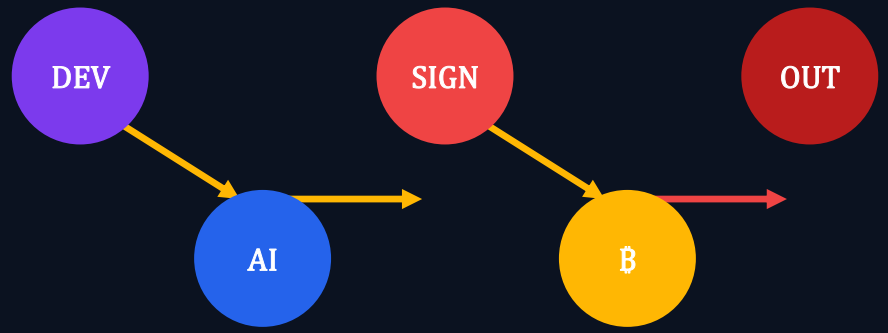
CUSTOMER SECURITY BRIEF

최근 금융·가상자산 해킹 사고 분석

바이낸스 · 롯데카드 · SGI서울보증

공격 루트 | 원인 | 시사점 | 해결 방안



핵심 관찰

"침입점"보다 더 중요한 것은
신뢰 경로 전체의 제어와 회복력이다

기준일 2026.11.05 | 공개자료 기반

분석 범위는 공개 확인 자료와 2차 기술 분석을 구분하여 표시

EXECUTIVE SUMMARY

세 사고는 서로 달랐지만, 실패한 통제는 놀랍도록 유사했다

임원 관점의 결론: "접점·권한·행위·복구" 네 축을 동시에 강화해야 한다

01 신뢰 경로 탈취

바이낸스: 개발자 단말 → 내부 AI 도구 → 배포 토큰 → 지갑 서명 서비스

02 기본 보안 부채

롯데카드: 장기 미패치·암호화 미이행·백신 미설치가 대규모 유출로 연결

03 엣지·복구 취약

SGI: 외부 노출 VPN/SSH 인증 통제 미흡 → 내부 확산 → 랜섬웨어

권고: 단기 "구멍 메우기"와 중기 "신뢰 구조 재설계"를 병행

0–30일

외부 접점·관리 포트·미패치 자산 전수 차단

MFA·계정 잠금·응급 패치·IOC/로그 보존

31–90일

PAM/JIT·서버 EDR·Egress DLP·불변 백업

권한과 데이터 이동을 상시 검증

91–180일

서명/승인 분리·개발망 제로트러스트·DR 훈련

신뢰 경로를 구조적으로 재설계

Sources: Binance [1][2], 금융위원회 [7][8], 보안뉴스 [11][12]

SCOPE & EVIDENCE

분석 범위와 신뢰도

"미국 바이낸스"는 미국 FBI가 귀속을 발표한 Binance.com 글로벌 사고로 해석했으며, Binance.US 별도 사고로 단정하지 않았다.

확정/공식 — HIGH

기업·감독당국·수사기관의 공식 발표
활용: 사고 규모·조치·제재

보도/조사 중 — MEDIUM

복수 언론 또는 관계자 취재 기반
활용: 초기 침투·세부 타임라인

기술 분석 — ANALYTIC

공개 IOC·아키텍처·취약점 기반 분석
활용: 통제 실패·개선 설계

대상 사고

BINANCE.COM — 2026.10.29

약 $6.34B 영향

공식 초기보고 + FBI 귀속

롯데카드 — 2025.08

297만 명 / 200GB

금융위 검사·제재 + 기술 분석

SGI서울보증 — 2025.07.14

약 81시간 장애

보도 기반 침투 경로 + 복구

주의: 공개조사가 진행 중인 세부 공격기법은 "추정/분석"으로 명시했으며, 고객사 적용 전 내부 로그·자산 현황으로 재검증해야 한다.

INCIDENT PORTFOLIO

세 사건의 "피해 방식"은 달랐다

금전 탈취 · 개인정보 유출 · 서비스 마비 — 그러나 모두 정상 신뢰 채널을 악용했다.

2026.10

BINANCE

자산 탈취

$6.34B

10개 체인 · 서명 서비스 악용

사업 영향 ●●●●●

2025.08

롯데카드

정보 유출

297만 명

최대 200GB · 온라인 결제 서버

사업 영향 ●●●●●

2025.07

SGI서울보증

가용성 마비

약 81h

보증업무 중단 · 랜섬웨어

사업 영향 ●●●●○

공통분모 정상처럼 보이는 경로 → 권한 확대 → 늦은 탐지 → 큰 피해

Sources: [1] Binance, [7] 금융위원회, [9] 연합뉴스, [11][12] 보안뉴스

CASE 1 — BINANCE.COM

2026년 바이낸스: 개발자 단말 침해가 지갑 서명으로 이어졌다

FBI는 북한 TraderTraitor의 소행으로 공식 귀속. Binance.US가 아닌 Binance.com 글로벌 플랫폼 사고.

$6.34B	$2.85B	5	98%
영향받은 디지털 자산 (초기보고 기준)	동결·차단된 자산 (2026.11.03 기준)	초기 XRP 유출에 사용된 핫월렛 수	영향 토큰 자산 보충 (2026.10.31 기준)

사건 요약

침입

공식

가짜 채용 인터뷰에서 악성 코드 저장소를 업무용 단말에 내려받게 함

권한 확대

공식

내부 AI 도구를 발판으로 배포 토큰과 다른 엔지니어 단말을 장악

탈취

공식

내부 지갑 서명 서비스를 악용해 정상 출금 절차 밖에서 다중 체인 거래 생성

핵심: 개인키 유출 증거가 없어도 "서명 권한·승인 경로"가 탈취되면 자산은 이동할 수 있다.

Sources: [1] Binance Initial Findings (2026-11-03), [2] FBI (2026-10-31)

CASE 1 — ATTACK ROUTE

바이낸스 공격 루트: 사람 → 단말 → AI → 배포 → 서명

정상 개발·운영 도구가 연결된 신뢰 사슬 전체가 공격 표면이 되었다.

1 가짜 채용
실제 플랫폼·화상면접으로 신뢰 형성

→

2 악성 과제
코드 저장소 설치 중 개발도구를 악성 버전으로 교체

→

3 단말 장악
0-day 악성코드·난독화로 C2 연결 및 흔적 은폐

→

4 AI 발판
내부 AI 도구를 통해 동료 엔지니어로 횡적 이동

→

5 배포 토큰
단말에 있던 컨테이너 배포 권한 토큰 탈취

→

6 서명 악용
서비스 컨테이너 배포 후 비인가 거래 서명·전송

ON-CHAIN IMPACT

1 다중 체인 유출
XRP · SOL · OP · BTC 등

→

2 EIP-7702 악용
핫월렛 실행권한을 악성 컨트랙트에 위임

→

3 출금중지 한계
온체인 권한은 일반 출금 인프라와 독립 동작

→

4 권한 해제
특수 절차로 위임 코드를 zero address로 제거

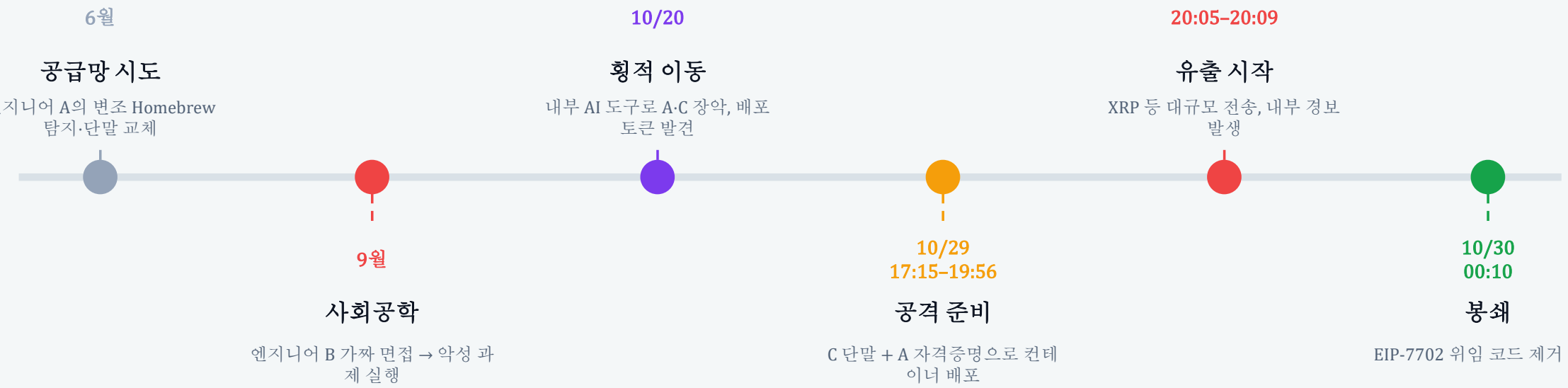
방어 포인트: 단말 보호만으로 부족 — 토큰 수명·워크로드 신원·서명 정책·온체인 권한을 각각 독립 검증

Source: [1] Binance Initial Findings and Response Update

CASE 1 — TIMELINE

장기간 준비 · 수분 내 탈취 · 수시간의 복잡한 봉쇄

"탐지 속도"뿐 아니라 "권한 해제 가능성"을 사전에 설계해야 한다.



의미 초기 이상징후는 있었지만, 역할 노출과 신뢰 관계 재구성까지 차단하지 못했다. 침해된 권한의 "잔존 효과"까지 제거하는 플레이북이 필요하다.

Source: [1] Binance (timeline and initial findings)

CASE 1 — ROOT CAUSES

바이낸스 원인: 단일 취약점이 아니라 5개 통제층의 연쇄 실패

각 층을 독립적으로 차단해야 "한 번의 실수"가 자산 이동으로 번지지 않는다.

L1	사람	정교한 가짜 채용·면접	피싱 저항형 교육·고위험 직군 모의훈련
L2	단말	개발도구 치환형 0-day 미탐지	격리 개발환경·허용목록·EDR 행위 탐지
L3	신원	단말 내 배포 토큰·동료 자격증명 악용	단기 토큰·워크로드 신원·PAM/JIT
L4	내부 AI	AI 도구가 횡적 이동의 연결점	테넌트 격리·도구권한 최소화·프롬프트/행위 감사
L5	서명/체인	정상 출금 밖 거래·EIP-7702 위임	정책 엔진·한도·독립 승인·권한 해제 런북

설계 원칙: "개인키 보호"를 넘어 "누가·어떤 코드가·어떤 컨텍스트에서·얼마를 서명하는가"를 검증

Source: [1] Binance; controls are report author recommendations

CASE 1 — RESPONSE

바이낸스 대응: 봉쇄·보충은 빨랐지만, 구조적 과제는 남았다

즉시 대응과 재발 방지 조치를 분리해 평가

1 즉시

출금 일시 중지
영향 주소 권한 취소
자산 동결·추적 공조

2 복구

영향 자산 100% 이상 준비
10/31 기준 98% 토큰 보충
Proof of Reserves 반영

3 재구축

지갑 시스템·내부 AI 도구 재구축
영향 단말 교체
자격증명·토큰 폐기

4 강화

디바이스 통제
지갑 서비스 리스크 통제
AI 행동 이상탐지 확대

우리 조직에 적용할 추가 방어

SIGNING POLICY

체인·자산·목적지·금액별 서명 정책과 독립 승인

TOKEN HYGIENE

단말 저장 금지, 15분 이하 단기 토큰, 자동 회수

DEVELOPER TRUST

업무 단말에서 외부 과제 실행 금지, 격리 샌드박스

REVOCATION DRILL

권한·토큰·온체인 위임 해제 훈련과 시간 목표

Sources: [1][3] Binance; [4] CNBC

CASE 1 — PATTERN EVOLUTION

바이낸스 계열 사고의 진화: 계정 → 브리지 → 운영 신뢰 경로

공격자는 방어가 강한 개인키 자체보다 "주변의 정상 권한"을 노린다.

2019

거래소 핫월렛

피싱·악성코드로 API 키·2FA 확보 → 7,000 BTC 단일 인출

핵심 통제

계정/거래 이상탐지

2022

BSC Token Hub

크로스체인 브리지의 저수준 증명 위조 → 200만 BNB 인출

핵심 통제

브리지 검증·라이브러리 안전

2026

Binance.com

개발자 단말·AI·배포 토큰 → 지갑 서명·온체인 권한 악용

핵심 통제

운영 신뢰 경로·서명 정책

패턴 변화: "비밀정보를 훔친다" → "검증 로직을 속인다" → "정상 운영권한으로 서명한다"

Sources: [5] Binance 2019, [6] BNB Chain 2022, [1] Binance 2026

KOREA FINANCIAL SECTOR

국내 금융권: 정보 유출과 서비스 마비가 동시에 현실화

기술적 실패가 소비자 보호·영업 제재·사회 인프라 중단으로 직결

DATA BREACH

롯데카드

297만 명

최대 200GB 유출

- 미패치 온라인 결제 시스템
- 암호화·백신 등 기본 통제 미이행
- 2026년 업무정지 1.5개월·과징금 50억 원

RANSOMWARE

SGI서울보증

약 81시간

주요 보증업무 차질

- 외부 노출 SSL-VPN/SSH 침투 보도
- 로그인 제한·IP 제한·MFA 미흡 가능성
- 복호화 키 추출 후 몸값 없이 서비스 재개

Sources: [7][8][9] 금융위·연합뉴스, [11][12] 보안뉴스

CASE 2 — LOTTE CARD

롯데카드: 8년 된 취약점·미패치·보호조치 미이행의 결합

공격 난이도보다 "보안 부채를 얼마나 오래 방치했는가"가 피해 규모를 결정했다.

297만 명
신용정보 유출
(금융위원회)

200GB
최대 반출 규모
(합동조사/회사 발표)

28만 명
부정사용 가능 정보 포함
(회사 발표)

1.5개월
신규회원 관련 업무정지
+ 과징금 50억 원

공식 검사에서 확인된 보안의무 위반

PATCH

정보처리시스템 보정(패치) 작업 미실시

ENCRYPT

주민등록번호·비밀번호 암호화 미이행

ENDPOINT

바이러스 백신 소프트웨어 미설치

규제 시사점: 해킹 사고가 "기술 부서의 문제"를 넘어 실제 업무정지와 매출·고객획득 제한으로 연결

Sources: [7] 금융위원회 제재 (2026-07-31), [9] 연합뉴스 (2025-09-18)

CASE 2 — ATTACK ROUTE

롯데카드 공격 루트: 미패치 WAS → 웹셸 → 소량 다회 유출

CVE·WAF 세부는 공개 기술 분석 기반이며, 공식 검사 결과의 "패치 미실시"와 일치한다.

1 취약 WAS
Oracle WebLogic
CVE-2017-10271 분석

→

2 원격 실행
SOAP/XML 역직렬화 경로로
RCE

→

3 웹셸 설치
지속성 확보·원격 명령 수행

→

4 내부 탐색
온라인 결제 서버 데이터 접근

→

5 저속 유출
작은 전송을 반복해 탐지 임계 회피

→

6 피해 확대
297만 명·최대 200GB

탐지 실패 지점

① 예방
8년 전 제공된 패치 미적용
자산·버전·패치 SLA 부재

② 차단
WAF만으로 WAS 취약성 상쇄 불가
본문 검사·가상패치·경로 차단 필요

③ 탐지
웹셸·서버 행위 가시성 부족
서버 EDR/FIM·명령행 감사

④ 유출
소량 다회 전송 누적 미탐지
세션 누적량·응답 DLP·Egress 분석

방어 포인트: 패치가 1순위, WAF는 보완책 — 서버 행위와 "나가는 데이터"까지 관찰해야 한다.

Sources: [7] 금융위(공식 원인), [8][9] 피해 규모, [10] 기술 분석

CASE 2 — ROOT CAUSES & FIX

롯데카드 원인과 해결: “보안 제품”보다 운영 통제가 먼저

패치·암호화·엔드포인트·유출 탐지를 운영 KPI로 고정해야 한다.

구분	통제 영역	관찰된 실패	권고 조치
원인	레거시/미패치	CVE 노출 장기화	인터넷 노출 자산 24h 확인, 긴급패치 72h, 예외 자동 만료
원인	데이터 보호	주민번호·비밀번호 암호화 미이행	토큰화·암호화·키분리, 보관기간 최소화
원인	서버 방어	백신 미설치·웹셸 지속성	서버 EDR/FIM, 웹루트 쓰기 통제, 스크립트 차단
원인	유출 가시성	소량 다회 전송 누적 탐지 부족	DLP + 프록시/DNS + 세션 누적 바이트 상관분석

운영 KPI 제안

Critical Patch	SLA 내 98% 이상	Sensitive Data	암호화/토큰화 100%	Server EDR	업무 서버 100%	Egress Alert	15분 내 조사 착수

Source: [7] 금융위원회; detailed controls are recommendations

CASE 3 — SGI SEOUL GUARANTEE

SGI서울보증: 외부 접점의 인증 통제 미흡이 업무 마비로 확대

침입 세부는 보도 기반이며, 공식 조사 미공개 영역은 확정 사실로 단정하지 않는다.

2025.07.14
랜섬웨어로
전산망 일부 마비

약 81시간
복구 완료까지
공개 분석 기준

SSL-VPN
최초 침투 지점으로
보도된 외부 접점

₩0
복호화 키 추출로
몸값 없이 재개 보도

공개 정보상 사고 흐름

초기 접근 — 보도

외부 노출 SSL-VPN 장비의 SSH 서비스에 반복 로그인 시도

내부 확산 — 분석

6월 중순 로그인 성공 추정 후 구조 파악·관리자 권한 및 서버 접근

영향 — 보도

랜섬웨어 배포·데이터 암호화로 보증서 발급 등 주요 서비스 차질

핵심: "망분리"가 있어도 외부 접점의 관리자 권한이 내부로 이어지면 가용성은 무너질 수 있다.

Sources: [11] 침투 경로, [12] 복구, [13] 기술 분석

CASE 3 — ATTACK ROUTE

SGI 공격 루트: 노출된 SSH → 반복 인증 → 횡적 이동 → 암호화

확정되지 않은 데이터 유출 여부는 별도 트랙으로 검증해야 한다.

1 외부 노출
SSL-VPN 장비
SSH 관리 서비스

→

2 반복 로그인
다수 IP·ID/PW 시도
Brute force/credential stuffing

→

3 인증 성공
계정 잠금·IP 제한·MFA 미흡 가능성

→

4 내부 이동
관리자 권한·서버 접근
업무망 구조 파악

→

5 방어 무력화
보안 프로세스 종료·복구 방해 분석

→

6 랜섬웨어
파일 암호화
업무 서비스 중단

차단 지점 — 앞에서 막을수록 비용이 낮다

EDGE
관리 포트 인터넷 차단·관리망/점프호스트

IDENTITY
피싱저항 MFA·잠금·IP/시간 정책

LATERAL
PAM/JIT·세그멘테이션·SMB/RPC 최소화

RECOVERY
불변 백업·DR 격리·정기 복구 훈련

포렌식 분기: "암호화"와 "정보 반출"은 다른 증거가 필요 — 외부 연결·대용량/저속 전송 로그를 별도 보존

Sources: [11][12] 보안뉴스, [13] PLURA 분석

CASE 3 — ROOT CAUSES & RECOVERY

SGI 원인과 해결: 엣지 통제·권한 경계·복구 독립성

복호화 성공은 행운에 가까운 결과 — 다음 사고는 불변 백업과 훈련으로 복구해야 한다.

1	엣지 노출	VPN 장비의 SSH 관리면이 인터넷과 연결	관리면 Any-Open 금지, 전용 관리망/점프호스트
2	인증 통제	로그인 횟수·속도·접속 IP·MFA 미흡 가능성	FIDO2 MFA, 잠금/지연, 지리·시간·기기 조건부 접근
3	권한·확산	초기 접점에서 업무망·서버로 이동 가능	PAM/JIT, 계정 분리, 마이크로세그멘테이션
4	복구 체계	랜섬웨어가 서비스 가용성을 직접 훼손	3-2-1-1-0 백업, 불변 저장소, 클린룸 복구

복구 운영 목표

RTO	핵심 서비스 4h 이내	RPO	15분 이내	격리	백업 계정·망·키 분리	훈련	분기 1회 전체 복구

Sources: [11][12]; RTO/RPO values are recommended targets to tailor by BIA

CROSS-CASE

사고별 공격·원인·영향 비교

서로 다른 산업 기술에서도 동일한 통제 공백이 반복된다.

구분	바이낸스	롯데카드	SGI서울보증
초기 접근	가짜 채용·악성 저장소	미패치 WebLogic 분석	SSL-VPN/SSH 반복 인증 보도
악용된 신뢰	개발자 단말·AI·배포 토큰	WAS·웹셸·온라인 결제 데이터	VPN 관리자 권한·내부망
탐지 공백	0-day·정상 운영권한	패치/EDR/유출 가시성	로그인 이상·횡적 이동
최종 영향	다중 체인 자산 탈취	297만 명 정보 유출	보증업무 서비스 마비
핵심 해법	워크로드 신원·서명 정책	패치·암호화·Egress DLP	엣지 MFA·PAM·불변백업

공통 결론: 경계 방어만이 아니라 "정상 권한의 오용"과 "복구 가능성"을 실시간 검증해야 한다.

Compiled from sources [1][7][9][10][11][12][13]

COMMON PATTERN

공통 공격 패턴: 신뢰를 통과한 뒤, 관찰이 약한 곳에서 폭발

공격 차단점을 “Kill Chain”이 아니라 “Trust Chain”으로 재배치

① 신뢰 형성
사람·공개서비스
채용/인터넷 접점

→

② 정상 권한 획득
계정·토큰·웹셸
인증·취약점

→

③ 내부 경로 이동
AI·망·서버
권한·세그먼트

→

④ 가치자산 접근
서명·DB·백업
핵심 시스템

→

⑤ 영향 실행
탈취·유출·암호화
비즈니스 피해

각 단계의 최소 통제

VERIFY
신원·기기·코드 출처 검증

LIMIT
권한·토큰 수명·거래 한도 최소화

OBSERVE
행위·데이터 이동·서명 패턴 관찰

CONTAIN
세션·권한·네트워크 즉시 격리

RECOVER
불변 백업·해제 런북·복구훈련

운영 질문: “이 단계가 뚫렸을 때 다음 단계로 넘어가지 못하게 하는 독립 통제가 있는가?”

Analytical synthesis based on the three cases

TARGET ARCHITECTURE

권고 보안 아키텍처: 6개의 독립 방어 게이트

제품 목록이 아니라 신뢰 경로의 승인·관찰·복구 구조를 설계한다.

G1

External Edge

공개 자산·관리포트 최소화
ASM + WAF + ZTNA

G2

Identity

FIDO2 MFA·PAM/JIT
조건부 접근

G3

Endpoint & Dev

격리 개발환경·EDR
서명된 패키지·허용목록

G4

Workload

단기 워크로드 신원
Secretless·토큰 자동회수

G5

Data / Signing

DLP·토큰화·서명정책
한도·독립 승인

G6

Resilience

불변 백업·클린룸
권한 해제·DR 훈련

통제 간 연결

TELEMETRY

ID·단말·네트워크·데이터·서명 로그를 공통 타임라인으로 연결

POLICY

고위험 행위는 실시간 차단, 예외는 기한·승인·증거를 남김

RECOVERY

차단 실패를 가정하고 복구 자산·키·계정을 운영망과 독립

ACTION ROADMAP

180일 실행 로드맵: 즉시 차단 → 통제 내재화 → 구조 전환

우선순위는 "인터넷 노출 × 관리자 권한 × 핵심자산 연결성"으로 결정

0–30일 긴급 차단

1. 외부 노출 VPN/SSH·관리 포트 전수조사
2. Critical 미패치 자산 응급 조치
3. 관리자 MFA·잠금·IP 제한 강제
4. 서버·지갑·DB 로그 보존 및 위협 헌팅

31–90일 통제 내재화

1. PAM/JIT·단기 토큰·비밀정보 금고
2. 서버 EDR/FIM·Egress DLP 확대
3. 민감정보 암호화/토큰화·보유 최소화
4. 불변 백업·복구 클린룸 구축

91–180일 구조 전환

1. 개발망/업무망 제로트러스트 분리
2. 고위험 서명·거래 독립 승인 정책
3. AI 도구·에이전트 권한 경계 재설계
4. 전사 침해·랜섬웨어·권한해제 훈련

GATE: 각 단계 종료 시 "증거 기반 검증" — 설정 캡처가 아니라 실제 차단·복구 테스트 결과로 승인

Recommended roadmap; sequencing should be adjusted after asset and BIA validation

MANAGEMENT DASHBOARD

경영진 대시보드: 보안 활동이 아니라 위험 감소를 측정

월간 추세 + 분기 실제 테스트 결과를 함께 보고

1 노출 자산

Critical 노출 0건

ASM 재탐색 기준

2 패치

Critical SLA 98%+

예외 자동 만료

3 특권 신원

MFA/PAM 100%

공용·장기 계정 0

4 탐지

MTTD < 15분

고위험 이벤트

5 봉쇄

MTTC < 30분

계정·단말·토큰

6 복구

RTO 달성 95%+

분기 복구훈련

7 데이터

민감정보 암호화 100%

평문 발견 0

8 서명/거래

정책 우회 0건

한도·목적지 검증

Red Flag: 지표가 "100%"여도 실제 침투·복구 테스트가 없으면 통제 효과를 입증할 수 없다.

Suggested metrics; calibrate targets to business criticality and regulatory obligations

CUSTOMER CHECKLIST

고객사 현장 진단 질문 12개

"예/아니오"가 아니라 증거 링크·담당자·완료기한을 함께 기록

1	외부 접점	인터넷에 노출된 VPN·SSH·관리 UI를 24시간 내 완전 식별할 수 있는가?
2	패치	Critical 자산의 버전·EOL·패치 예외가 단일 장부에서 관리되는가?
3	MFA	관리자·원격접속·개발/배포 계정에 피싱 저항형 MFA가 적용됐는가?
4	토큰	배포·API 토큰이 단말에 장기 저장되지 않고 자동 만료·회수되는가?
5	개발환경	외부 코드/면접 과제를 업무 단말에서 실행하지 못하도록 격리했는가?
6	AI 도구	내부 AI 도구가 자격증명·운영권한에 접근할 수 있는 범위를 감사하는가?
7	서버	업무 서버에서 웹셸·명령행·파일 변경을 실시간 탐지하는가?
8	데이터	민감정보가 암호화·토큰화되고 평문 검색이 정기 수행되는가?
9	유출	소량 다회·장기 저속 유출을 세션 누적량으로 탐지하는가?
10	서명/승인	고위험 거래/배포가 한 사람·한 서비스만으로 승인될 수 없는가?
11	봉쇄	계정·단말·토큰·온체인 권한을 30분 내 해제하는 런북이 있는가?
12	복구	운영망 침해를 가정한 불변 백업·클린룸 복구를 분기마다 증명하는가?

Use this checklist as a workshop agenda and evidence register

DECISION

지금 필요한 의사결정 4가지

최근 사고는 "예산 부족"보다 "권한과 책임의 분산"을 더 선명하게 보여준다.

01 외부 접점 Zero-Tolerance

인터넷 노출 관리면·Critical 미패치 자산은 예외 없이 즉시 차단 또는 CEO/CISO 승인

02 특권·서명 이중 통제

배포·DB·지갑/거래 등 가치자산 접근은 독립 승인과 단기 권한으로 전환

03 관찰 범위 확장

로그인 성공/실패뿐 아니라 코드·토큰·데이터 이동·서명 행위를 통합 관찰

04 복구를 생산처럼 운영

불변 백업·클린룸·권한 해제 런북을 실제 서비스 수준으로 정기 검증

최종 메시지: 공격자는 가장 약한 "제품"이 아니라 가장 길게 이어진 "신뢰 경로"를 찾는다.

APPENDIX — SOURCES

주요 출처 1/2

공식 발표를 우선하고, 기술 세부는 2차 분석으로 보완

[1] Binance — Initial Findings and Response Update (2026-11-03)
https://www.binance.com/en/blog/community/3229153443759566763

[2] FBI — North Korea Responsible for $6B+ Binance Attack (2026-10-31)
https://www.fbi.gov/investigate/cyber/alerts/2026/north-korea-responsible-for-6-billion-binance-attack

[3] Binance — Security Incident Update (2026-10-30)
https://www.binance.com/en/support/announcement/detail/c5a8729a97ac486d963784d96c5642d7

[4] CNBC — Binance $6.3B hack explainer (2026-10-30)
https://www.cnbc.com/2026/10/30/billions-in-crypto-frozen-in-binance-hack-heres-what-happens-next-.html

[5] Binance — 2019 Security Breach Update
https://www.binance.com/en/support/announcement/detail/360028031711

[6] BNB Chain — 2022 Ecosystem Update / bridge exploit
https://www.bnbchain.org/en/blog/bnb-chain-ecosystem-update

[7] 금융위원회 — 롯데카드 업무정지·과징금 (2026-07-31)
https://www.fsc.go.kr/no010101/87455

[8] 금융위원회 — 롯데카드 정보유출 긴급 대책회의 (2025-09-18)
https://www.fsc.go.kr/comm/getFile?srvcId=BBSTY1&upperNo=85319&fileTy=ATTACH&fileNo=1

출처 사용 원칙 사고 규모·제재·공식 조치는 1차 자료 우선 / 공격 세부는 공개 범위와 확정성 라벨을 함께 표기

URLs are embedded as hyperlinks

주요 출처 2/2 · 한계 및 가정

기준일 이후 조사 결과가 변경될 수 있으므로 최종 제출 전 업데이트 확인 권고

[9] 연합뉴스 — 롯데카드 297만 명·200GB 발표 (2025-09-18)
https://www.yna.co.kr/view/AKR20250918105252002

[10] PLURA — 롯데카드 WebLogic/WebShell 기술 분석 (2025-09-22)
https://blog.plura.io/ko/threats/case-lottecard_weblogic/

[11] 보안뉴스 — SGI 최초 침투 경로 SSL-VPN 보도 (2025-07-17)
https://www.boannews.com/media/view.asp?idx=138214&kind=1

[12] 보안뉴스 — 금융보안원 복호화 키 추출 보도 (2025-07-18)
https://www.boannews.com/media/view.asp?idx=138237

[13] PLURA — SGI 침투·랜섬웨어 분석 (2025-07-22)
https://blog.plura.io/ko/threats/case-sgic_credential_stuffing/

[14] KISA — 랜섬웨어 대응 가이드라인 안내 (2023-08-03)
https://www.kisa.or.kr/402/form?postSeq=2299

한계 및 가정

- “미국 바이낸스”는 FBI가 공식 귀속한 Binance.com 글로벌 사고를 의미하며 Binance.US 별도 사고로 해석하지 않음.
- 롯데카드의 CVE-2017-10271·웹셸 상세는 공개 기술 분석에 기반; 공식 제재자료는 패치 미실시·암호화 미이행·백신 미설치를 확인.
- SGI 침입 경로·인증 통제 상세는 언론/공개 분석 기반이며, 당시 데이터 유출 여부는 공개 확정 정보가 제한적.
- 권고 RTO/RPO·SLA는 예시 목표로, 고객사 BIA·규제·시스템 중요도에 따라 조정 필요.