삼성 오픈소스 컨퍼런스
오픈소스로 만나보는 DevSecOps

우아한형제들 조민재
minjae.cho@gmail.com

SOSCON 2018
SAMSUNG OPEN SOURCE CONFERENCE 2018

2018년 10월 18일

조민재 (a.k.a 뽀빠이)

- 서비스개발보안 및 인프라보안
- (현) 우아한형제들 정보보안팀
  (사)화이트해커연합 하루(HARU) 이사
  보안컨퍼런스 김치콘(kimchicon.org) 운영진
  차세대 보안리더 양성 프로그램(BoB) 취약성분석 멘토
- (전) 야후!코리아, NHN, 쿠팡 등 기업체 근무 +19년쯤 경력
  OWASP Korea 한국지부 이사 (OWASP Top10 2013 번역 / 2017 감수)
- FreeBSD project, OWASP Zed Attack Proxy project, Tor project

오늘의 이야기

DevSecOps

DevSecOps?

CI/CD

DevOps

Lean

Agile

Public Cloud

Scrum


THE WORLD IS CHANGING


intuit
CapitalOne
NETFLIX
BT
NOKIA
facebook
YAHOO!
vm
the magic of macy's
workday
WELLS FARGO
Expedia
CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION
mlbam
우아한 형제들

NETFLIX

- 운영 환경과 동일한 환경에서 1,000여 가지 지표 선정
- **100점 만점에 90점이** 넘어야 배포 승인
- IRC를 통해 상황 공유
- 배포 시 기존 인스턴스를 놔두고 **새로운 인스턴스 배포**

- **하루 2번** 마이너 배포 **일주일에 한 번** 메이저 배포
- 비트토런트 프로토콜 이용하여 **전세계** 배포
  - **빌드 15분, 배포 15분**
- IRC에서 응답하지 않는 개발자의 코드는 제외하고 배포
- 배포 후 **외부 SNS**를 크롤링해 장애여부 모니터링
- 배포 후 장애 발생 시 **롤백하지 않고** 빠르게 재배포


보안
NOT
IS CHANGING


In the beginning...
There was Waterfall


Requirements
Analysis
Design
Coding
Testing
Acceptance
Risk Analysis
Design Review
Code Review
Penetration Test
Finding anything late creates a cycle of waste

데브옵스 때문에 오히려 보안이 망가지고 있다?

2018-10-06

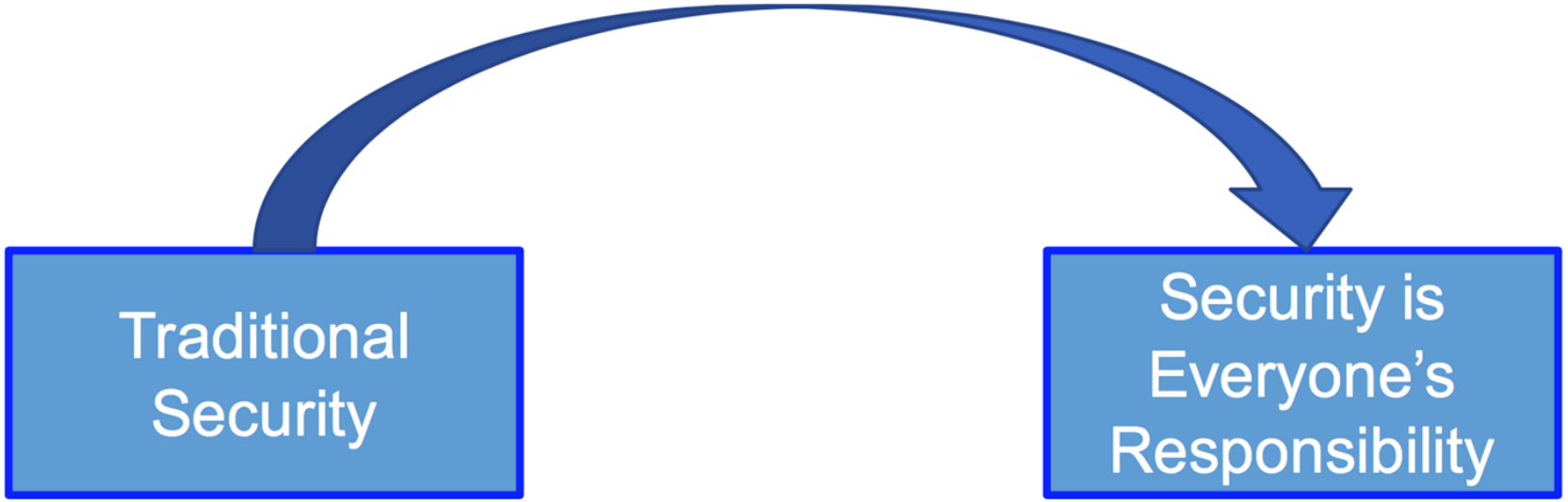
애플리케이션, 디지털 변혁 시대 기업들의 핵심 가치
속도 경쟁만 불꽃 튀어...보안은 여전히 뒷전

[보안뉴스 문가용 기자] 보안 업체 화이트햇 시큐리티(WhiteHat Security)가 최근 보고서를 통해 웹 기반 애플리케이션들이 여전히 기업들의 위험 요소로서 남아있다고 발표했다. 하지만 이번 보고서의 가장 충격적인 내용은 데브옵스 개발 환경 때문에 보안 문제가 더 많이 생기고 있다는 것이다.

문화적 충돌

DevOps Culture	Traditional Security Culture
Team-based decision making	Top-down risk management
Extended information sharing	Need-to-know restrictions
Fail fast and Fail forward	Zero failure
Limiting Change	Ready to say “No!”
Dev + Ops	Separation of Duty

Culture Hacking



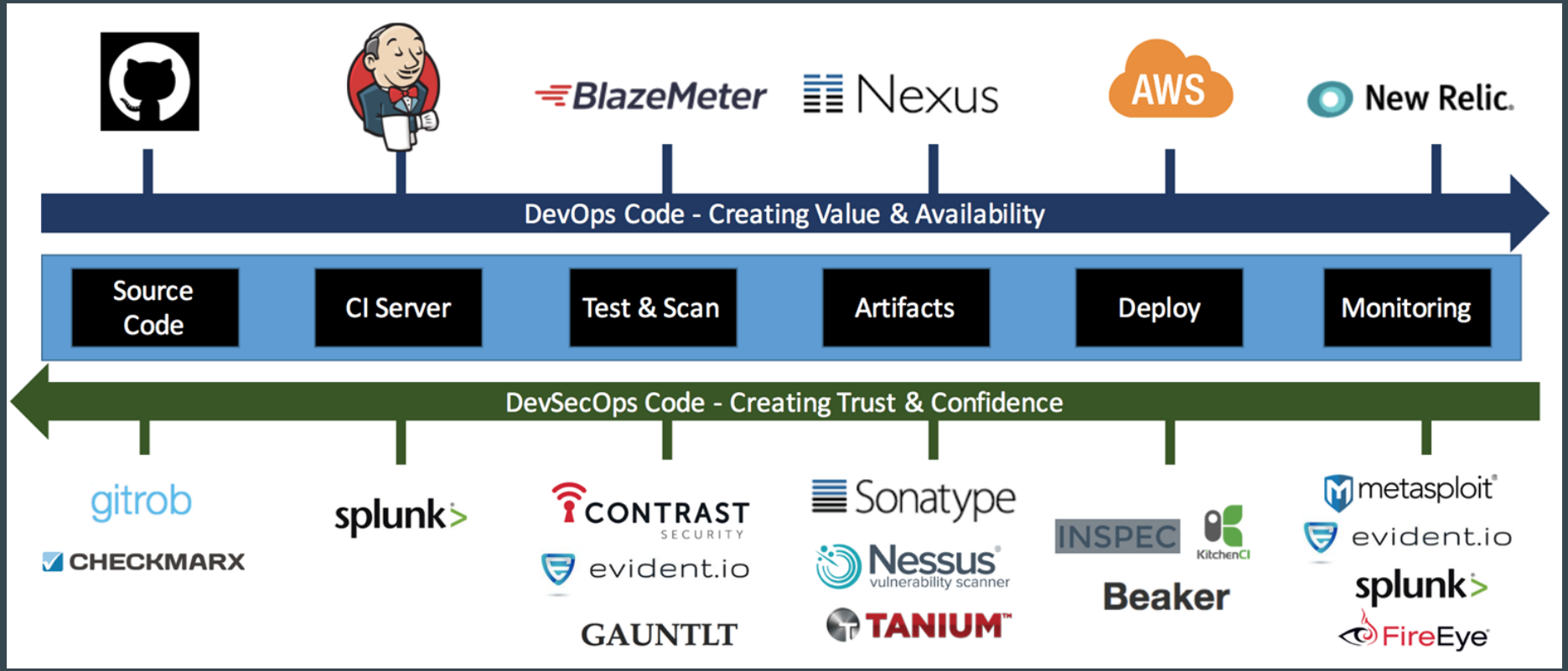
DEVSECOPS

DevSecOps
= DevOps + Security

DevSecOps

그러면 어떻게 하죠?

DevSecOps : 구축 사례



DevSecOps

오픈소스를 사용해봅시다!

SANS DevSecOps Toolchain

PRE-COMMIT | COMMIT (CI) | ACCEPTANCE | PRODUCTION | OPERATIONS

SANS DevSecOps Toolchain

Pre-Commit

Security activities before code is checked in to version control

Threat Modeling/Attack Mapping:
- Attacker personas
- Evil user stories
- Raindance
- Mozilla Rapid Risk Assessment
- OWASP ThreatDragon

Security and Privacy Stories:
- OWASP ASVS
- SAFECode Security Stories

IDE Security Plugins:
- DevSkim
- FindSecurityBugs
- Puma Scan
- SonarLint

Pre-Commit Security Hooks:
- git-hound
- git-secrets
- Repo-supervisor
- ThoughtWorks Talisman

Secure Coding Standards:
- CERT Secure Coding Standards
- OWASP Proactive Controls

Manual and Peer Reviews:
- Gerrit
- GitHub pull request
- GitLab merge request
- Review Board

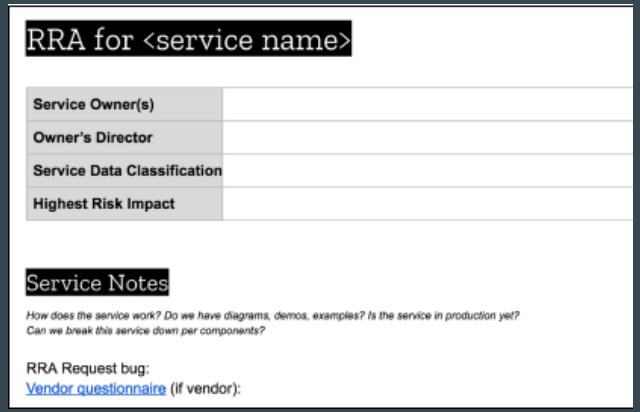
COMMIT (CI) → ACCEPTANCE → PRODUCTION → OPERATIONS

SANS DevSecOps Toolchain

PRE-COMMIT

Threat Modeling

- OWASP User Security Stories
- OWASP Application Security Verification Standards
- Mozilla's Rapid Risk Assessment(RRA)
- OWASP Thread Dragon



RRA for <service name>

Service Owner(s)	
Owner's Director	
Service Data Classification	
Highest Risk Impact	

Service Notes

How does the service work? Do we have diagrams, demos, examples? Is the service in production yet? Can we break this service down per components?

RRA Request bug:
Vendor questionnaire (if vendor):

스스로 물어야 할 다섯 가지 핵심 질문

1. 무엇을 보호하고 싶은가?
2. 누구로부터 보호하고 싶은가?
3. 그것을 보호할 필요성이 얼마나 있는가?
4. 실패할 경우 어떠한 나쁜 결과가 초래되는가?
5. 나쁜 결과들을 막기 위해 얼마나 많은 어려움을 극복할 의향이 있는가?

SANS DevSecOps Toolchain

PRE-COMMIT

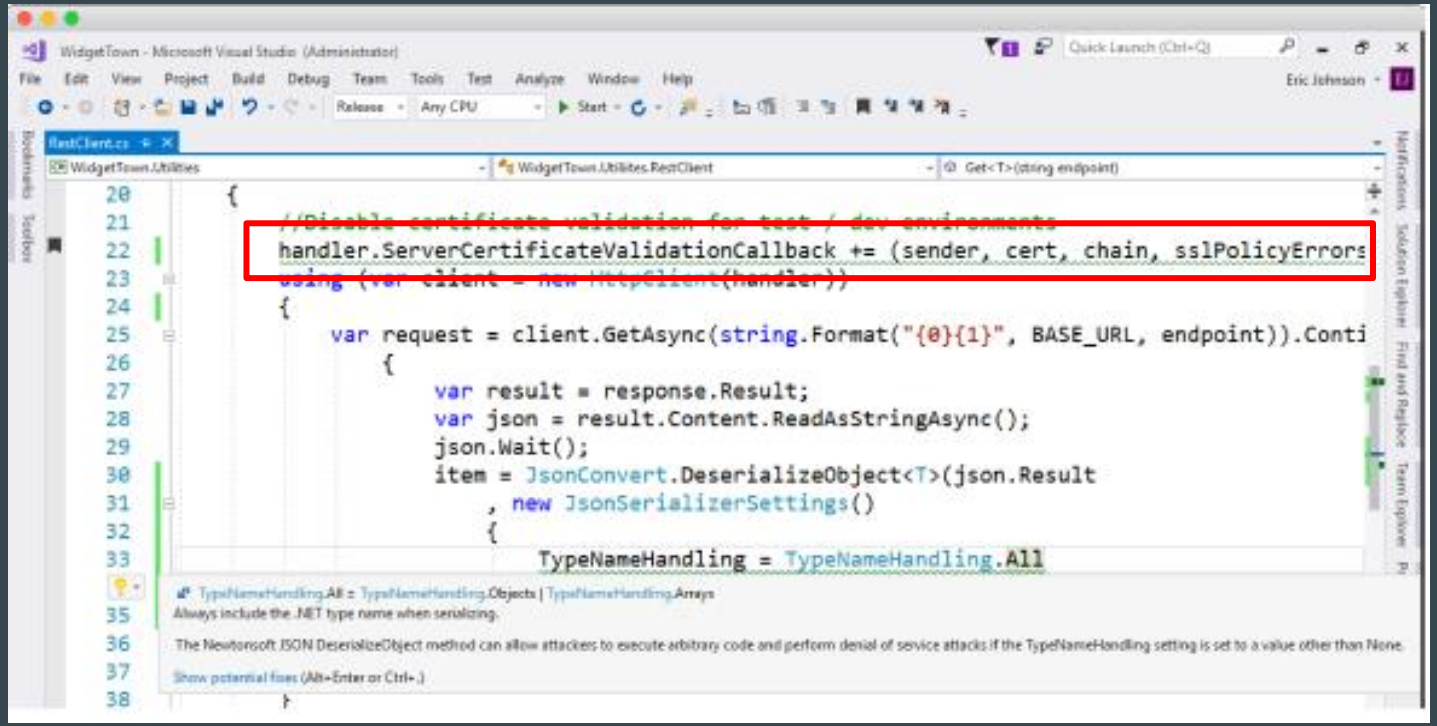
IDE Security Plugins

- FindSecurityBugs plugin : Eclipse, IntelliJ
  - http://find-sec-bugs.github.io
- Puma Scan plugin : Visual Studio
  - http://github.com/pumasecurity/puma-scan
- Microsoft DevSkim : VSCode, Sublime, Visual Studio
  - http://github.com/Microsoft/DevSkim
- SonarLint : Visual Studio, IntelliJ, Eclipse, VSCode, Atom
  - https://www.sonarlint.org

SANS DevSecOps Toolchain

PRE-COMMIT

IDE Security Plugins



SANS DevSecOps Toolchain

PRE-COMMIT

PRE-COMMIT Hooks

- Local : pre-commit
- Server-side : pre-commit, post-receive
- Tools
  - AWS Labs git-secrets (https://github.com/awslabs/git-secrets)
  - Talisman (https://github.com/thoughtworks/talisman)
  - Auth0 repo-supervisor (https://github.com/auth0/repo-supervisor)

```
$ git commit -m "testing git-secrets"

Web/Licensing/appsettings.json:5:
    "AccessKey": "AKIAJNQ7C2FCRR6B4VWA",
Web/Licensing/appsettings.json:6:
    "SecretKey": "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"

[ERROR] Matched one or more prohibited patterns
```

SANS DevSecOps Toolchain

PRE-COMMIT | **Commit (Continuous Integration)** | ACCEPTANCE | PRODUCTION | OPERATIONS

Fast, automated security checks during the build and Continuous Integration steps

Static Code Analysis (SCA):
- FindSecurityBugs
- Brakeman
- ESLint
- Phan

Security Unit Tests:
- JUnit
- Mocha
- xUnit

Infrastructure as Code Analysis:
- ansible-lint
- Foodcritic
- puppet-lint
- cfn_nag

Dependency Management:
- OWASP Dependency Check
- Bundler-Audit
- Gemnasium
- PHP Security Checker
- Retire.JS
- Node Security Platform

Container Security:
- Actuary
- Anchore
- Clair
- Dagda
- Docker Bench
- Falco

Container Hardening:
- Bane
- CIS Benchmarks
- grsecurity

SANS DevSecOps Toolchain

COMMIT(CI)

Static Code Analysis

- FindSecurityBugs : Java(Spring, Struts)
  - http://find-sec-bugs.github.io
- Phan : PHP (with composer)
  - http://github.com/etsy/phan
- NodeJsScan : JavaScript
  - https://github.com/ajinabraham/NodeJsScan
- Brakeman : Ruby
  - https://brakemanscanner.org/
- Bandit : Python
  - https://github.com/PyCQA/bandit/
- Flawfinder : C/C++
  - https://dwheeler.com/flawfinder/
- Puma Scan : C#
  - https://github.com/pumasecurity/puma-scan
- Gosec : Golang
  - https://github.com/securego/gosec/

SANS DevSecOps Toolchain

COMMIT(CI)

Container Security

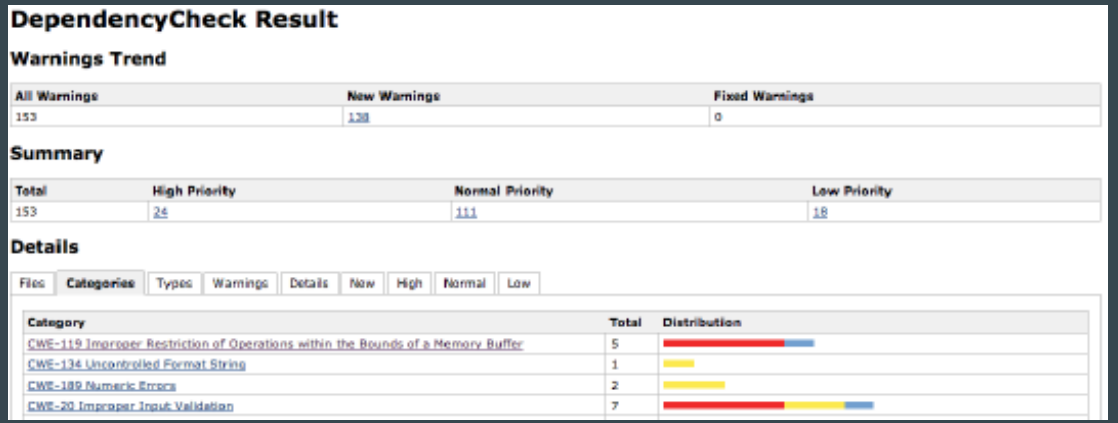
- Docker Benchmark Inspec Profile
  - https://github.com/dev-sec/cis-docker-benchmark
- Anchore
  - https://anchore.com/opensource/
- Actuary
  - https://github.com/diogomonica/actuary
- Clair
  - https://github.com/coreos/clair
- Falco
  - https://falco.org/

SANS DevSecOps Toolchain

COMMIT(CI)

Dependency Management

- OWASP Dependency Check : Java, .NET, Ruby, Python, Node.js
  - https://www.owasp.org/index.php/OWASP_Dependency_Check
- PHP Security Checker : PHP
  - http://github.com/etsy/phan
- Bundler-Audit : Ruby
  - https://github.com/rubysec/bundler-audit
- NPM Audit / Retire.JS : Node.js
  - https://docs.npmjs.com/cli/audit
  - https://retirejs.github.io/retire.js/



DependencyCheck Result

Warnings Trend

All Warnings	New Warnings	Fixed Warnings
153	138	0

Summary

Total	High Priority	Normal Priority	Low Priority
153	24	111	18

Details

Files | Categories | Types | Warnings | Details | New | High | Normal | Low

Category	Total	Distribution
CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer	5	
CWE-134 Uncontrolled Format String	1	
CWE-189 Numeric Errors	2	
CWE-20 Improper Input Validation	7	

SANS DevSecOps Toolchain

PRE-COMMIT | COMMIT(CI) | Acceptance (Continuous Delivery) | PRODUCTION

Automated security acceptance, functional testing, and deep out-of-band scanning during Continuous Delivery

Infrastructure as Code:
- Ansible
- Chef
- Puppet
- SaltStack
- Terraform
- Vagrant

Immutable Infrastructure:
- Docker
- rkt

Security Scanning:
- Arachni
- nmap
- sqlmap
- sslyze
- ZAP
- ssh_scan

Cloud Configuration Management:
- AWS CloudFormation
- Azure Resource Manager
- Google Cloud Deployment Manager

Security Acceptance Testing:
- BDD-Security
- Gauntlt
- Mittn

Infrastructure Tests:
- Serverspec
- Test Kitchen

Infrastructure Compliance Checks:
- HubbleStack
- InSpec

SANS DevSecOps Toolchain

PRE-COMMIT | COMMIT(CI) | ACCEPTANCE

Production (Continuous Deployment)

Security checks before, during, and after code is deployed to production

Security Smoke Tests:
- ZAP Baseline Scan
- nmap
- ssllabs-scan

Configuration Safety Checks:
- AWS Config
- AWS Trusted Advisor
- Microsoft Azure Advisor
- Security Monkey
- OSQuery

Secrets Management:
- Ansible Vault
- Blackbox
- Chef Vault
- Docker Secrets
- Hashicorp Vault
- Pinterest Knox

Cloud Secrets Management:
- AWS KMS
- Azure Key Vault
- Google Cloud KMS

Cloud Security Testing:
- CloudSploit
- Nimbostratus

Server Hardening:
- dev-sec.io
- SIMP

Host Intrusion Detection System (HIDS):
- fail2ban
- OSSEC
- Samhain

SANS DevSecOps Toolchain

PRE-COMMIT | COMMIT(CI) | ACCEPTANCE | PRODUCTION

Operations

Continuous security monitoring, testing, audit, and compliance checks

Fault Injection:
- Chaos Kong
- Chaos Monkey

Cyber Simulations:
- Game day exercises
- Tabletop scenarios

Penetration Testing:
- Attack-driven defense
- Bug Bounties
- Red team exercises

Threat Intelligence:
- Diamond Model
- Kill Chain
- STIX
- TAXII

Continuous Scanning:
- OpenSCAP
- OpenVAS
- Prowler
- Scout2
- vuls

Blameless Postmortems:
- Etsy Morgue

Continuous Monitoring:
- grafana
- graphite
- statsd
- seyren
- sof-elk
- ElastAlert
- 411

Cloud Monitoring:
- CloudWatch
- CloudTrail
- Reddalert

Cloud Compliance:
- Cloud Custodian
- Compliance Monkey
- Forseti Security

SANS DevSecOps Toolchain

PRE-COMMIT | COMMIT (CI) | ACCEPTANCE | PRODUCTION | OPERATIONS

DevSecOps!
감사합니다.