

# THE SHIFT TO RUGGED DEVOPS SECURITY IN YOUR PIPELINES

RENÉ VAN OSNABRUGGE  
@RENEVO

All Day DevOps

X Xpirit

COMPLIANCY



X Xpirit

All Day DevOps



# COMPLIANCY

System Implementation Assessment		Findings	Action Items
1	System1	Success! System1 is fully implemented.	Yes
2	System2	Success! System2 is fully implemented.	
3	Hub	Success! Hub is fully implemented.	
4	Node	Success! Node is fully implemented.	
5	Gateway	Success! Gateway has been implemented and is functional.	
6	Controller	Success! Controller is fully implemented and is functional.	
7	Storage	Success! Storage is fully implemented and is functional.	
8	Processor	Success! Processor is fully implemented and is functional.	
9	Network	Success! Network is fully implemented and is functional.	
10	RelayControl	Success! RelayControl is fully implemented and is functional.	
11	RelayControlAdapter	Success! RelayControlAdapter is fully implemented and is functional.	
12	RelayControlDriver	Success! RelayControlDriver is fully implemented and is functional.	
13	ProcessorDriver	Success! ProcessorDriver is fully implemented and is functional.	
14	ProcessorDriver	Success! ProcessorDriver is fully implemented and is functional.	ProcessorDriver is now live.
15	ProcessorDriver	Success! ProcessorDriver is fully implemented and is functional.	ProcessorDriver is now live.
16	Processor	Success! Processor is fully implemented and is functional.	
17	HubDriver	Success! HubDriver is fully implemented and is functional.	
18	HubDriver	Success! HubDriver is fully implemented and is functional.	
19	Processor	Success! Processor is fully implemented and is functional.	
20	Processor	Success! Processor is fully implemented and is functional.	

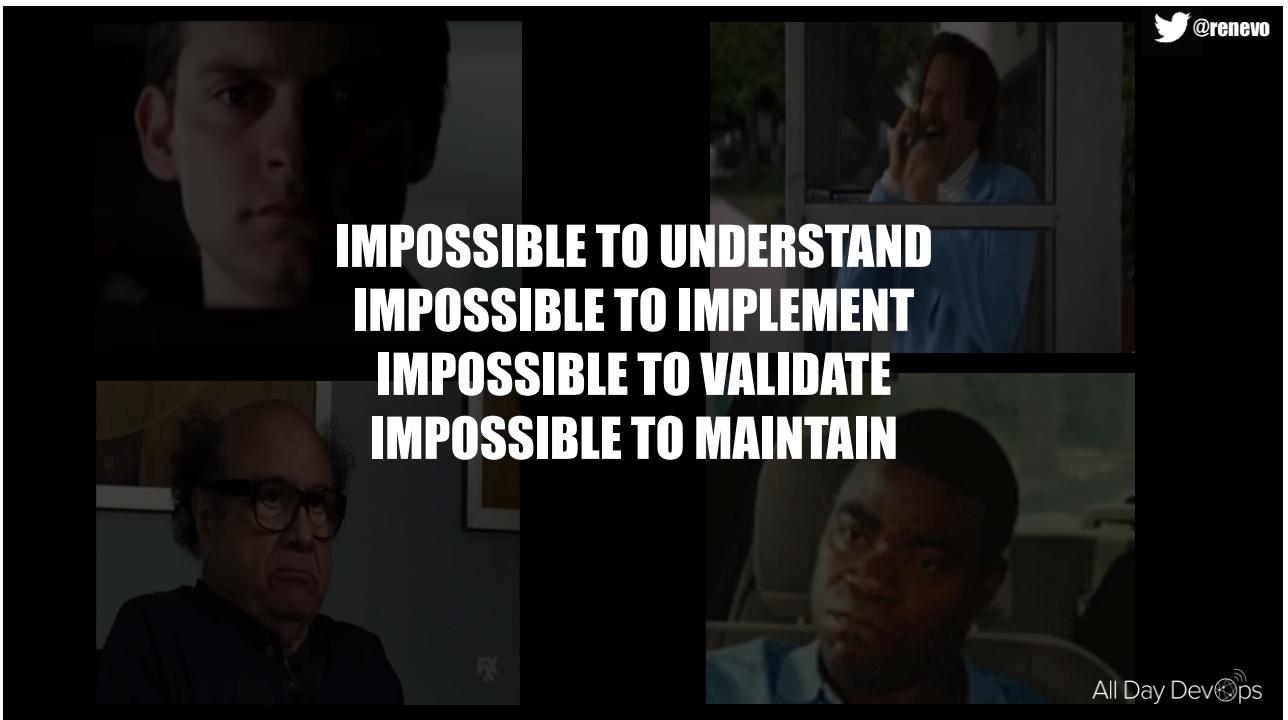
The system must display a warning message indicating that only authorised use is permitted before allowing users to log-in (for all user accounts).

*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

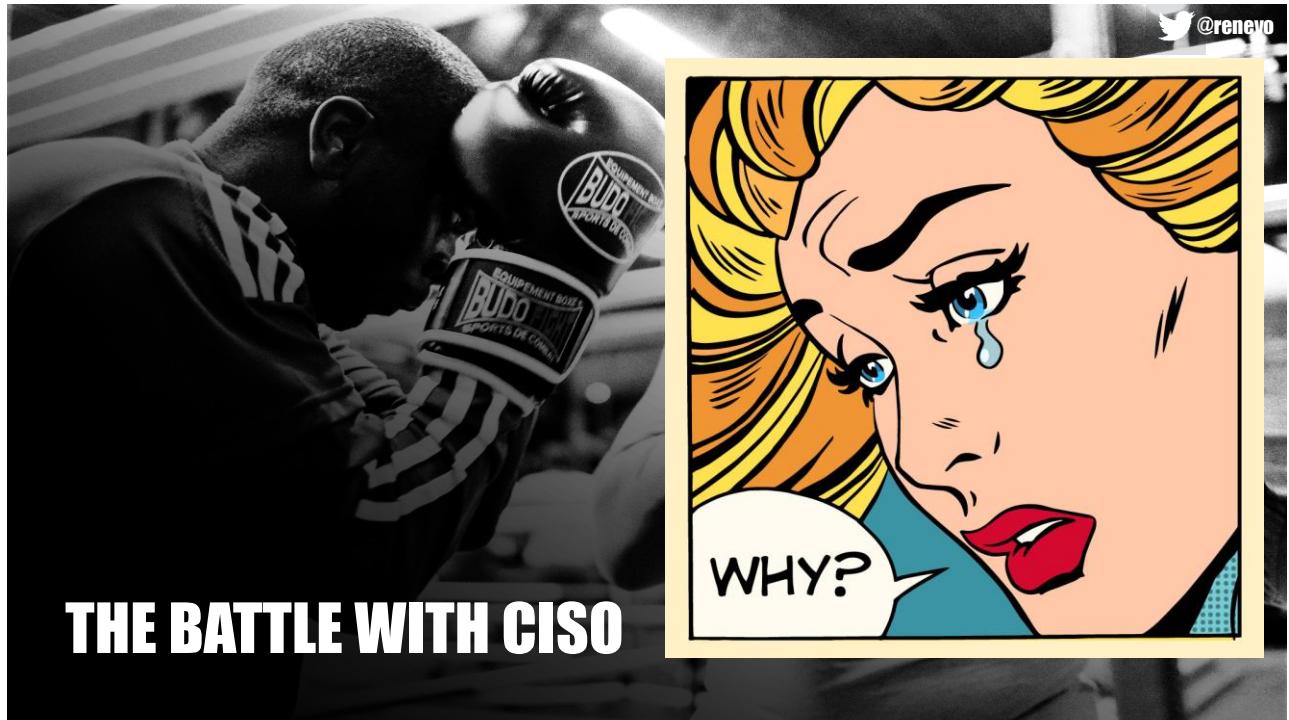


All Day DevOps



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





# THE CLASSIC “SECURITY” MODEL

 @renevo



All Day DevOps

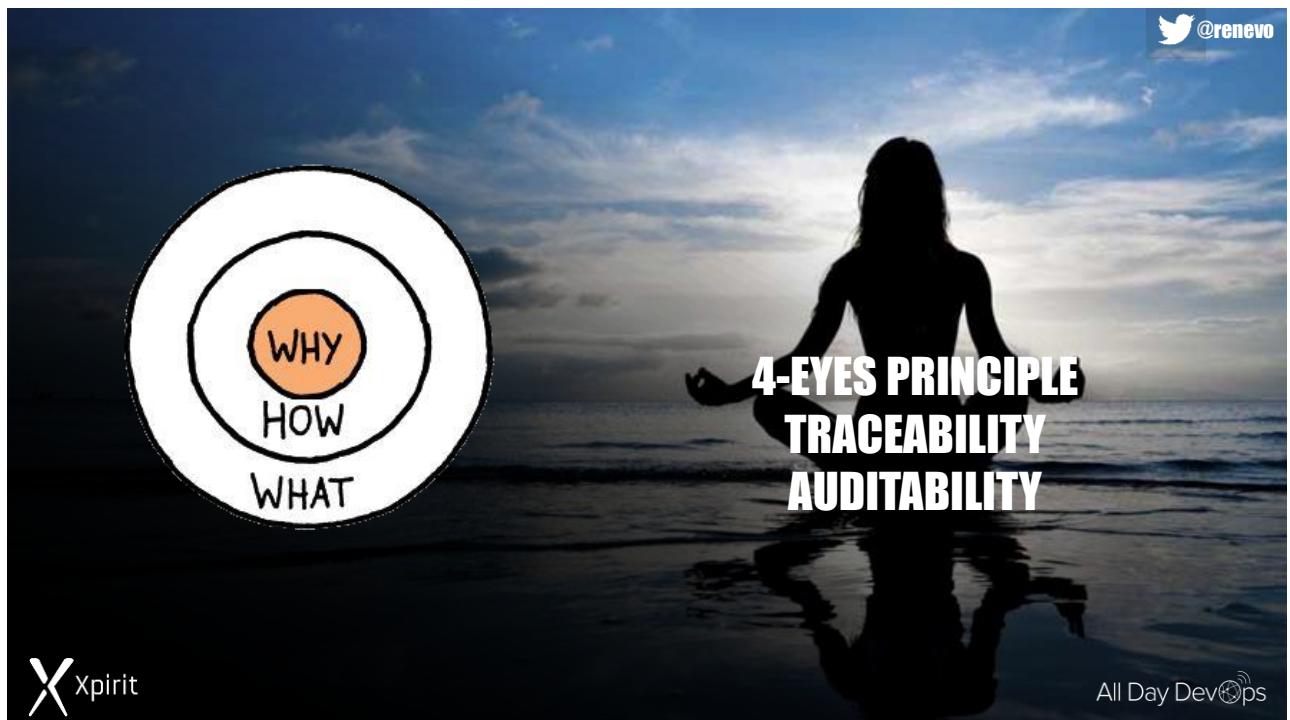
 @renevo



ISO 27001  
COBIT  
SOX  
PCI  
AUTHORITIES  
ETC.



All Day DevOps





## 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 largest breaches of 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

[Share it](#)

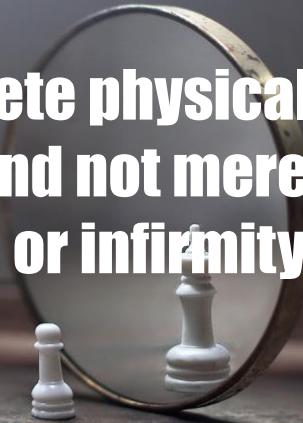
### Dive Brief:

- 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.

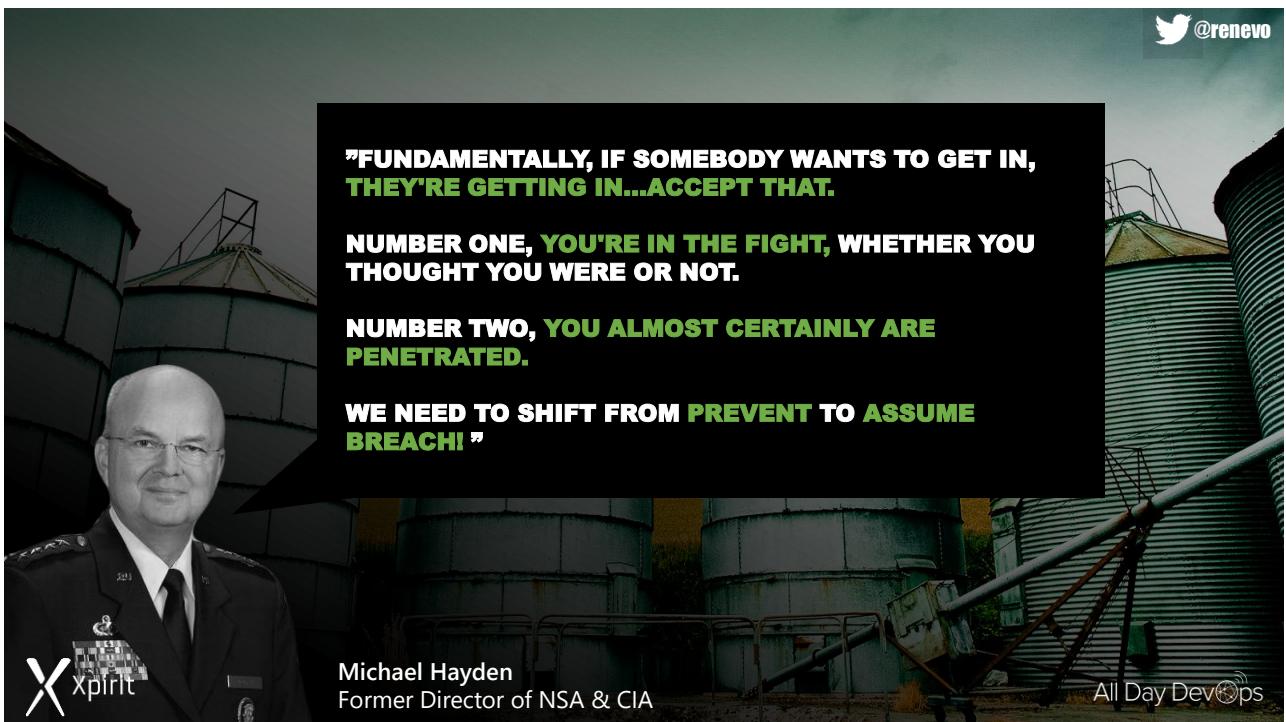
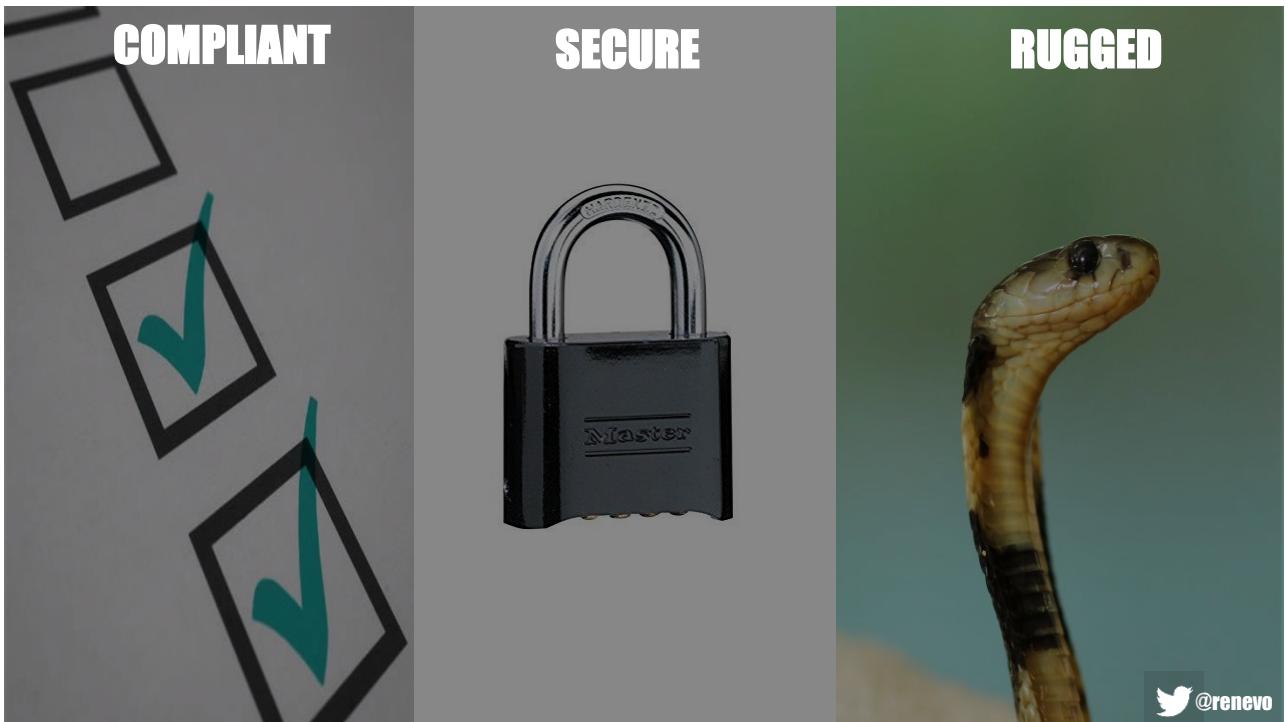
All Day DevOps



**“Health is a state of complete physical, mental and social well-being, and not merely the absence of disease or infirmity.”**



*World Health Organization, 1948*



**"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

All Day DevOps

The image is a composite. On the left, a portrait of Michael Hayden in a military uniform is shown. He is wearing glasses and has a name tag on his collar. To his right is a large industrial facility with several large, corrugated metal silos. In the center, there is a black rectangular box containing the quoted text. The Twitter handle '@renevo' is also present in the top right corner of this central box.



@renevo



All Day DevOps



## IT STARTS WITH AWARENESS !

**Claudia Pellegrino** @c\_pellegrino · Apr 4  
Does T-Mobile Austria in fact store customers' passwords in clear text  
@tmobileat? @PWTooStrong @Telekom\_hilft

**SeloX** @Selox\_AUT  
Replying to @c\_pellegrino @PWTooStrong @Telekom\_hilft  
Had the same issue with T-Mobile Austria. Apparently they are saving the password in clear because employees have access to them (you have tell them your password when you're taking to them on the phone or in a shop) and they are not case sensitive

113 908 2.0K

**T-Mobile Austria**  

Replying to @c\_pellegrino @PWTooStrong @Telekom\_hilft  
Hello Claudia! The customer service agents see the first four characters of your password. We store the whole password, because you need it for the login for [mein.t-mobile.at](#)  
^andrea

**T-Mobile**  lgate.t-mobile.at

**SeloX** @Selox\_AUT  
Replying to @c\_pellegrino @PWTooStrong @Telekom\_hilft  
Had the same issue with T-Mobile Austria. Apparently they are saving the password in clear because employees have access to them (you have tell them your password when you're taking to them on the phone or in a shop) and they are not case sensitive

189 18.9K

27 21 31

**KD.**  @prettyboy\_kd · 17 Aug 2016  
My new debit card!! Blue looks good



148 1.0K 833

**NETFLIX**

**We're sorry to say goodbye**

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply [restart your membership](#) to enjoy all the best TV shows & movies without interruption.

**RESTART MEMBERSHIP**

We're here to help if you need it. Visit the [Help Center](#) for more info or [contact us](#).

-Your friends at Netflix

Questions? Call 1-868-579-7172  
This account email has been sent to you as part of your Netflix



# SHIFT LEFT SECURITY

## Make them part of your team!

All Day DevOps



## HOW DO WE DO THAT?

BUILD

RUN

IDENTIFY

PREVENT

REACT

# NOT OR...BUT AND!

PREVENT BREACH

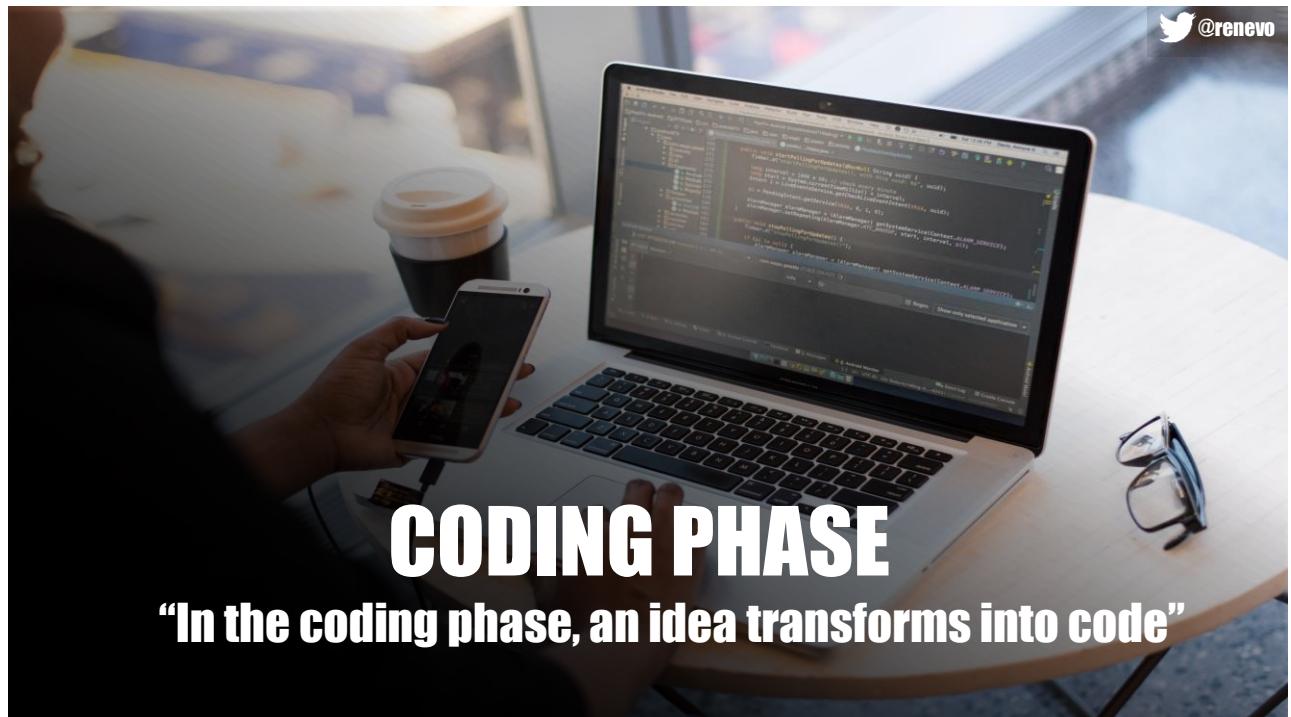
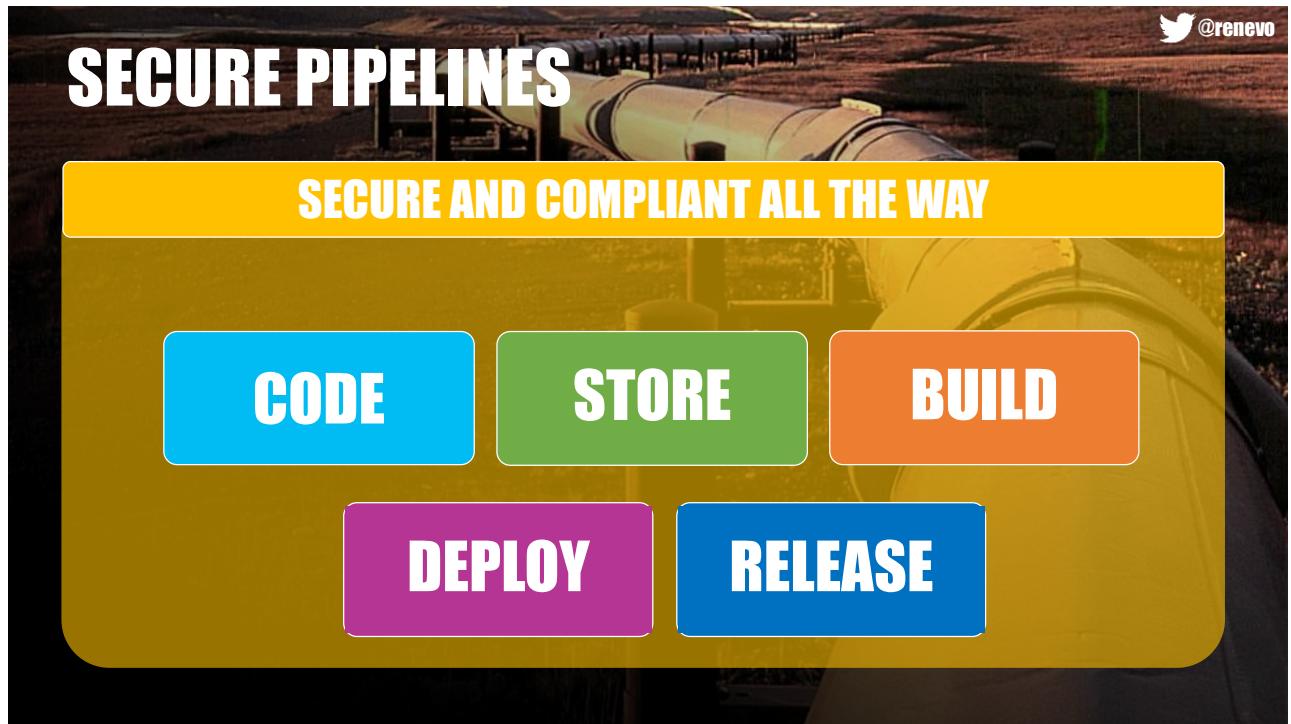
IDENTIFY

ASSUME BREACH

PREVENT

REACT

# PREVENT BREACH





## 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



All Day DevOps



## STORING PHASE

“In the storing phase you make “your” code “our” code and ensure it is safe”



## 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



All Day DevOps

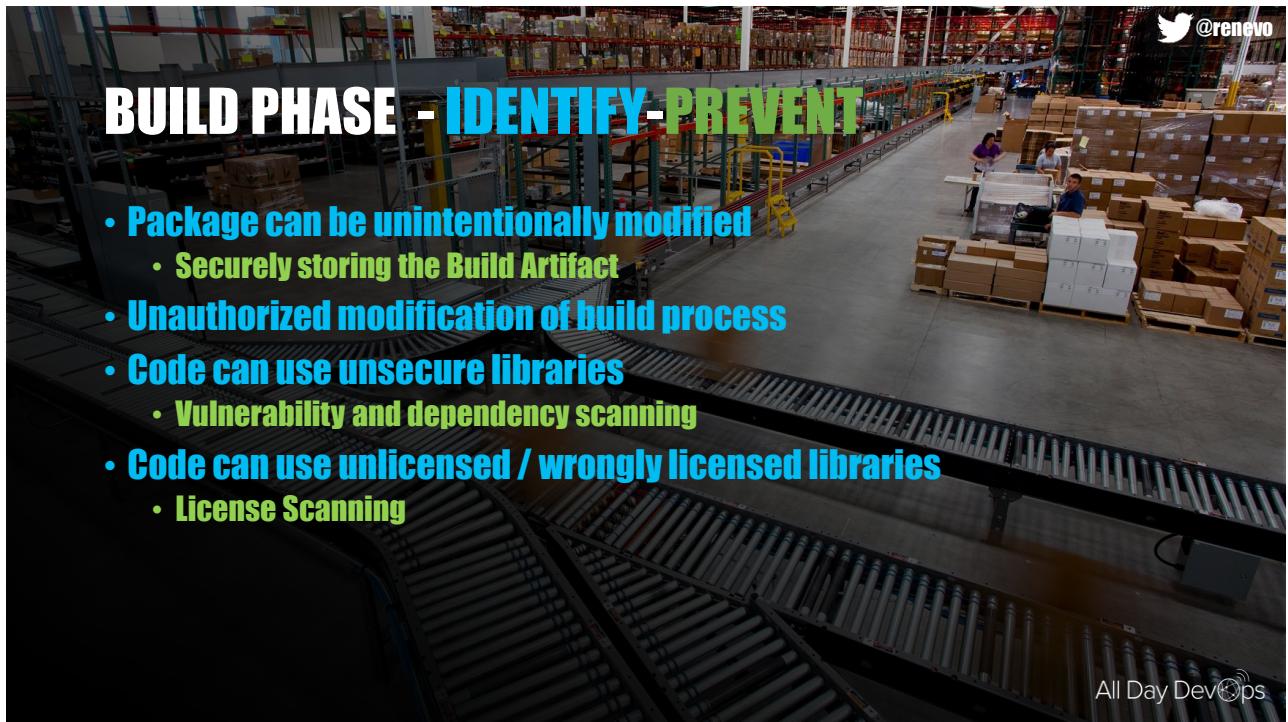


## BUILD PHASE

“In the build phase we transform the product from code and script into an immutable and versioned package”

**BUILD PHASE - IDENTIFY-PREVENT**

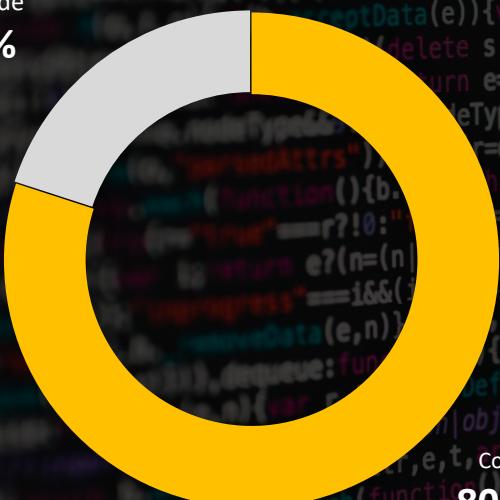
- Package can be unintentionally modified
  - Securely storing the Build Artifact
- Unauthorized modification of build process
- Code can use unsecure libraries
  - Vulnerability and dependency scanning
- Code can use unlicensed / wrongly licensed libraries
  - License Scanning



**All Day DevOps**

**YOUR CODE VS. THEIR CODE**

Original Code  
10-20%  
(max)



Components  
80 – 90 %

**Icons:**

- Node.js: Red hexagon with a white diamond inside.
- Java: Orange coffee cup icon.
- NPM: Red square with the letters "npm".
- JavaScript: Yellow square with the letters "JS".
- Angular: Blue square with a white bird icon.
- React: Blue square with a white circular icon.

**All Day DevOps**

# AND THEN THERE IS LICENSING

Restrictive

ATTRIBUTION

BSD  
MIT  
Apache

DOWNSTREAM

MPL  
EPL  
MS-RL

COPYLEFT

GPL  
LGPL  
AGPL

Permissive

All Day DevOps

## DEPLOY / RELEASE PHASE

“THIS IS THE PHASE WHERE THE ARTIFACTS MOVE FROM YOUR  
“PROTECTED” ENVIRONMENT INTO THE OPEN”

## DEPLOY / RELEASE PHASE - IDENTIFY-PREVENT

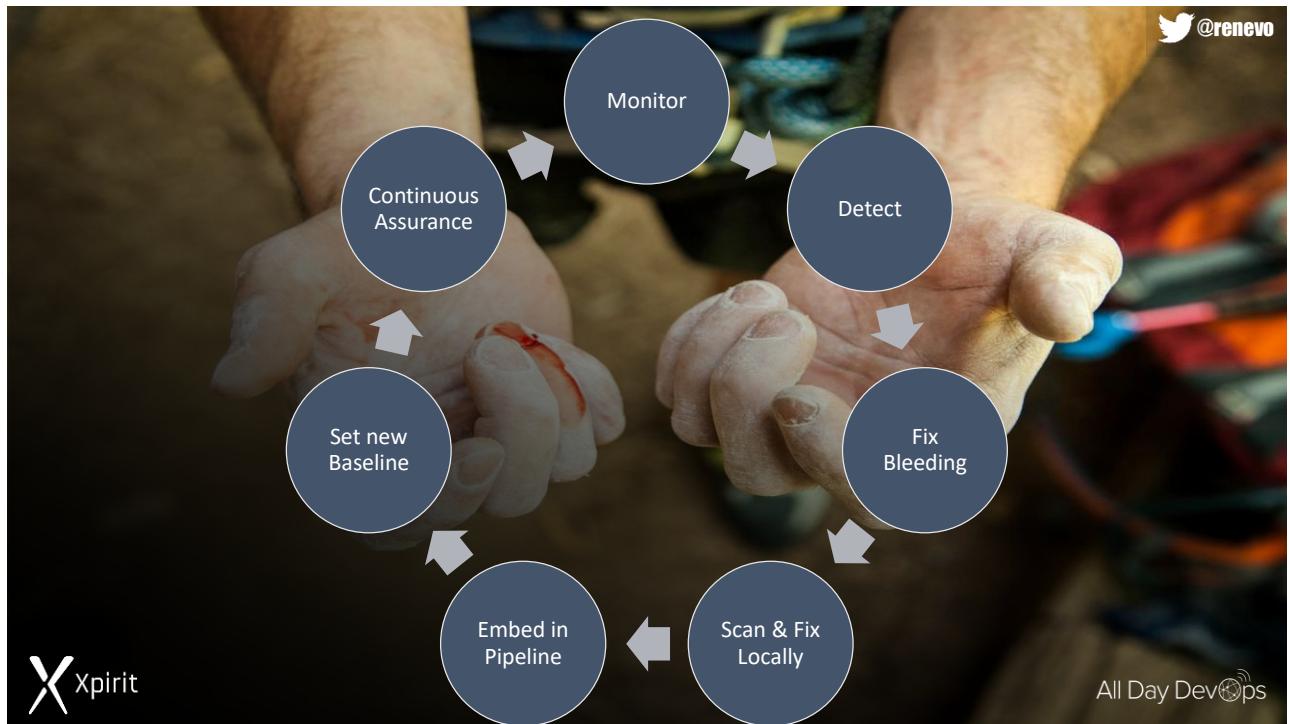
- Unauthorized change in the release steps
  - Enforce 4 eyes-principle on the release pipeline
- Target environment accessible by multiple process
  - Set up secure Endpoints to target environment
- Deployed application has obvious vulnerabilities
  - Run Dynamic Security Tests on Infrastructure
  - 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



All Day DevOps

## ASSUME BREACH / RUN

**PREVENT BREACH****IDENTIFY****ASSUME BREACH****PREVENT****REACT**



# WRAP UP

**Compliancy ≠ Security**  
**Start with why and challenge everything**  
**Shift from Prevent Breach to Assume breach**  
**Make security a 1<sup>st</sup> class citizen**  
**Move from secure to rugged**  
**Detect, Respond, Recover**

All Day DevOps

## Thank You All Day DevOps Sponsors

### Platinum Sponsors



### Gold Sponsors



GitLab



GENERAL DYNAMICS  
Information Technology



### Media Sponsors



SCALED AGILE



# Thank You All Day DevOps Supporters



## René van Osnabrugge Xpirit Netherlands

@renevo  
rvanosnabrugge@xpirit.com  
<https://roadtoalm.com>



### Attributions

Pictures: <https://unsplash.com> / <https://www.flickr.com/photos/wocintechchat>  
 Gifs: <https://giphy.com>  
 Music: <https://open.spotify.com/user/rvanosnabrugge/playlist/0BWgsHPM5iwgk8ZGMHeoY?si=I9-tV8FTRGS17AhKbz-KA>  
 Video: <https://www.youtube.com/watch?v=47u3n1kXowE>

Thanks: Geert, Marcel, Alex, Jasper, Xpirit





Meet me in the Slack channel for Q&A

**[bit.ly/addo-slack](https://bit.ly/addo-slack)**

All Day DevOps