



OWASP

TM

Seoul Chapter

Security Compliance Engineer :
스타트업 보안 인증 실전 경험

25.9.23.

예스24, 랜섬웨어 피해 규모 100억 원 추산...2,000만 회원 대상 보상조치 나서

전체 회원 대상 보상안 발표...상품권 및 구독 혜택 제공

KT-SKT, 5개월 만에 뒤바뀐 운명 ... '해킹 마케팅' 다시 불 붙나

강필성 기자

입력 2025-09-15 10:37 | 수정 2025-09-15 10:46



'롯데카드' 297만 명 정보 털렸다...뒤늦은 사과 "보안 강화하겠다"

입력 2025-09-18 20:38 | 수정 2025-09-18 21:31



[속보] 李 대통령 “보안 사고 반복되는 기업, ‘징벌적 과징금’ 등 강력 조치”

입력 2025.09.04. 오후 3:29 기사원문

김수연 기자


96 214

가가



개인정보 안전관리 체계 강화 방안(案)

2025. 9.

 개인정보보호위원회

소개

- 현) 라포랩스
- 전) KISA, 금융보안원, 카카오뱅크
- ISMS-P 인증심사원 / Kubestronaut
- KITRI 화이트햇스쿨 멘토
- AWSKRUG 보안소모임 오거나이저



목차

1. Security Compliance Engineer란?
2. SCE 실전 사례
3. QnA



OWASPTM

Seoul Chapter

1. Security Compliance Engineer란?

1. Security Compliance Engineer란?

Security Manager / 정보보호 담당자

조직의 정보보호 관리 체계를 책임지는 관리자. 보안 정책과 절차를 수립하고, 법적 요구사항 준수

1. Security Compliance Engineer란?

Security Manager / 정보보호 담당자

조직의 정보보호 관리 체계를 책임지는 관리자. 보안 정책과 절차를 수립하고, 법적 요구사항 준수

1. 정책 수립

2. 컴플라이언스 준수

3. 거버넌스 리스크 관리

1. Security Compliance Engineer란?

Security Compliance Engineer

컴플라이언스와 기술에 대한 이해를 기반으로 정책을 수립. 수립한 정책이 준수되도록 기술적으로 구현하고 이를 운영 및 모니터링

1. Security Compliance Engineer란?

Security Compliance Engineer

컴플라이언스와 기술에 대한 이해를 기반으로 정책을 수립. 수립한 정책이 준수되도록 기술적으로 구현하고 이를 운영 및 모니터링

1. 기술에 기반한 정책

2. 정책에 기반한 기술

1. Security Compliance Engineer란?

| 구분 | Security Manager | Security Compliance Engineer |
|-------|--|---|
| 핵심 역할 | 정책·절차 수립 및 규제 준수 관리 | 정책을 기술적으로 구현·운영, 증적 자동화 |
| 관점 | 정책 중심 | 정책 + 기술 융합 |
| 주요 업무 | <ul style="list-style-type: none">- 정책/지침 관리- 규제기관·외부감사 대응- 리스크 관리, 경영진 보고 | <ul style="list-style-type: none">- 클라우드/시스템 환경 보안 구현- 컴플라이언스 준수 운영- 인증 심사 증적 자동화 |
| 특징 | 법규 해석, 거버넌스, 관리적 통제 | 실효성 있는 정책 수립, 보안 운영 자동화 |
| 한계 | 기술 변화 대응에 한계 | 과도한 업무량(?) |

1. Security Compliance Engineer란?

우리는 왜

Security Compliance Engineer가

되어야 할까요?

1. Security Compliance Engineer란?

기술의 몰이해로 인한 비현실적인 정책 수립

1. Security Compliance Engineer란?

기술의 몰이해로 인한 비현실적인 정책 수립

기술의 부족으로 인한 비효율적인 관리체계 운영

기술의 몰이해로 인한 비현실적인 정책 수립

기술의 부족으로 인한 비효율적인 관리체계 운영

정책 '수립'과 '운영' 주체 분리에 따른 비효율

1. Security Compliance Engineer란?

최근 3년내 14개 글로벌 기업의 SCE 채용공고 분석

■ 정책·컴플라이언스

- 컴플라이언스 프레임워크
SOC 2, ISO 27001, NIST 800-53, FedRAMP, PCI DSS, HIPAA 등 다중 프레임워크 경험
- 정책·문서화·SSP
정책·절차·SOP, System Security Plan(SSP) 작성·관리, 증적 관리 및 보고
- 감사·심사 대응
외부 심사, 3PAO 협업, 연속 모니터링 및 증적 수집

■ 기술·운영

- 클라우드 보안 운영
AWS·Azure·GCP 보안 통제 설계, Kubernetes·Docker 활용
- 자동화·스크립팅 & GRC
Python 등 스크립팅, Vanta/Drata/OneTrust 활용, 증적 자동화
- 취약점·운영 보안
취약점 관리·시정조치, 탐지/대응
- 리스크·POA&M
리스크 평가, RMF, Plan of Actions & Milestones 작성·트래킹

■ 협업·조율

- 제3자·고객 대응
벤더 보안평가, RFP/보안 설문 대응, 고객 보안 질의
- 커뮤니케이션/협업
엔지니어링·제품·법무·IT 부서와 협업, 요구사항 번역/조율

1. Security Compliance Engineer란?

■ 정책·컴플라이언스

- 컴플라이언스 프레임워크
SOC 2, ISO 27001, NIST 800-53, FedRAMP, PCI DSS, HIPAA 등 다중 프레임워크 경험
- 정책·문서화·SSP
정책·절차·SOP, System Security Plan(SSP) 작성·관리, 증적 관리 및 보고
- 감사·심사 대응
외부 심사, 3PAO 협업, 연속 모니터링 및 증적 수집

**컴플라이언스를 기술적으로 구현 및 자동화해
실효성 있는 관리체계를 운영하는 담당자**

AWS/Azure/GCP 보안 통제 설계, Kubernetes/Docker 활용

취약점 관리·시정조치, 탐지/대응

• 리스크·POA&M

리스크 평가, RMF, Plan of Actions & Milestones 작성·트래킹

■ 협업·조율

- 제3자·고객 대응
벤더 보안평가, RFP/보안 설문 대응, 고객 보안 질의
- 커뮤니케이션/협업
엔지니어링·제품·법무·IT 부서와 협업, 요구사항 번역/조율

Security Compliance Engineer로서 갖춰야 할 Skill

- 국내외 보안 컴플라이언스 해석 능력
- Cloud Security
- DevSecOps
- Automation (PaC..?)

(정해진 답이 아닌 개인적인 의견입니다)

Security Compliance Engineer로서 갖춰야 할 **Insight**

- 현실에 뒤떨어진 규제와 최신 기술 사이에서 발생하는 간극을 인지하고 이를 맞추는 능력
- 규제 해석과 기술을 통해 ‘안되는 보안’에서 ‘되는 보안’으로 만드는 능력

(정해진 답이 아닌 개인적인 의견입니다)



OWASPTM

Seoul Chapter

2. SCE 실전 사례

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

(ISMS-P) 2.10.2 클라우드 보안

(ISO 27001) 매핑 불가(다수의 통제항목과 연관)

| 항 목 | 2.10.2 클라우드 보안 |
|---------|--|
| 인증기준 | 클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다. |
| 주요 확인사항 | <ul style="list-style-type: none">클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서(SLA 등)에 반영하고 있는가?클라우드 서비스 이용 시 서비스 유형에 따른 보안위험을 평가하여 비인가 접근, 설정오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 수립·이행하고 있는가?클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가 접근, 권한 오·남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호대책을 적용하고 있는가?클라우드 서비스의 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하고 있는가? |

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

(ISMS-P) 2.10.2 클라우드 보안

(ISO 27001) 매핑 불가(다수의 통제항목과 연관)

클라우드 **설정 변경을 통제**하고 운영 현황을 **정기적으로 모니터링**하는가?



PROWLER

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

Cloud Custodian

- 클라우드 리소스에 정책을 자동 적용하는 오픈소스
- 보안 컴플라이언스 요구사항을 코드로 정의 가능
- 규정 위반 리소스를 실시간으로 탐지해 차단 / 알람 / 수정

Prowler


- 클라우드 보안 점검 오픈소스
- CIS, ISO, GDPR, HIPAA 등 다양한 글로벌 프레임워크 지원
- 취약점 진단 및 컴플라이언스 상태 보고서 생성

보안 위협이 있는 프로비저닝을 실시간으로 모니터링하고 싶다!
(규칙 작성도 쉽고 + 규칙 작성의 자유도가 보장되고 + 편하게 조회하고)

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

```
1  policies:
2    - name: SecurityGroup-ingress-any-rule-detection
3      resource: security-group
4      description: Monitor Ingress SG rule settings in real-time and notify via Slack
5      mode:
6        type: cloudtrail
7        role: {role}
8        events:
9          - source: ec2.amazonaws.com
10            event: AuthorizeSecurityGroupIngress
11            ids: "responseElements.securityGroupRuleSet.items[].groupId"
12          - source: ec2.amazonaws.com
13            event: ModifySecurityGroupRules
14            ids: "requestParameters.ModifySecurityGroupRulesRequest.GroupId"
15        tags:
16          C7n: "true"
17      filters:
18        - or:
19          - type: ingress
20            Cidr:
21              value: "0.0.0.0/0"
22          - type: ingress
23            CidrV6:
24              value: ":::/0"
25      actions:
26        - type: notify
27          slack_template: slack-custom-template
28          to:
29            - slack://#backend-monitor-security-alarm
30      transport:
31        type: sqs
32        queue: {sqs}
33        region: ap-northeast-2
```

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

**Security Automation Bot** 앱 오후 2:48

@security_team Security Risk Detected

AWS Security Policy Alert

Account
[REDACTED]

User Name
[REDACTED]@rapportlabs.kr


SecurityGroup ID
sg-0218e3c0d5d6689b1


Description
SecurityGroup Ingress Any rule Detected



Region
ap-northeast-2

Source IP
[REDACTED]

SecurityGroup Rule ID
sgr-04be689f1e20454ca

 1






2개의 댓글 오늘 마지막 댓글이 달린 시간: 오후 3:27

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

```
1  policies:
2    - name: S3-public-access-detection
3      resource: aws.s3
4      description: Monitor S3 bucket public access settings in real-time and notify via Slack
5      mode:
6        type: cloudtrail
7        role: arn:aws:iam::{account_id}:role/CloudCustodianRole
8      tags:
9        C7n: "true"
10     events:
11       - source: "s3.amazonaws.com"
12         event: PutBucketPublicAccessBlock
13         ids: "requestParameters.bucketName"
14     filters:
15       - type: check-public-block
16         RestrictPublicBuckets: false
17         BlockPublicAcls: false
18         BlockPublicPolicy: false
19         IgnorePublicAcls: false
```

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

**Security Automation Bot** 앱 오후 2:43

@security_team Security Risk Detected

AWS Security Policy Alert

Account
[Redacted]


User Name
[Redacted]


Bucket Name
[Redacted]




Region
ap-northeast-2

Source IP
[Redacted]

Description
S3 Bucket Public Access Allow Detected

 1





5개의 댓글 2일 전 마지막 댓글

클라우드의 보안 설정을 매일 편하게 점검 및 관리하고 싶다!

2. SCE 실전 사례 / Case1. 클라우드 보안 관리

```
1  name: Run Damoa Prowler
2
3  on:
4    workflow_dispatch:
5    schedule:
6      - cron: "0 20 * * *"
7
8  env:
9    VAULT_ADDR: ${vars.VAULT_ADDR}
10   VAULT_AUDIENCE: ${vars.VAULT_AUDIENCE}
11
12  jobs:
13    run-prowler:
14      runs-on: ubuntu-latest
15      defaults:
16        run:
17          shell: bash
18      permissions:
19        id-token: write
20        contents: read
21        actions: read
```

```
23  steps:
24    - uses: actions/checkout@v4
25    - uses: actions/setup-python@v5
26      with:
27        python-version: '3.11'
28        cache: 'pip'
29        cache-dependency-path: |
30          requirements.txt
31
32    - name: Install prowler
33      run: |
34        pip install -r requirements.txt
35        prowler -v
36
37    - name: Configure AWS Credentials
38      uses: aws-actions/configure-aws-credentials@v4
39      with:
40        aws-region: ap-northeast-2
41        role-to-assume: [REDACTED]
42        role-session-name: GitHubActions
43        role-duration-seconds: 21600
44
45    - run: |
46        prowler aws --security-hub --region ap-northeast-2 --send-sh-only-fails
47      continue-on-error: true
```

2. SCE 실전 사례 / Case1. 클라우드 보안 관리



Security Automation Bot 앱 오전 5:45



AWS 취약점 점검 현황(2025-09-11 기준)



총 취약점(CRITICAL) : 15건



신규 취약점 : 1건



해결 취약점 : 0건



신규 취약점 현황



취약점 : Find secrets in Lambda functions code.



심각도 : CRITICAL



개수 : 1개



1



1개의 댓글 7일 전

2. SCE 실전 사례 / Case2. Github 시크릿 유출 차단

(ISMS-P) 2.8.1 보안 요구사항 정의 / 2.8.5 소스 프로그램 관리

(ISO 27001) 8.25 Secure development life cycle / 8.28 Secure coding

| | | |
|------|-------------------------------|--|
| 8.25 | Secure development life cycle | Control Rules for the secure development of software and systems shall be established and applied. |
|------|-------------------------------|--|

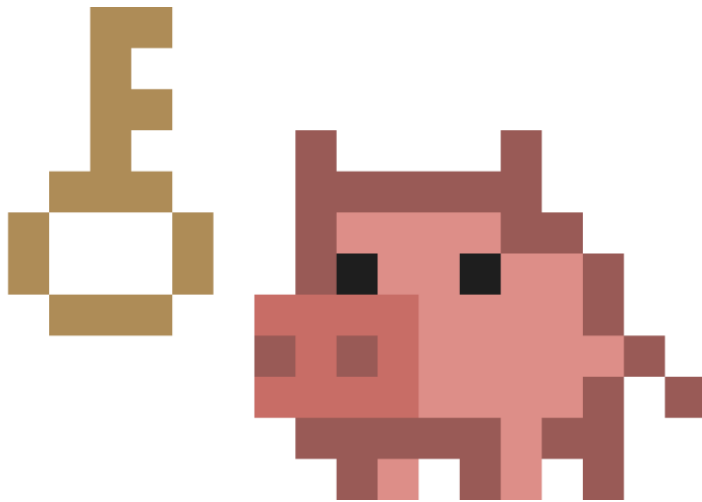
| | | |
|------|---------------|--|
| 8.28 | Secure coding | Control Secure coding principles shall be applied to software development. |
|------|---------------|--|

2. SCE 실전 사례 / Case2. Github 시크릿 유출 차단

(ISMS-P) 2.8.1 보안 요구사항 정의 / 2.8.5 소스 프로그램 관리

(ISO 27001) 8.25 Secure development life cycle / 8.28 Secure coding

깃헙에 **시크릿이 유출되지 않도록 통제**하는가?



2. SCE 실전 사례 / Case2. Github 시크릿 유출 차단


TruffleHog







- 시크릿 탐지 오픈소스로 800 종 이상의 시크릿 탐지
- pre-commit hook을 활용해 깃헙 액션에서 실시간 탐지 가능
- --only-verified 옵션을 통해 오탐 최소화



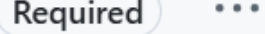



2. SCE 실전 사례 / Case2. Github 시크릿 유출 차단



커밋에 시크릿이 존재하지 않게 하고싶다!


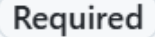
2. SCE 실전 사례 / Case2. Github 시크릿 유출 차단



 **All checks have passed**
12 successful checks






 **Trufflehog** Successful in 24s — Required workflow passed



 **Trufflehog / Trufflehog / Scan (pull_request_target)** Successful in 19s



2. SCE 실전 사례 / Case2. Github 시크릿 유출 차단

github-actions bot commented 3 days ago

✖ TruffleHog checks 실패



- 실패 사유 : 시크릿이 탐지되었습니다.
- 스캔 범위 : e65c57495f6b0ae43e9d1f2a85acb576a608a001 ... ee4e9a801496
- 감지 건수 : 1
- 조치 방법 : 시크릿이 검출된 커밋을 삭제하고, 시크릿 제거 후 force-push 해주세요.
- 탐지 예외가 필요한 시크릿인 경우 #security-request 채널로 요청해주세요.


시크릿 존재 커밋


- b719b9ff1715 (1개 위치)


시크릿 위치

| Secret Type | File:Line | Commit |
|-------------|-----------------------|--------------|
| Slack | sec:1 | b719b9ff1715 |

 **PR 내 시크릿 탐지**  @security_team

 PR 링크 : PR #22: Create sec

 PR 작성자 : zero-rpls

 시크릿 종류 : Slack

2. SCE 실전 사례 / Case3. PC보안설정 미조치 시 내부망 접속차단

(ISMS-P) 2.10.6 업무용 단말기기 보안

(ISO 27001) 8.1 User end point devices / 8.9 Configuration management

| 항 목 | 2.10.6 업무용 단말기기 보안 |
|---------|--|
| 인증기준 | PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다. |
| 주요 확인사항 | <ul style="list-style-type: none">PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안설정 등의 보안 통제 정책을 수립·이행하고 있는가?업무용 단말기를 통하여 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료공유프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립·이행하고 있는가?업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유·노출을 방지하기 위하여 보안대책을 적용하고 있는가?업무용 단말기기에 대한 접근통제 대책의 적절성에 대하여 주기적으로 점검하고 있는가? |

Security Day에 PC 보안설정 점검을 편하게 하고 싶다!
(NAC이 없지만, NAC과 유사한 효과를 내고 싶다)

2. SCE 실전 사례 / Case3. PC보안설정 미조치 시 내부망 접속차단



Security Automation Bot 앱 오후 1:21

[PC보안설정 조치 요청 안내]

안녕하세요 Security Team입니다.

PC보안설정이 취약해 해킹에 노출된 상태입니다. 2025-09-18까지 보안설정을 완료해주세요.

2025-09-18에 2차 점검을 실시 예정이며, 조치되지 않은 경우 구글 드라이브 및 스프레드시트 접속이 차단됩니다.

궁금하신 점은 #security-request 채널로 문의해주세요.

자세한 조치방법은 Security Automation Bot 앱 메세지 로 안내드렸습니다. 감사합니다.

대상 인원 :



Security Automation Bot 앱 오후 2:14

[PC보안설정 미조치에 따른 GWS 접속 차단 안내]

안녕하세요 Security Team입니다.

PC보안조치 기간(10일)이 경과했으나, 아직 조치되지 않은 분은 GWS 접속이 차단되어 안내드립니다.

자세한 조치방법은 Security Automation Bot 앱 메세지 로 안내드렸습니다. 감사합니다.

대상 인원 :



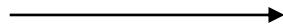
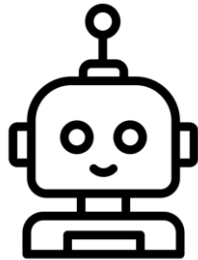
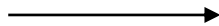
Security Automation Bot 앱 오늘 오후 3:45

PC 보안설정이 완료되어 GWS 접근차단이 해제되었습니다. 감사합니다!

여전히 GWS 접근이 되지 않는 경우 #Security-request 채널로 문의해주세요.

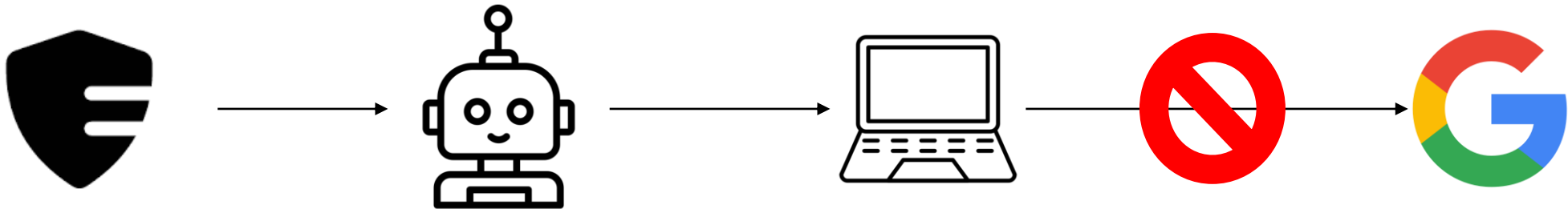
2. SCE 실전 사례 / Case3. PC보안설정 미조치 시 내부망 접속차단

ngrok

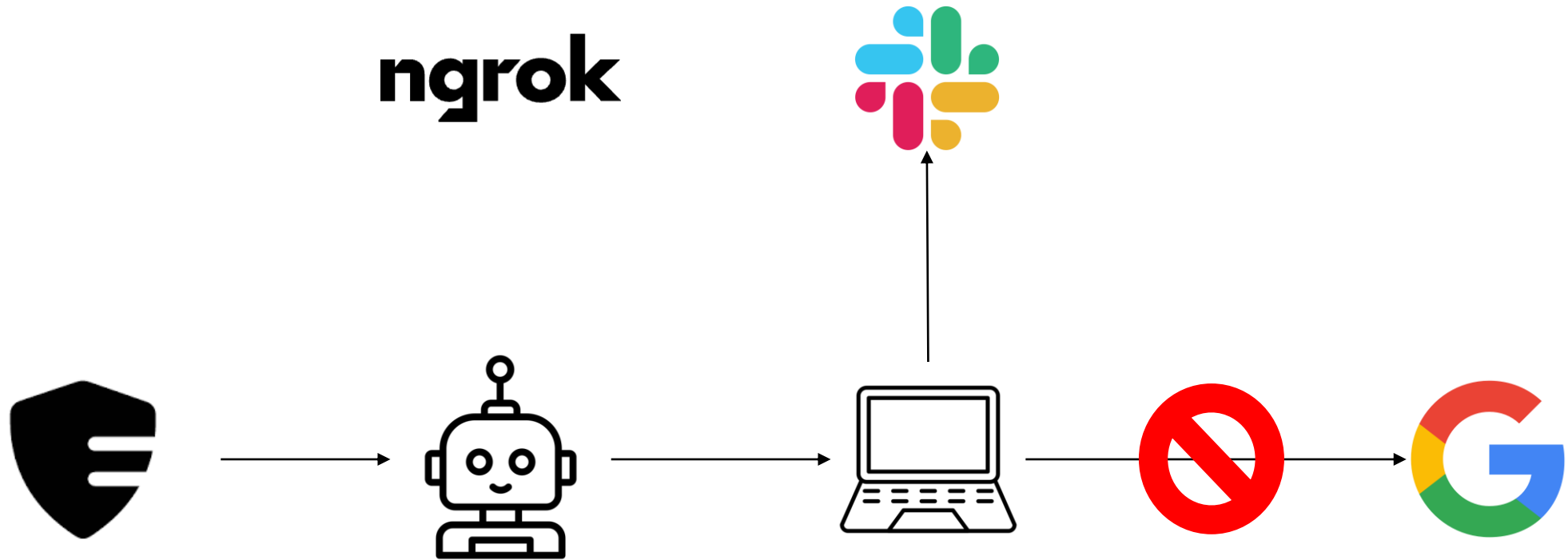


2. SCE 실전 사례 / Case3. PC보안설정 미조치 시 내부망 접속차단

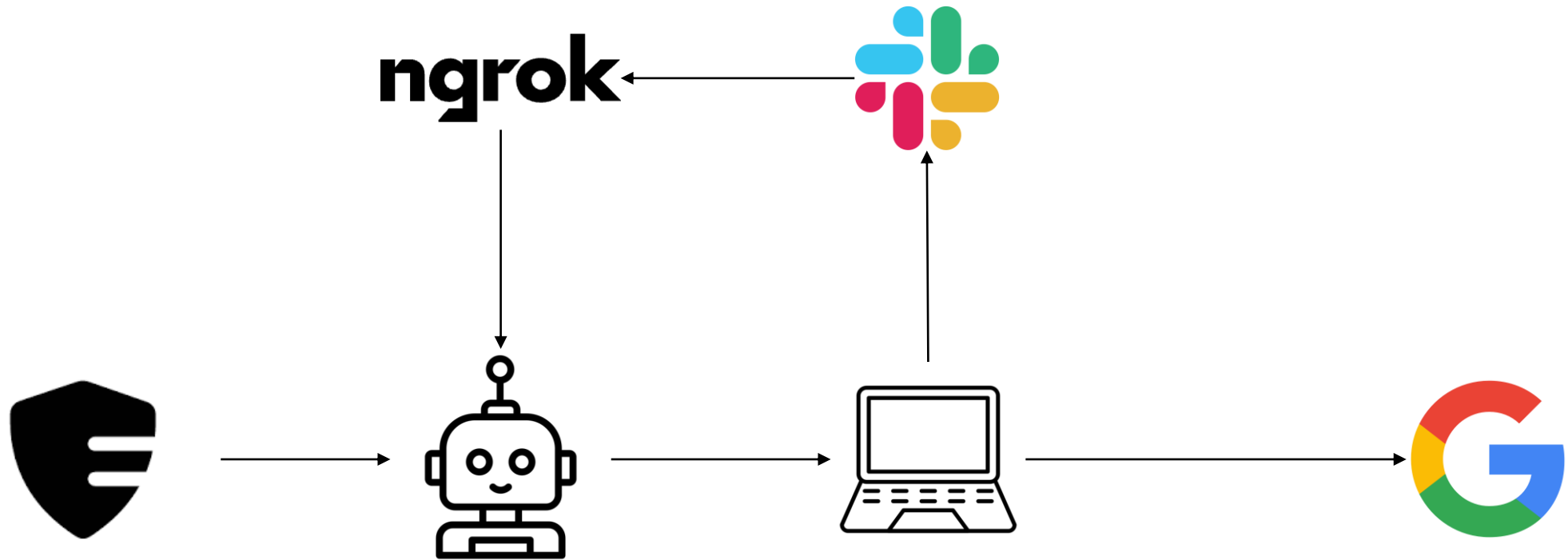
ngrok



2. SCE 실전 사례 / Case3. PC보안설정 미조치 시 내부망 접속차단



2. SCE 실전 사례 / Case3. PC보안설정 미조치 시 내부망 접속차단



2. SCE 실전 사례 / Case4. 피싱메일 훈련 시스템 구축

(ISMS-P) 2.11.4 사고 대응 훈련 및 개선

(ISO 27001) 6.3 Information security awareness, education and training

| 항 목 | 2.11.4 사고 대응 훈련 및 개선 |
|---------|---|
| 인증기준 | 침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다. |
| 주요 확인사항 | <ul style="list-style-type: none">• 침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련계획을 수립하고 이에 따라 연 1회 이상 주기적으로 훈련을 실시하고 있는가?• 침해사고 및 개인정보 유출사고 훈련 결과를 반영하여 침해사고 및 개인정보 유출사고 대응체계를 개선하고 있는가? |

피싱메일 훈련을 유연하게 구성하고 언제든지 하고 싶다!

(KISA에서 제공하는 플랫폼은 이용이 불편하고, 제약이 크다)

2. SCE 실전 사례 / Case4. 피싱메일 훈련 시스템 구축

Namacheap

- 도메인 등록과 DNS 호스팅을 제공하는 서비스
- 손쉽게 도메일 보안 설정 가능

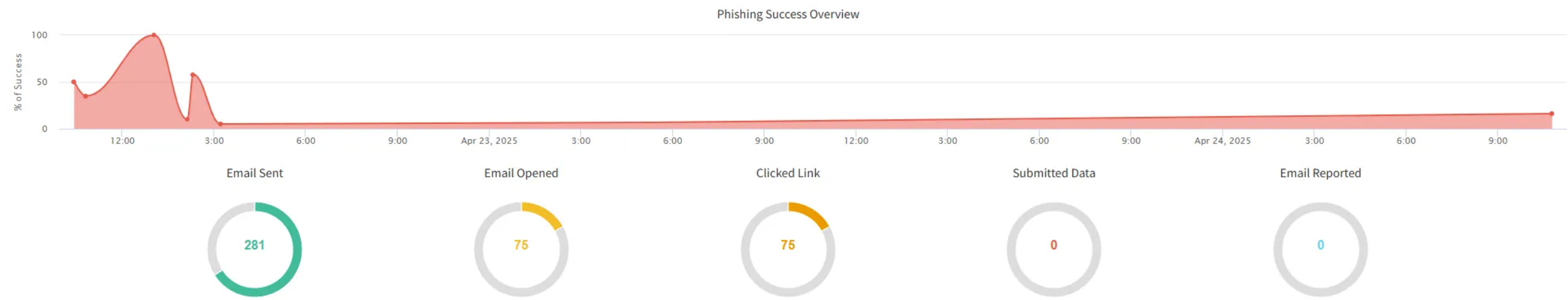
Zoho Mail

- 비즈니스용 이메일 호스팅 서비스
- 사용자 계정 메일 도메인을 직접 관리 가능

Gophish

- 오픈소스 피싱 훈련 프레임워크로 손쉽게 캠페인 운영 가능
- 사용자 맞춤형 피싱 메일 발송 및 클릭 입력 등 반응 추적 지원
- 결과 리포트 제공

Dashboard



Recent Campaigns

View All

Show 10 entries

Search:

| Name | Created Date | | | | | | Status | |
|---------------------|------------------------------|-----|----|----|---|---|-------------|--|
| 사업팀 성과급(에러 인원 추가) | April 24th 2025, 10:46:10 am | 138 | 23 | 23 | 0 | 0 | In progress | |
| 사업팀 성과급 | April 22nd 2025, 3:13:00 pm | 29 | 9 | 9 | 0 | 0 | In progress | |
| 제품팀 비엔지니어 성과급 | April 22nd 2025, 2:19:15 pm | 29 | 17 | 17 | 0 | 0 | In progress | |
| FE+SE 깃헙 토큰 | April 22nd 2025, 2:07:07 pm | 38 | 4 | 4 | 0 | 0 | In progress | |
| 팔도감 조직 병합(에러 인원 추가) | April 22nd 2025, 1:02:28 pm | 2 | 2 | 2 | 0 | 0 | In progress | |
| 팔도감 조직 병합 | April 22nd 2025, 10:48:07 am | 25 | 10 | 10 | 0 | 0 | In progress | |
| 계약지 | April 22nd 2025, 10:25:14 am | 26 | 16 | 16 | 0 | 0 | In progress | |

우리는 왜

Security Compliance Engineer가

되어야 할까요?

위험을 찾는게 아니라, 위험이 찾아오는 환경
자동화된 환경을 구축해 신속하고 정확한 보안
정책을 현실로 구현하고 운영하는 능력



OWASPTM

Seoul Chapter

3. QnA