Incident Forensic Analysis Report

침해사고 포렌식 보고서

Kubernetes 기반 클라우드 침해사고 사건

작 성 자 서현재

소 속 시큐리티아카데미

제 출 일 2026-06-03

문서 버전 v1.0

목 차

1. 사고 개요

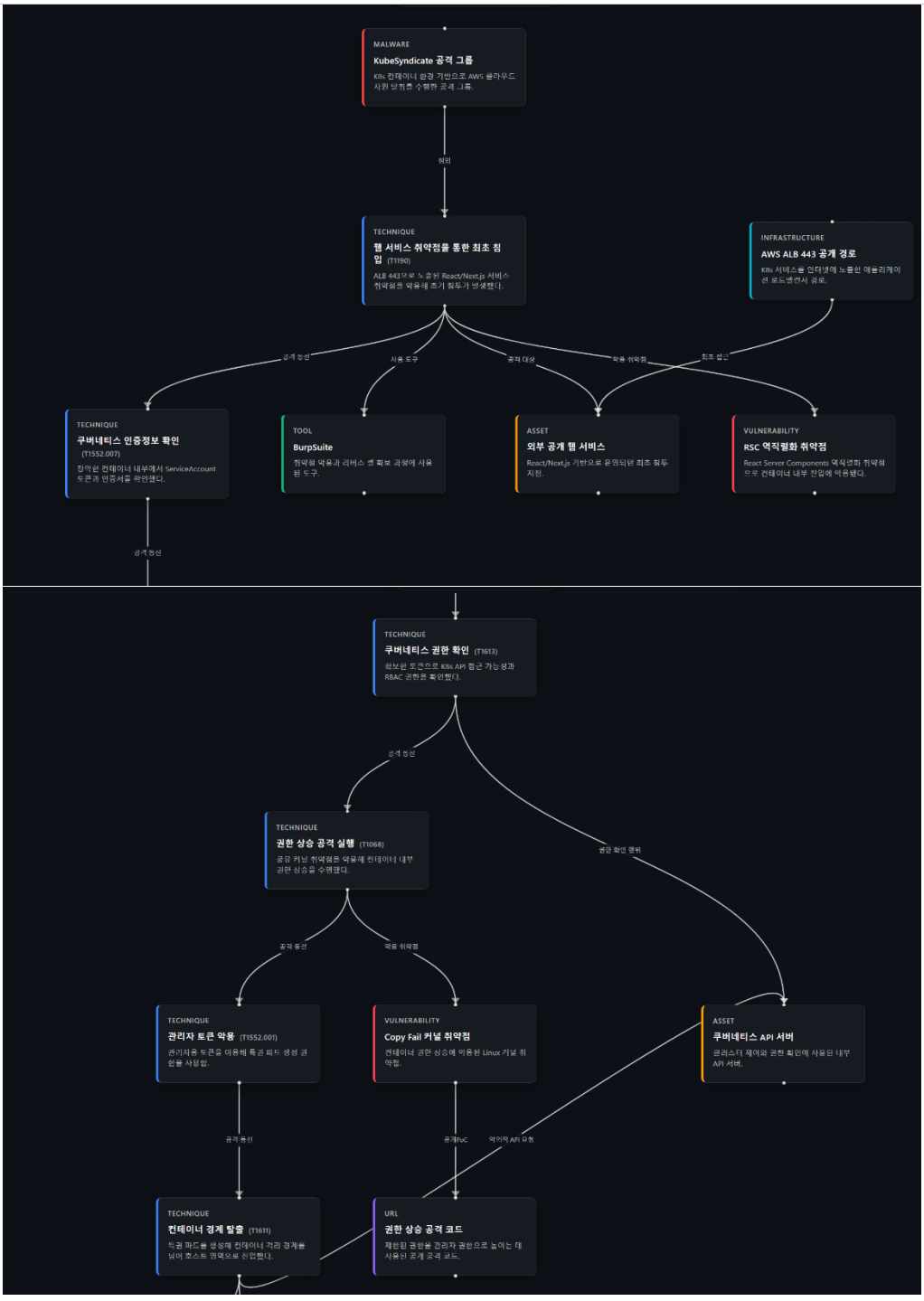
› 육하원칙(누가·언제·무엇을·어떻게)에 따라 사고를 한눈에 파악할 수 있도록 요약합니다.

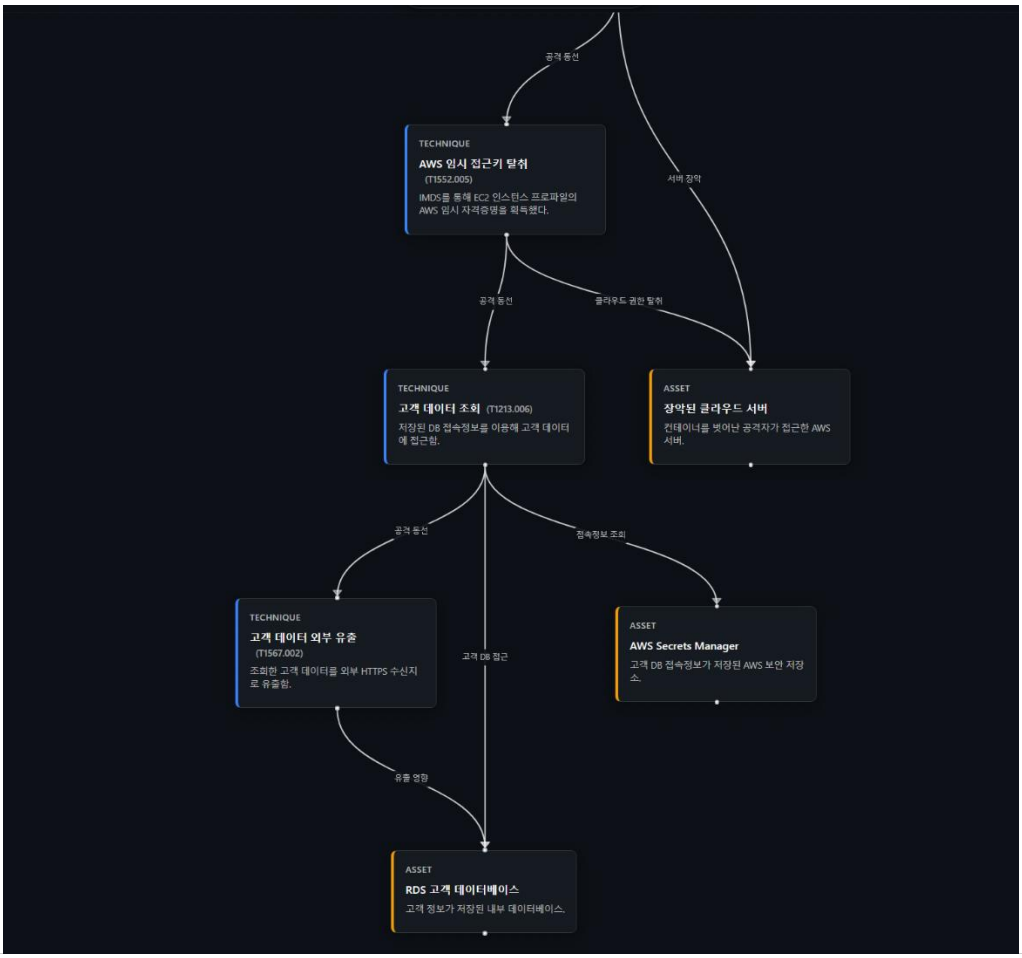
사고 명칭	Kubernetes 기반 클라우드 침해사고 분석
사고 유형	외부 공개 웹 서비스 침해, 내부 권한 확대, 클라우드 접속 권한 조회, 고객 데이터 조회 및 외부 전송 명령
의뢰인 / 담당 부서	KISIA 프로젝트 / DF 분석
사고 인지 일시	2026-05-28 06:53:10 UTC / 15:53:10 KST
사고 발생 추정 일시	2026-05-28 06:53:10 UTC / 15:53:10 KST
대응 착수 일시	핵심 탐지 이후 분석 착수
분석 기간	핵심 이벤트 2026-05-28 06:53:10 UTC / 15:53:10 KST ~ 2026-05-28 07:06:39 UTC / 16:06:39 KST
사고 심각도	심각 - 내부 권한 확대와 고객 데이터 접근 정황 확인
현재 처리 상태	분석 완료, 즉시 조치 및 영향 범위 확인 필요

1.1. 사고 요약

공격자는 외부 공개 서비스에서 명령 실행 통로를 만든 뒤, 내부 권한 범위를 확인하고 서버 관리자 수준 권한과 클라우드 접속 권한 정보까지 접근한 정황이 확인된다.
고객 주문 데이터 조회와 외부 전송 명령은 확인되었으나, 실제 외부 수신 성공 여부와 유출 규모는 네트워크 및 DB 로그로 추가 확인해야 한다.

[그림 1] 침해사고 관계도


MALWARE
KubeSyndicate 공격 그룹
K8s 컨테이너 환경 기반으로 AWS 클라우드 자원 탈취를 수행한 공격 그룹.
하위
TECHNIQUE
웹 서비스 취약점을 통한 최초 침입 (T1190)
ALB 443으로 노출된 React/Next.js 서비스 취약점을 악용해 초기 침투가 발생했다.
INFRASTRUCTURE
AWS ALB 443 공개 경로
K8s 서비스를 인터넷에 노출한 애플리케이션 로드밸런서 경로.
공격 전선
사용 도구
공격 대상
악용 취약점
최초 접근
TECHNIQUE
쿠버네티스 인증정보 확인 (T1552.007)
탈취된 컨테이너 내부에서 ServiceAccount 토큰과 인증서를 확인했다.
TOOL
BurpSuite
취약점 악용과 리버스 셸 확보 과정에 사용된 도구.
ASSET
외부 공개 웹 서비스
React/Next.js 기반으로 운영되던 최초 침투 지점.
VULNERABILITY
RSC 역직렬화 취약점
React Server Components 역직렬화 취약점으로 컨테이너 내부 진입에 악용됐다.
공격 전선
TECHNIQUE
쿠버네티스 권한 확인 (T1613)
획보된 토큰으로 K8s API 접근 가능 성과 RBAC 권한을 확인했다.
공격 전선
권한 확인 완료
TECHNIQUE
권한 상승 공격 실행 (T1068)
공유 커널 취약점을 악용해 컨테이너 내부 권한 상승을 수행했다.
공격 증선
악용 취약점
TECHNIQUE
관리자 토큰 악용 (T1552.001)
관리자용 토큰을 이용해 특권 파드 생성 권한을 사용했다.
VULNERABILITY
Copy Fail 커널 취약점
컨테이너 권한 상승에 이용된 Linux 커널 취약점.
ASSET
쿠버네티스 API 서버
클러스터 제어와 권한 확인에 사용된 내부 API 서버.
공격 증선
공개PoC
악의적 API 요청
TECHNIQUE
컨테이너 경계 탈출 (T1611)
특권 파드를 생성해 컨테이너 격리 경계를 넘어 호스트 영역으로 진입했다.
URL
권한 상승 공격 코드
제한된 권한을 관리자 권한으로 높이는 데 사용된 공개 공격 코드.


공격 동선
TECHNIQUE
AWS 임시 접근키 탈취
(T1552.005)
IMDS를 통해 EC2 인스턴스 프로파일의 AWS 임시 자격증명을 획득했다.
서버 장악
공격 동선
클라우드 권한 탈취
TECHNIQUE
고객 데이터 조회 (T1213.006)
저장된 DB 접속정보를 이용해 고객 데이터에 접근함.
ASSET
장악된 클라우드 서버
컨테이너를 벗어난 공격자가 접근한 AWS 서버.
공격 동선
접속정보 조회
TECHNIQUE
고객 데이터 외부 유출
(T1567.002)
조회한 고객 데이터를 외부 HTTPS 수신지로 유출함.
고객 DB 접근
ASSET
AWS Secrets Manager
고객 DB 접속정보가 저장된 AWS 보안 저장소.
유출 영향
ASSET
RDS 고객 데이터베이스
고객 정보가 저장된 내부 데이터베이스.

2. 분석 대상

[표] 증거 목록

번호	파일명 / 시스템명	수집 위치	파일 크기	해시값 (MD5 / SHA-1)
1	query_results.csv	Timesketch star 이벤트 및 comment	15.2 KB	MD5 EE79E1BD91CC635FFA2C17C0EEEBEEF4 SHA1 04E05C343B7FF00F7AB4FEC8BD566B4CF0E90406
2	METADATA	Timesketch export 조건과 재현성 근거	566 B	export 조건 기록
3	Wazuh alerts CSV	전체 경보 흐름과 전후 맥락 확인	484.2 KB	MD5 4E5577BDBEA09994DC6D54AA128A53E0 SHA1 28A87426EC087D7343A2086F68C131D24F3FF213
4	Wazuh manifest	변환 이력과 원본 해시 근거	703 B	SHA256 2FA67B5F7F77A24606124F2A40A51C7EE5B83CC68FEA266D61E4ECC798A784A0
5	Wazuh alerts/archive 원본	원본 로그 보존 근거	500.4 KB / 18.45 MB	원본 증거
6	FlowViz JSON / manifest	공격 흐름 시각화와 출처 근거	19.5 KB / 1.1 KB	MD5 8C400E0B91975CAAE917FAF1BE5CAA73 SHA1 08BE05C8251D1E442BC3094CEAF27CA44A08BDA1

2.1. 분석 환경 및 도구

구분	도구 / 환경	버전	용도
원본 로그	Wazuh alerts/archive	프로젝트 산출물 기준	원본 증거 보존과 탐지 근거 확인
타임라인	Timesketch	프로젝트 산출물 기준	star, tag, comment 기반 핵심 이벤트 선별
시각화	FlowViz	프로젝트 산출물 기준	비전문가·경영진용 공격 흐름 시각화
분석 기준	MITRE ATT&CK / SB-04	프로젝트 산출물 기준	공격 단계와 대응 커버리지 점검
보고서 작성	AI 작성 보조	프로젝트 산출물 기준	분석 기준에 맞춘 보고서 초안 구성

2.2. 분석 기준

항목	판단 기준	한계 / 비고
핵심 이벤트	query_results.csv의 star 이벤트와 comment를 최우선 근거로 사용	star 이벤트라도 원문과 맞지 않으면 단정하지 않음
전체 경보 맥락	Wazuh 전체 경보로 전후 흐름과 반복 경보를 확인	핵심 판단 근거가 아닌 보조 근거
이상 징후 선별	정상 업무 흐름에서 설명하기 어려운 명령 실행, 권한 확대, 데이터 조회를 우선 분석	경보 존재만으로 공격 성공을 단정하지 않음
MITRE 활용	공격 기법 나열이 아니라 대응 커버리지 점검 기준으로 사용	기법명만으로 피해 범위를 단정하지 않음

3. 분석 결과 요약

핵심 결론은 공격 흐름, 고객 데이터 위험, 즉시 승인할 대응 조치 중심으로 요약하였다.
동일한 공격 흐름에서 원격 명령 통로 생성, 내부 권한 확인, 권한 확대, 클라우드 접속 권한 조회, 고객 데이터 조회, 외부 전송 명령이 순차적으로 확인되었다.

3.1. 분석 관점

확인 항목	분석 관점	확인 근거	판단 결과
초기 침투	외부 공개 서비스가 명령 실행 통로로 악용됐는지 확인	Shell Spawn, Reverse Shell, 외부 IP	외부 진입 정황 확인
권한 확대	내부 권한 확인 뒤 더 높은 권한으로 확장했는지 확인	RBAC review, exploit 실행, Root Gained	서버 관리자 수준 권한 확보 정황
내부 확산	컨테이너를 넘어 운영 영역과 클라우드 권한 정보까지 접근했는지 확인	host namespace, IMDS, instance role	내부 확산 정황 확인
데이터 접근	고객 데이터 조회와 외부 전송 명령이 연결되는지 확인	mysql, customer_orders, curl POST	데이터 유출 위험 확인
판단 한계	확인된 사실과 추가 확인 범위를 구분	네트워크 로그, DB 접속 로그	외부 수신 성공 여부는 추가 확인 대상

3.2. 사고 타임라인

일시	출발지 / 대상	행위	근거 (로그·아티팩트)
2026-05-28 06:53 UTC	외부 IP -> react-app	외부 공격자가 서버에 원격 명령을 내릴 수 있는 통로 생성	Shell Spawn, Reverse Shell, T1190/T1059.004
2026-05-28 06:54 UTC	react-app -> Kubernetes API	내부 서비스 계정 권한 범위 확인	RBAC review, T1552.007/T1613
2026-05-28 06:54 UTC	react-app	취약점을 이용해 더 높은 권한 확보 시도 및 성공 정황	/tmp/exp.py, T1068
2026-05-28 06:55 UTC	react-app	Kubernetes 인증정보 확인	kubeconfig read, T1552.001
2026-05-28 06:57 UTC	pwned-pod-final	서버 운영 영역과 클라우드 권한 정보에 접근	host namespace, IMDS, T1611/T1552.005
2026-05-28 07:05 UTC	pwned-pod-final -> RDS	고객 주문 데이터가 저장된 데이터베이스 조회	mysql, customer_orders, T1213.006
2026-05-28 07:06 UTC	pwned-pod-final -> 외부 수신지	고객 데이터 파일을 외부 사이트로 전송하려는 명령 확인	curl POST, webhook.site, T1567.002

3.3. MITRE ATT&CK 매트릭스

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
T1190 외부 공개 서비스 악용	T1059.004 명령 실행		T1068 권한 확대 공격		T1552.007 서비스 계정 접속 정보	T1613 Kubernetes 권한 확인
			T1611 컨테이너 경계 확장		T1552.001 Kubeconfig 확인	
					T1552.005 클라우드 권한 정보 조회	T1213.006 고객 데이터 조회
						T1567.002 외부 전송은 상세표에 기재

3.4. MITRE ATT&CK 기법 상세

기법 ID	사용 기술	설명
T1190	외부 공개 서비스 악용	외부 공개 React/Next.js 서비스에서 원격 명령 통로가 생성된 정황이 확인된다.
T1059.004	명령 실행	정상 서비스 흐름과 다른 쉘·파이썬 명령 실행이 확인된다.
T1552.007 / T1552.001	내부 접속정보 확인	서비스 계정 접속정보와 kubeconfig 확인 정황이 확인된다.
T1613	Kubernetes 권한 확인	내부 시스템에서 접근 가능한 권한 범위를 확인한 정황이 확인된다.
T1068	권한 확대	취약점 악용 도구 실행 뒤 서버 관리자 수준 권한 확보 정황이 이어진다.
T1611	컨테이너 경계 확장	침해된 실행 환경이 서버 운영 영역으로 확장된 정황이 확인된다.
T1552.005	클라우드 권한 정보 조회	클라우드 접속 권한 정보 경로에 접근한 정황이 확인된다.
T1213.006 / T1567.002	데이터 조회 및 외부 전송	고객 주문 데이터 조회와 외부 사이트 전송 명령이 확인된다.

4. 공격 흐름 분석

공격 단계	통제 실패 지점	사용 기법 (TTPs)	공격 인과 분석
1. 초기 침투	외부 공개 웹 서비스가 공격자의 명령 실행 통로로 악용된 정황	T1190, T1059.004	공격자가 회사 외부에서 접근 가능한 서비스 경로를 통해 내부 실행 환경에 들어온 흐름이다.
2. 내부 접속정보 확인	침해된 실행 환경에서 내부 서비스 계정과 설정 파일을 확인한 정황	T1552.007, T1552.001	공격자가 내부 시스템에서 어느 권한을 사용할 수 있는지 확인한 단계다.
3. Kubernetes 권한 확인	내부 권한 범위를 확인하고 다음 행동 가능성을 점검한 정황	T1613	내부 운영 환경으로 확장 가능한지를 확인한 흐름이다.
4. 권한 확대	취약점 악용 도구를 실행해 더 높은 시스템 권한을 확보한 정황	T1068	공격자가 서버 관리자 수준의 영향력으로 확장한 과정이다.
5. 컨테이너 경계 확장	컨테이너를 넘어 서버 운영 영역에 접근한 정황	T1611	침해 범위가 단일 실행 환경을 넘어 내부 운영 영역으로 넓어진 단계다.
6. 클라우드 권한 정보 조회	클라우드 자원 접근에 필요한 임시 권한 정보를 조회한 정황	T1552.005	공격자가 사내 클라우드 자원으로 접근 범위를 넓힐 수 있는 위험이 생긴 단계다.
7. 고객 데이터 조회	고객 주문 데이터가 저장된 데이터베이스를 조회한 정황	T1213.006	고객 데이터 영향 가능성이 실제로 발생한 단계다.
8. 외부 전송 시도	고객 데이터 파일을 외부 사이트로 전송하려는 명령이 확인된 정황	T1567.002	데이터 외부 유출 위험이 확인되며 실제 수신 성공 여부는 추가 확인 대상이다.

5. 침해지표

유형	지표 값	설명
외부 IP	52.78.86.94	원격 명령 통로 연결 목적지
Pod	react-app-685875587f-hv72r	최초 침해와 명령 실행이 확인된 실행 환경
Pod	pwned-pod-final	내부 운영 영역과 클라우드 권한 정보 접근 정황이 확인된 실행 환경
파일	/tmp/exp.py	권한 확대 공격 도구로 탐지된 파일
Metadata path	169.254.169.254 / security-credentials	클라우드 권한 정보 조회 경로
데이터베이스	customer_orders	고객 주문 데이터 조회 대상
외부 URL	webhook.site/1607b201-4617-4cd9-aaeb-97baa2da222a	외부 전송 명령 목적지

6. 피해 범위 및 영향

구분	영향 받은 자산	피해 내용	영향 수준
외부 공개 서비스	React/Next.js 서비스	공격자의 원격 명령 통로로 악용된 정황	심각
내부 실행 환경	Kubernetes pod / node 영역	내부 권한 확인과 서버 운영 영역 접근 정황	심각
클라우드 권한	AWS instance role	클라우드 접속 권한 정보 조회 정황	높음
고객 데이터	RDS customer_orders	고객 주문 데이터 조회와 외부 전송 명령 확인	심각
서비스 가용성	웹 서비스	서비스 중단 정황은 현재 로그상 명확하지 않음	중간
대외 리스크	고객정보 및 법무 검토	실제 외부 수신 성공 여부에 따라 신고·고지 판단 필요	높음

6.1. 영향 평가

기밀성은 고객 데이터 조회와 외부 전송 명령으로 위험이 높다. 무결성은 서버 관리자 수준 권한 확보 정황으로 위험이 높다. 서비스 중단은 현재 로그상 명확하지 않다.

7. 대응 및 개선 방안

7.1 의사결정 요약

판단 항목	현재 판단	의사결정 사항	근거
사고 단계 격상	외부 공개 서비스 침해가 내부 권한 확대와 고객 데이터 접근 위험으로 확장된 사고로 판단	관련 실행 환경 격리, 증거 보존, 접속 권한 회수 승인	핵심 이벤트와 Wazuh 탐지 로그
고객 데이터 보호	고객 주문 데이터 조회와 외부 전송 명령이 확인됨	DB 계정 교체, 외부 전송 차단, 데이터 접근 범위 확인 승인	DB 조회 로그와 외부 전송 명령
확산 차단	내부 운영 영역과 클라우드 권한 정보까지 접근 범위가 넓어진 정황 확인	의심 서버 격리, 서비스 계정 토큰 회수, 클라우드 권한 점검 승인	권한 확인과 클라우드 권한 정보 조회 로그
대외 판단	고객정보 유출 가능성이 있어 법무·개인정보보호 관점 검토 필요	추가 로그 확인 후 신고·고객 고지 필요 여부 판단	고객 데이터 조회와 외부 전송 정황

7.2. 근본 원인

직접 원인은 외부 공개 서비스 침해 이후 내부 권한 확대가 가능했던 점이다. 추정 원인은 웹 취약점 노출, 과도한 내부 권한, 클라우드 접속 권한 보호 미흡이다.

7.3. 개선 권고 사항

구분	번호	권고 사항	우선 순위	목표 및 기대 효과	담당 / 기한
외부 전송 차단	1	의심 실행 환경과 관련 서버를 격리하고 삭제 전 로그·이미지·볼륨을 보존한다.	즉시	확산 차단과 증거 보존	네트워크팀 / 즉시
	2	서비스 계정, 클라우드 접속 권한, DB 계정 비밀번호를 회수·교체한다.	즉시	노출 가능 권한 재사용 차단	
	3	의심 외부 IP와 외부 수신지를 차단하고 사고 시간대 외부 전송 로그를 보존한다.	즉시	데이터 반출 경로 차단	
탐지 개선	4	DB 접속·쿼리 로그로 customer_orders 접근 범위와 전송 성공 여부를 확인한다.	높음	고객정보 영향 범위 판단	보안운영팀 / 2주
	5	웹 취약점 조치, 최소권한, 클라우드 권한 정보 보호 정책을 적용한다.	높음	동일 경로 재발 방지	
	6	정상 기준선을 만들고 명령 실행·권한 확대·외부 전송 징후를 우선 탐지하도록 룰을 정비한다.	중기	정상 로그 속 이상 징후 선별 강화	

8. 결론›

8.1. 종합 결론

본 사고는 외부 공개 웹 서비스 침해가 내부 운영 영역과 고객 데이터 영역으로 확장된 침해사고로 판단된다. 따라서 즉시 격리, 권한 회수, 외부 전송 차단, 고객 데이터 영향 확인이 필요하다.

9. 부록

부록에는 보고서 작성에 사용한 원본 증거, 변환 이력, 용어, 참고 문헌을 정리하였다.

9.1. 첨부 자료 목록

- query_results.csv: Timesketch star 이벤트와 comment 최우선 근거
- Wazuh alerts/archive: 전체 경보 흐름과 원본 로그 근거

9.2. 수록 파일 목록

- FlowViz 출처: **https://spacebar-mitre-attack-campaigns.vercel.app/campaigns/SB-04/**

9.3. 용어 정의

- MITRE ATT&CK: 공격 행위를 표준 기법으로 분류하고 대응 범위를 점검하는 기준
- Timesketch star event: 분석가가 핵심 이벤트로 선별한 타임라인 항목
- IMDS: 클라우드 서버의 접속 권한 정보를 제공하는 메타데이터 서비스

9.4. 참고 문헌

- SB-04 campaign reference: **https://spacebar-mitre-attack-campaigns.vercel.app/campaigns/SB-04/**
- GitHub reference: **https://github.com/Jseanxx/Spacebar-MITRE-ATTACK-campaigns.git**