

OWASP TOP 10 NON-HUMAN IDENTITY

John, Crime CEO



NICE TO MEET YOU

김동현

Cremit CEO / Founder

ex-Sendbird

11+ Cybersecurity Experience

DevSecOps, AuthZ, AuthN, NHI

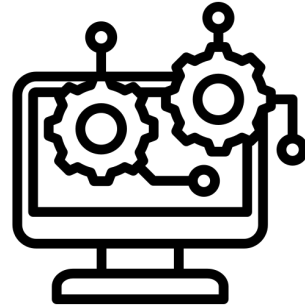
NON HUMAN IDENTITY?

API

APPLICATION

SERVICE

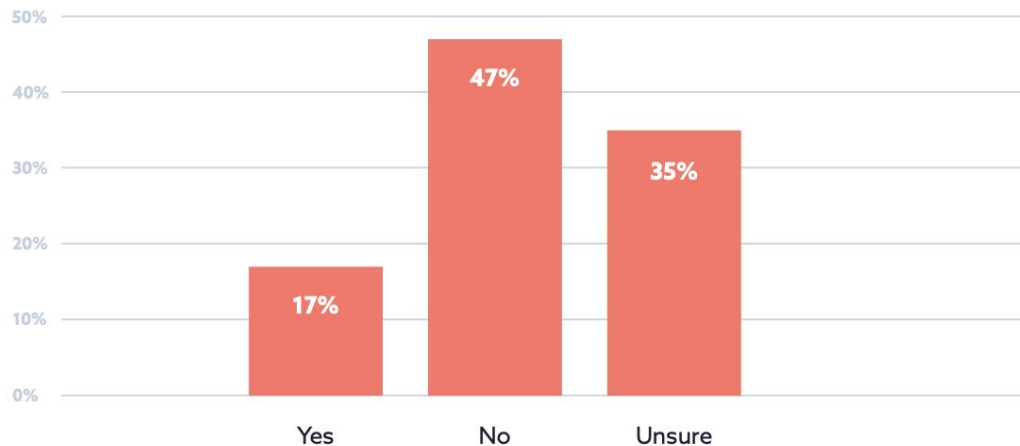
WORKLOAD



THE STATE OF NHI SECURITY




Experienced security incidents related to NHI



OWASP NHI TOP 10



PROJECTS CHAPTERS EVENTS ABOUT 

OWASP Non-Human Identities Top 10

[Main](#) [Join](#) [Contributors](#)

We're thrilled to introduce the [OWASP Non-Human Identities Top 10 for 2025!](#)

This comprehensive list highlights the most critical challenges in integrating Non-Human Identities (NHIs) into the development lifecycle, ranked based on exploitability, prevalence, detectability, and impact.

What is Non-Human Identities top 10?

The Non-human identity (NHI) top 10 is a comprehensive list of the most pressing security risks and vulnerabilities human identities present to organizations.

Non-Human Identities Top 10 Information

 Incubator Project

OWASP
DOCUMENTATION PROJECT

OWASP NHI TOP 10



Translate the introduction and NHI1 threat into Korean #18

Merged

TalAstrix merged 2 commits into `OWASP:main` from `ben-cremit:main` on Feb 6

Conversation 5

Commits 2

Checks 0

Files changed 2



ben-cremit commented on Feb 2

Start the Korean translation.

Hello. Dear OWASP contributors

My name is Ben and I founded and run an NHI security company in South Korea.

I'm glad to be able to contribute to OWASP, which I learnt a lot about as a student!



**NHI1:
IMPROPER
OFFBOARDING**

NHI1 취약점은 악용하기는 쉽지만, 탐지하고
보안하는건 매우 어렵습니다.

1.

사용 중지된 어플리케이션의
NHI를 폐기하지 않은 경우

2.

퇴사한 직원이 관리하던 NHI를
폐기하지 않은 경우

3.

퇴사한 직원이 접근 가능했던
NHI를 폐기하지 않은 경우

ATTACK SCENARIOS



THREAT NEWS



Singapore

Fired employee accessed company's computer 'test system' and deleted servers, causing it to lose S\$918,000

The 39-year-old man, who was "confused and upset" after being fired, deleted 180 virtual servers from NCS' computer system.

**NHI2:
SECRET
LEAKAGE**

API Key, token, webhook 등의 내부유출, 외부유출로 인한 incident가 지속적으로 발생하고 있습니다.

1.

AWS, Azure, GCP 등의 CSP 액세스 키 유출로 인한 사고

2.

Jira, Notion 등의 협업도구 API Key 유출로 인한 내부 자료 유출 사고

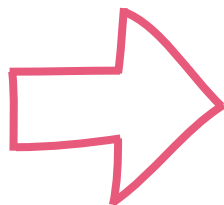
3.

Webhook 유출로 인해 C&C로 악용되는 사례

VERCEL FRONTEND LEAKAGE STATE RESEARCHED BY CREMIT

700,000 → 60,000 → 6,657

0.5%



```
5607: function(e, t, r) {  
  var s = r(7904);  
  r(3094),  
  new s.c({  
    region: "eu-west-2",  
    credentials: {  
      accessKeyId: "AKIARKLJLQFWX1",  
      secretAccessKey: "8xlBxPp8V!"  
    }  
  })  
},  
3094: function(e, t, r) {
```

THREAT

← Blog

38TB of data accidentally exposed by Microsoft AI researchers

Wiz Research found a data exposure incident on Microsoft's AI GitHub repository, including over 30,000 internal Microsoft Teams messages – all caused by one misconfigured SAS token



Hillai Ben-Sasson, Ronny Greenberg

September 18, 2023

10 minute read



31%

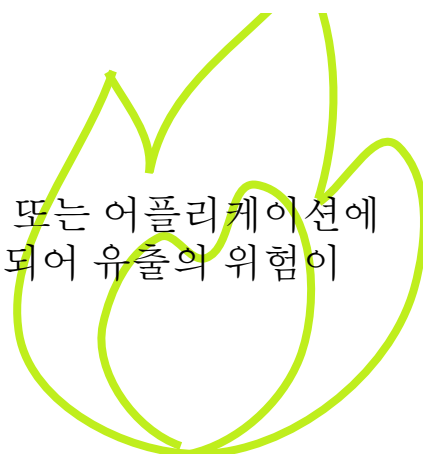
Secret 관리 부족으로 인한 사고

21%

초기 조치 중 Secret 관련한 작업 비율

37%

환경 변수 또는 어플리케이션에 하드코드 되어 유출의 위험이 있음



NHI3:

VULNERABLE

3-PARTY NHI

IDE Plugin, SaaS, 클라우드 연동 시 공급업체의 사고로 인한 NHI 유출이 발생할 수 있습니다

1.

Github, VSCode 내 존재하는
악성
어플리케이션/Plugin으로
인한 유출

2.

취약한 BI(Business Insights)
도구로 인한 내부 NHI 데이터
유출

3.

AWS, GCP, Azure 등
클라우드에 접근하기 위한
프로그램 / 취약 및 Supply
chain attack 사례

Beyond Security 유출로 인한 미국 재무부 해킹사고



24.12.05

이상행위 발견



24.12.08

API KEY 유출 확인



24.12.30

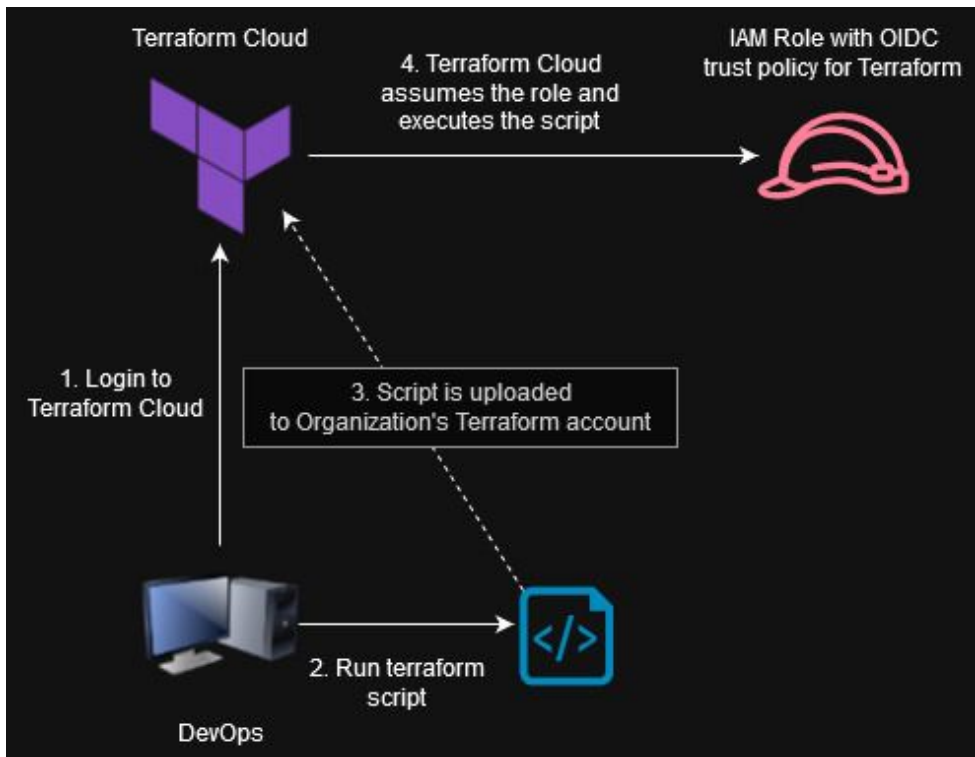
워크스테이션과 민감 자료가
외부로 반출된 것을 확인



**NH14:
INSECURE
AUTHENTICATION**

Provider	Documentation	Issuer/OIDC Provider URL	Policy State
Terraform Cloud	Terraform Docs	https://app.terraform.io	EnforceTrustedOIDC
GitLab	GitLab Docs ID Token Auth	https://gitlab.com	EnforceTrustedOIDC
IBM Turbonomic SaaS	IBM Docs IBM Docs Support Page	https://rh-oidc.s3.us-east-1.amazonaws.com/22ejnvnturfmt6km08idd0nt4hekbn7 https://rh-oidc.s3.us-east-1.amazonaws.com/23e3sd27sju1hoo6ohfs68vbno607tr https://rh-oidc.s3.us-east-1.amazonaws.com/23ne21h005qjl3n33d8dui5dlrmv2tmg https://rh-oidc.s3.us-east-1.amazonaws.com/24jrf12m5dj7ljfb4ta2frhrcoadm26 https://oidc.op1.openshiftapps.com/2f785sojlpb85i7402pk3qogugim5nfb https://oidc.op1.openshiftapps.com/2c51blsaqa9gkjt0o9rt11mle8mmropu	EnforceTrustedOIDC EnforceTrustedOIDC EnforceTrustedOIDC EnforceTrustedOIDC EnforceTrustedOIDC EnforceTrustedOIDC
Shisho.dev	Shisho Docs	https://tokens.cloud.shisho.dev	EnforceTrustedOIDC
Scalr	Scalr Docs	https://scalr.io	EnforceTrustedOIDC
GitHub Audit Log Streaming	GitHub Docs	https://oidc-configuration.audit-log.githubusercontent.com	EnforceTrustedOIDC

NH14: INSECURE AUTHENTICATION



1.

AWS IAM Role with OIDC를 생성 시 신뢰관계 정책을 Terraform Cloud에서 Assume하는걸 허용

2.

공격자는 다른 테넌트의 Terraform Cloud를 만들고, 해당 테넌트로 피해자의 Account 권한을 Assume

3.

테라폼 클라우드 내에서 악성행위 수행

**NHI5:
OVER-PRIVILEGED
NHI**

NHI5: OVER-PRIVILEGED NHI

NHI의 특성 상 과도한 권한을 부여 받는 경우가 많고, 유출사고 발생 시 광범위한 범위의 피해를 끼칠 수 있습니다.

50%

Azure Security State 2025 보고서에 따르면 50%는 Super Identity 입니다.

5X

Human Identity는 3400만개인 반면, NHI는 1.7억개 입니다.

17.6%

NHI는 모든 S3에 접근할 수 있는 권한을 가지고 있습니다.

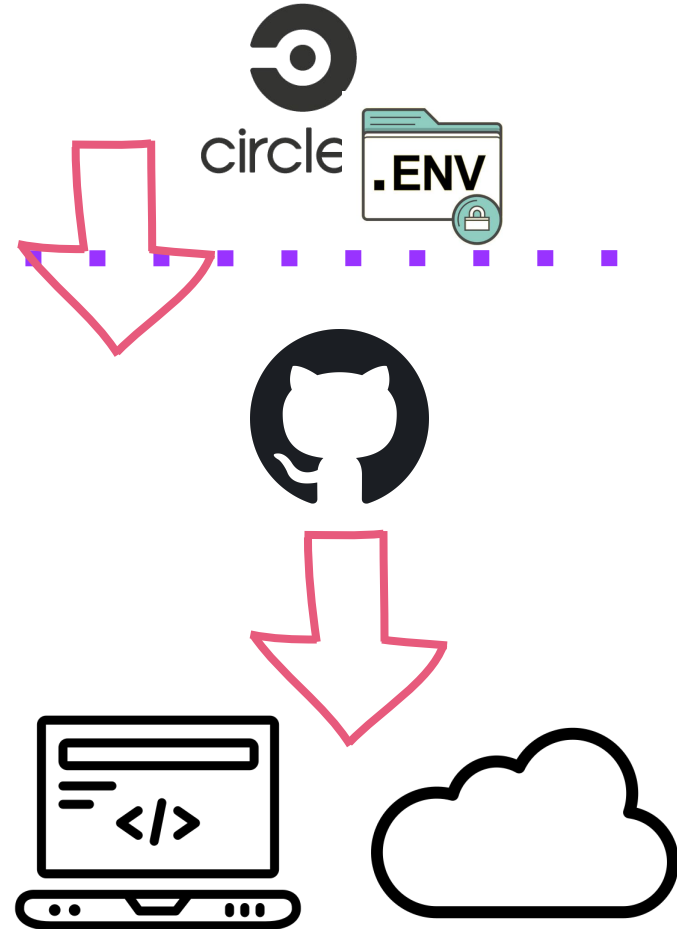
NHI5: OVER-PRIVILEGED NHI

CIRCLECI NEWS | JAN 12, 2023 | 13 MIN READ

CircleCI incident report for January 4, 2023 security incident



Rob Zuber
Chief Technology Officer



NHIG:

**INSECURE CLOUD
DEPLOYMENT
CONFIGURATION**

CI/CD 파이프라인 내 하드코딩된 Secret,
잘못된 구성을 통한 취약점이 발생할 수
있습니다.

발견가능성

32%

파급력

어려움, 조직 내 권한을 먼저
획득

구성 오류로 인한 사고 발생률

파이프라인 내 NHI, Secret은
일반적으로 매우 높은 권한을
부여받음

Select trusted entity Info

Trusted entity type

AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

Identity provider

gitlab.com



Create new

Audience

https://gitlab.com



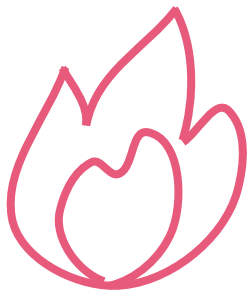
Condition - (optional)

Add condition

NH16: INSECURE CLOUD DEPLOYMENT CONFIGURATION

CI/CD 로그 상 확인

Secrets 변수에 접근 가능한
유저의 권한상승 가능



```
name: Deploy to AWS

on:
  push:
    branches:
      - main

jobs:
  deploy:
    runs-on: ubuntu-latest
    steps:
      - name: Checkout code
        uses: actions/checkout@v2

      - name: Configure AWS credentials
        uses: aws-actions/configure-aws-credentials@v2
        with:
          aws-access-key-id: ${ secrets.AWS_ACCESS_KEY_ID }
          aws-secret-access-key: ${ secrets.AWS_SECRET_ACCESS_KEY }
          aws-region: us-west-2

      - name: Deploy to S3
        run: aws s3 sync ./build s3://my-bucket
```



**NHI7:
LONG-LIVED
SECRETS**

장기적으로 사용되는 자격증명, Secret은
잠재적 위협/컴플라이언스 위반사항이 됩니다.

46%

AWS Cloud의 사용자 중 장기
자격증명을 사용하고 있는 비중

60%

주요 CSP사들의 자격증명 중
1년 이상 사용되는 비율

51%

자격증명 순환 주기를 관리하고
있지 않은 조직의 비율

rabbit data breach: all r1
responses ever given can be
downloaded



NHI7: LONG-LIVED SECRETS



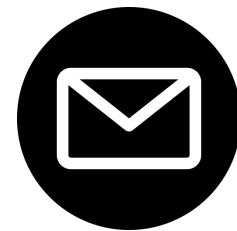
rabbit's response

we have internal confirmation that the rabbit team is aware of this leaking of api keys and have chosen to ignore it. the api keys continue to be valid as of writing.

IIElevenLabs



TWILIO
SendGrid



NHI8-9:

ENVIRONMENTS

ISOLATION, NHI

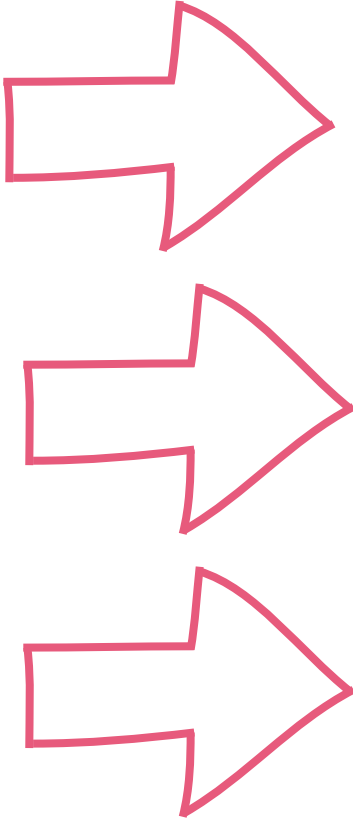
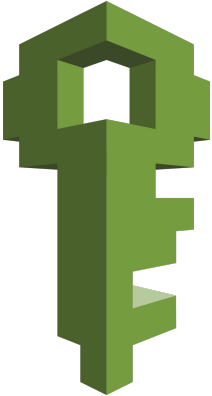
REUSE

NHI를 프러덕션/스테이징/개발환경에 관계 없이 섞어서 사용하는 경우 피해범위가 폭발적으로 확산될 수 있습니다.

32%






보안 사고의 원인이 된 경우

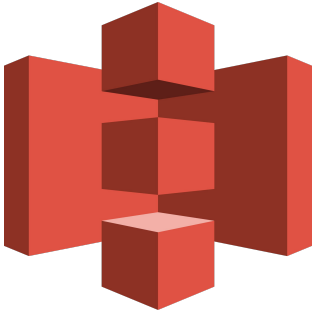
NHI8-9: ENVIRONMENTS ISOLATION, NHI RE-USE



AWS accounts (5)

Q Filter accounts by name, ID

- ▶  **Cremit APN**
- ▶  **cremit-develop**
- ▶  **cremit-prod**
- ▶  **cremit-staging**
- ▶  **Operation**





**NHI 10:
HUMAN USE OF NHI**

서비스/자동화/머신을 위한 Identity를 사람이 사용하며 공유/악용되는 사례

75%

서비스 계정 오용을 통해 보안 위협을 초래할 수 있게 된 비율

32%

사람이 사용하는 NHI를 탐지하기 어려워 하고 있는 조직의 비율

26%

과도한 권한을 가지고 있는 비율

Local code

You plan to use this access key to enable application code in a local development environment to access your AWS account.

 Application running on an AWS compute service

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

 Third-party service

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

 Application running outside AWS

You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

 Other

Your use case is not listed here.

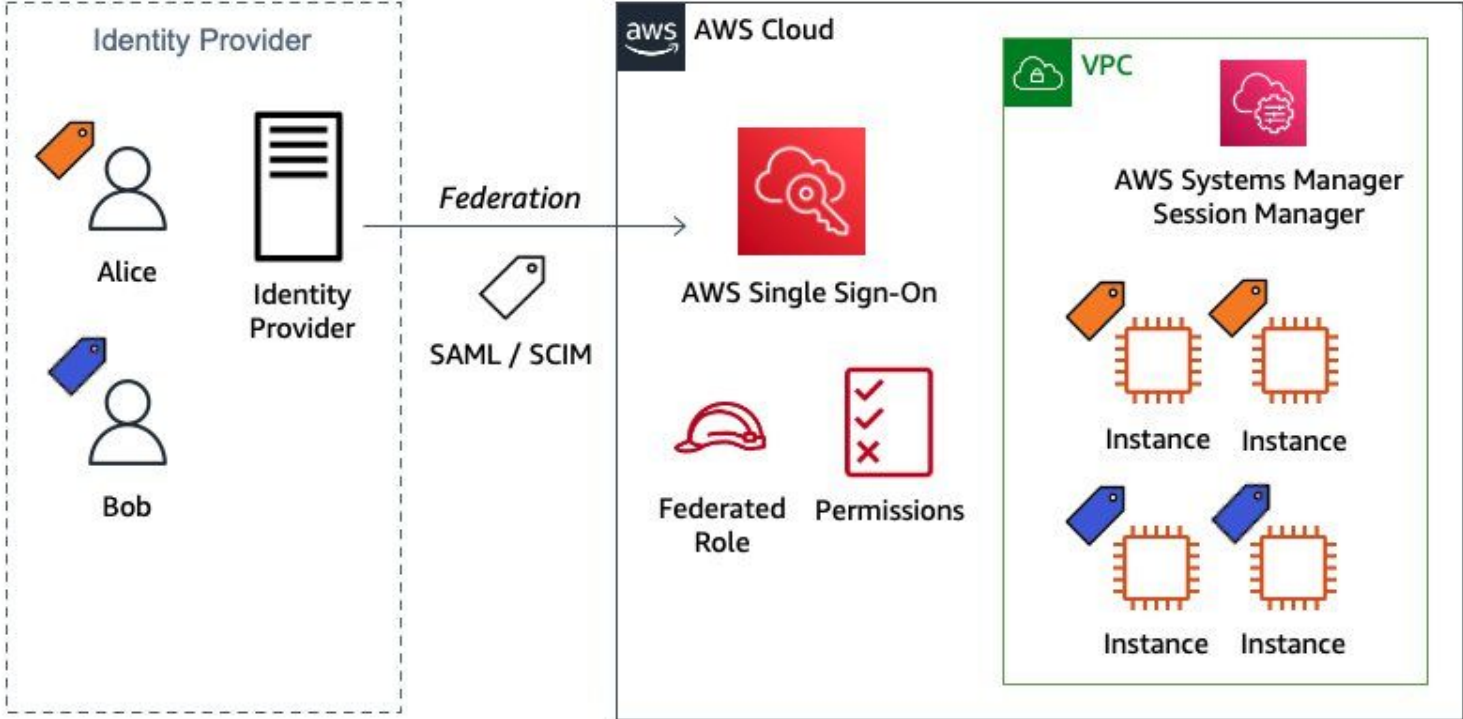
⚠ Alternative recommended

Use IAM Roles Anywhere to generate temporary security credentials for non AWS workloads accessing AWS services. [Learn more about providing access for non AWS workloads.](#) [↗](#)

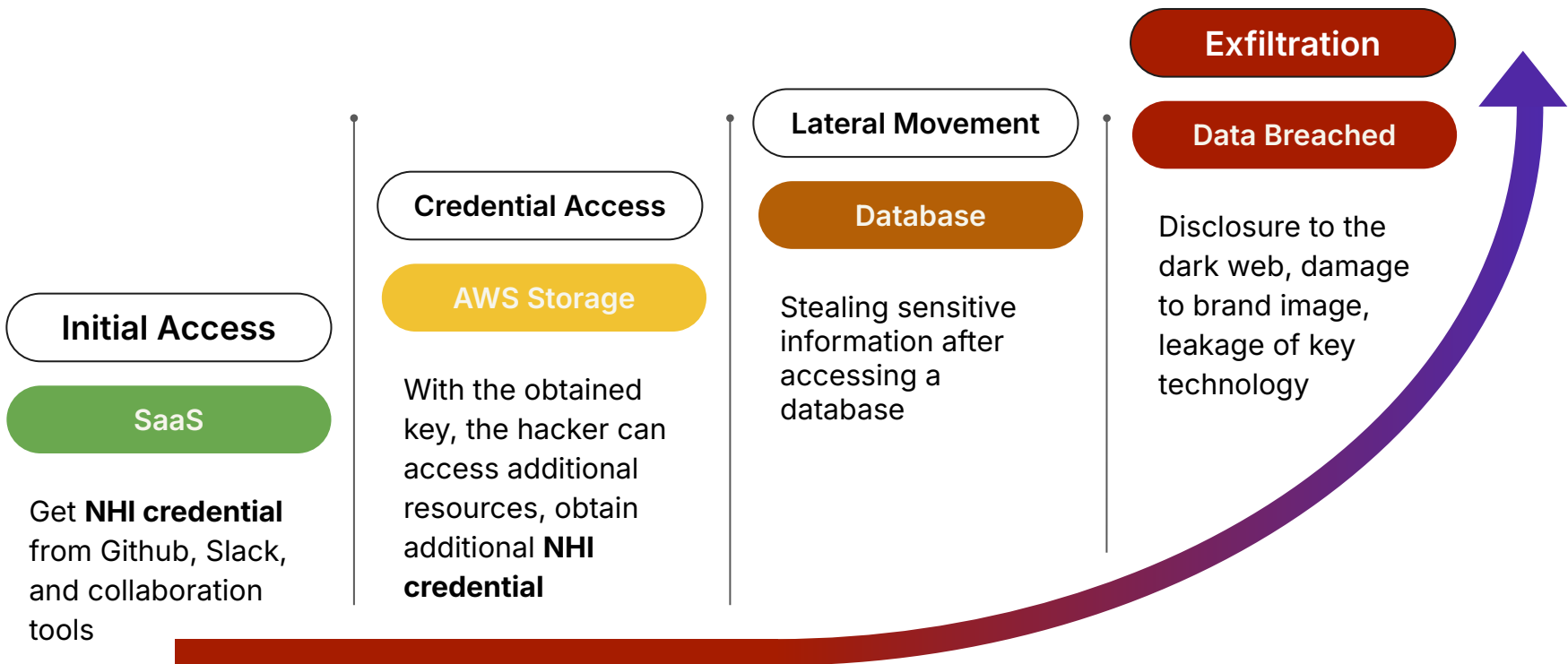
Cancel

Next

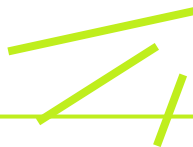
NHI10: HUMAN USE OF NHI



ID/Password를 획득한 공격자



CREMIT



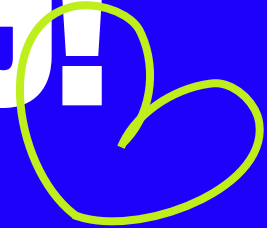
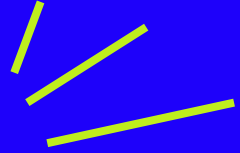
NHI SECURITY

김동현

BEN@CRMEIT.IO

HI@CREMIT.IO

THANKS FOR
LISTENSTING!



STICKER SHEET

