CREMIT RESEARCH

NHI 보안 플레이북

비인간 ID(Non-Human Identity)를 찾고, 고치고, 관리하기 위한 실무 레퍼런스

2026 Q2 에디션 · cremit.io

목차

> **이 문서의 독자**
>
> 보안 엔지니어, DevSecOps 리드, CISO, 플랫폼 팀. API 키·서비스 계정·OAuth 토큰이 인간 사용자보다 45배 많은데 거버넌스 로드맵에 올라간 적 없는 조직을 위한 레퍼런스입니다.

PART 1

NHI 보안 문제란 무엇인가?

비인간 ID(NHI)는 사람이 아니라 워크로드를 인증하는 모든 크리덴셜, 키, 식별자를 의미합니다. 카테고리는 생각보다 넓습니다.

- **서비스 계정** — 작업 실행용 IAM 사용자/역할
- **API 키** — Stripe, Slack, OpenAI 등이 발행한 정적 문자열
- **액세스 토큰** — OAuth 베어러, JWT, 리프레시 토큰
- **머신 인증서** — mTLS, 코드 서명, 디바이스 인증서
- **SSH 키** — 배포 키, CI 러너 키
- **클라우드 워크로드 ID** — AWS IAM Role, GCP 서비스 계정, K8s ServiceAccount
- **Webhook 시크릿**, **DB 크리덴셜**, **AI 에이전트 크리덴셜**

공통점: 사람이 비밀번호를 타이핑하지 않는다는 것. 이 하나의 사실이 많은 전제를 무너뜨립니다. API 호출에 MFA를 걸 수 없고, 로그만 봐서는 누가 실제로 키를 쓰고 있는지 알 수 없습니다.

지금 NHI가 중요한 이유

지난 5년간 세 가지 흐름이 겹쳤습니다. **SaaS 스프롤**(평균 엔터프라이즈가 130개 이상의 앱을 운영, 각각 독자적 NHI 풋프린트), **마이크로서비스**(모놀리스가 하나의 크리덴셜로 처리하던 자리에 수백 개의 서비스 간 크리덴셜), **AI 에이전트**(2년 전에는 거의 존재하지 않았던 새 NHI 클래스).

> **"45:1"의 실제 모습**
>
> AWS, GitHub, SaaS 80여 개를 쓰는 2,000명 규모 엔지니어링 조직: **약 2,000명의 인간, 약 40,000건의 SaaS 그랜트, 90,000개 이상의 활성 NHI**. 보수적 수치입니다.

알아야 할 숫자들

2,380만
2024년 공개 GitHub 탐지 시크릿 건수 (YoY +25%) — GitGuardian State of Secrets Sprawl 2025

5년
Toyota 액세스 키가 공개 저장소에 방치된 기간. 296,019명 고객 정보 노출로 이어짐

70%+
최근 3년간 클라우드 침해 중 체인 어딘가에 NHI 손상이 포함된 비율

사례: TOYOTA 타임라인

액세스 키가 공개 저장소에 커밋됐고, 당시 시크릿 스캐닝은 잡아내지 못했습니다. 키는 고객 데이터 서비스 인증에 쓰였고, 약 5년간 유효했습니다. 노출이 최종적으로 공개됐을 때 약 30만 명에게 고지가 필요했습니다. 2부의 Kill Chain 단계가 이 단일 사건에 전부 등장합니다.

전체 플레이북(4-5페이지)에서 이어집니다: Uber 2016 사건, 중간 회전 시간, Stripe/Slack 케이스 분석.

PART 2

NHI Kill Chain

NHI Kill Chain은 비인간 ID가 실무에서 무너지는 가장 흔한 9가지 방식의 택소노미입니다. 이론적 위협 모델이 아니라 실제 사건과 대응 경험에서 도출된 패턴 언어입니다.

각 패턴은 이름, 한 문장 정의, 발생 이유, 환경에서 볼 탐지 신호, 다음 리뷰에서 꺼낼 핵심 질문 구조를 따릅니다.

9가지 NHI Kill Chain 패턴. 5번 Zombie는 가장 탐지가 덜 되는 실패 유형입니다.

패턴 1-3

1 Ghost Key (고스트 키)

아무도 생성하거나 소유하거나 기억하지 않는 크리덴셜이 환경에 존재한다.

발생 이유: M&A, 계약직, 일회성 PoC, 사장된 프로젝트가 맥락보다 오래 남는 크리덴셜을 남깁니다.

탐지 신호: 소유자 필드 없는 IAM 사용자, 티켓이나 런북 없는 서비스 계정, 현 SRE 팀 합류 이전부터 회전되지 않은 키.

> "우리 환경의 모든 권한 있는 크리덴셜에 대해, 그 키가 무엇을 하고 왜 존재하는지 오늘 답할 수 있는 사람이 있습니까?"

2 Shadow Key (섀도 키)

보안/플랫폼 팀이 존재 자체를 모르는 크리덴셜이 존재한다.

발생 이유: 승인 워크플로 밖에서 생성 — 개인 PAT, 자체 발행 웹훅 시크릿, 현업에서 승인된 OAuth 그랜트.

탐지 신호: org 전역 스코프 PAT, SaaS 관리자 콘솔의 미검토 OAuth 그랜트.

> "활성 NHI 리스트의 단일 출처는 무엇이고, 그것이 완전하다는 확신은 얼마나 됩니까?"

3 Aged Key (에이지드 키)

원래 보안 수준이 더 이상 신뢰 가능하지 않을 만큼 오래 유효한 크리덴셜이다.

발생 이유: 회전은 고통스럽습니다. 팀이 미루고, 1년 넘은 키는 영구 존재로 굳어집니다.

> "프로덕션 크리덴셜의 허용 가능한 최대 수명은 얼마이고, 오늘 그것을 초과하는 크리덴셜은 몇 개입니까?"

패턴 4-6

4 Over-shared Key (오버-셰어드 키)

단일 크리덴셜이 너무 많은 시스템에 중복돼 회전이 운영적으로 불가능하다.

> **필드 노트**
> Series B 핀테크의 프로덕션 Stripe 시크릿이 14개 위치에 존재 — 퇴사자 2명의 노트북, 2023년 Slack 고정 메시지, Confluence 런북, 계약직의 Dockerfile 포함. 회전 조율에만 6주가 걸렸습니다.

> "가장 중요한 프로덕션 시크릿을 오늘 회전하면 몇 개 시스템이 깨질지 알고 있습니까?"

5 Zombie Key (좀비 키) (가장 탐지가 덜 되는 패턴)

스캐너에서는 resolved인데, 공급자에서는 여전히 유효한 크리덴셜이다.

발생 이유: 엔지니어가 소스에서 문자열을 제거하고 알림을 닫지만, IdP에서 폐기하지 않습니다. 스캐너는 만족, 키는 여전히 받아들여집니다.

> "유출 크리덴셜 발견을 닫을 때, 공급자 측 폐기가 필수 단계입니까?"

6 Drifted Key (드리프티드 키)

타이트한 스코프로 프로비저닝됐으나, 실효 권한이 조용히 확장됐다.

탐지 신호: 생성 시점보다 부착 정책이 늘어난 IAM Role, 명시 용도와 무관한 능력을 가진 서비스 계정.

> "가장 많이 쓰이는 상위 20개 서비스 계정의 실효 권한을 마지막으로 리뷰한 것이 언제입니까?"

패턴 7-9

7 Public Key (퍼블릭 키)

스캐너가 도달할 수 있는 공개 위치에 크리덴셜이 존재한다.

우발적 git 푸시, 잘못 구성된 버킷, 공개 Postman 컬렉션, 서버 사이드 키가 박힌 클라이언트 JS 번들, 컴파일 모바일 앱. 대부분 조직은 이미 해결했다고 착각하지만, 2024년 공개 GitHub 2,380만 건은 그 반대를 말합니다.

8 Unattributed Key (언어트리뷰티드 키)

활성 사용 중이지만, 관측 스택이 어떤 워크로드/누구의 책임인지 말해주지 못하는 크리덴셜이다.

> "가장 권한 높은 NHI가 한 시간 안에 악용된다면, 워크로드/소유자를 식별하는 데 얼마나 걸립니까?"

9 Governance Gap (거버넌스 갭)

NHI 거버넌스의 구조적 부재.

대부분 조직에 NHI 보안의 단일 책임자가 없습니다. 사람 ID는 IAM, 엔드포인트는 보안 팀, 클라우드는 플랫폼 팀 — NHI는 그 사이 갭에 떨어져 있습니다. 지정 소유자가 없으면 앞의 여덟 패턴이 체계적으로 고쳐질 수 없습니다.

NHI Kill Chain 한눈에 보기

1페이지 레퍼런스. 인쇄해서 붙여두세요.

#	패턴	정의	주요 탐지 신호
1	Ghost Key	소유자 불명 크리덴셜	소유자 필드 없음, 폐기 프로젝트 이름
2	Shadow Key	보안/플랫폼이 모르는 크리덴셜	미검토 OAuth 그랜트, org 스코프 PAT
3	Aged Key	신뢰 윈도우 초과 수명	12개월 초과 생성일, 회전 이력 없음
4	Over-shared Key	너무 많은 시스템에 복제	여러 저장소에 동일 시크릿 해시
5	Zombie Key	스캐너는 resolved, 공급자는 유효	IdP 폐기 없는 "Resolved" 알림
6	Drifted Key	조용히 권한 확장	프로비저닝 후 추가된 IAM 정책
7	Public Key	스캐너 도달 가능한 공개 위치	공개 소스 시크릿 스캐닝 알림
8	Unattributed Key	워크로드 귀속 불가 활성 크리덴셜	워크로드 메타 없는 인증 로그
9	Governance Gap	NHI 보안 책임자 부재	팀 간 갭에 떨어진 책임

PART 3

"Out of Scope" 문제

버그 바운티 프로그램은 exploit-chain 취약점을 위해 설계됐습니다. 크리덴셜 노출은 CVSS에 맞지 않습니다. 연구자가 노출된 조직 크리덴셜을 보고하면 예측 가능한 결과가 나옵니다. "out of scope"로 분류되고 기각됩니다.

> **사례 1 — SLACK BOT TOKEN**
>
> 공개 GitHub 저장소에 **3년간** 존재. 조직 전반 채널·파일 접근 허용. 공식 버그 바운티로 신고. 분류: **out of scope**. 실제 조치: 조직이 조용히 키를 폐기하고 광범위 리뷰까지 수행했습니다.

> **사례 2 — ASANA ADMIN API KEY**
>
> 전체 워크스페이스 읽기/쓰기 권한으로 **2년간** 노출. 공식 버그 바운티 신고. 분류: **out of scope** (통합된 별도 법인 기원). 실제 조치: 역시 폐기.

왜 반복되는가

1. **CVSS가 맞지 않습니다.** Exploit chain도, 공격 복잡도도, 필요 권한도 없음 — 크리덴셜 자체가 액세스입니다.
2. **"그거 misconfiguration이잖아."** 그러나 RCE도 나쁜 코드의 결과이고, 우리는 RCE를 원인이 아닌 영향으로 평가합니다. 이중 잣대가 성립하지 않습니다.
3. **시간이 보이지 않습니다.** 3년 노출이 어제 유출과 동일한 점수를 받습니다.

NHI Exposure Severity Index

CVSS의 보완 프레임워크. 실제 발견된 크리덴셜 평가에 특화된 6축 모델. 각 축은 1~5 점수.

축	측정 대상	Slack 사례
Privilege Scope	읽기 전용 → 무제한 관리자	4
Cumulative Risk Duration	24시간 미만 → 다년 노출	5
Blast Radius	단일 리소스 → 다조직 영향	4
Exposure Accessibility	인증 필요 → 공개 인덱싱	5
Data Sensitivity	공개 정보 → 규제 PII/시크릿	4
Lateral Movement Potential	격리 → 크로스 서비스 피벗	5

Slack 사례 합계: 27/30. 3개 이상 축이 4 또는 5면, 버그 바운티 트리아지 분류와 무관하게 Severity 1 사건입니다.

더 나은 스코프를 관철시키는 법

1. 조직 크리덴셜 노출을 명시적으로 프로그램 스코프에 포함시키세요.
2. 이 건들을 CVSS가 아니라 NHI Index를 쓰는 별도 트리아지 큐로 라우팅하세요.
3. 회전 SLA를 공개하세요 — 크리덴셜 노출을 진지하게 다룬다는 가장 효과적인 공개 시그널입니다.

PART 4

한국 ISMS-P 크로스워크

ISMS-P 강화 인증기준은 2027 의무화가 다가오면서, 크리덴셜 관리·접근 통제·감사 로깅 영역에서 NHI Kill Chain 대응 체크리스트와 놀라울 만큼 겹칩니다.

Kill Chain 패턴	가장 가까운 ISMS-P 컨트롤 영역
Ghost Key	2.5.1 사용자 계정 관리 — 자산 소유자의 유일 식별
Shadow Key	2.5.2 사용자 식별 및 인증 — 인벤토리 완전성
Aged Key	2.5.4 비밀번호 관리 — 크리덴셜 생애주기·회전
Over-shared Key	2.5.3 사용자 접근권한 관리 — 최소권한·분리
Zombie Key	2.9.4 로그 및 접속기록 관리 + 2.5.1 — 폐기 증거
Drifted Key	2.5.5 접근통제 관리 — 주기적 권한 리뷰
Public Key	2.11.5 외부자 보안 + 2.10.6 업무용 단말기기 보안
Unattributed Key	2.9.2 성능·장애관리 + 2.9.4 — 로그 귀속
Governance Gap	1.1.1 경영진의 참여 + 1.1.2 최고책임자의 지정

2026년 준비 캘린더

- **Q2 2026 (지금):** NHI 인벤토리 수립. 불완전해도 없는 것보단 낫고, 심사원은 추세를 봅니다.
- **Q3 2026:** 최상위 권한 NHI 상위 20개 회전 구현, 회전 런북 문서화.
- **Q4 2026:** 감사 로그 귀속 갭 해소.
- **Q1 2027:** 내부 감사 수행, 외부 심사 전 갭 remediation.

PART 5

30-60-90 액션 플레이북

1주차 — 인벤토리

모든 클라우드 IAM 익스포트, 상위 10개 SaaS 활성 API 키, IdP의 OAuth 그랜트, 소스 컨트롤의 배포 키와 PAT. 단일 스프레드시트. 금요일에 CISO에게 전달할 수 있는 단일 목록. *완전성 > 세련됨.*

2주차 — 소유자 없는 것 식별

각 항목에 단일 인간 소유자를 이름으로 지정. 48시간 내에 지정할 수 없는 항목 플래그. 소유자 없는 크리덴셜 리스트 산출 — 즉시적 리스크 표면.

3주차 — 수명과 회전

생성일 기준 정렬. 12개월 초과 모든 크리덴셜: 최소 1회 회전 여부 확인 또는 예약. 매주 3개씩 회전하는 큐 가동.

4주차 — CI/CD와 노출 탐지

푸시 *및* 히스토리에 대한 시크릿 스캐닝. 공급자 측 폐기를 알림 닫힘 조건으로 요구(Zombie 패턴 차단). PR 리터럴 크리덴셜 차단 CI 정책.

30-60-90 로드맵

- **30일:** 인벤토리, 소유자 없는 리스트, Zombie 패턴 닫힘 워크플로 강화, aged key 회전 큐.
- **60일:** 프로덕션 NHI 소유권 100%, OAuth 리뷰 프로세스, 상위 20 회전 런북, 외부 모니터링.
- **90일:** 드리프트 탐지, 귀속 갭 해소, 버그 바운티 스코프 업데이트, 주간 Kill Chain 대시보드.

> **실제로 의미 있는 성공 지표**
>
> 소유자 없는 크리덴셜 수 → 0 수렴 · 12개월 이하 권한 크리덴셜 비율 >90% · 유출 탐지 후 평균 폐기 시간 <4시간 · Zombie 발견 = 0

PART 6

Cremit 소개

Cremit은 비인간 ID 문제에 집중하는 한국 보안 회사입니다. 주력 제품 **Argus**는 소스 컨트롤·CI/CD·SaaS·클라우드 전반에서 크리덴셜 노출을 찾고 귀속시키고 remediation하는 엔지니어링 팀을 위한 시크릿 탐지 및 NHI 거버넌스 플랫폼입니다.

Cremit Research는 NHI Kill Chain 시리즈, NHI Exposure Severity Index, 그리고 실제 크리덴셜 노출 사례에 대한 지속적 필드 분석을 발행하며, 그 상당 부분이 이 플레이북에 합성됐습니다.

NHI 갭을 닫을 준비가 되셨나요?

Argus를 14일간 무료로 사용해 보세요. GitHub 조직을 연결하면 1시간 내에 고스트·섀도·aged·over-shared·zombie 키의 랭킹 리스트를 받아보실 수 있습니다. 신용카드 불필요.

무료 체험 시작 →