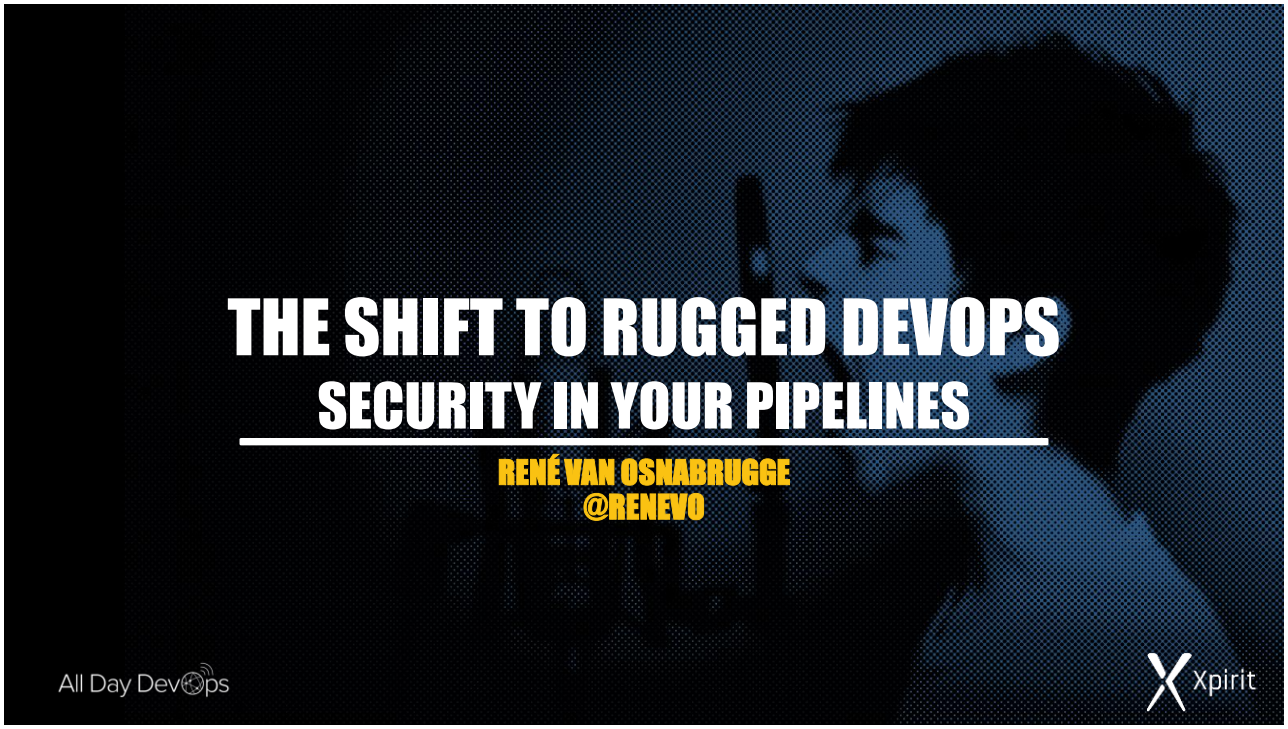
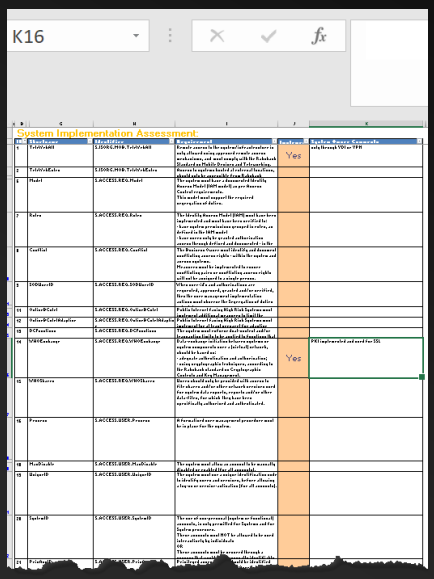

THE SHIFT TO RUGGED DEVOPS
SECURITY IN YOUR PIPELINES
RENÉ VAN OSNABRUGGE
@RENEVO
All Day DevOps
Xpirit


COMPLIANCY
Xpirit
All Day DevOps

@renevo

COMPLIANCY



The system must display a warning message indicating that only authorised use is permitted before allowing users to log-on (for all user accounts).

Access to information and system functions should be restricted, in accordance with the documented model.

Logged information should not contain passwords, cryptographic keys or any other confidential information in clear text

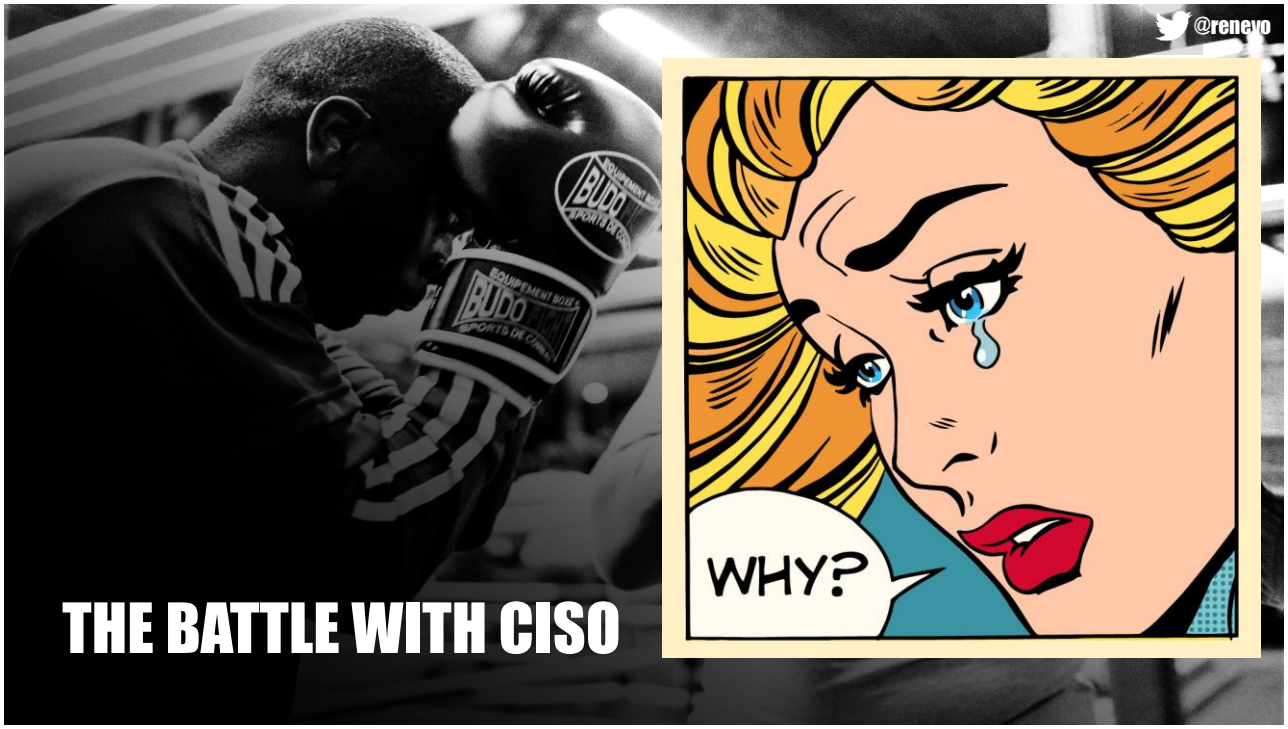
Xpirit

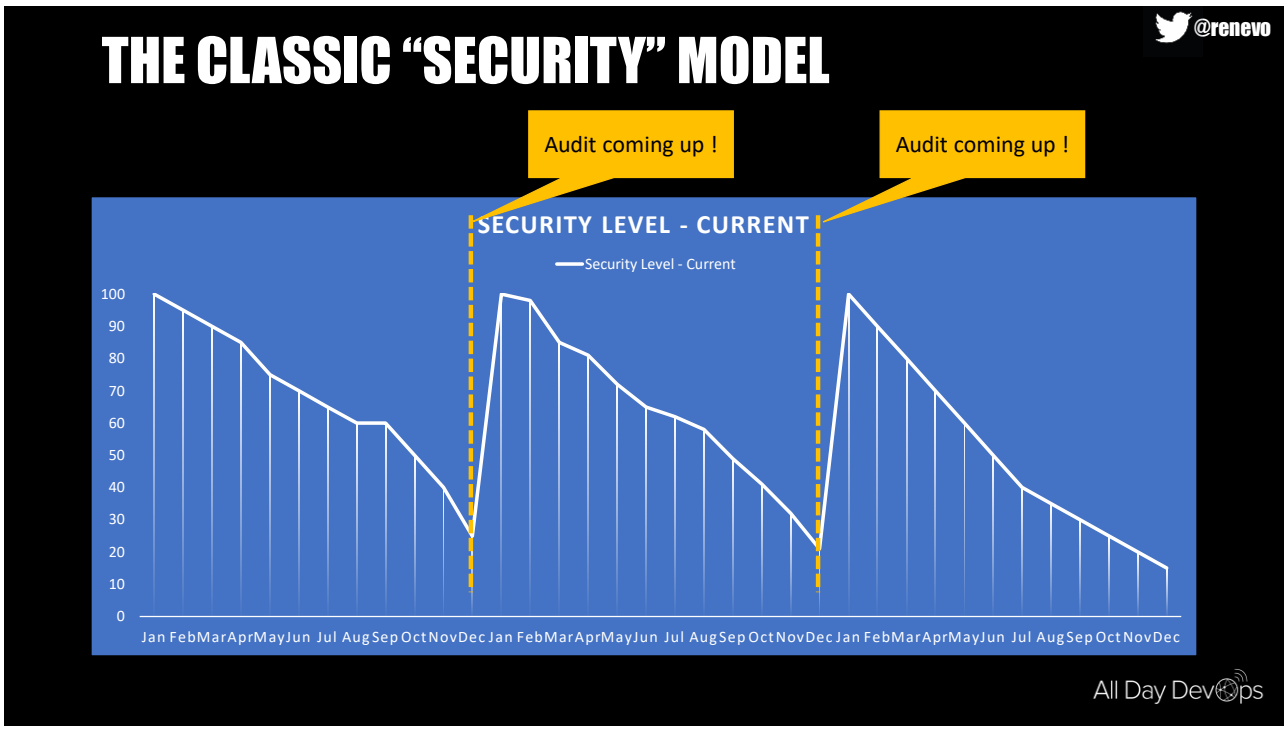
All Day DevOps

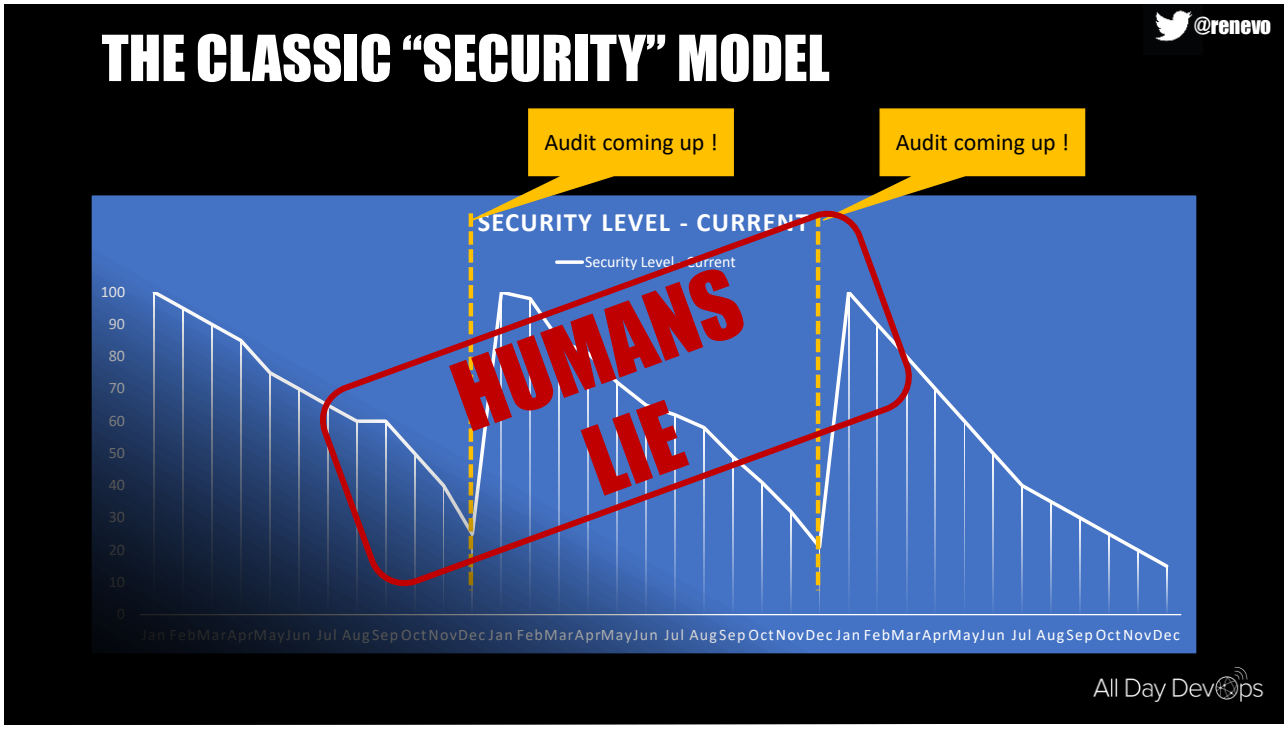
@renevo

IMPOSSIBLE TO UNDERSTAND
IMPOSSIBLE TO IMPLEMENT
IMPOSSIBLE TO VALIDATE
IMPOSSIBLE TO MAINTAIN

All Day DevOps

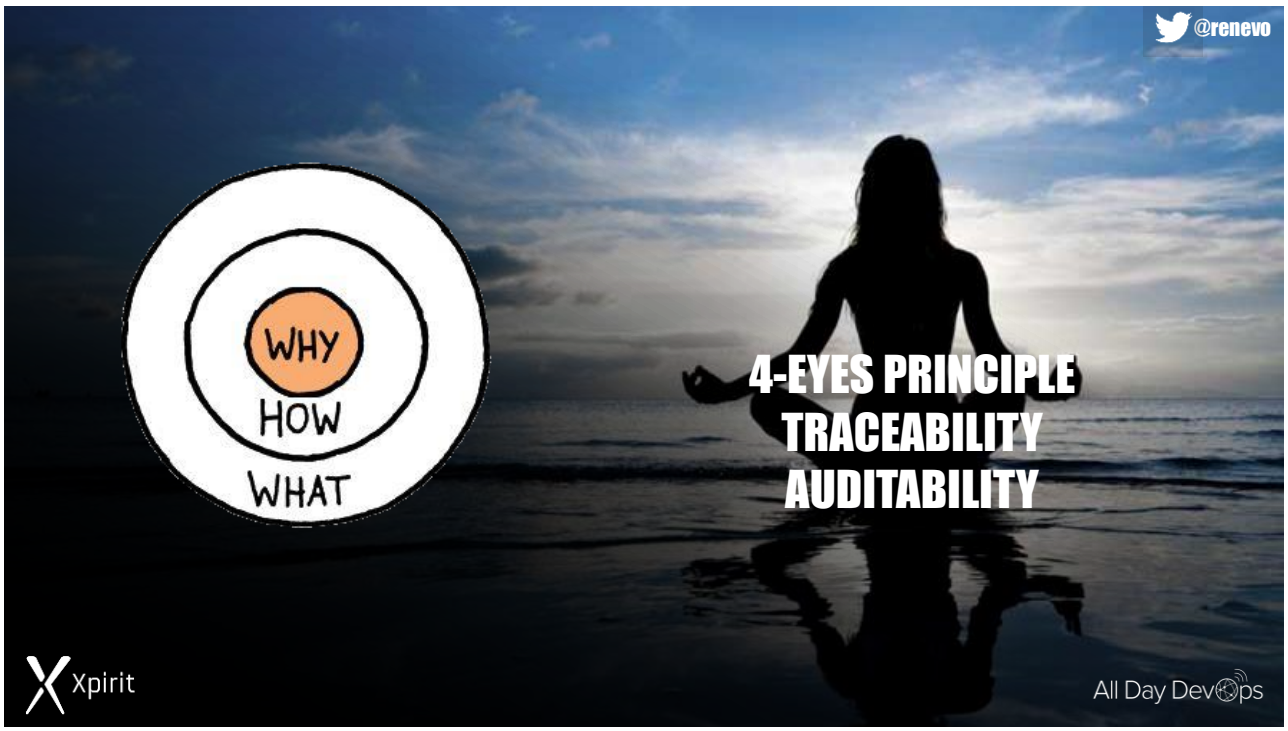

@renevo
WHY?
THE BATTLE WITH CISO


@renevo
THE CLASSIC "SECURITY" MODEL
Audit coming up !
Audit coming up !
SECURITY LEVEL - CURRENT
Security Level - Current
100
90
80
70
60
50
40
30
20
10
0
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
All Day DevOps


@renevo
THE CLASSIC "SECURITY" MODEL
Audit coming up !
Audit coming up !
SECURITY LEVEL - CURRENT
Security Level - Current
HUMANS LIE
100
90
80
70
60
50
40
30
20
10
0
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
All Day DevOps


@renevo
ISO 27001
COBIT
SOX
PCI
AUTHORITIES
ETC.
Xpirit
All Day DevOps


@renevo
WHY
HOW
WHAT
CONFIDENTIALITY
INTEGRITY
AVAILABILITY
Xpirit
All Day DevOps


@renevo
WHY
HOW
WHAT
4-EYES PRINCIPLE
TRACEABILITY
AUDITABILITY
Xpirit
All Day DevOps

@renevo

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Sept. 7, 2017

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers.

The attack on the company represents one of the la
personally sensitive information in recent years, an
cybersecurity threat for the agency since 2015.

BRIEF

Cyberattack cost Maersk up to $300M

AUTHOR

Edwin Lopez
@EdwinLopezT37

PUBLISHED

Nov. 8, 2017

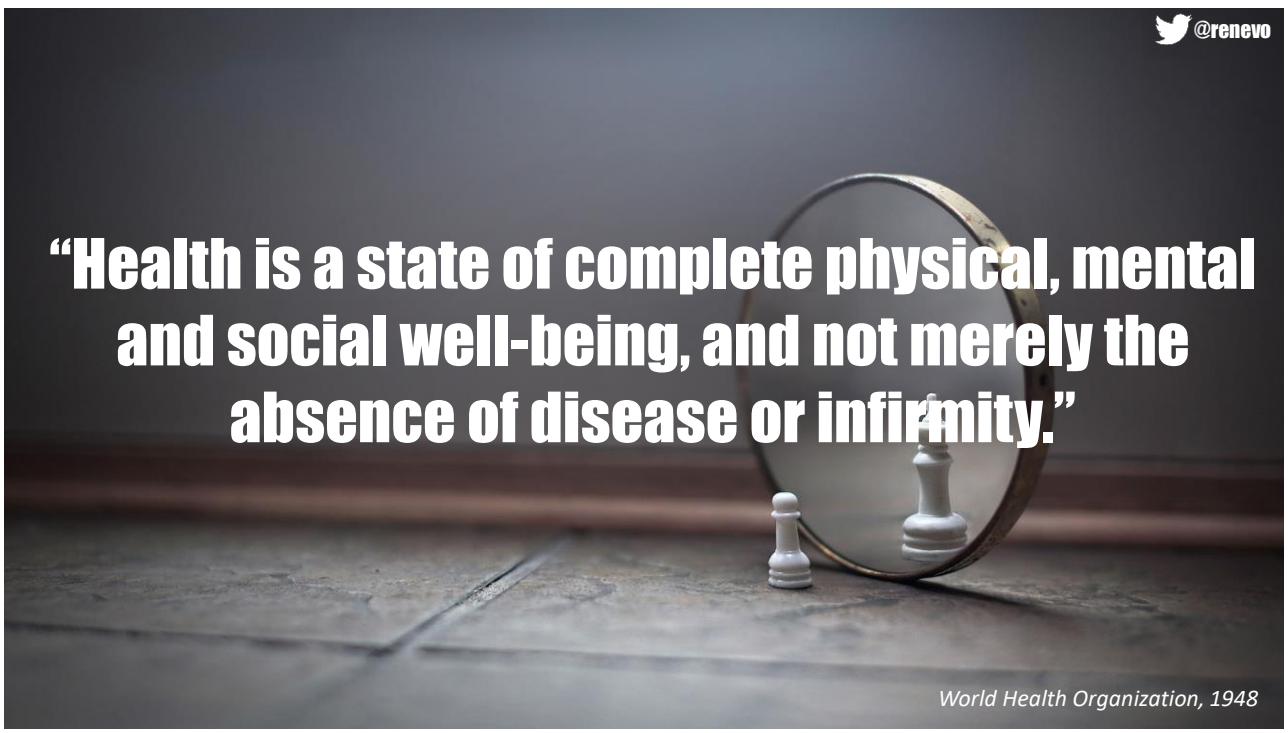
Dive Brief:

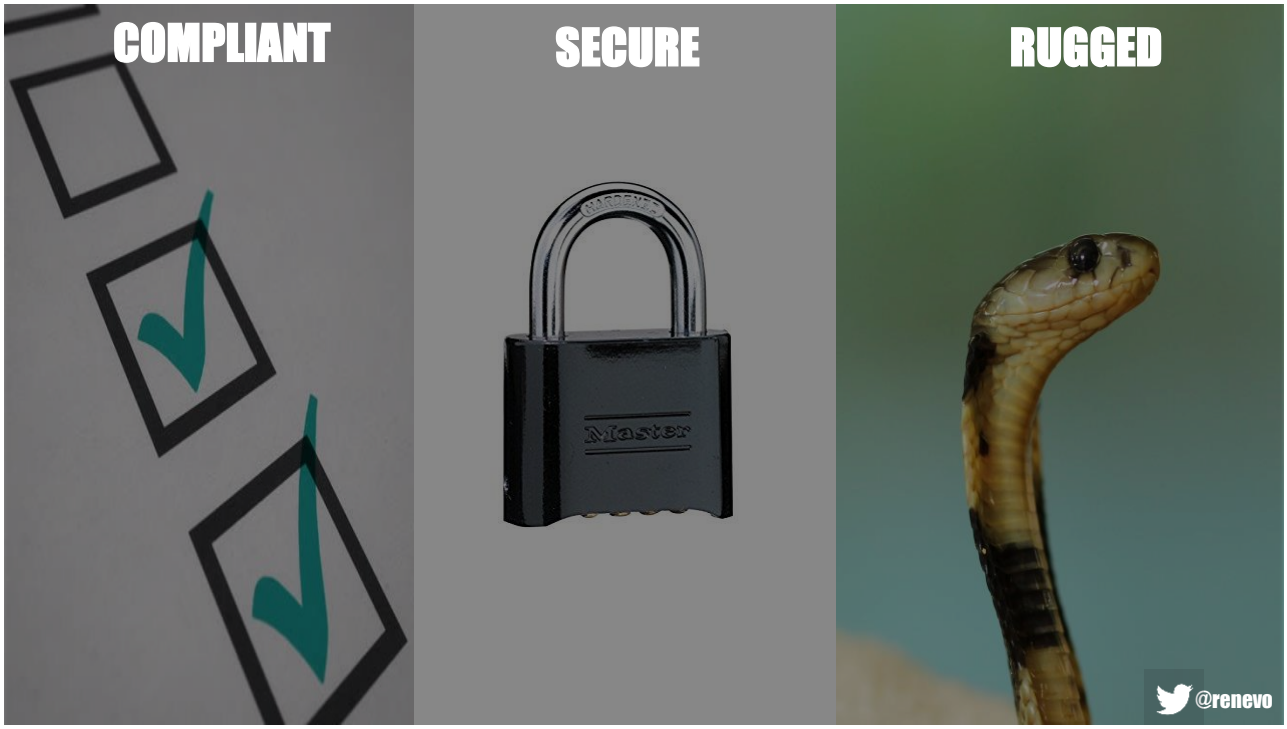
- The June 27 Nyetya cyberattack cost A.P. Moller – Maersk (Maersk Group) $250 to $300 million, CEO Soren Skou said during an earnings call with investors on Tuesday.
- Maersk Line was hit hard, recording a $220 million net operating profit/loss after tax (NOPAT). "Had we not (had) the cyberattack, Maersk Line would have made a delivery in the NOPAT in the range of $450 million to $500 million for the quarter, consistent with almost 10% return on the invested capital," said Skou.

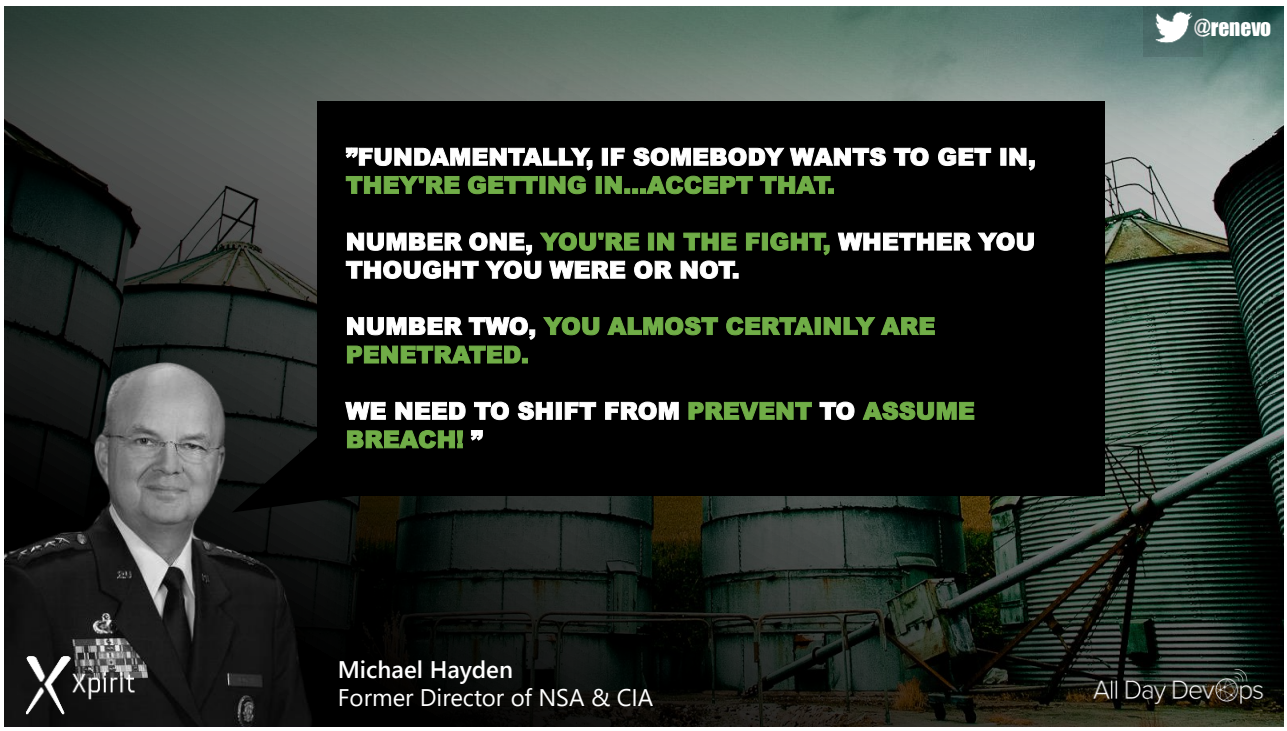
Xpirit

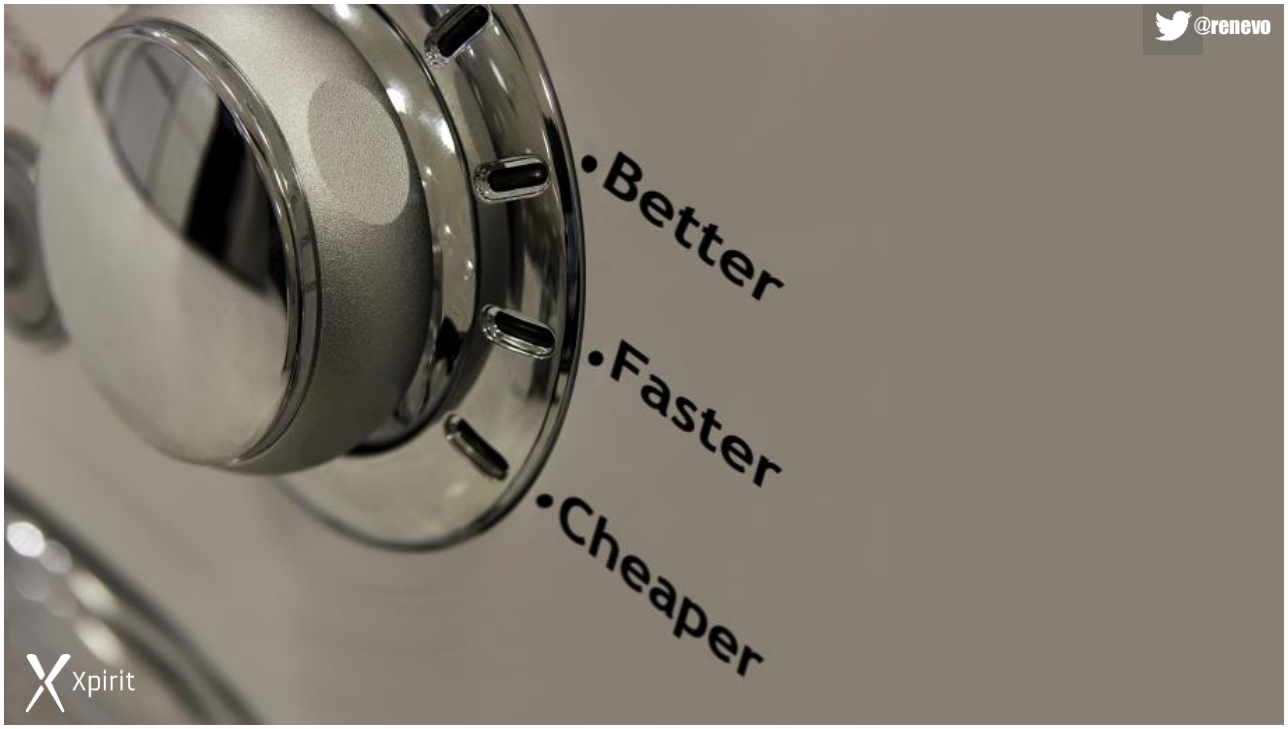
All Day DevOps

@renevo



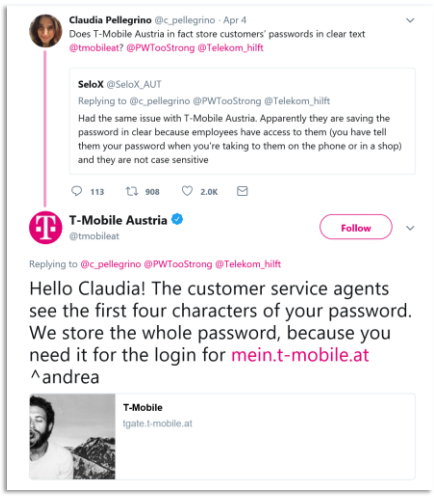

COMPLIANT
SECURE
RUGGED
Master
@renevo

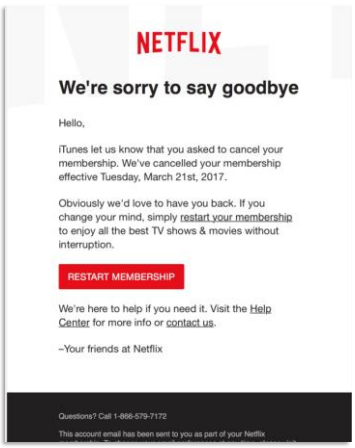

@renevo
"FUNDAMENTALLY, IF SOMEBODY WANTS TO GET IN, THEY'RE GETTING IN...ACCEPT THAT.
NUMBER ONE, YOU'RE IN THE FIGHT, WHETHER YOU THOUGHT YOU WERE OR NOT.
NUMBER TWO, YOU ALMOST CERTAINLY ARE PENETRATED.
WE NEED TO SHIFT FROM PREVENT TO ASSUME BREACH! "
Michael Hayden
Former Director of NSA & CIA
Xpirit
All Day DevOps


@renevo
•Better
•Faster
•Cheaper
Xpirit

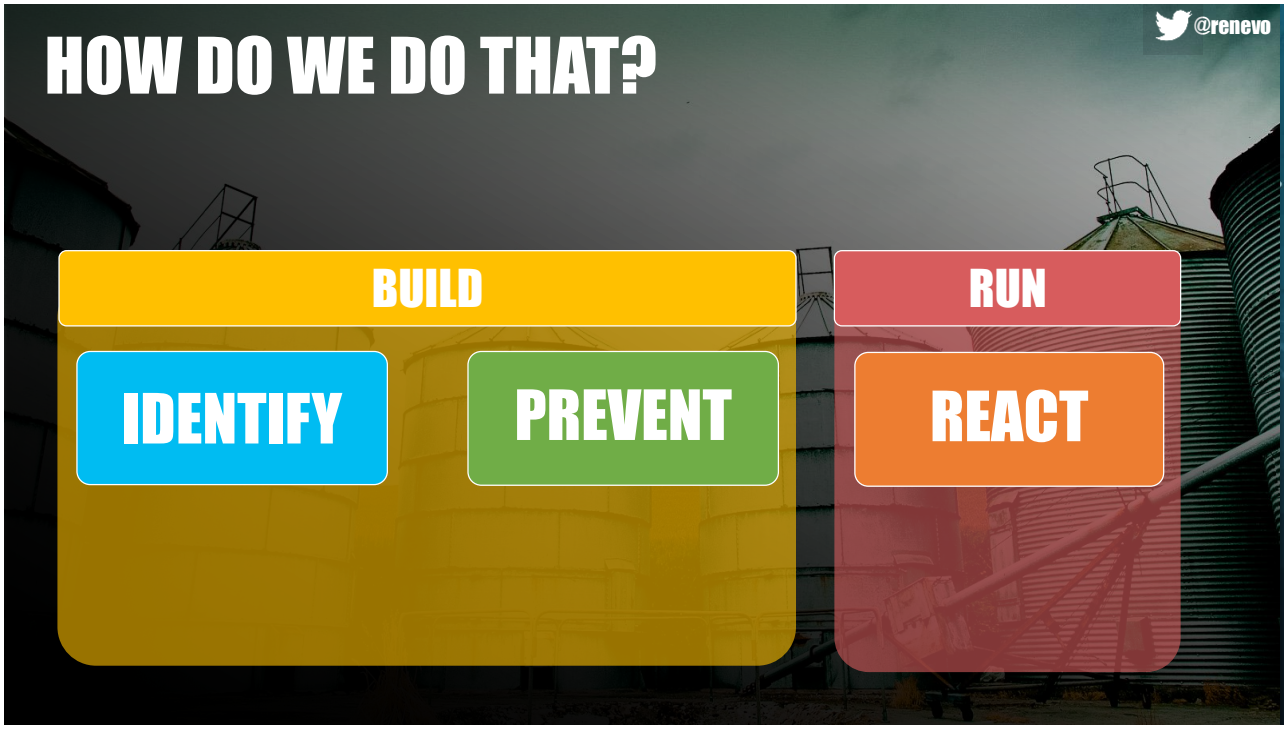

@renevo
SECURITY IS THE NEXT SILO TO TEAR DOWN
All Day DevOps

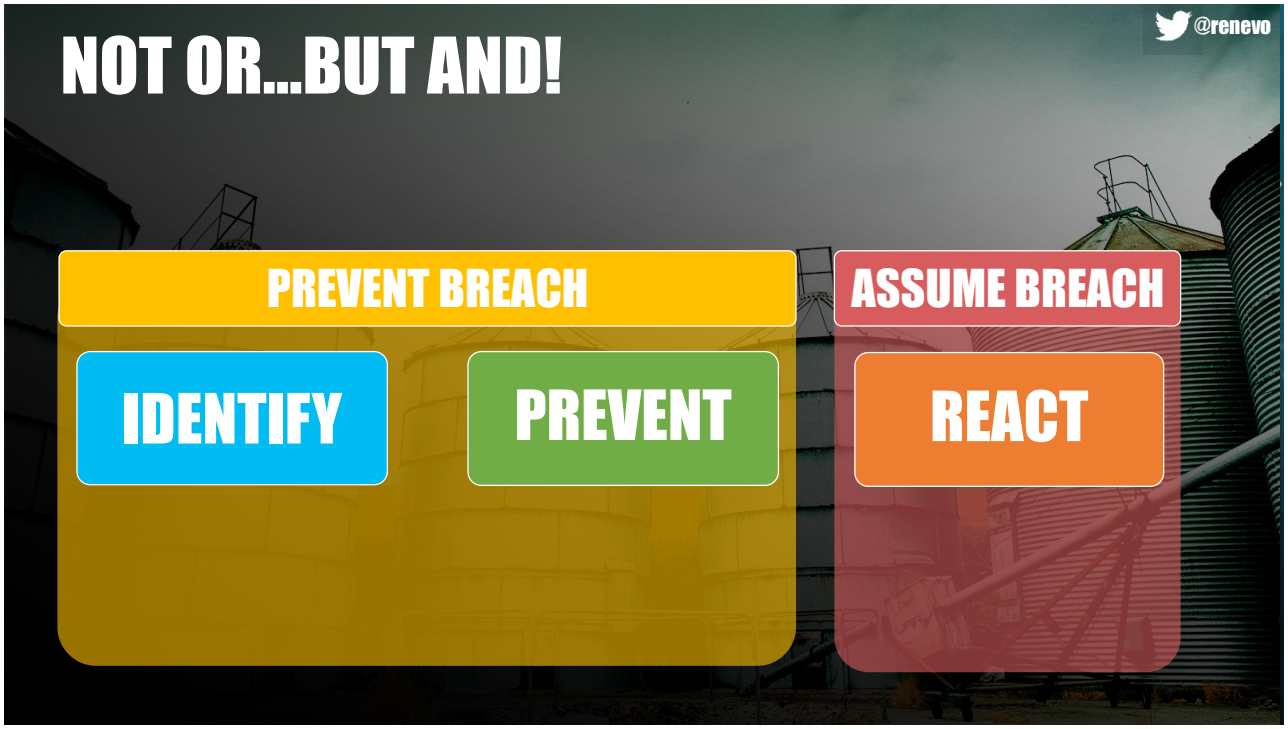
IT STARTS WITH AWARENESS !



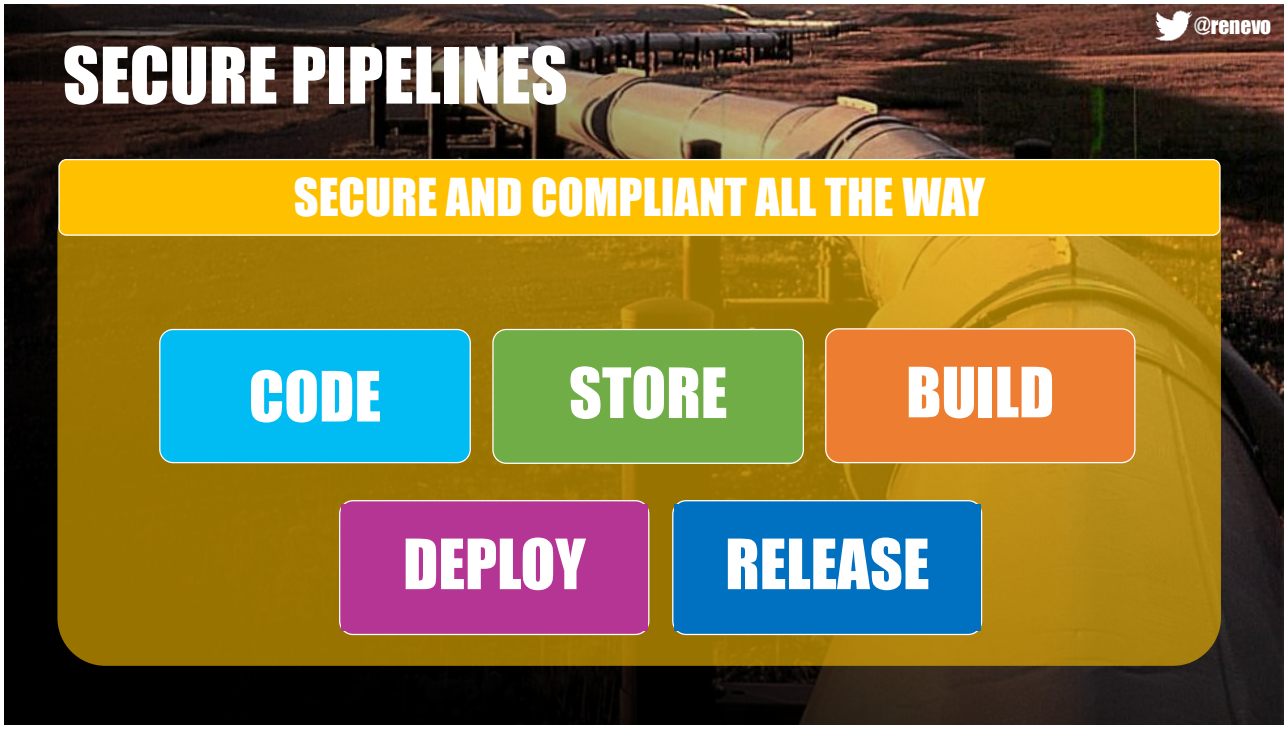


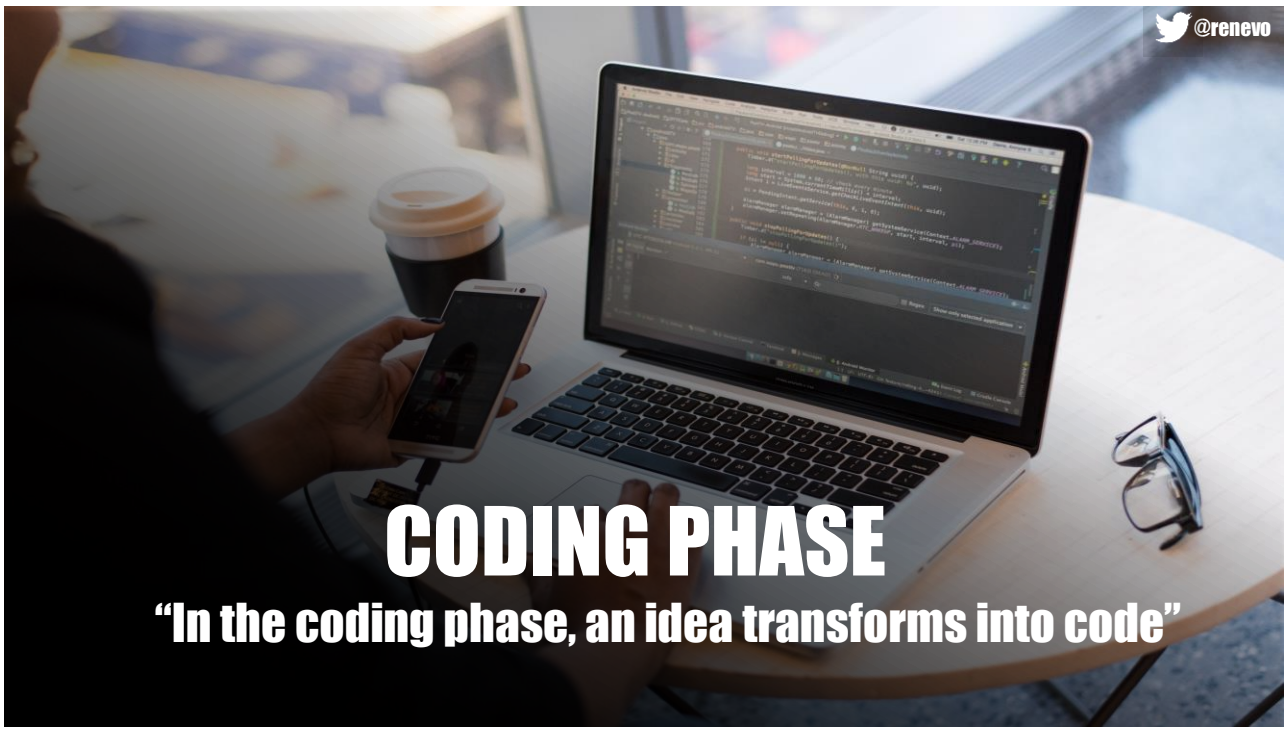

@renevo
SHIFT LEFT SECURITY
Make them part of your team!
All Day DevOps


@renevo
HOW DO WE DO THAT?
BUILD
RUN
IDENTIFY
PREVENT
REACT


NOT OR...BUT AND!
@renevo
PREVENT BREACH
ASSUME BREACH
IDENTIFY
PREVENT
REACT


PREVENT BREACH
All Day DevOps


@renevo
SECURE PIPELINES
SECURE AND COMPLIANT ALL THE WAY
CODE
STORE
BUILD
DEPLOY
RELEASE


@renevo
CODING PHASE
"In the coding phase, an idea transforms into code"

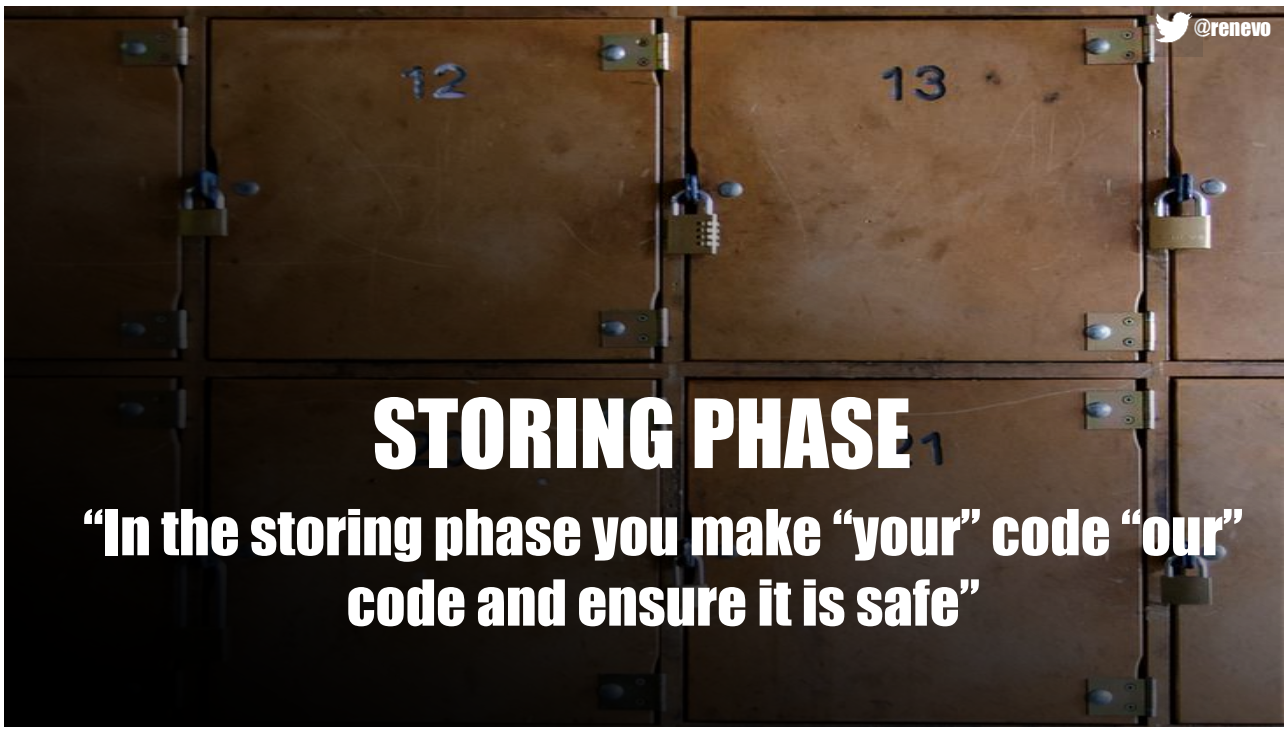
@renevo

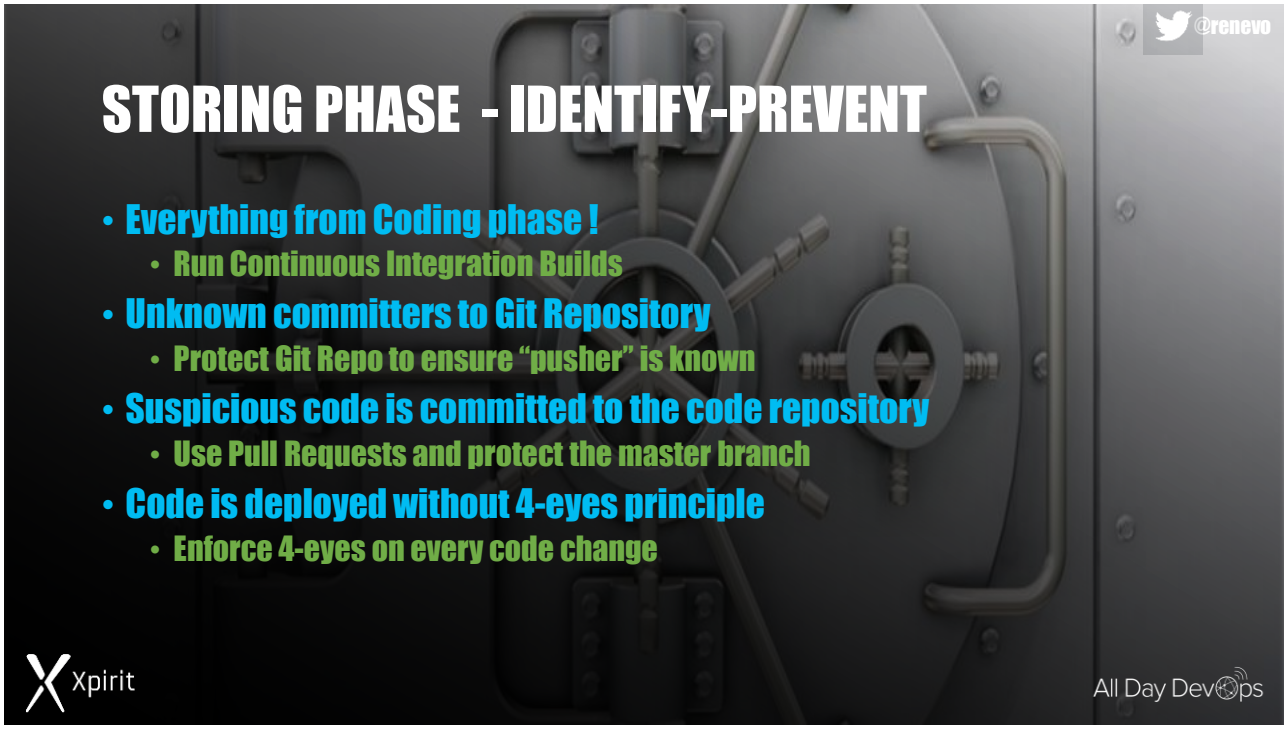
CODING PHASE - IDENTIFY-PREVENT

- Bad coding practices resulting in Technical Debt
  - First stage - Static Code Analysis
- Non Deployable code
  - Compiling / Syntax Checking
- Untested code and therefore unintended consequences
  - Unit Tests
- Passwords/Secrets etc. exposed in code
  - Credential and Secret Scanning

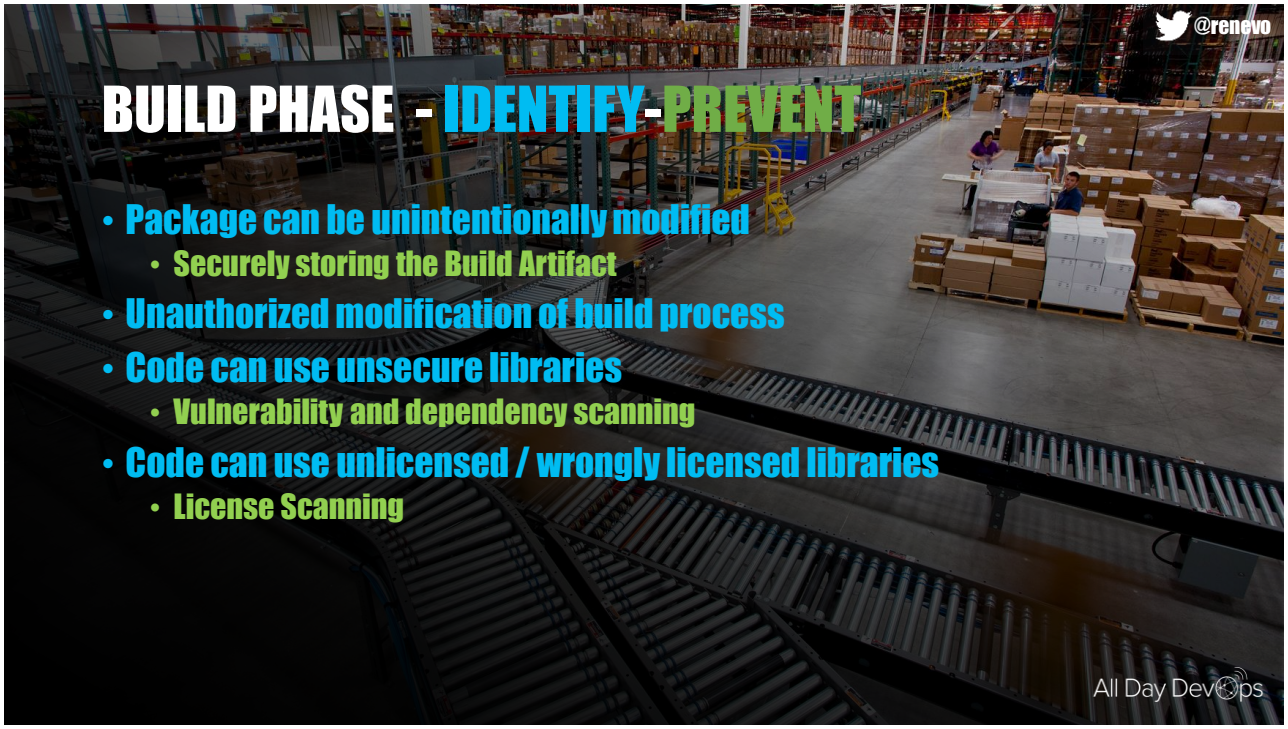
Xpirit

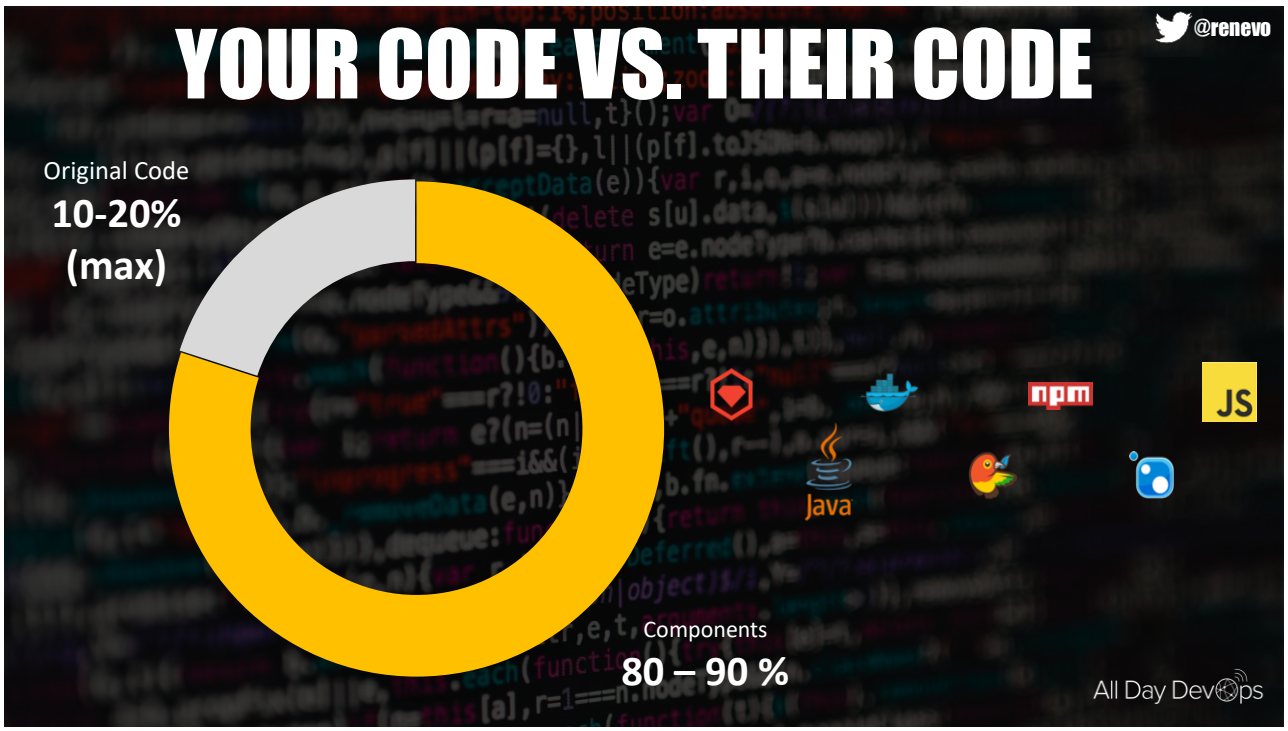
All Day DevOps




@renevo
STORING PHASE - IDENTIFY-PREVENT
• Everything from Coding phase !
• Run Continuous Integration Builds
• Unknown committers to Git Repository
• Protect Git Repo to ensure "pusher" is known
• Suspicious code is committed to the code repository
• Use Pull Requests and protect the master branch
• Code is deployed without 4-eyes principle
• Enforce 4-eyes on every code change
Xpirit
All Day DevOps


@renevo
BUILD PHASE
"In the build phase we transform the product from code and script into an immutable and versioned package"


@renevo
BUILD PHASE - IDENTIFY-PREVENT
• Package can be unintentionally modified
• Securely storing the Build Artifact
• Unauthorized modification of build process
• Code can use unsecure libraries
• Vulnerability and dependency scanning
• Code can use unlicensed / wrongly licensed libraries
• License Scanning
All Day DevOps


@renevo
YOUR CODE VS. THEIR CODE
Original Code
10-20%
(max)
Components
80 – 90 %
Java
npm
JS
All Day DevOps

@renevo

AND THEN THERE IS LICENSING

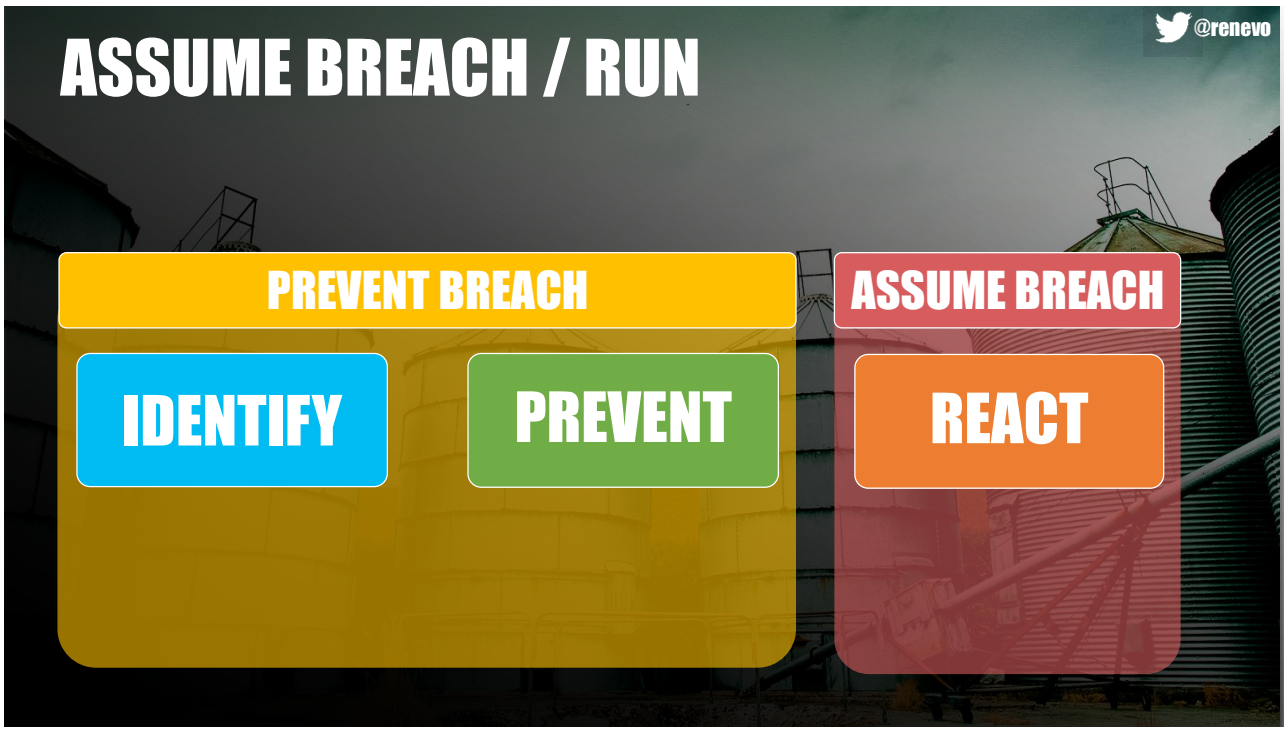
Restrictive

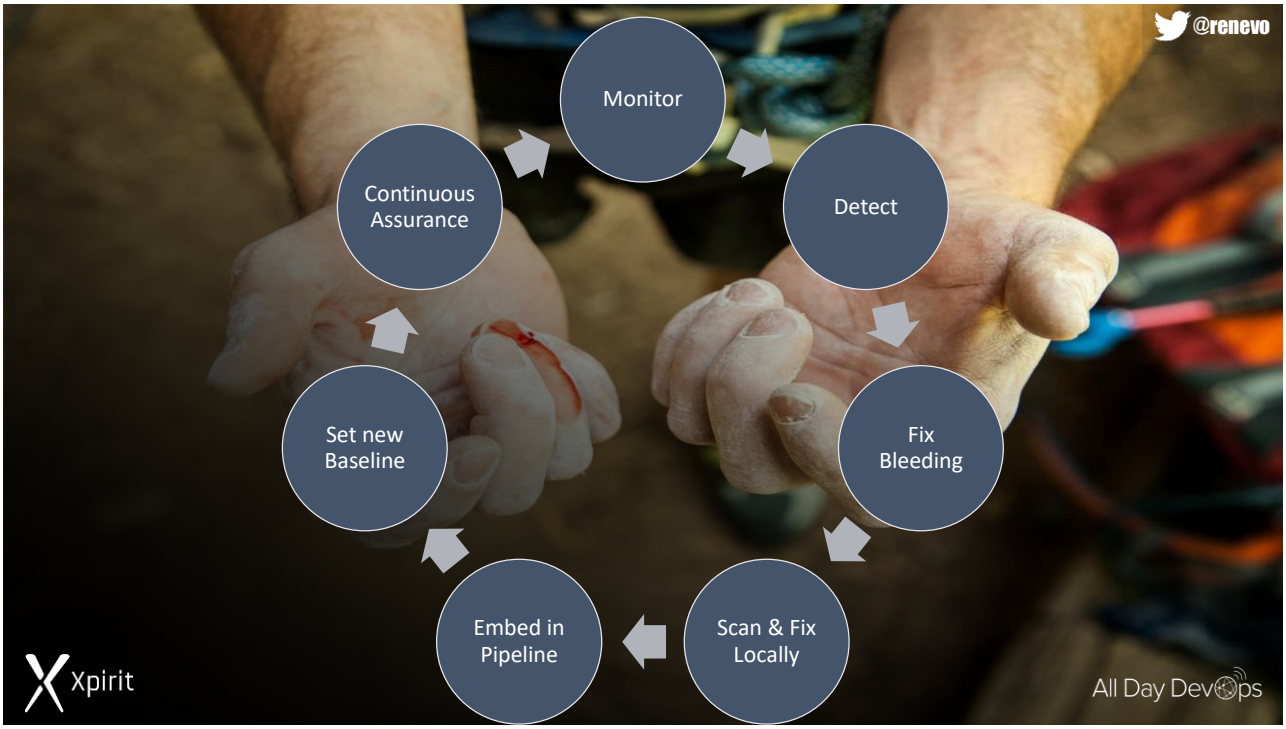
ATTRIBUTION	DOWNSTREAM	COPYLEFT
BSD MIT Apache	MPL EPL MS-RL	GPL LGPL AGPL

Permissive

All Day DevOps


@renevo
DEPLOY / RELEASE PHASE - IDENTIFY-PREVENT
• Unauthorized change in the release steps
• Enforce 4 eyes-principle on the release pipeline
• Target environment accessible by multiple process
• Set up secure Endpoints to target environment
• Deployed application has obvious vulnerabilities
• Run Dynamic Security Tests on Infrastructure
• Run Tests that require a deployed application
• Deployed application has unexpected consequences on availability etc.
• Build in a mechanism to separate functional from technical release
• Monitor key metrics after deployment
• Secrets are exposed during deployment process
Xpirit
All Day DevOps

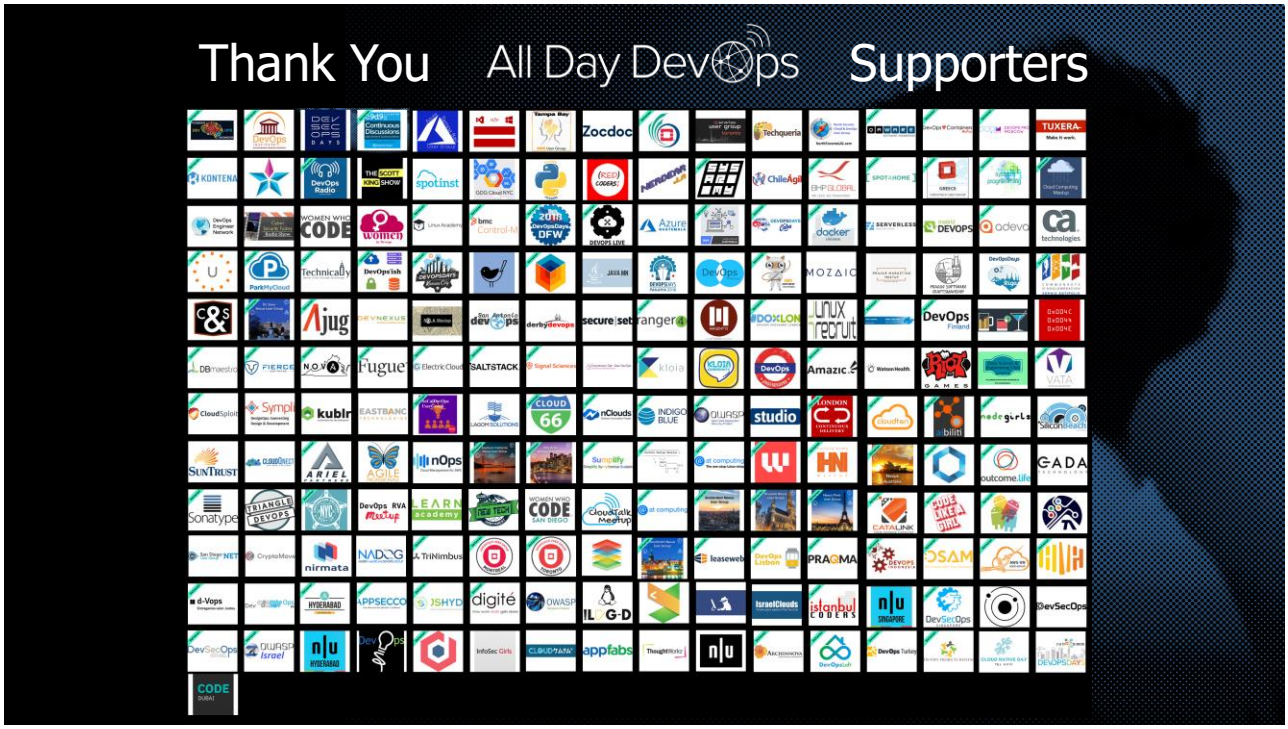

@renevo
ASSUME BREACH / RUN
PREVENT BREACH
ASSUME BREACH
IDENTIFY
PREVENT
REACT


@renevo
Monitor
Detect
Fix Bleeding
Scan & Fix Locally
Embed in Pipeline
Set new Baseline
Continuous Assurance
Xpirit
All Day DevOps


@renevo
AND COMPLIANCY?
betfair
Xpirit
All Day DevOps
PA


WRAP UP
Compliancy ≠ Security
Start with why and challenge everything
Shift from Prevent Breach to Assume breach
Make security a 1st class citizen
Move from secure to rugged
Detect, Respond, Recover
All Day DevOps


Thank You All Day DevOps Sponsors
Platinum Sponsors
Sonatype
cloudbees
Gold Sponsors
puppet
GitLab
XebiaLabs
GENERAL DYNAMICS
Information Technology
DEVNET
Carnegie Mellon University
Software Engineering Institute
CHEF
SCALED AGILE
Media Sponsors
TechBeacon
DevOps.com
DZone
Solutions Review



René van Osnabrugge

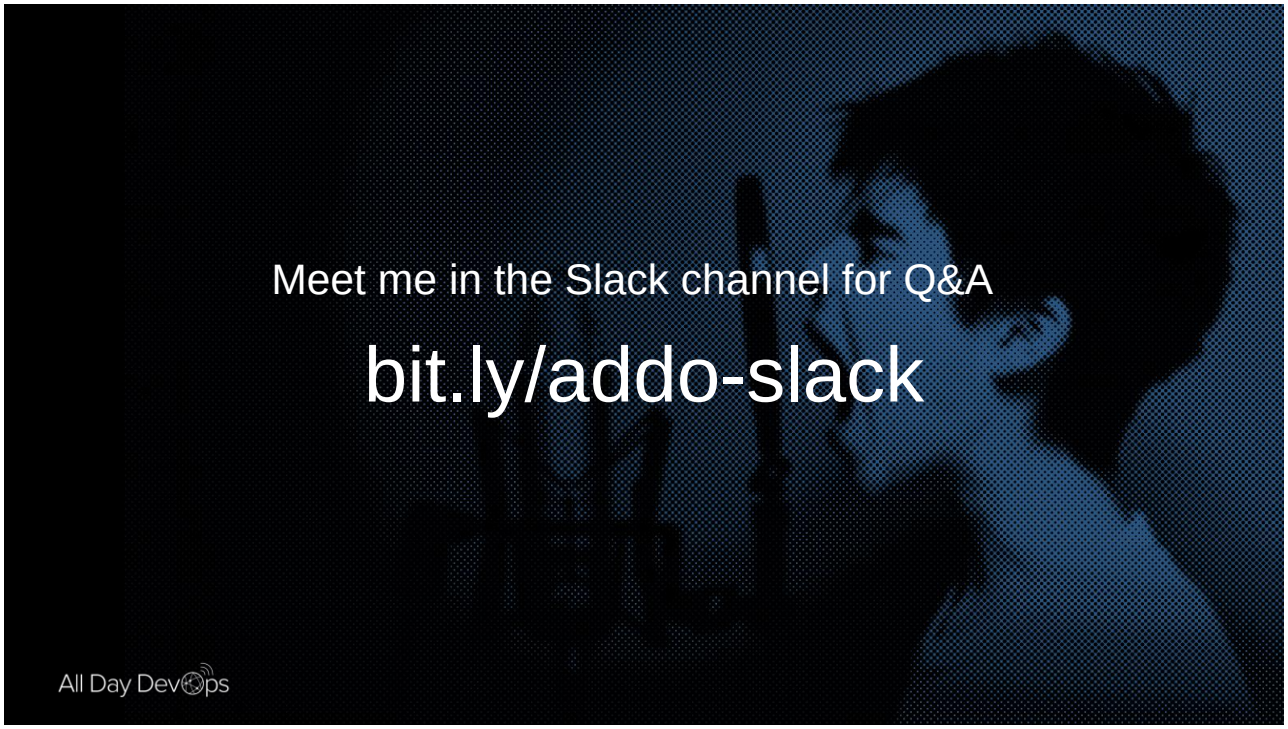
Xpirit Netherlands
@renevo
rvanosnabrugge@xpirit.com
https://roadtoalm.com

Microsoft® MVP Most Valuable Professional

Attributions

Pictures: https://unsplash.com / https://www.flickr.com/photos/wocintechchat
Gifs: https://giphy.com
Music: https://open.spotify.com/user/rvanosnabrugge/playlist/0BWgsNPM5iwgk8ZGlMHeoY?si=I9-tV8FTR8S1J7AhKBz-KA
Video: https://www.youtube.com/watch?v=47u3n1kK0wE
Thanks: Geert, Marcel, Alex, Jasper, Xpirit

Xpirit


Meet me in the Slack channel for Q&A
bit.ly/addo-slack
All Day DevOps