

1 평범한 보안관제 화면

오전 8시 43분.
보안관제 시스템에
평범한 로그인 기록 하나가
올라온다.

보안관제 시스템 ● 실시간 로그

시간	사용자	이벤트	접속 정보	상태
08:43:12	kim.hyunwoo	VPN 로그인	10.10.15.23	✓ 성공
08:43:15	kim.hyunwoo	MFA 인증	-	✓ 성공
08:43:18	kim.hyunwoo	그룹웨어 접속	-	✓ 성공
08:43:33	kim.hyunwoo	파일서버 접근	-	✓ 성공

위험 현황
정상 98.7%

접속 추이

보안관제
08:43

- VPN 접속 성공
- 해외 IP 아님
- MFA 정상 인증
- 접근 권한 이상 없음

시간	사용자	이벤트	접속 정보	상태
08:43:12	kim.hyunwoo	VPN 로그인	10.10.15.23	✓ 성공
08:43:15	kim.hyunwoo	MFA 인증	-	✓ 성공
08:43:18	kim.hyunwoo	그룹웨어 접속	-	✓ 성공
08:43:33	kim.hyunwoo	파일서버 접근	-	✓ 성공

이상 징후 없음.
다음 로그.



계정 이름도 익숙했다.
김현우 대리.
문제는 아무도
그 이름을 다시
확인하지 않았다는
것이였다.

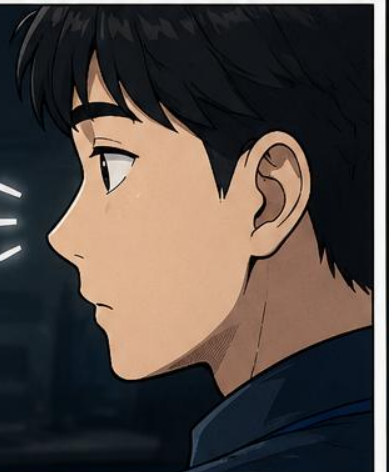
사용자 정보



kim.hyunwoo

정상 사용자

부서 : 사업전략팀
직급 : 대리
계정 상태 : 활성
마지막 로그인 : 08:43:12



기억하세요!

퇴사자 계정이 남아 있으면 누구나 다시 회사 시스템에 접근할 수 있습니다.

퇴사자 계정

권한 회수

MFA

로그 모니터링

2 사업전략팀 긴장된 회의

같은 시각, 사업전략팀 회의실

이번 건
반드시 해야 합니다.

대형 입찰 프로젝트

D-30

- ✓ 경쟁사 대비 선제 제안
 - ✓ 가격 전략 및 공급 조건 수립
- 제안서 완성 및 제출



경쟁사보다
먼저 제출해야 해...



가격 전략이
핵심인데...



수치 하나라도
틀리면 안 돼...

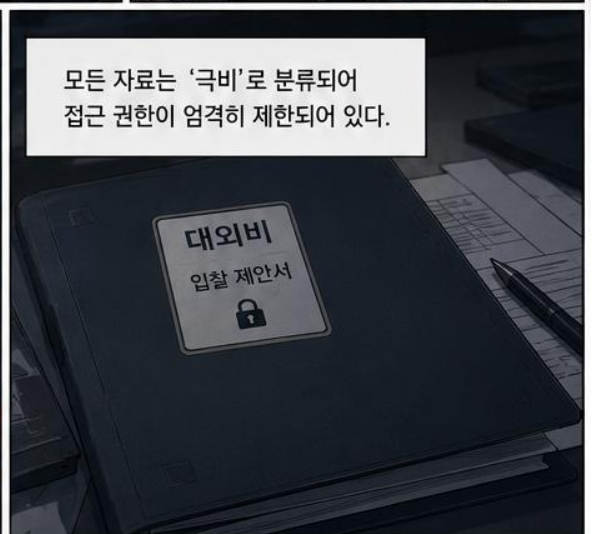


입찰 제안서 핵심 항목

- | | | |
|----|----------------|----|
| 01 | 가격 정책 및 수익 구조 | 극비 |
| 02 | 공급 조건 및 일정 | 극비 |
| 03 | 협력사 단가표 | 극비 |
| 04 | 리스크 분석 및 대응 방안 | 극비 |

대외비

모든 자료는 '극비'로 분류되어
접근 권한이 엄격히 제한되어 있다.



대형 입찰 프로젝트, 모든 정보는 극비! 단 하나의 실수도 용납되지 않는다.

그날 오후, ERP 운영 담당자는 인사팀으로부터 메일 한 통을 받는다.

✉ 메일

보낸 사람 인사팀
받는 사람 ERP 운영 담당자
제목 지난달 퇴사자 계정 정리 현황 요청드립니다.

안녕하세요.
지난달 퇴사자 계정 정리 현황을 확인 부탁드립니다.
감사합니다.

담당자는 시스템을 조회한다.

ERP 계정 관리 시스템

사용자 검색 김현우

검색

이름	김현우	계정 상태	활성화
부서	사업전략팀	권한	일반사용자
직급	대리	최종 로그인	2025-05-15 07:12
입사일	2021-03-02	MFA 등록	등록됨
퇴사일	2025-04-15		

어?
김현우 대리...
계정 상태가
활성화?

이름	김현우	계정 상태	활성화
부서	사업전략팀	권한	일반사용자
직급	대리	최종 로그인	2025-05-15 07:12
입사일	2021-03-02	MFA 등록	등록됨
퇴사일	2025-04-15		

퇴사일은 한 달 전.
그런데 계정은 여전히 활성화였다.



여기서 잠깐!

퇴사 처리 후에도 계정이 남아있으면, 권한이 그대로 유지되어 내부 정보 유출의 위험이 발생할 수 있습니다!

퇴사자 계정 관리 체크 포인트

- 퇴사 사실 통보
- 계정 비활성화/삭제
- 권한 회수 확인

4 충격적인 발견

담당자는 로그와 계정 정보를 더 자세히 확인한다.



사용자 상세 정보



김현우 대리

계정 활성화

부서 : 사업전략팀
 직급 : 대리
 입사일 : 2021-03-02
 퇴사일 : 2025-04-15
 최종 로그인 : 2025-05-15 07:12

계정 상태 : **활성화**
 접근 권한 : 일반사용자
 MFA 등록 : 등록됨



로그 기록을 조회하자, 퇴사 이후에도 다양한 시스템에 접속한 흔적이 확인된다.

접속 로그 조회 결과

일시	접속 시스템	접속 유형	접속 IP	결과
2025-04-16 07:12	VPN	로그인	10.10.15.23	✓ 성공
2025-04-16 07:15	이메일	웹 접속	10.10.15.23	✓ 성공
2025-04-16 07:18	그룹웨어	접속	10.10.15.23	✓ 성공
2025-04-16 07:25	파일 서버	폴더 접근	10.10.15.23	✓ 성공
2025-04-16 07:27	파일 서버	파일 다운로드	10.10.15.23	✓ 성공
...
2025-05-15 07:12	VPN	로그인	10.10.15.23	✓ 성공



퇴사 이후에도 계정이 그대로 활성 상태로 유지되고 있었다.



퇴사자 계정
(김현우 대리)



- ✓ VPN 접속 가능
- ✓ 이메일 이용 가능
- ✓ 파일 열람/다운로드 가능
- ✓ 그룹웨어 접근 가능

접근 권한 그대로 유지

! 계정이 살아있는 동안, 내부 정보를 자유롭게 접근하고 가져갈 수 있는 상태였다.

누군가 회사의 핵심 정보를 마음껏 가져갈 수 있었던 상황.



! 내부 정보 유출 위험 심각



퇴사자 계정이 그대로 살아있으면, 회사의 핵심 정보가 무방비로 노출됩니다.

- #퇴사자 계정
- #계정 활성화
- #접근 권한
- #내부 정보 유출
- #로그 분석

5 과거 접속 기록 확인

담당자는 과거 로그를 다시 조회하기 시작한다.

퇴사 이후에도 계속 접속하고 있는데...?

로그 조회

사용자: 김현우
 기간: 2025-04-01 ~ 2025-05-15
 [조회]

접속 이력 요약

총 접속 일수	총 로그인 횟수	접속 시스템	다운로드 용량
23일	87회	6개	18.0 GB

퇴사한 다음 날부터 끊임없이 접속한 기록이 이어진다.



접속 경로

- VPN 접속 87회
- 메일 접속 31회
- 그룹웨어 접속 18회
- 파일 서버 접근 53회
- ERP 시스템 접근 22회

모든 접근이 정상으로 처리됐어...?

주요 시스템 접속 현황

- 메일 시스템 ✔ 정상
- 그룹웨어 ✔ 정상
- 파일 서버 ✔ 정상
- ERP 시스템 ✔ 정상
- 문서관리 시스템 ✔ 정상
- 전자결재 시스템 ✔ 정상

차단된 기록이 단 한 건도 없다고...?

최근 접속 기록 (일부)

일시	접속 시스템	결과
2025-05-14 09:12	VPN	✔ 성공
2025-05-14 09:18	메일	✔ 성공
2025-05-14 09:25	파일 서버	✔ 성공
2025-05-14 10:03	ERP	✔ 성공
...
2025-05-15 07:12	VPN	✔ 성공

최근까지도 접속했네...

퇴사일 이후, 단 하루도 빠짐없이 접속이 이어졌다.

**이럴 수가...!
아무 조치도 없었다고?**



퇴사자 계정이 그대로 남아 있으면, 언제나 내부 시스템에 접근할 수 있습니다.

#퇴사자 계정

#지속 접속

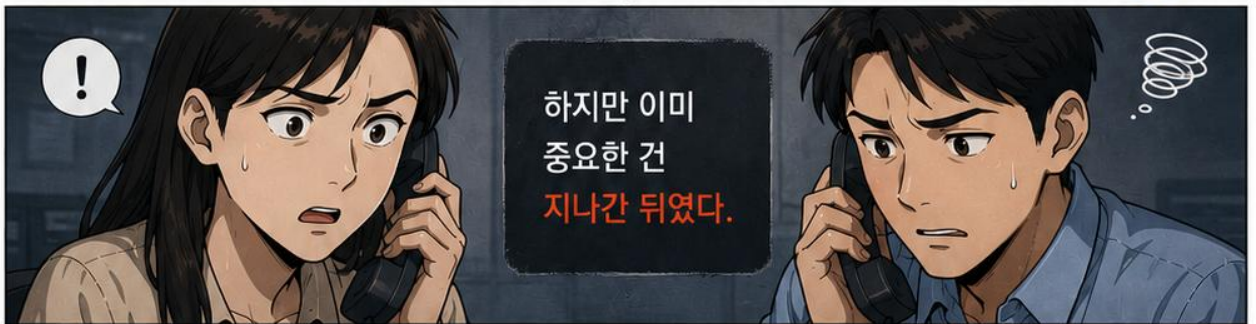
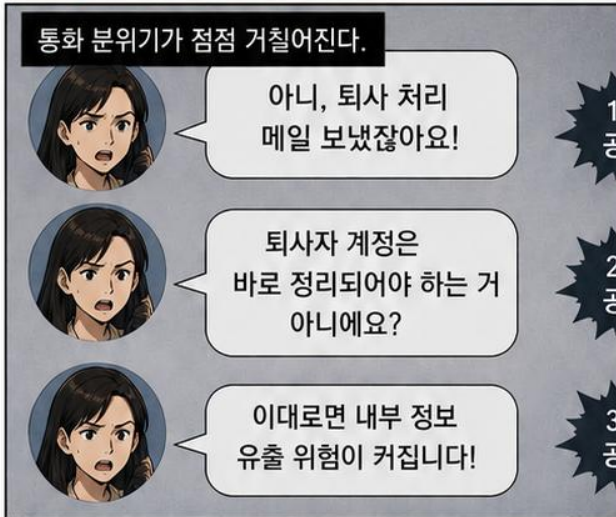
#계정 활성화

#접근 권한

#로그 분석

#내부 정보 유출

6 인사팀 vs 운영팀 통화



부서 간 인계·협업 절차가 명확하지 않으면, 퇴사자 계정은 그대로 남아 위험이 됩니다.

- 퇴사 통보
- 계정 종료 요청
- 권한 회수
- 시스템 반영 확인



퇴사 처리의 마지막 단계는 '계정 종료 및 권한 회수'입니다.

7 보안팀 긴급 분석

보안팀은 즉시 로그 분석을 시작한다.



긴급 분석 결과

내부 정보 유출 가능성 높음

퇴사 후 첫 로그인 시점
2025-04-16 07:12

접속 위치
국내 ISP 회선

총 다운로드 용량
18.0 GB

다운로드한 주요 문서 목록

파일명	문서 유형	용량
신규 사업 전략 문서	내부 전략	4.2 GB
가격 정책 자료	영업 기밀	3.6 GB
협력사 단가표	영업 기밀	2.8 GB
입찰 제안서 초안	입찰 자료	5.1 GB
내부 조직 개편안	내부 문서	2.3 GB
...

총 다운로드 용량 **18.0 GB**

이 정도면...
거의 사업부
전체 자료잖아!

퇴사 후에도 정상 권한으로
모든 시스템에 접근하고, 대용량
자료를 다운로드했다.

접속 타임라인 (퇴사 이후)

- 04-16 07:12 • VPN 접속 ✓ 성공
- 04-16 07:15 • 이메일 접속 ✓ 성공
- 04-16 07:18 • 그룹웨어 접속 ✓ 성공
- 04-16 07:25 • 파일 서버 접근 ✓ 성공
- 04-16 07:27 • 파일 다운로드 시작 ✓ 성공
- ...
- 05-15 07:12 • VPN 접속(마지막) ✓ 성공

하루, 이틀, 일주일...
아무 차단 없이 계속 접속했다.

주요 접근 시스템



김현우 대리
(퇴사자 계정)

- 이메일 시스템 정상 접근
- 그룹웨어 정상 접근
- 파일 서버 정상 접근
- ERP 시스템 정상 접근
- 문서관리 시스템 정상 접근

퇴사자 계정이 남아 있어, 현직 직원과 동일한 권한을 사용했다.

18.0 GB의
내부 정보가 유출되었다.



퇴사 후에도 계정이 남아 있으면,
중요 정보는 언제든지 외부로 유출될 수 있습니다.

#퇴사자 계정

#권한 회수

#로그 분석

#접근 권한

#내부 정보 유출

#계정 관리

8 경쟁사 제안서 비교

보안팀은 유출된 자료가 경쟁사 제안서에 반영되었을 가능성을 확인하기 시작한다.



유출 의심 자료

입찰 제안서 초안_v3.pptx
최종 수정일 : 2025-04-10 22:47

2025년 A 프로젝트 제안서 (초안)

3. 제안 범위

- 시스템 통합 및 구축
- 데이터 이관
- 유지보수 3년



경쟁사에서 제출한 제안서의 내용과 유사한 부분이 다수 발견된다.

당사 제안서 (초안)

3. 제안 범위

- 시스템 통합 및 구축
- 데이터 이관
- 유지보수 3년



4. 추진 일정

분석 2주 설계 3주 구축 8주 운영 3년

경쟁사 제안서

3. 제안 범위

- 시스템 통합 및 구축
- 데이터 이관
- 유지보수 3년



4. 추진 일정

분석 2주 설계 3주 구축 8주 운영 3년



내용은 물론,
오탈자까지
똑같다고...?



동일한 오탈자/표현 비교

당사 제안서 (초안)

5. 기대 효과

- 운영 효율성 향상
- 비용 절감 효과
- 고객 만족도 제고
- (**응답속도** 개선)

경쟁사 제안서

5. 기대 효과

- 운영 효율성 향상
- 비용 절감 효과
- 고객 만족도 제고
- (**응답속도** 개선)



내부 자료가 외부로 유출되어
경쟁사 제안서에 반영된 정황 확인!



퇴사자 계정이 남아있으면,
핵심 정보가 경쟁력을 잃고 회사의 신뢰가 무너집니다.



내부 문서 유출은 곧
기업의 경쟁력 손실로 이어집니다.

#내부 정보 유출

#퇴사자 계정

#접근 권한

#경쟁사 유출

#정보보호

#로그 분석

9 긴급 임원회의

경쟁사 유출 정황이 확인되자, 임원회의가 긴급 소집되었다.



핵심 쟁점

퇴사자 계정 관리 실패



회사 후에도 계정이 활성 상태로 유지됨

권한 회수 미흡



접근 권한이 그대로 남아 모든 시스템 이용 가능

부서 간 책임 공백



인사팀과 운영팀 사이 요청·확인 절차 부재

내부 정보 유출 위험



핵심 문서 유출 가능성으로 회사 신뢰·매출 타격 우려



단 한 개의 계정, 단 한 번의 누락이 회사 전체를 위협할 수 있습니다.

계정 관리와 권한 회수는 선택이 아닌 필수입니다.



10 사고 원인 정리

조사 결과, 사고의 원인은 명확한 '책임 공백'이었다.

인사팀

IT 운영팀

퇴사자
공지 메일
발송했어요.

보냈으니
이제 끝!

계정, 권한
회수 요청은
안 들어왔는데요?

요청 없으면
그대로
유지하는 게
원칙이지.

**책임
공백**

누구도 악의가 없었지만, 결과는 심각했다.

퇴사자 계정은
정리되지 않았고,



계정 활성화 상태 유지

계정, 권한 회수 요청은
그대로 남아,



접근 권한 회수 누락

퇴사 이후에도
지속적인 접속이
가능했고,



로그인 · VPN 접속 가능

내부 정보에 대한
접근이 자유로웠다.



내부 정보 접근 가능

“보냈다”와 “안 받았다” 사이에서,
회사의 핵심 정보가 유출될 수 있는 길이 열려 있었다.



사고 원인 핵심 요약

- | | | | | | |
|---|--|--------|-----------------------------|---|---------------|
| 1 | | 인사팀 | 퇴사자 공지 메일 발송 | → | 요청이 전달되었다고 판단 |
| 2 | | IT 운영팀 | 계정, 권한 회수 요청 메일 미수신 | → | 요청 없음으로 계정 유지 |
| 3 | | 퇴사자 계정 | 계정 상태 '활성화' 유지 | → | 접근 권한 회수되지 않음 |
| 4 | | 결과 | 퇴사 후에도 시스템 접속 및 내부 정보 접근 가능 | → | 정보 유출 위험 발생 |



업무 처리의 '착각'이 만든 책임 공백이
회사의 핵심 정보를 위협합니다.

- 퇴사자 계정 관리 절차 명확화
- 계정 종료 및 권한 회수 확인 프로세스 필수
- 부서 간 커뮤니케이션 및 기록 관리 강화

11 추가 분석 결과

보안팀은 추가 분석을 통해, 퇴사자 계정이 그대로 활용되고 있었음을 확인했다.




MFA도 살아 있고, 비밀번호도 그대로... 권한까지 모두 유지?

퇴사자 계정 추가 분석 결과

김현우 대리 퇴사자 계정

퇴사일 : 2025-04-15
최종 로그인 : 2025-05-15 07:12

🔒 **MFA 기기 유지**




등록된 MFA 기기가 여전히 활성 상태

🔑 **비밀번호 변경 없음**


퇴사 이후에도 비밀번호 변경 기록 없음

👤 **권한 회수 없음**



파일 서버, 그룹웨어 등 접근 권한 그대로 유지

MFA 기기 상태 확인



퇴사 후에도 MFA 승인이 가능했던 거야?

⚠️ MFA 기기 회수 절차 누락

비밀번호 변경 이력

변경 일시	변경자	변경 결과
2025-03-02	김현우	성공
2025-03-15	김현우	성공
2025-04-01	김현우	성공
2025-04-15	-	-
2025-05-15	-	-

퇴사일 이후로 변경 기록이 전혀 없어...

⚠️ 비밀번호 변경 및 무효화 미실시

계정 권한 현황

시스템	권한 상태
파일 서버	읽기/쓰기
그룹웨어	관리자
ERP	사용자
메일 시스템	사용자
사내 메신저	사용자
...	...

민감 시스템까지 모두 접근 가능 상태였어...

⚠️ 권한 회수 절차 누락



누군가의 부주의가 만든 작은 틈, 그 틈으로 퇴사자는 아무런 제약 없이 회사의 핵심 정보에 접근할 수 있었다.

퇴사자 계정, 반드시 다음 사항을 확인하세요!

🔒 **MFA 기기 회수 확인**

등록된 MFA 기기 반드시 회수

🔑 **비밀번호 변경/무효화**

퇴사 즉시 비밀번호 변경 또는 무효화

👤 **접근 권한 회수**

모든 시스템의 접근 권한 즉시 회수

🔍 **로그 모니터링 강화**

퇴사 이후 비정상 접근 지속 모니터링

퇴사자의 계정을 방치하는 순간, 내부 정보 유출은 현실이 됩니다!
계정 관리의 작은 실수가, 회사의 미래를 위협합니다.

12 교훈과 마무리

침입은 늘
외부에서 시작되지 않는다.

때로는, 우리의 부주의한
'내부 관리 공백'에서
시작된다.

로그 분석 대시보드

⚠ 퇴사자 계정 접근 탐지
위험도: HIGH

- VPN 접속
- MFA 인증 성공
- 파일 접근
- 데이터 다운로드

계정 상태

김현우 대리

계정 활성화

권한: 전체 접근

퇴사일: 2025-04-15

접속 로그 요약

사용하지 않는
계정은
가장 위험한
계정이다.

퇴사한 그날, 계정은
비활성화 되어야 한다.

퇴사자 계정 관리 미흡

퇴사 처리 후에도
계정이 활성화 상태로
남아 있었다.



김현우 대리
퇴사일: 2025-04-15

계정 활성화



권한 회수 누락

시스템 접근 권한과
데이터 접근 권한이
회수되지 않았다.



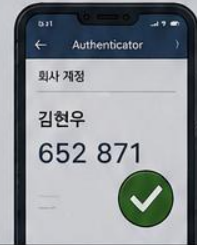
부서 간 책임 공백

인사팀과 운영팀의
커뮤니케이션 부재로
책임이 공백이 생겼다.



MFA 및 보안 통제 미흡

MFA 기기 유지, 비밀번호 변경
없음으로 내부자처럼
접근이 가능했다.



보안은 기술이 아닌,
'관리의 완성도'에서 결정된다.

퇴사자 계정
권한 회수
MFA 관리
접근 통제
로그 분석

우리가 반드시 기억해야 할 교훈



퇴사 처리는 **'메일 발송'**으로 끝나지 않습니다.



계정 종료와 **권한 회수**는 반드시 확인되어야 합니다.



사용하지 않는 계정은 **가장 위험한 계정**입니다.



내부 계정 관리 부주의는 **대규모 정보유출**로 이어질 수 있습니다.



지금 바로, **퇴사자 계정 관리 프로세스**를 점검하세요!
우리의 작은 관심이 회사를 지키는 가장 확실한 보안입니다.