Cremit

도구를 넘어서

DevSecOps 문화 구축하기

OWASP Seoul | November 2025

김동현 | Cremit CEO | ben@cremit.io

OWASP

Cremit

발표자 소개

김동현 (Ben)

Cremit CEO & Founder

OWASP Seoul Chapter Leader

11+ Years in Cybersecurity

경력

- 보안 스타트업 창업 및 운영
- 보안 컨설팅 & 교육
- 다양한 산업분야 In-house Security Engineer

Cremit

1

한국의 DevSecOps 현실

Cremit

우리는 어떻게 접근하고 있나요?

보안 도구 구매 → 도입 비용 계산 → ROI 측정

우리 조직도 이렇게 하고 있지 않나요?

Cremit

흔한 오해

DevSecOps = CI/CD + 보안 도구

✕

이것만으로는 충분하지 않습니다

Cremit

2

도구만으로는 부족하다

Cremit

현실: 도구는 있지만...

SAST

DAST

SCA

SBOM

→

보안 사고는
여전히 발생

Cremit

왜 실패하는가?

개발자

스캔 결과 무시

보안팀

고립된 상태

운영팀

협업 부재

팀 간 사일로 = 실패의 원인

문제의 본질

문화의 부재

도구는 수단일 뿐, 목적이 아닙니다

Cremit

3

DevSecOps = 문화

Cremit

"문화를 만든다"는 것

한국 지하철 문화를 생각해보세요

두 줄로 서서 내리는 사람 먼저 → 아무도 강요하지 않지만, 모두가 따릅니다

*처음엔 안내 방송과 표지판이 있었지만, 이제는 **자연스러운 습관**이 되었습니다*

"문화는 선언하는 것이 아니라,
매일의 행동이 쌓여 만들어지는 것입니다."

씨앗을 심는 일
한 번의 교육, 한 번의 회의가 아닌
반복되는 작은 행동들의 축적

함께 만드는 약속
"이것이 우리가 일하는 방식이다"라는
암묵적 합의를 형성하는 과정

습관이 되는 순간
누가 시키지 않아도
자연스럽게 보안을 고려하게 되는 상태

OWASP

Cremit

문화란 무엇인가?

- 개발자가 보안을 자신의 일로 받아들임
- 팀 간 협업과 공동 책임
- 작은 성공의 반복

Cremit

문화 구축의 두 축

기술적 실행

무엇을 할 것인가

문화적 실행

어떻게 함께 할 것인가

Cremit

4

기술적 실행 아이템

Cremit

7가지 기술적 실행 아이템

Secret Detection
하드코딩된 비밀 정보 탐지

SAST
소스 코드 정적 분석

DAST
실행 환경 동적 분석

SCA
오픈소스 의존성 취약점

SBOM
소프트웨어 구성 요소 관리

Container Scan
이미지 취약점

IaC Scan
인프라 코드 보안

Cremit

Secret Detection

하드코딩된 비밀 정보 탐지

```
# Bad practice - 절대 하지 마세요!
API_KEY = "sk-1234abcd5678efgh..."
DB_PASSWORD = "super_secret_123"
```

추천 도구: git-secrets | OWASP Deep Secrets

난이도: ★☆☆ (시작하기 쉬움)

Cremit

DAST

동적 애플리케이션 보안 테스트

- 실행 중인 애플리케이션을 테스트
- 실제 공격 시나리오 시뮬레이션
- 런타임 취약점 발견

(구) OWASP ZAP - 무료 오픈소스 DAST 도구

Cremit

SCA

소프트웨어 구성 분석

- 오픈소스 라이브러리 취약점 스캔
- 라이선스 컴플라이언스 확인
- 의존성 트리 분석

OWASP Dependency-Check - CVE 데이터베이스 기반 스캔

Cremit

OWASP Wrong Secrets

시크릿 관리 교육 플랫폼

- 실습 기반 보안 교육
- 다양한 시크릿 유출 시나리오
- Kubernetes, Cloud 환경 지원
- CTF 스타일의 챌린지

github.com/OWASP/wrongsecrets

OWASP

Cremit

OWASP 생태계 요약

Secret Detection	→	**OWASP Deep Secrets**
Secret 교육	→	**OWASP Wrong Secrets**
DAST	→	**(구) OWASP ZAP**
SCA	→	**OWASP Dependency-Check**
가이드라인	→	**OWASP DevSecOps Guideline**

Tip: 쉬운 것부터 시작하세요 (Secret Detection 추천)

Cremit

5

문화적 실행 아이템

Cremit

왜 기술만으로는 부족한가

도구만 있을 때

- 스캔 결과 무시
- 알림 피로
- 책임 전가
- 반복되는 실수

문화가 있을 때

- 자발적 개선
- 공동 책임
- 지속적 학습
- 예방 중심

Cremit

6가지 문화적 실행 아이템

1. 리더십 회의
2. 합동 킥오프
3. 주간 성공 공유
4. 팀 회고
5. 지표 투명화
6. 인센티브

Cremit

1 리더십 회의

경영진의 지원 없이는 문화가 뿌리내리지 못합니다

왜 중요한가?

보안 문화는 Top-down으로 시작됩니다. 경영진이 보안의 가치를 이해하고 지원할 때, 팀은 보안에 시간과 리소스를 투자할 수 있습니다.

어떻게 실행하나요?

- 월 1회 보안 현황 브리핑
- 리소스 확보를 위한 데이터 기반 근거 제시
- 보안 투자 ROI 시각화

Cremit

2 개발-보안 합동 킥오프

사일로를 깨는 첫 번째 단추

왜 중요한가?

프로젝트 시작 시점에 개발팀과 보안팀이 함께 모이면, 보안 요구사항이 '나중에 추가할 것'이 아닌 '처음부터 고려할 것'이 됩니다.

어떻게 실행하나요?

- 프로젝트 시작 시 보안 요구사항 공유
- 위협 모델링 워크샵 진행
- 공동 목표 설정 및 책임 분배

Cremit

3 주간 성공 공유

작은 성공을 축하하면 큰 변화가 시작됩니다

왜 중요한가?

보안은 종종 '안 좋은 소식'만 전달합니다. 발견된 취약점을 빠르게 해결한 사례를 공유하면, 보안이 팀의 성과가 됩니다.

어떻게 실행하나요?

- 발견된 취약점 공유 (비난 없이, 학습 목적)
- 빠르게 해결된 케이스 축하
- Slack/Teams 채널에서 주간 하이라이트 공유

4 팀 회고

함께 돌아보고, 함께 개선합니다

왜 중요한가?

스프린트 회고에 보안 항목을 추가하면, 보안이 개발 프로세스의 자연스러운 일부가 됩니다. 반복되는 문제 패턴을 발견하고 근본 원인을 해결할 수 있습니다.

어떻게 실행하나요?

- 스프린트 회고에 "보안" 섹션 추가
- 무엇이 잘 되었나? 개선점은?
- 구체적인 액션 아이템 도출

5 지표 투명화

보이지 않으면 개선할 수 없습니다

왜 중요한가?

모두가 볼 수 있는 대시보드는 책임감을 만듭니다. 숫자가 투명해지면 팀은 자연스럽게 개선하려고 노력합니다.

어떻게 실행하나요?

- 실시간 보안 메트릭 대시보드 구축
- 팀별 취약점 현황 시각화
- 트렌드 변화 추적 및 공유

Cremit

6 인센티브와 인정

올바른 행동을 강화합니다

왜 중요한가?

사람들은 인정받는 행동을 반복합니다. 보안에 기여한 사람을 공개적으로 칭찬하면, 다른 사람들도 따라합니다.

어떻게 실행하나요?

- 보안 챔피언 프로그램 운영
- 내부 버그 바운티 운영
- 공개적 인정: "이 취약점을 발견한 OOO님 감사합니다!"

Cremit

기술 + 문화

= DevSecOps

OWASP

Cremit

6

문화의 ROI

Cremit

문화도 측정할 수 있다

기술 지표

취약점 해결 시간MTTR (Mean Time To Remediate)

재발률동일 유형 취약점 재발생 비율

Shift-Left 비율개발 단계 vs 운영 단계 발견 비율

자동화 커버리지CI/CD 파이프라인 보안 스캔 적용률

문화 지표

보안 교육 참여율분기별 교육 이수 비율

자발적 보고 건수개발자가 스스로 보고한 보안 이슈

보안 챔피언 활동률팀별 보안 챔피언 참여도

개발자 보안 설문"보안이 내 일이다" 동의 비율

Cremit

감사합니다

DevSecOps는 도구가 아니라 문화입니다.

기술적 실행 + 문화적 실행 = 진정한 보안

작게 시작하고, 함께 성장하세요.

Ben

Cremit CEO

ben@cremit.io