ABN·AMRO

DevSecOps At Scale

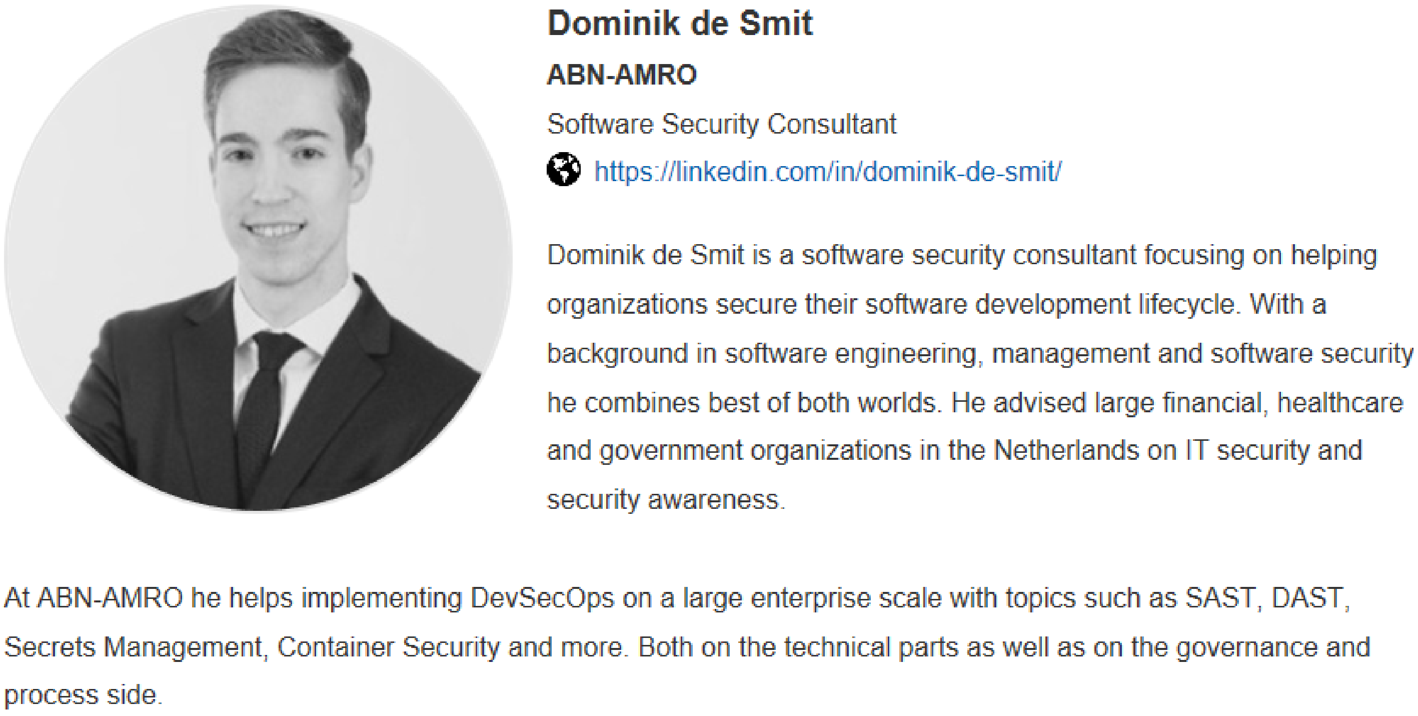
How Team Autonomy Helps The Enterprise Stay Secure

All Day Devops (17-10-2018)

ABN AMRO

Dominik de Smit & Wiebe de Roos

About us – Domink de Smit



Dominik de Smit

ABN-AMRO

Software Security Consultant

🌍 https://linkedin.com/in/dominik-de-smit/

Dominik de Smit is a software security consultant focusing on helping organizations secure their software development lifecycle. With a background in software engineering, management and software security he combines best of both worlds. He advised large financial, healthcare and government organizations in the Netherlands on IT security and security awareness.

At ABN-AMRO he helps implementing DevSecOps on a large enterprise scale with topics such as SAST, DAST, Secrets Management, Container Security and more. Both on the technical parts as well as on the governance and process side.

ABN AMRO

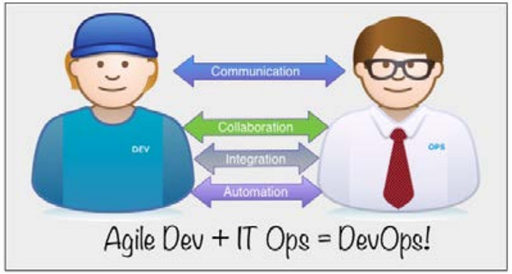
ABN AMRO is a leading bank
with an operating income of EUR 8588 million

Headquartered in Amsterdam

22,000 employees servicing retail, private and corporate finances worldwide

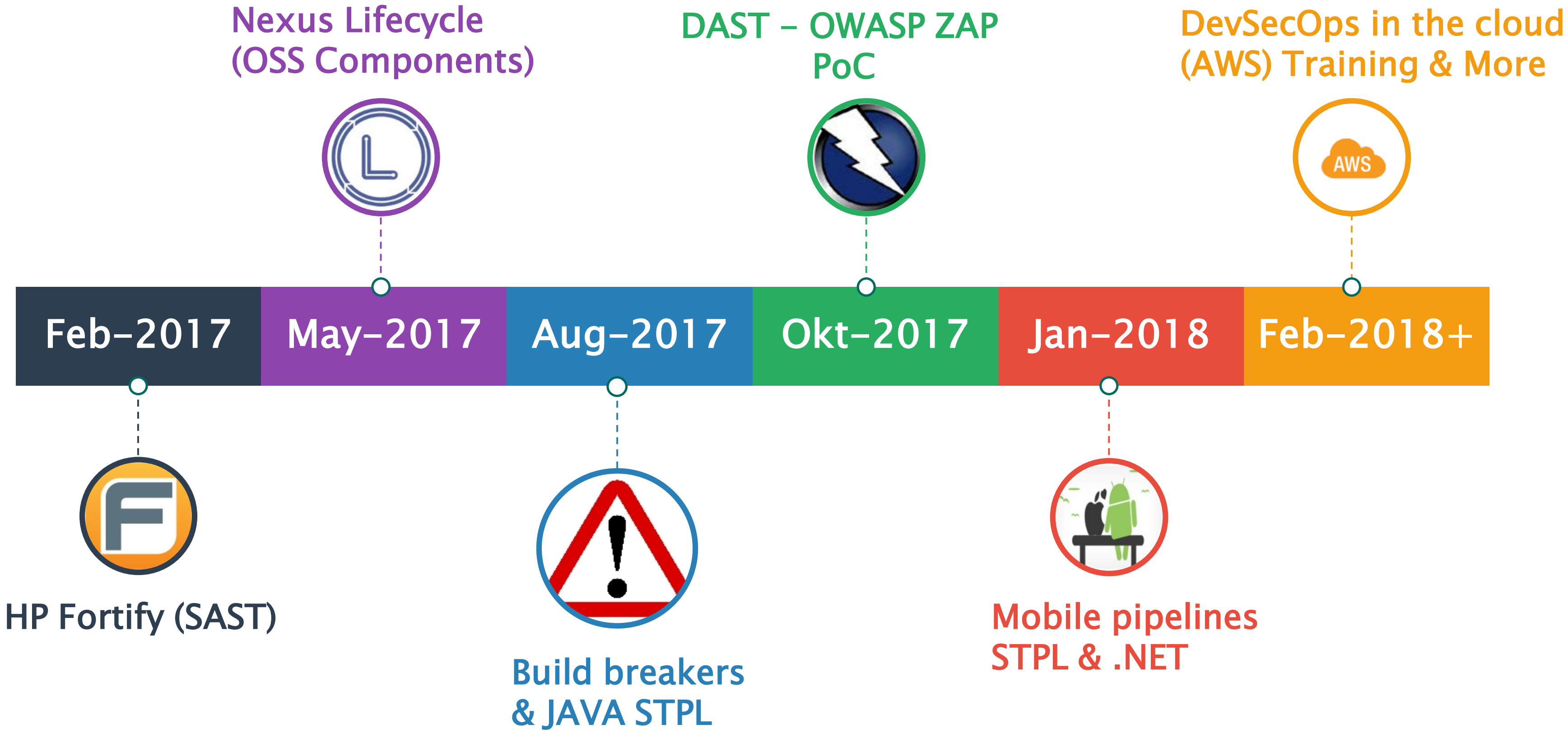
5,000 associates working in IT

350+ agile teams



The journey of ABN Amro

The DevSecOps journey (1)



Feb-2017

May-2017

Aug-2017

Okt-2017

Jan-2018

Feb-2018+

HP Fortify (SAST)

Nexus Lifecycle (OSS Components)

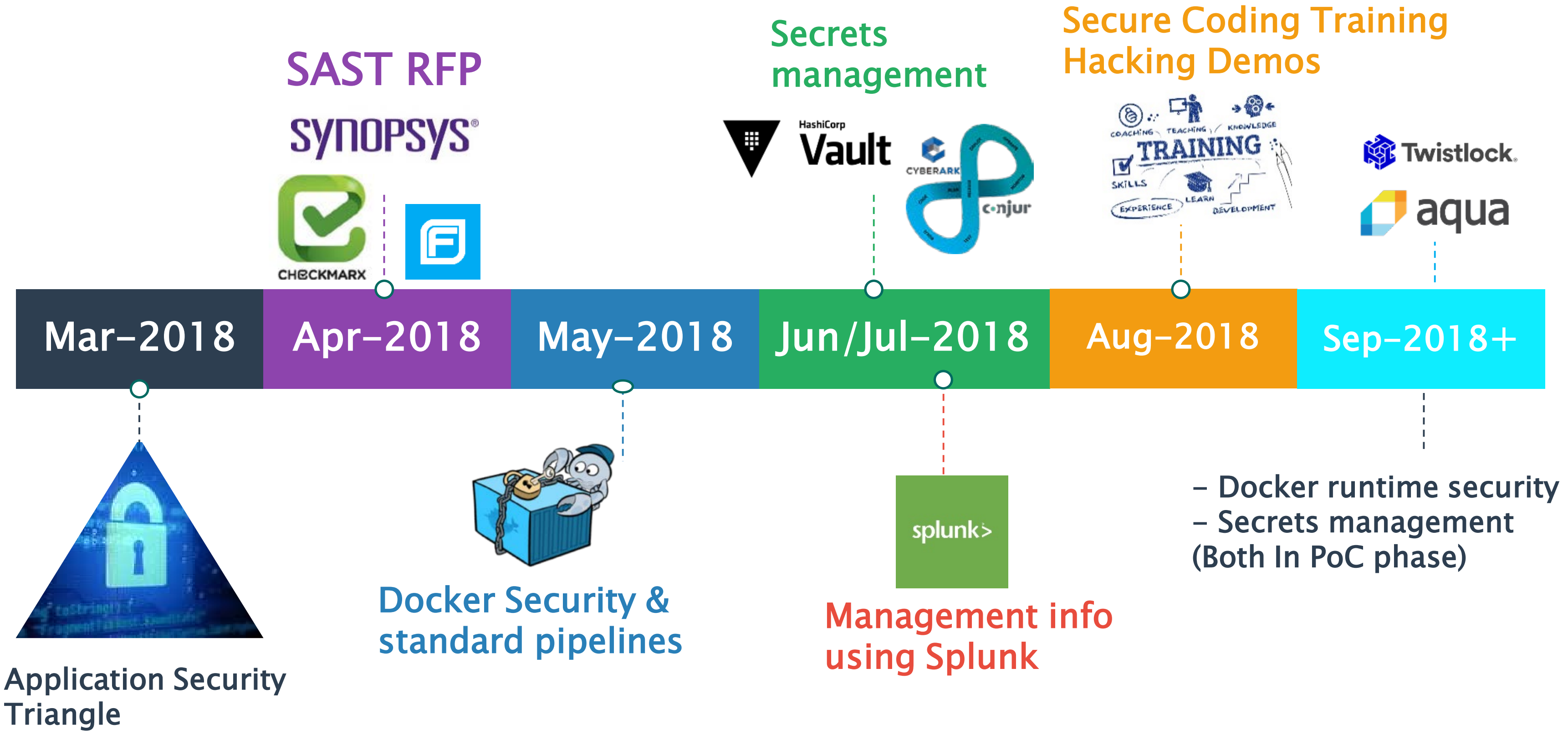
Build breakers & JAVA STPL

DAST – OWASP ZAP PoC

Mobile pipelines STPL & .NET

DevSecOps in the cloud (AWS) Training & More

The DevSecOps journey (2)



Mar-2018

Application Security Triangle

Apr-2018

SAST RFP

May-2018

Docker Security & standard pipelines

Jun/Jul-2018

Secrets management

Management info using Splunk

Aug-2018

Secure Coding Training
Hacking Demos

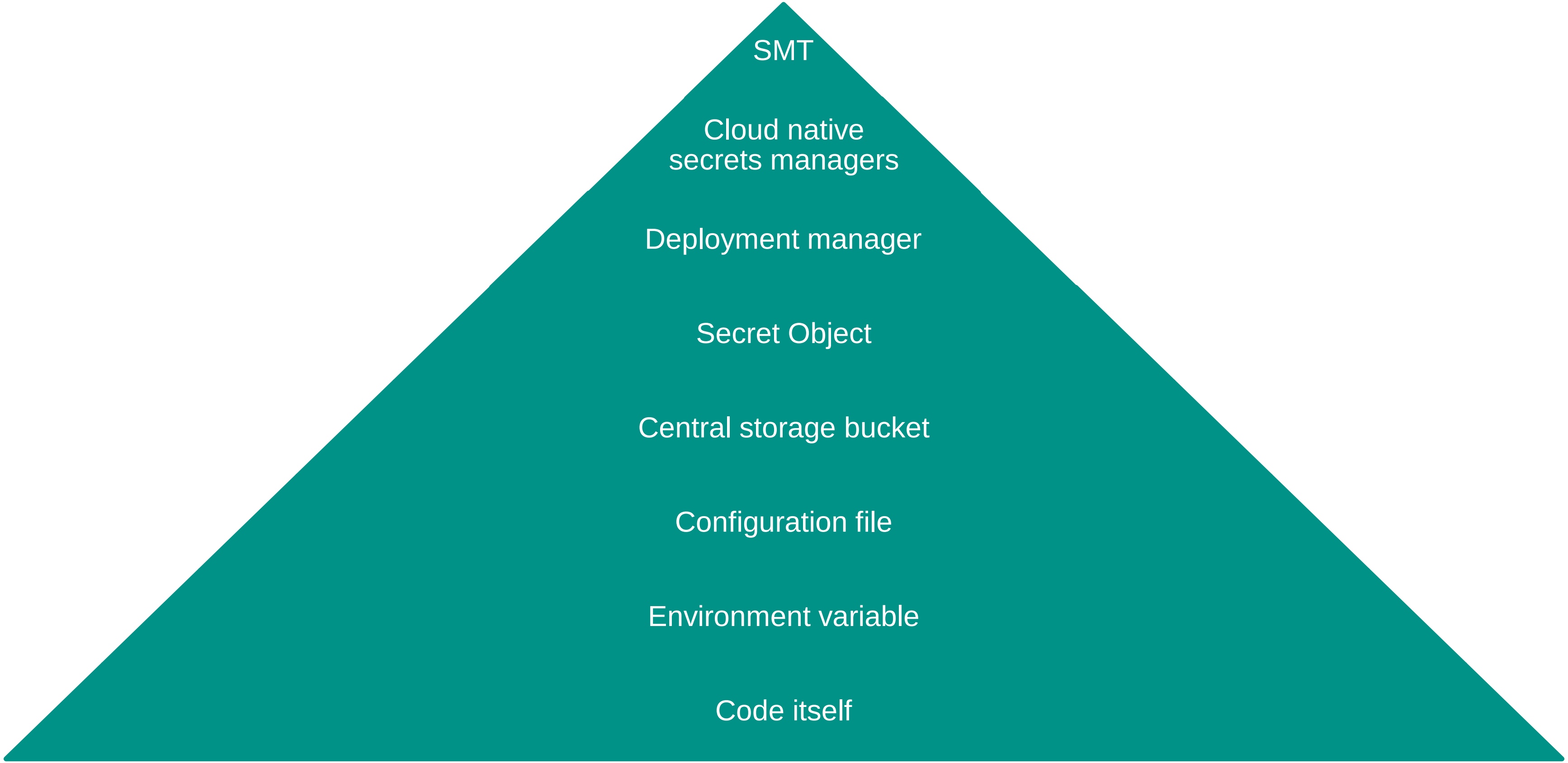
Sep-2018+

- Docker runtime security
- Secrets management

(Both In PoC phase)

Secrets everywhere

Secrets Management



SMT

Cloud native secrets managers

Deployment manager

Secret Object

Central storage bucket

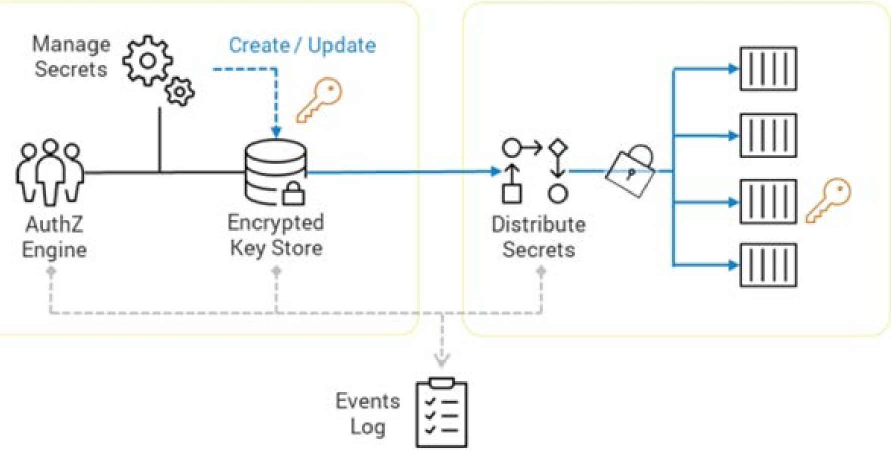
Configuration file

Environment variable

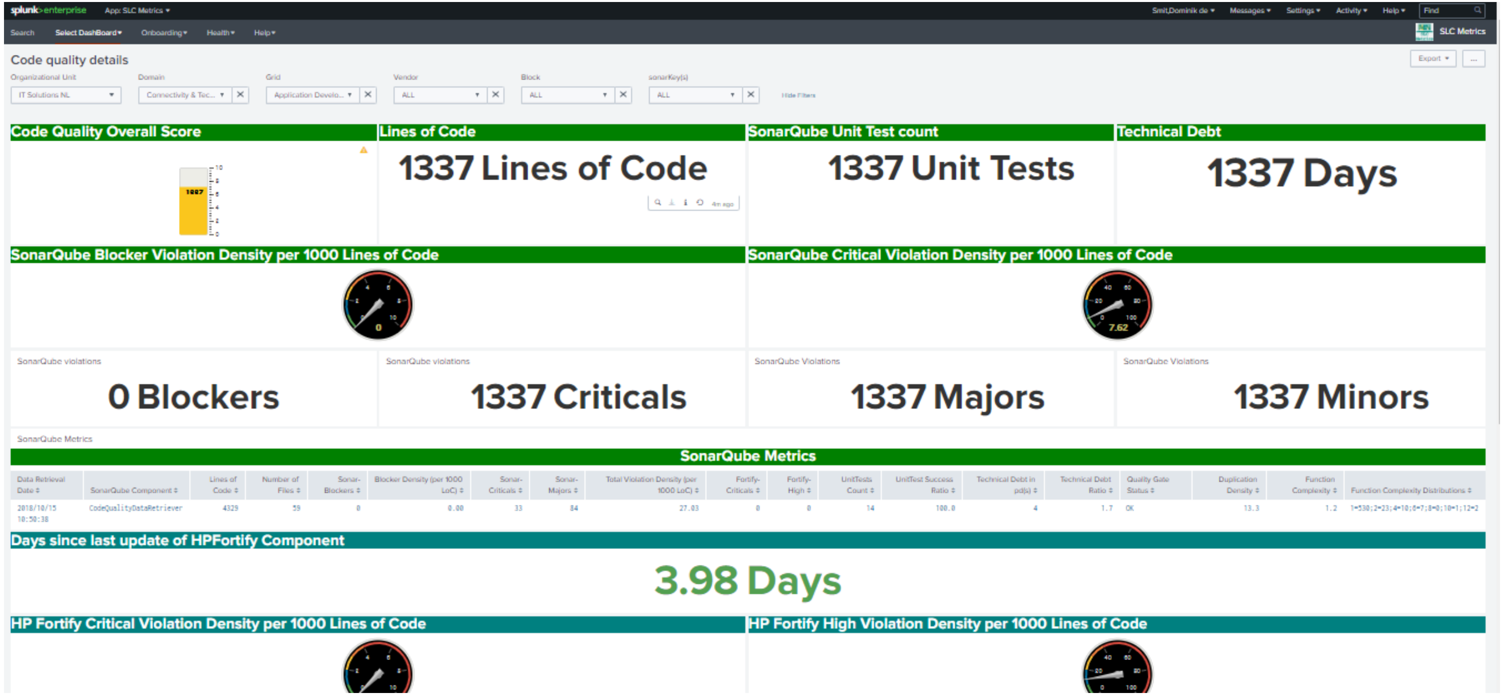
Code itself

Secrets Management

- Centralized secrets management
- Integrate seamlessly with Cloud platforms
- Prevent massive overhead (e.g. containers, microservices) → Dynamic secrets
- Start with static → move to dynamic
- Should be very easy for teams to implement
- Automated onboarding for teams



Metrics (Splunk)



Code quality details

Organizational Unit: IT Solutions NL ▾

Domain: Connectivity & Tec... ▾ ✕

Grid: Application Develo... ▾ ✕

Vendor: ALL ▾ ✕

Block: ALL ▾ ✕

sonarKey(s): ALL ▾ ✕

Code Quality Overall Score

Lines of Code

1337 Lines of Code

SonarQube Unit Test count

1337 Unit Tests

Technical Debt

1337 Days

SonarQube Blocker Violation Density per 1000 Lines of Code

0

SonarQube Critical Violation Density per 1000 Lines of Code

7.62

SonarQube violations

0 Blockers

SonarQube violations

1337 Criticals

SonarQube Violations

1337 Majors

SonarQube Violations

1337 Minors

SonarQube Metrics

SonarQube Metrics

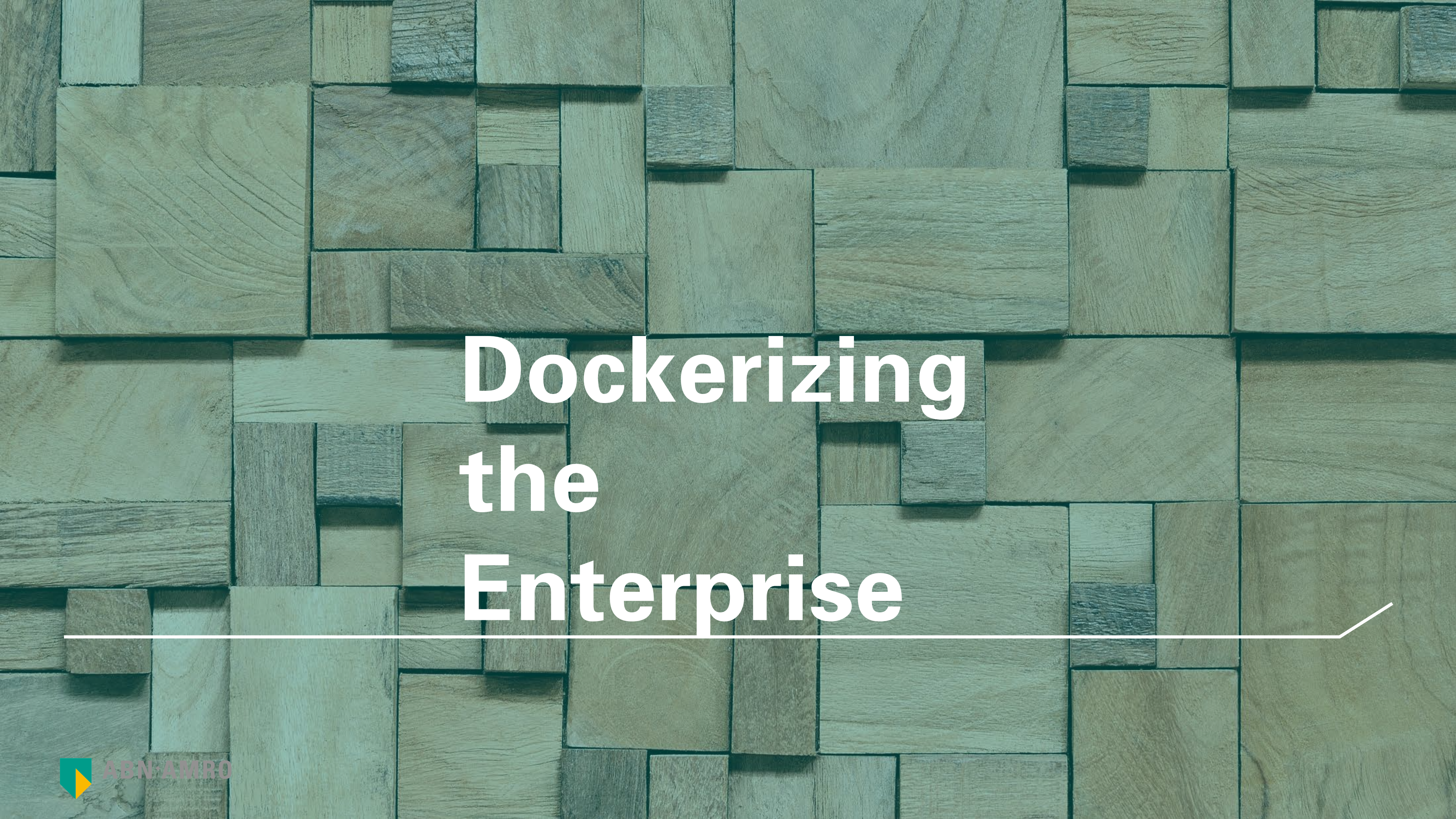
Data Retrieval Date ⇕	SonarQube Component ⇕	Lines of Code ⇕	Number of Files ⇕	Sonar-Blockers ⇕	Blocker Density (per 1000 LoC) ⇕	Sonar-Criticals ⇕	Sonar-Majors ⇕	Total Violation Density (per 1000 LoC) ⇕	Fortify-Criticals ⇕	Fortify-High ⇕	UnitTests Count ⇕	UnitTest Success Ratio ⇕	Technical Debt in pd(s) ⇕	Technical Debt Ratio ⇕	Quality Gate Status ⇕	Duplication Density ⇕	Function Complexity ⇕	Function Complexity Distributions ⇕
2018/10/15 10:50:38	CodeQualityDataRetriever	4329	59	0	0.00	33	84	27.03	0	0	14	100.0	4	1.7	OK	13.3	1.2	1=530;2=23;4=10;6=7;8=0;10=1;12=2

Days since last update of HPFortify Component

3.98 Days

HP Fortify Critical Violation Density per 1000 Lines of Code

HP Fortify High Violation Density per 1000 Lines of Code



Dockerizing the Enterprise

About us – Wiebe de Roos

Wiebe de Roos

ABN-AMRO

CI/CD Consultant/Engineer

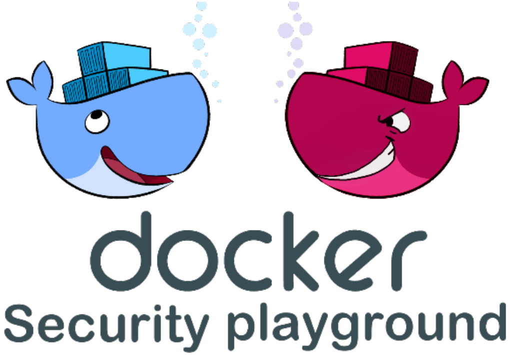
https://linkedin.com/in/wiebe-de-roos/

Wiebe de Roos has more than 10 years of experience in various IT-related roles like (Java) developer and ICT consultant. He worked for different companies both in The Netherlands and abroad. Currently he is being hired by ABN-AMRO as a CI/CD Consultant / Engineer with a strong focus on security.

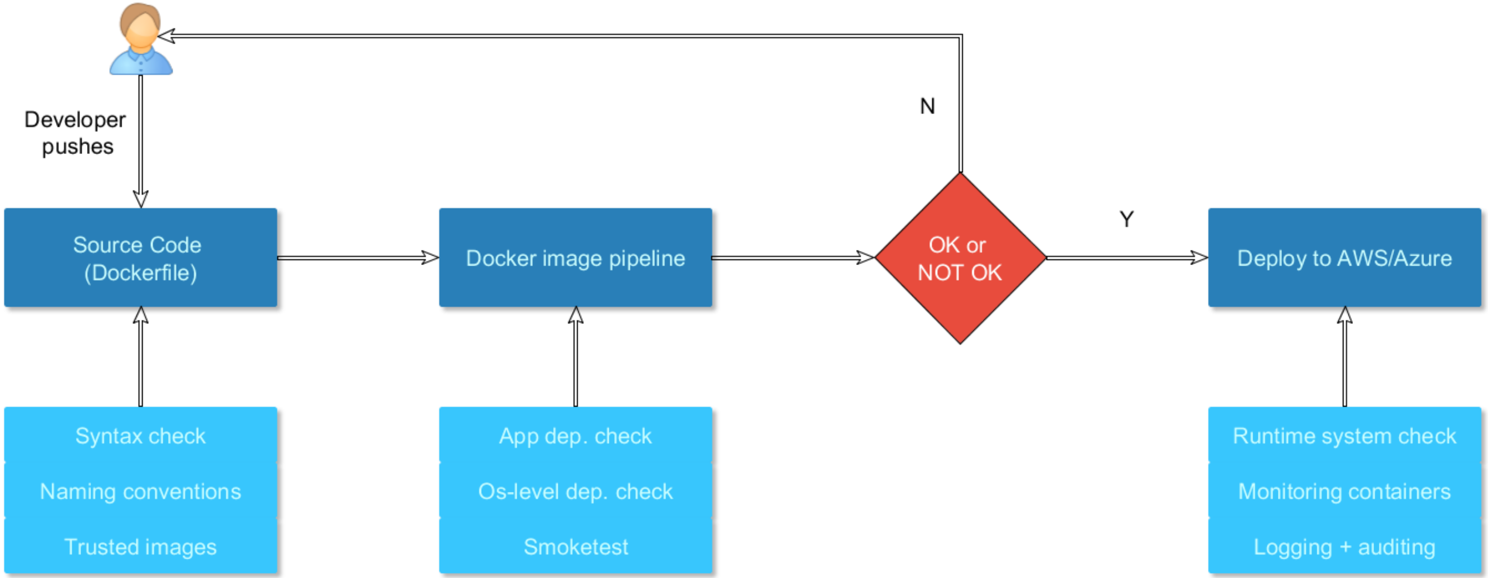
At ABN-AMRO he works at different (enterprise grade) projects ranging from the implementation of Jenkins Enterprise in AWS to the implementation and roll out of different (Docker) security related tools. Both working on the technical as well as the organizational aspects.

Birth of Docker @ ABN AMRO

- Q3 2017: Jenkins standard pipelines for all technologies
- Q1 2018: Birth of the Docker image pipelines (v1)
- Q2 2018: Docker security awareness & guidelines established
- Q3 2018: Docker images pipeline - building blocks for all teams (v2)
- Q4 2018: Docker runtime security scanning
- Q1 2019: All Dockerized systems secured from top to bottom



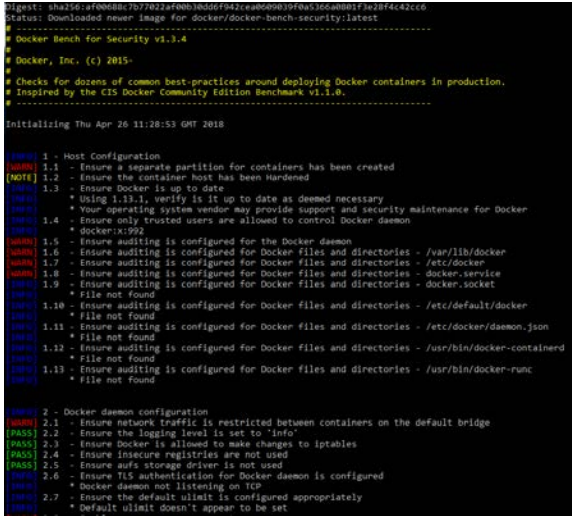
Docker Container Security – CI/CD processes



Docker Container Security steps

```
v1.6.2-6-gcfb547a: Pulling from hadolint/hadolint
Status: Downloaded newer image for hadolint/hadolint:v1.6.2-6-gcfb547a
/dev/stdin:3 DL3005 Do not use apt-get upgrade or dist-upgrade
/dev/stdin:3 DL3009 Delete the apt-get lists after installing something
/dev/stdin:4 DL3008 Pin versions in apt get install. Instead of `apt-get install <package>` use `apt-get install <package>=<version>`
/dev/stdin:4 DL3015 Avoid additional packages by specifying `--no-install-recommends`
```

1. Check source code



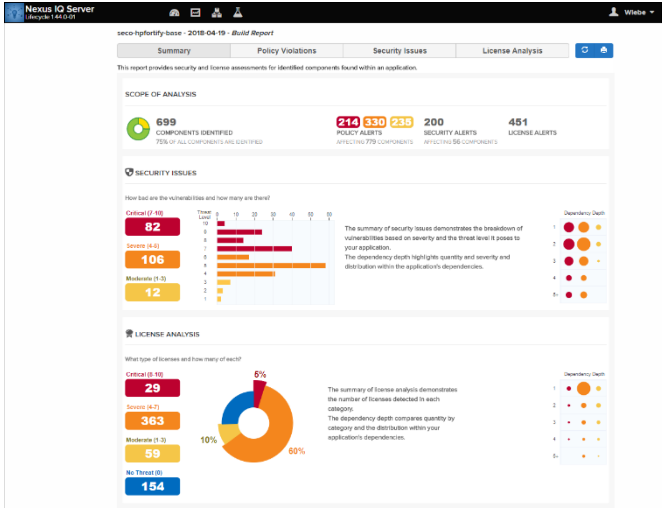
```
Digest: sha256:af00688c7b77022af00b30dd6f942cea0609039f0a5366a0801f3e28f4c42cc6
Status: Downloaded newer image for docker/docker-bench-security:latest
# ------------------------------------------------------------------------------
# Docker Bench for Security v1.3.4
#
# Docker, Inc. (c) 2015-
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Inspired by the CIS Docker Community Edition Benchmark v1.1.0.
# ------------------------------------------------------------------------------

Initializing Thu Apr 26 11:28:53 GMT 2018


[INFO] 1 - Host Configuration
[WARN] 1.1  - Ensure a separate partition for containers has been created
[NOTE] 1.2  - Ensure the container host has been Hardened
[INFO] 1.3  - Ensure Docker is up to date
[INFO]       * Using 1.13.1, verify is it up to date as deemed necessary
[INFO]       * Your operating system vendor may provide support and security maintenance for Docker
[INFO] 1.4  - Ensure only trusted users are allowed to control Docker daemon
[INFO]       * docker:x:992
[WARN] 1.5  - Ensure auditing is configured for the Docker daemon
[WARN] 1.6  - Ensure auditing is configured for Docker files and directories - /var/lib/docker
[WARN] 1.7  - Ensure auditing is configured for Docker files and directories - /etc/docker
[WARN] 1.8  - Ensure auditing is configured for Docker files and directories - docker.service
[INFO] 1.9  - Ensure auditing is configured for Docker files and directories - docker.socket
[INFO]       * File not found
[INFO] 1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker
[INFO]       * File not found
[INFO] 1.11 - Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json
[INFO]       * File not found
[INFO] 1.12 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-containerd
[INFO]       * File not found
[INFO] 1.13 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-runc
[INFO]       * File not found


[INFO] 2 - Docker daemon configuration
[WARN] 2.1  - Ensure network traffic is restricted between containers on the default bridge
[PASS] 2.2  - Ensure the logging level is set to 'info'
[PASS] 2.3  - Ensure Docker is allowed to make changes to iptables
[PASS] 2.4  - Ensure insecure registries are not used
[PASS] 2.5  - Ensure aufs storage driver is not used
[INFO] 2.6  - Ensure TLS authentication for Docker daemon is configured
[INFO]       * Docker daemon not listening on TCP
[INFO] 2.7  - Ensure the default ulimit is configured appropriately
[INFO]       * Default ulimit doesn't appear to be set
```

3. Check running systems



seco-hpfortify-base - 2018-04-19 - *Build Report*

This report provides security and license assessments for identified components found within an application.

SCOPE OF ANALYSIS

699 COMPONENTS IDENTIFIED
75% OF ALL COMPONENTS ARE IDENTIFIED

214 330 235 POLICY ALERTS
AFFECTING 779 COMPONENTS

200 SECURITY ALERTS
AFFECTING 56 COMPONENTS

451 LICENSE ALERTS

SECURITY ISSUES

How bad are the vulnerabilities and how many are there?

Critical (7-10) 82
Severe (4-6) 106
Moderate (1-3) 12

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application.
The dependency depth highlights quantity and severity and distribution within the application's dependencies.

LICENSE ANALYSIS

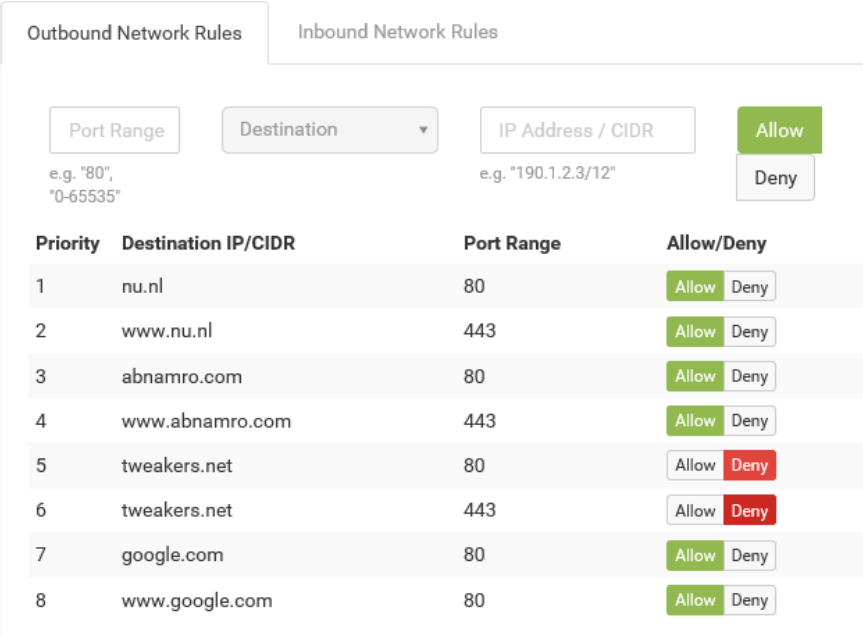
What type of licenses and how many of each?

Critical (8-10) 29
Severe (4-7) 363
Moderate (1-3) 59
No Threat (0) 154

The summary of license analysis demonstrates the number of licenses detected in each category.
The dependency depth compares quantity by category and the distribution within your application's dependencies.

2. Check dependencies

Docker runtime security scanning

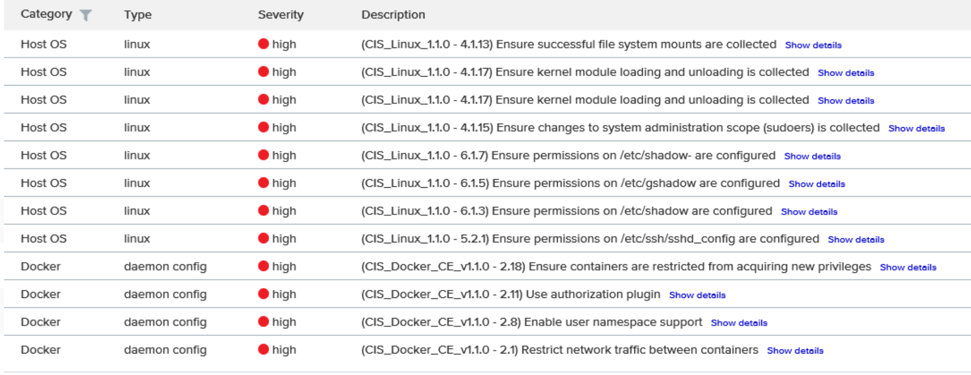


e.g. "80", "0-65535"

e.g. "190.1.2.3/12"

Priority	Destination IP/CIDR	Port Range	Allow/Deny
1	nu.nl	80	[✓ Allow] Deny
2	www.nu.nl	443	[✓ Allow] Deny
3	abnamro.com	80	[✓ Allow] Deny
4	www.abnamro.com	443	[✓ Allow] Deny
5	tweakers.net	80	Allow [✓ Deny]
6	tweakers.net	443	Allow [✓ Deny]
7	google.com	80	[✓ Allow] Deny
8	www.google.com	80	[✓ Allow] Deny

Block outbound network access

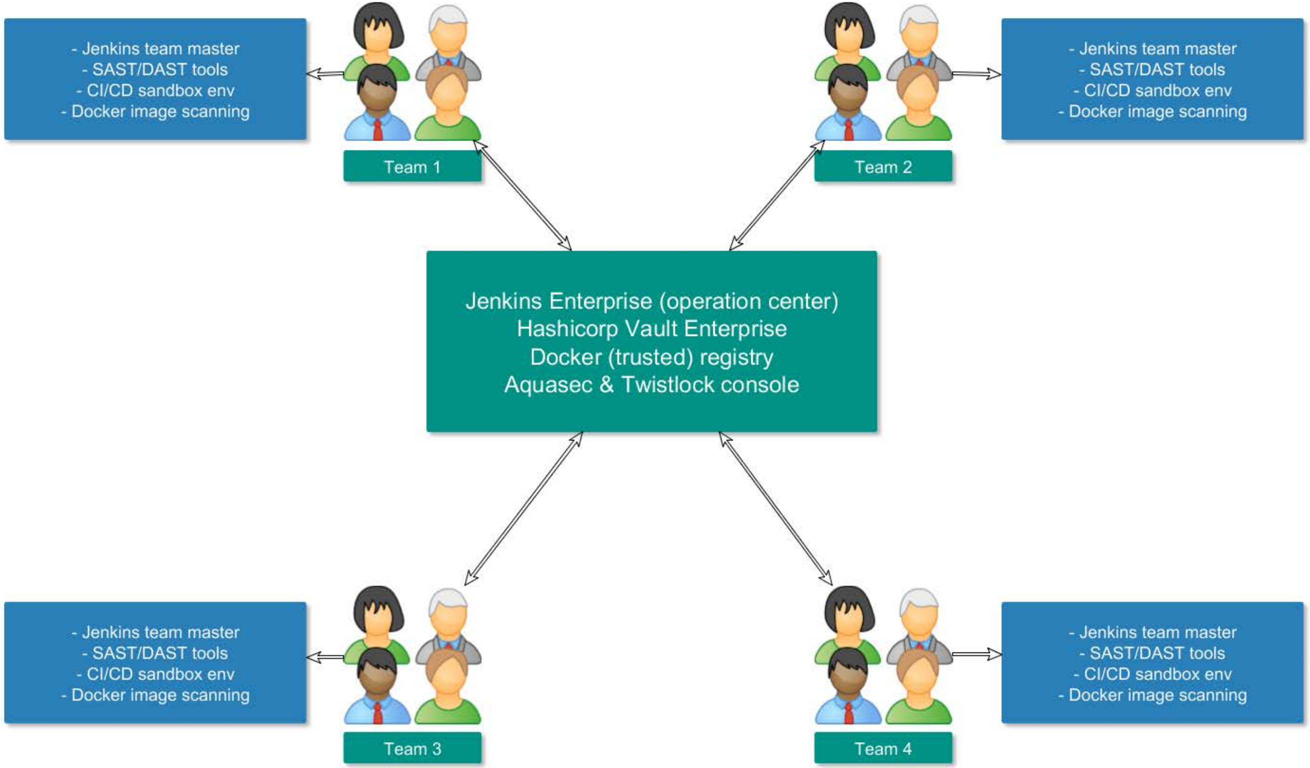


Category	Type	Severity	Description
Host OS	linux	● high	(CIS_Linux_1.1.0 - 4.1.13) Ensure successful file system mounts are collected Show details
Host OS	linux	● high	(CIS_Linux_1.1.0 - 4.1.17) Ensure kernel module loading and unloading is collected Show details
Host OS	linux	● high	(CIS_Linux_1.1.0 - 4.1.17) Ensure kernel module loading and unloading is collected Show details
Host OS	linux	● high	(CIS_Linux_1.1.0 - 4.1.15) Ensure changes to system administration scope (sudoers) is collected Show details
Host OS	linux	● high	(CIS_Linux_1.1.0 - 6.1.7) Ensure permissions on /etc/shadow- are configured Show details
Host OS	linux	● high	(CIS_Linux_1.1.0 - 6.1.5) Ensure permissions on /etc/gshadow are configured Show details
Host OS	linux	● high	(CIS_Linux_1.1.0 - 6.1.3) Ensure permissions on /etc/shadow are configured Show details
Host OS	linux	● high	(CIS_Linux_1.1.0 - 5.2.1) Ensure permissions on /etc/ssh/sshd_config are configured Show details
Docker	daemon config	● high	(CIS_Docker_CE_v1.1.0 - 2.18) Ensure containers are restricted from acquiring new privileges Show details
Docker	daemon config	● high	(CIS_Docker_CE_v1.1.0 - 2.11) Use authorization plugin Show details
Docker	daemon config	● high	(CIS_Docker_CE_v1.1.0 - 2.8) Enable user namespace support Show details
Docker	daemon config	● high	(CIS_Docker_CE_v1.1.0 - 2.1) Restrict network traffic between containers Show details

Check Docker hosts

Team autonomy

Team Autonomy – Tools & processes



- Jenkins team master
- SAST/DAST tools
- CI/CD sandbox env
- Docker image scanning

Team 1

Team 2

Team 3

Team 4

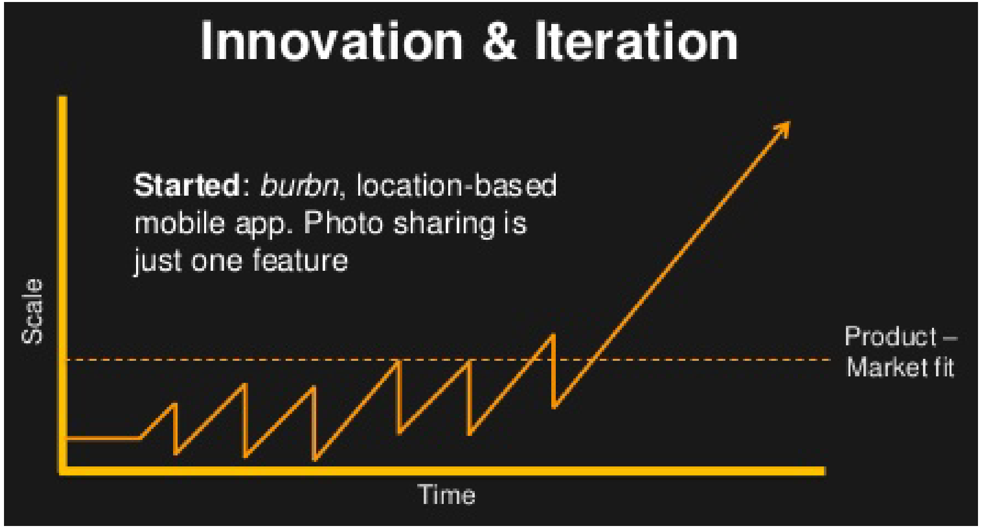
Jenkins Enterprise (operation center)
Hashicorp Vault Enterprise
Docker (trusted) registry
Aquasec & Twistlock console

Cloud first for true team autonomy

- Every team gets it's own VPC
- Infrastructure & configuration as code:
  - First phase: Amazon CFT & Azure ARM
  - Second phase: Terraform
- License to public program as "quality gate"
- Security is key part of the intake

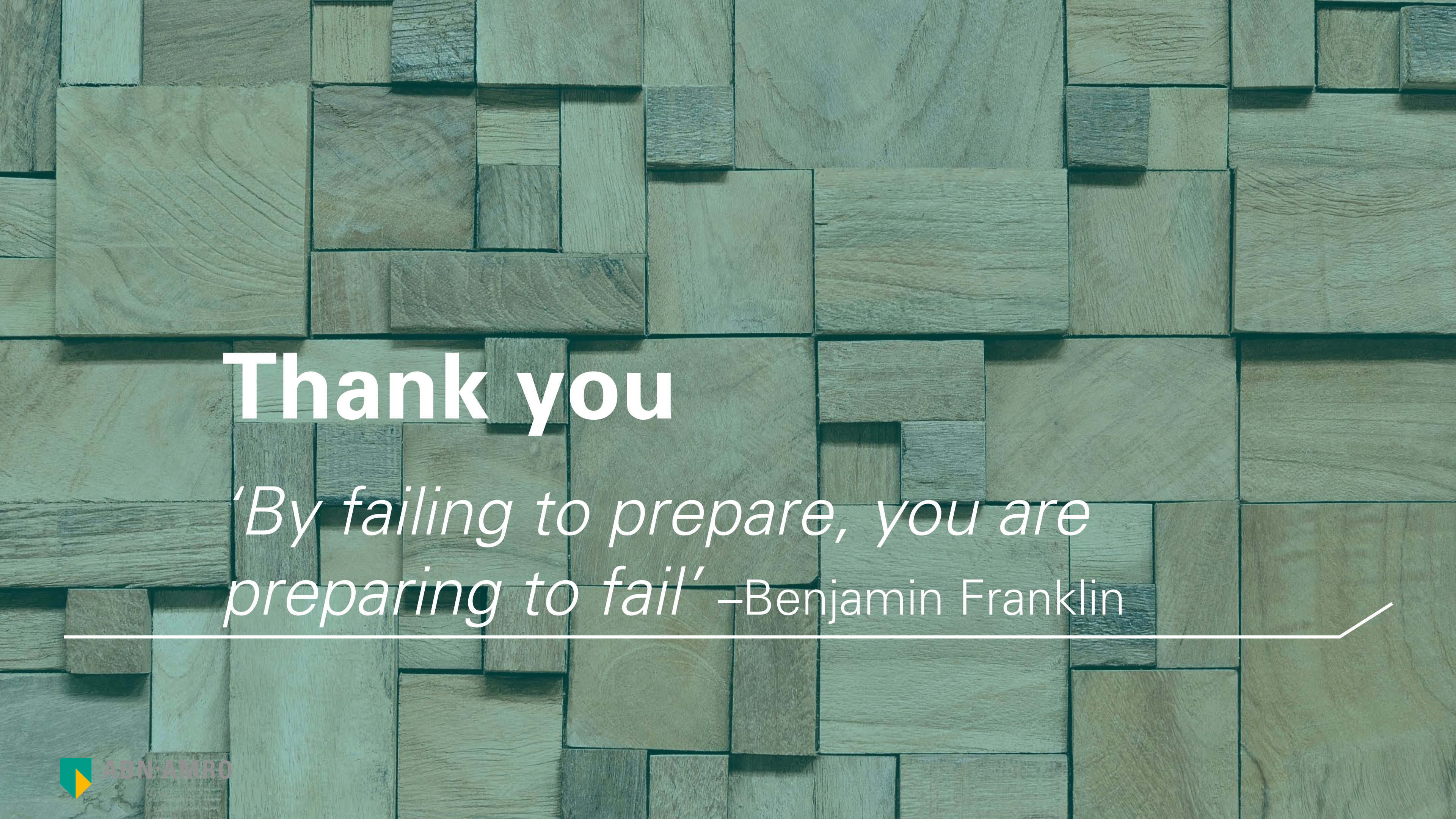
Key benefits for team Autonomy

- Blocking processes are removed
- Speed up innovation / experimentation by teams
- Best practices are shared → spread the knowledge
- Prevention on re-inventing the wheel
- Tech talent will choose for ABN-AMRO
- Faster time 2 market



5 DevSecOps challenges for the enterprise

1. Onboard all teams to centralized tools (Jenkins, Vault, Runtime container scanning, etc)
2. Get rid of the old way of working
3. Automate review processes for all tools (e.g. review false positives)
4. Choosing the best tools
5. Focus of the management for the right activities with the right information



Thank you

‘By failing to prepare, you are preparing to fail’ –Benjamin Franklin