DevSecOps хэрэгжүүлсэн туршлагаас...

Implementing Software Supply Chain Security using DevSecOps

С.Дөлмандах - Аравт Технологи

Дөлмандах

- 20 жилийн туршлага
  - Системийн администратор
  - Хөгжүүлэгч
    - Python, JavaScript, React (React Native)...
  - Зөвлөх
    - DevSecOps
    - Cloud Native, Kubernetes
    - Чанарын удирдлага
    - Автоматжуулалт


CERTIFIED
kubernetes
ADMINISTRATOR


Istio
CERTIFIED
Associate


CERTIFIED
kubernetes
APPLICATION
DEVELOPER


GitLab
Certified
Services
Engineer
Professional


Vault
CERTIFIED
ASSOCIATE
HCVA0-002

Software is eating the world

Marc Andreessen, 2011

9.22 их наяд $

Cybercrime cost, 2024

87 тэрбум $

Cyber security cost, 2024

80:1

Developers vs security engineers

Шийдэл байна уу 

Cost of remediation

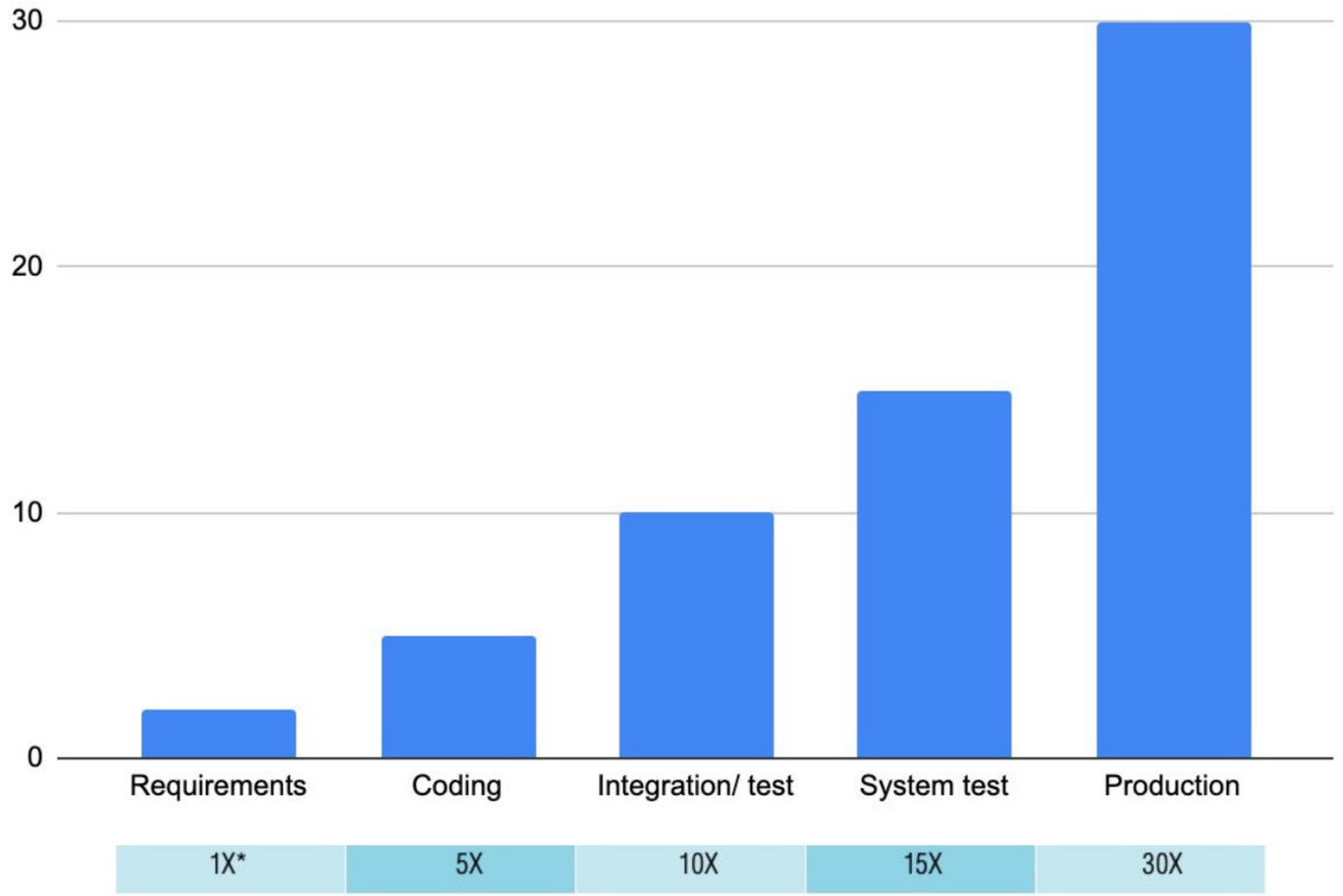
Software bugs cost $59.5 billion annually*
Cost of software developer: $300/hour**

Hours to fix bug
Cost

@ coding stage: 2.4*	$720
@ Integration stage: 4.1*	$1,230
@ System stage: 6.2*	$1,860
@ Production stage: 13.1*	$3,930

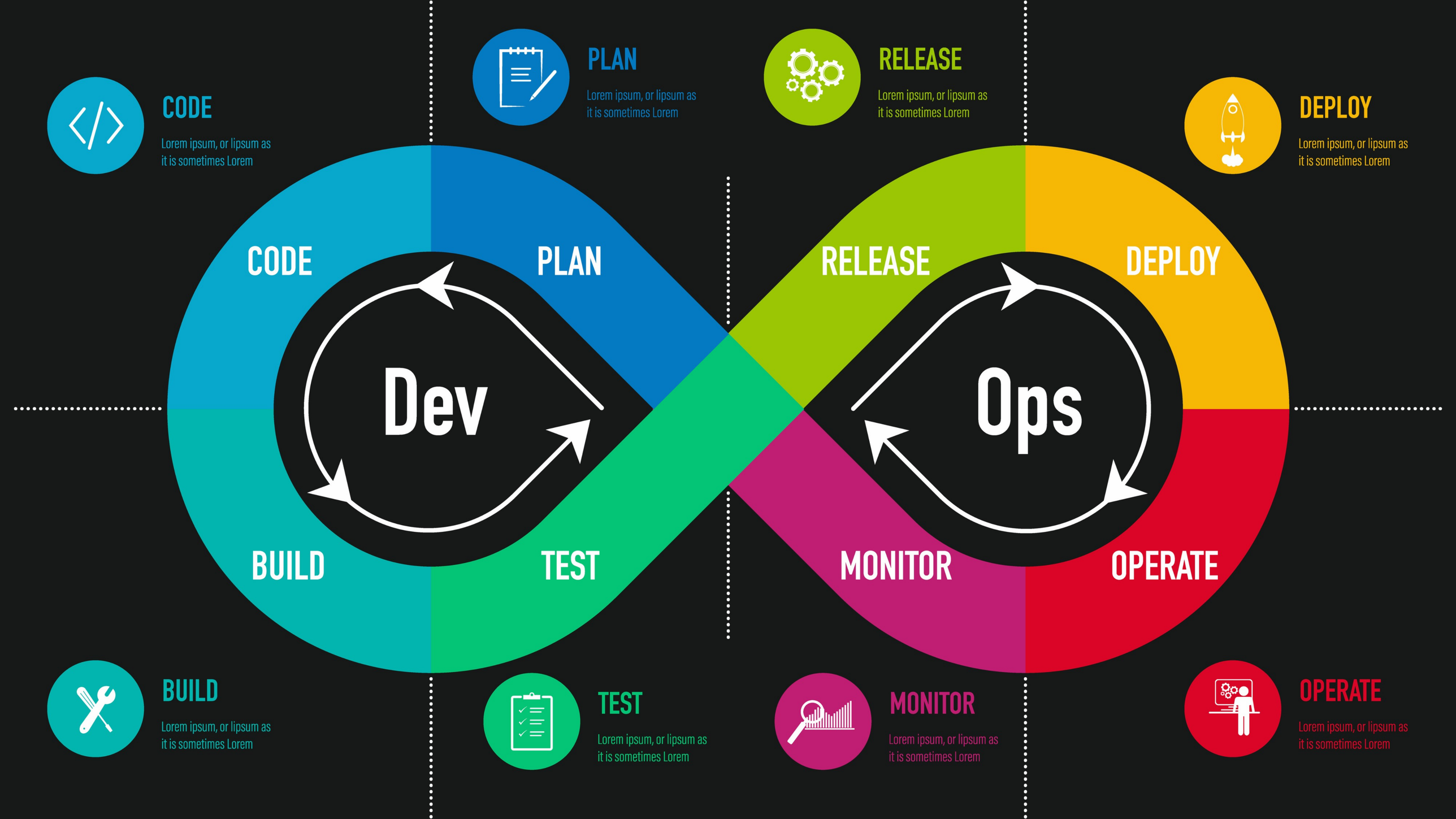
*(NIST - Impact of Inadequate Software Testing
**2019 SW Dev Price Guide

Stage of remediation



DevOps

Shift 👈 (left)


CODE
Lorem ipsum, or lipsum as it is sometimes Lorem
PLAN
Lorem ipsum, or lipsum as it is sometimes Lorem
RELEASE
Lorem ipsum, or lipsum as it is sometimes Lorem
DEPLOY
Lorem ipsum, or lipsum as it is sometimes Lorem
CODE
PLAN
RELEASE
DEPLOY
Dev
Ops
BUILD
TEST
MONITOR
OPERATE
BUILD
Lorem ipsum, or lipsum as it is sometimes Lorem
TEST
Lorem ipsum, or lipsum as it is sometimes Lorem
MONITOR
Lorem ipsum, or lipsum as it is sometimes Lorem
OPERATE
Lorem ipsum, or lipsum as it is sometimes Lorem

DevOps

Албан тушаал эсвэл хэлтэс биш....

- Нийтлэг алдаа
  - Тусдаа DevOps хэлтэс байгуулдаг
  - Хөгжүүлэлт болон үйл ажиллагааг нийлүүлдэг
  - Ийм албан тушаал үүсгэдэг, бүгдийг даатгадаг

DevOps

Албан тушаал эсвэл хэлтэс биш....

- Сэтгэлгээ, хандлага болон соёлын өөрчлөлт
  - Хөгжүүлэгч илүү хариуцлага, үүрэг хүлээнэ
  - Үүргийг нь дагаж эрхийг нь нэмж өгнө
  - Автоматжуулах
- Platform Engineering

Надад тулах цэг өг, тэгвэл би дэлхийг эргүүлж чадна

Архимед, МЭӨ 287—212

DevSecOps

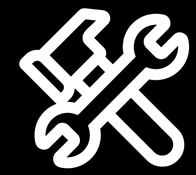
Shift 👈 (left)

Хөгжүүлэгчид аюулгүй
байдлыг хариуцуулах юм уу 

DevSecOps

Бодит байдал дээр...

- Олон төрлийн хэл болон технологийг бүгдийг мэдэх боломжгүй
- Бизнесийн өрсөлдөөний улмаас хурдан хөгжүүлэх, нэвтрүүлэх шаардлагатай
- Хөгжүүлэгч болон аюулгүй байдлын инженерийн тооны харьцаа
- Хөгжүүлэгч өөрөө кодоо маш сайн мэднэ 😎



Багажыг нь өг

Secret detection

Эмзэг мэдээлэл бий юу

- Код болон тохиргооны файл дахь эмзэг мэдээлэл
  - Нууц үг
  - Крипто түлхүүр
  - Хандах эрхийн токэн
- Өөрчлөлт бүрт ажиллуулж шалгах
- Илэрсэн бол өөрчилж, солих. Нэгэнт хувилбар удирдах системээр тарчихсан

Secret detection

Эмзэг мэдээлэл бий юу

- Хэрэгжүүлэхэд маш хялбар
- Нууц үг болон токеныг тусгай угтвартай болгох, илрүүлэхэд хялбар б
  - HashiCorp Vault - hvs. эсвэл hvb.
  - GitLab - glpat-,
  - GitHub - ghp

Dependency scanner

Цоорхойтой сан ашиглаагүй биз

- Ашиглаж байгаа програм хангамж, сангийн хувилбарыг шалгана
  - Аюулгүй байдлын эрсдэл илэрсэн эсэх
  - Илэрсэн эрсдэлийн зэрэг (severity)
- Тогтмол хуваарийн дагуу ажиллуулах, шалгах
- Хувилбар шинэчлэх ажлыг тогтмолжуулах
- Software Bill Of Material буюу орцыг тогтмол хөтлөх

Static Application Security Testing (SAST)

(алдаатай код байна уу

- Кодын хэв шинжийг шалгаж эрсдэлтэй эсэхийг шалгана
  - SQL Injection
  - Information disclosure/security
  - Stack buffer overflow
  - Uncontrolled resource consumption
- Кодын өөрчлөлт бүрт ажиллуулна

Бусад багажууд

- Dynamic Application Security Testing (DAST)
- Infrastructure as Code (IaC) scanner
- Container scanner
- Fuzz testing

Илрүүлчихлээ,
🕵️♂️эгээд яах билээ 🤷‍♂️

Бодлого, дүрэм маш чухал

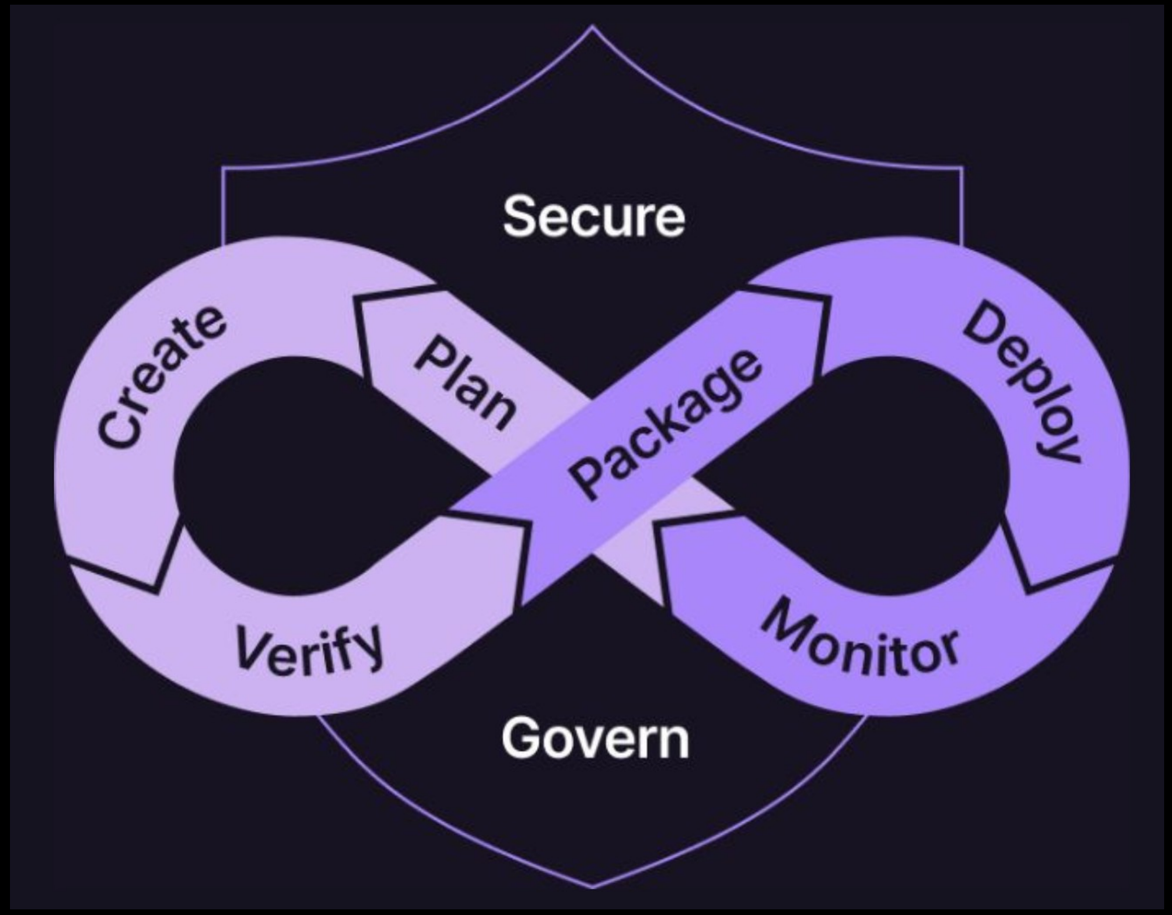
Хэн, хэзээ, хэрхэн...

- Хэн, хэзээ ажиллуулах вэ?
  - Өөрчлөлт бүрт автоматаар ажиллах - Secret detection, SAST
  - 7 хоног тутам ажиллах - Dependency scanner
- Өөрчлөлт дээр эрсдэл илэрвэл яах билээ?
  - Үндсэн код руу нийлүүлэхээс сэргийлэх боломжтой юу?
- Үндсэн кодонд эрсдэл илэрвэл яах билээ?
  - Хэн, хэзээ засах билээ? Тоог хэрхэн буулгах вэ?
- Хөгжүүлэгчийн ажлын үнэлгээнд хэрхэн нөлөөлөх вэ?

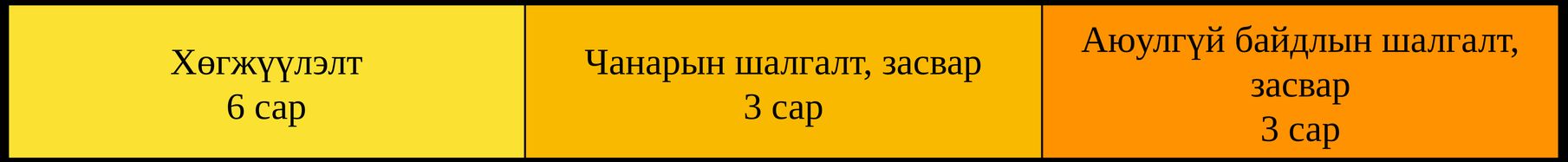
DevSecOps

Үр дүн

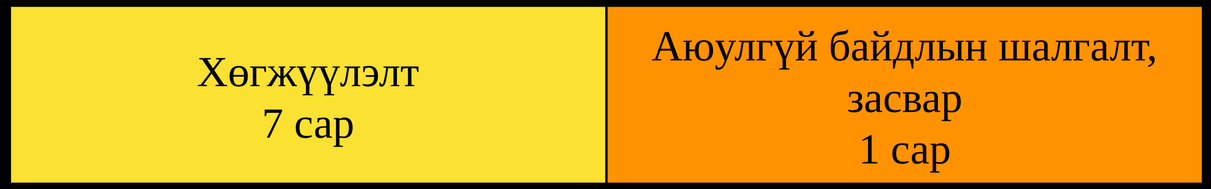
- Бодит үнэнтэй нүүр тулсан 😳
- Шинэ соёл, хамтын ажиллагаа
- Эрсдэлийн тоо хэмжээ 📉
- Хөгжүүлэгчийн бүтээмж 🚀



Уламжлалт



DevSecOps



Чанар, хяналтын тогтолцоо

CIS Software Supply Chain Security Guide...

- Өөрчлөлт бүрийг хувилбар удирдах системд бүртгэнэ - 1.1.1
- Хөгжүүлэгч үндсэн кодыг шууд өөрчлөх боломжгүй байна - 1.1.14
  - Өөрчлөлт бүрийг тус тусын мөчирт (branch) хийж хийж, чанарын шаардлага хангаж байгаа эсэхийг шалгана - 1.1.9
  - Өөрчлөлт бүрийг эрсдэлтэй эсэхийг автоматаар шалгана - 1.1.18
  - Өөрчлөлт нь эмзэг мэдээлэл агуулж байгаа эсэхийг шалгана - 1.5.1
  - Өөрчлөлтийг дор хаяж 2 хүн хянаж, зөвшөөрөл өгнө - 1.1.3
  - Өөрчилж буй кодын эзнээс зөвшөөрөл авна - 1.1.7

Чанар, хяналтын тогтолцоо

CIS Software Supply Chain Security Guide...

- Програм яг үндсэн эх кодоос үүссэн үү?
  - Шинэ хувилбар гаргахад хүний гараар дамждаг юм биш биз
  - Хөгжүүлэгч эх кодыг өөрчилсөн байх вий
  - Хөгжүүлэгчийн компьютер халдлагад өртсөн байх вий
- Хувилбар гаргах процессыг автоматжуулах
  - Хэн, хэзээ автомат процессыг эхлүүлсэн
  - Эх кодын аль өөрчлөлтийг (commit) агуулж байгаа эсэх бүртгэл

Анхаарал тавьсанд
баярлалаа 🙏