mojaloop

DevSecOps Improvement Update

Core Team – Kim, Pedro, Lewis, Godfrey, Miguel, Sam & Victor

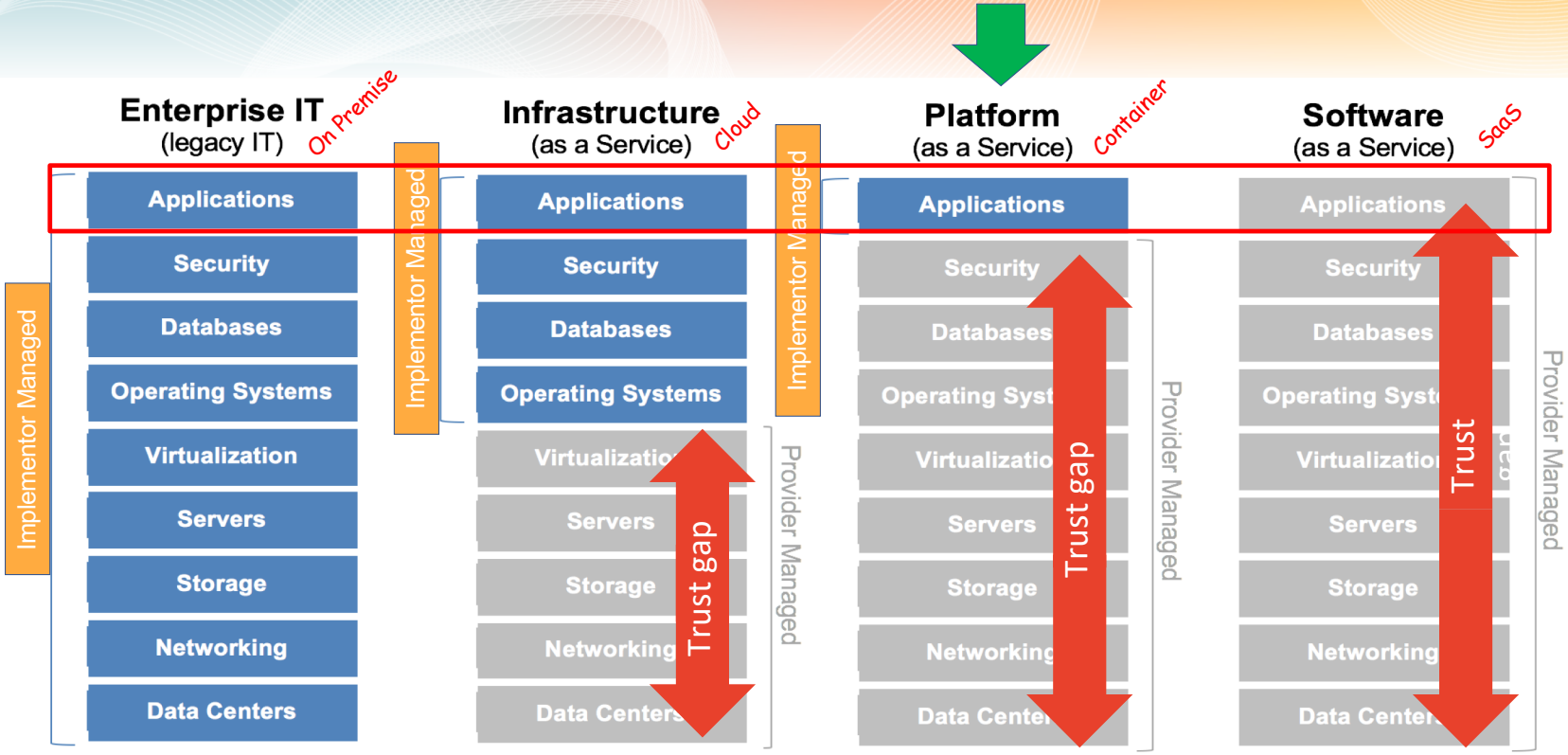
DevSecOps Initiative Overview

Improve security, quality and compliance of the Mojaloop Platform by leveraging mainly open source tools and community support.

Underpinning Principles:

- Deep integration into DevOps and CI\CD processes (All security must be automated gates to keep the DevOps workflow from slowing down)
- Developer centric and inclusive (Empower and delegate with trust security integration activities to the devops teams)
- Open source first approach to tooling (Commercial tools to be considered only if open source tools does not fulfil the requirements)
- Adapt Application Security to Cloud Native Technologies (Containers and Microservices)

DevSecOps Model & Framework



Output:

- Provision of a security guidelines based on the Platform as a Service Model – Implementers to adapt to their own environment and policies
- Alignment to CIS benchmarks and CSA cloud security essentials for IaaS and PaaS

DevSecOps Epics

Code Level Security Epics – PI 7 Focus

- Epic 3: Open Source Quality & Security (Vulnerabilities, Licence compliance, & operational risk)
- Epic 4: Static Code Analysis (SCA) (Dev, Build & Release)
- Epic 5: Container Security (Create, Release & Runtime)

Solution Wide Architecture Epics – Backlog for PI 8

- Epic 1: JavaScript to Typescript Conversion (Typescript preferred but not mandated)
- Epic 2: Architecture / Solution wide concerns (Identities, Service to Service Authentication, API GW etc..)
- Epic 6: Threat Modelling (STRIDE Model)
- Epic 7: Cloud Security (Cloud Agonistic – CIS Benchmarks & CSA Essentials)
- Epic 8: Mojaloop DevSecOps Model (PaaS based Golden Standard)

Under Discussion – Backlog for PI 8 if approved

- Epic 9 : GDPR Compliance (Focusing on the data security technical requirements)
- Epic 10: PCI Compliance (Limit scope to ATM integration)
- Epic 11 : Mojaloop Bug Bounty Programme (Vulnerability Reward Programme)

mojaloop

It's coffee time...

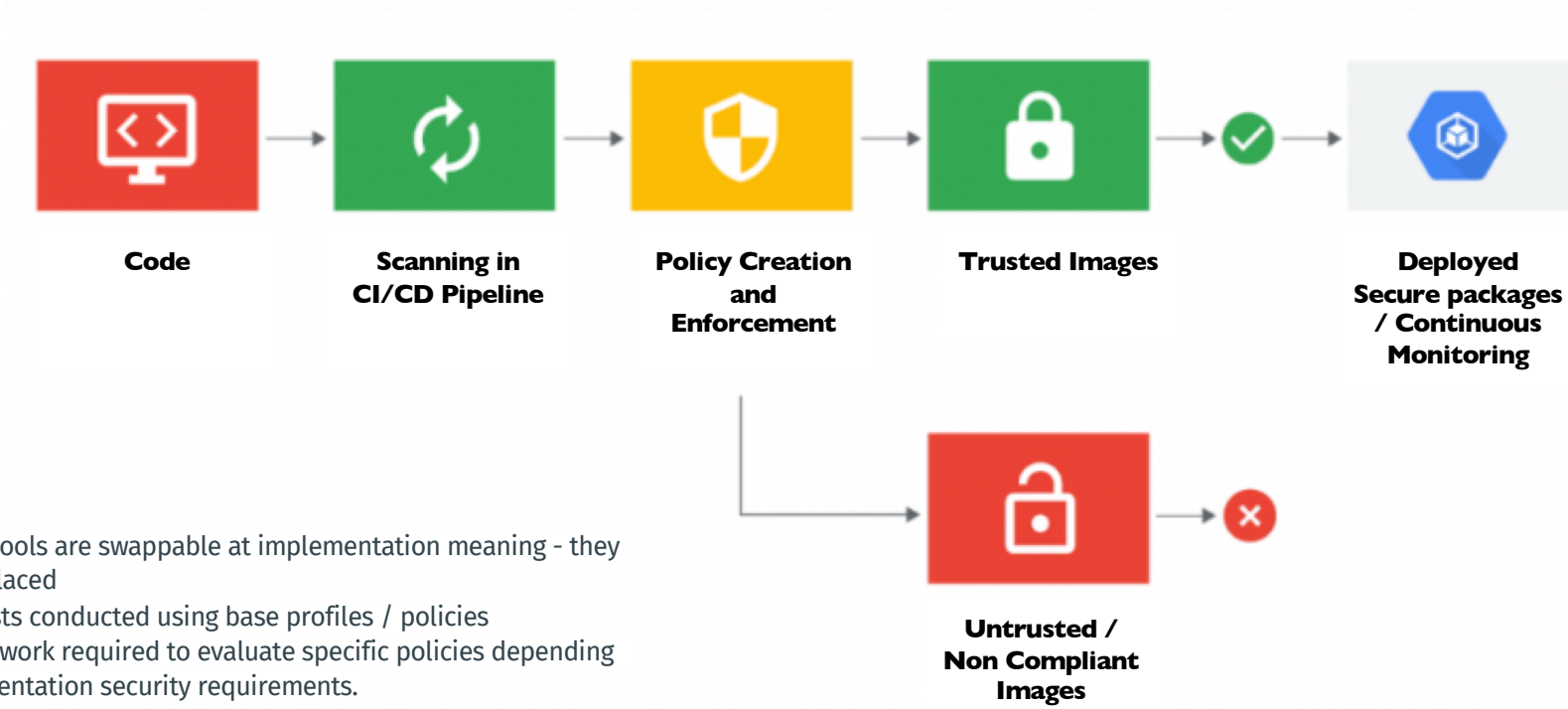
Container Security & Open Source Security - Tools Integration Update

Oops I spilled my coffee

No coasters over here

Lewis & Victor

DevSecOps - How it all fits



- Proposed tools are swappable at implementation meaning - they can be replaced
- Current tests conducted using base profiles / policies
- Additional work required to evaluate specific policies depending on implementation security requirements.

Epic 3: Open Source Quality & Security
#1154 license-scanner updates

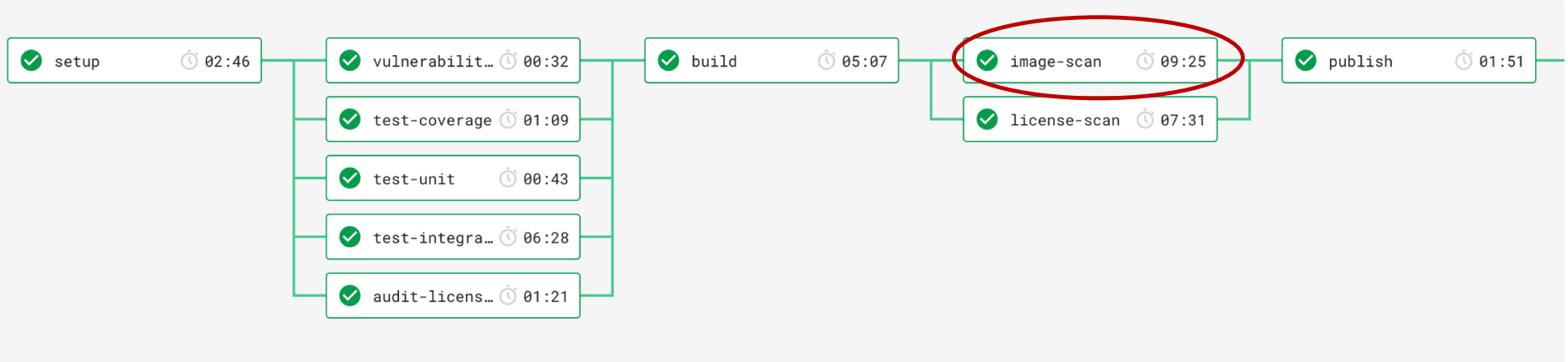
- Change from blacklist to whitelist model

Modules*	Jan-20	Oct-19
Top-level module references (directly in package.json, not nested dependencies)		
Total first-level module dependencies:	382	378
Unique first-level module dependencies:	**131**	127
Total module references (in package-lock.json files, all nested dependencies)		
Total module dependencies:	16,758	15,813
Unique module dependencies:	**1567**	1457

*Across active repos

Epic 5: Container Security Tools
anchore-cli, AppArmor

- Anchore: static container analysis tool
  - ‘Deeper’ scans than npm vulnerabilities alone
- Now integrated as part of our container + helm release cycle



Epic 5: Container Security Tools
Anchore-cli, AppArmor

- Produces image summaries in .json files
- Built automated tools for summarizing into excel/csv:

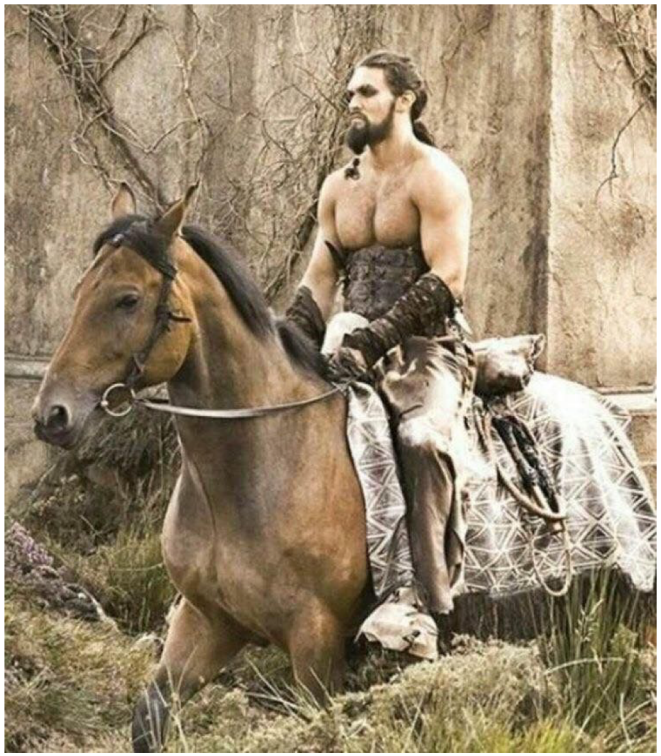
	bulk-api-adapter	central-event-processor	central-settlement	email-notifier	ml-api-adapter	mojaloop-simulator	quoting-service
Critical	0	0	0	0	0	2	0
High	4	4	4	4	4	20	4
Medium	6	6	9	5	5	9	6
Low	2	2	2	2	2	4	2

WARNING:

JSON file snippets ahead.

```
{
    "feed": "nvdv2",
    "feed_group": "nvdv2:cves",
    "fix": "None",
    "nvd_data": [
        {
            "cvss_v2": {
                "base_score": 7.5,
                "exploitability_score": 10.0,
                "impact_score": 6.4
            },
            "cvss_v3": {
                "base_score": 9.8,
                "exploitability_score": 3.9,
                "impact_score": 5.9
            },
            "id": "CVE-2017-10989"
        }
    ],
    "package": "sqlite-3.0.3",
    "package_cpe": "cpe:/a:-:sqlite:3.0.3:-:~~~node.js~~",
    "package_cpe23": "cpe:2.3:a:-:sqlite:3.0.3:-:-:-:-:-:-:~~~node.js~~",
    "package_name": "sqlite",
    "package_path": "/src/node_modules/sqlite/package.json",
    "package_type": "npm",
    "package_version": "3.0.3",
    "severity": "Critical",
    "url": "https://nvd.nist.gov/vuln/detail/CVE-2017-10989",
    "vendor_data": [],
    "vuln": "CVE-2017-10989"
},
```


mojaloop-simulator_v8.8.0-snapshot-vuln.json



momoa_horseback_jason.png

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2017-10989 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, mishandles undersized RTree blobs in a crafted database, leading to a heap-based buffer over-read or possibly unspecified other impact.

Source: MITRE

+View Analysis Description

QUICK INFO

CVE Dictionary Entry:
CVE-2017-10989
NVD Published Date:
07/07/2017
NVD Last Modified:
10/02/2019

https://nvd.nist.gov/vuln/detail/CVE-2017-10989

```
"content": [
    {
        "filename": "/bin",
        "gid": 0,
        "linkdest": null,
        "mode": "00755",
        "sha256": null,
        "size": 0,
        "type": "dir",
        "uid": 0
    },
    {
        "filename": "/bin/arch",
        "gid": 0,
        "linkdest": "/bin/busybox",
        "mode": "00777",
        "sha256": null,
        "size": 12,
        "type": "slink",
        "uid": 0
    },
```

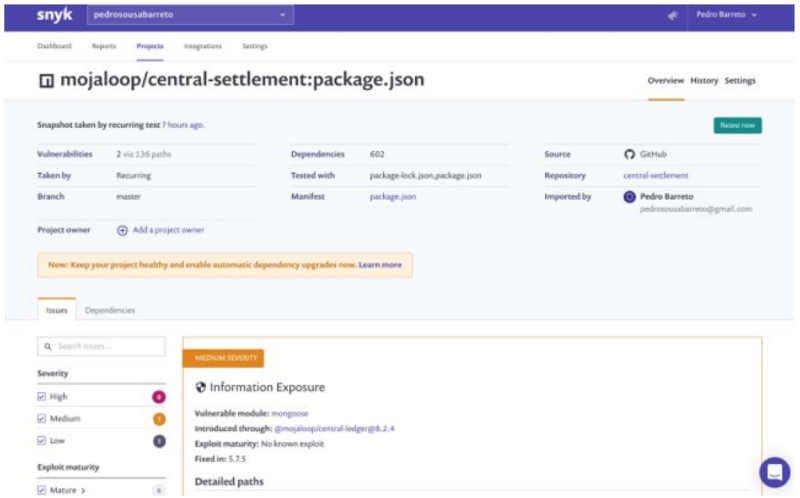

mojaloop-simulator_v8.8.0-snapshot-content-files.json

momoa_frangapani_jason.jpeg

Epic 3: Open Source Quality & Security
#1155 snyk for app scanning

snyk.io

"Enabling more than 400,000 developers to continuously find and fix vulnerabilities in open source libraries and containers"



Epic 3: Open Source Quality & Security
#1155 snyk for app scanning

	High	Med	Low
bulk-api-adapter	0	0	0
central-event-processor	0	0	0
central-settlement	0	**1**	**1**
email-notifier	0	0	0
ml-api-adapter	0	0	0
mojaloop-simulator	0	0	0
quoting-service	0	0	**1**

	Level	Type	Module	Fix available?	Exploit available?	Link
central-settlement	Med	Information Exposure	mongoose	yes	no	https://app.snyk.io/vuln/SNYK-JS-MONGOOSE-472486
central-settlement	Low	Information Disclosure	mongoose	yes	yes	https://app.snyk.io/vuln/SNYK-JS-KINDOF-537849
quoting-service	Low	Information Disclosure	kind-of (from knex)	yes	yes	https://app.snyk.io/vuln/SNYK-JS-KINDOF-537849

Epic 3: Open Source Quality & Security
#1155 snyk for app scanning

Pros

- Integrates with CircleCI (has specific orb)
- Can be executed locally using a CLI (ex: pre-commit hooks)
- Can ignore specific vulnerabilities or fail only above certain threshold (high/med/low)
- Slack integration and email reports
- Ability to automatically create a PR with the fixes (package version upgrades)
- Unlimited tests for OSS public projects
- Large and up-to-date vulnerability database

Cons

- Fancy reports not available in free version
- License compliance management not available in free version
- API not available in free version

Epic 3: Open Source Quality & Security
#1155 snyk for app scanning

	Level	Type	Component	Fix available?	Exploit available?	Link
ml-api-adapter	High	Out-of-bounds Write	musl@1.1.20-r4	yes	no	https://app.snyk.io/vuln/SNYK-ALPINE39-MUSL-458529
ml-api-adapter	High	Arbitrary File Overwrite	node@10.15.3	yes(10.18.0)	yes	https://app.snyk.io/vuln/SNYK-UPSTREAM-NODE-538285
ml-api-adapter	High	Arbitrary File Write	node@10.15.3	yes(10.18.0)	yes	https://app.snyk.io/vuln/SNYK-UPSTREAM-NODE-538286
ml-api-adapter	Low	Denial of Service (DoS)	node@10.15.3	yes(10.16.3)	no	https://app.snyk.io/vuln/SNYK-UPSTREAM-NODE-459326
ml-api-adapter	Low	Unauthorized File Access	node@10.15.3	yes(10.18.0)	yes	https://app.snyk.io/vuln/SNYK-UPSTREAM-NODE-538287
Others	** likely same as ml-api-adapter as they share the same base image **					

Epic 3: Open Source Quality & Security
Docker-bench-security

- A script that checks for best-practices around deploying Docker containers in production.
- Uses CIS Benchmark v.17.06 - https://www.cisecurity.org/benchmark/docker/
- Conducts 105 security tests across Docker runtime environment.

```
# ------------------------------------------------------------------------------
# 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 Tue Jan 28 12:46:13 UTC 2020


[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 19.03.5, 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
[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
[INFO] 1.8  - Ensure auditing is configured for Docker files and directories - docker.service
[INFO]      * File not found
```

Epic 3: Open Source Quality & Security
Docker-bench-security

```
[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
[WARN] 2.8  - Enable user namespace support
[PASS] 2.9  - Ensure the default cgroup usage has been confirmed
[PASS] 2.10  - Ensure base device size is not changed until needed
[WARN] 2.11  - Ensure that authorization for Docker client commands is enabled
[WARN] 2.12  - Ensure centralized and remote logging is configured
[INFO] 2.13  - Ensure operations on legacy registry (v1) are Disabled (Deprecated)
[WARN] 2.14  - Ensure live restore is Enabled
[WARN] 2.15  - Ensure Userland Proxy is Disabled
[PASS] 2.16  - Ensure daemon-wide custom seccomp profile is applied, if needed
[WARN] 2.17  - Ensure experimental features are avoided in production
[WARN] 2.18  - Ensure containers are restricted from acquiring new privileges
```

Epic 3: Open Source Quality & Security
Docker-bench-security

```
[INFO] 5 - Container Runtime
[WARN] 5.1  - Ensure AppArmor Profile is Enabled
[WARN]      * No AppArmorProfile Found: k8s_compose_compose-6c67d745f6-nvtz8_docker_97fb646d-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_compose_compose-api-57ff65b8c7-7f5nx_docker_97d92eb4-1038-11ea-812f-00155d0b0118_4
[WARN]      * No AppArmorProfile Found: k8s_coredns_coredns-6dcc67dcbc-vt5kh_kube-system_87125631-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_coredns_coredns-6dcc67dcbc-4trll_kube-system_870becbd-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_kube-proxy_kube-proxy-lxb2h_kube-system_870bffa0-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_POD_compose-api-57ff65b8c7-7f5nx_docker_97d92eb4-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_POD_compose-6c67d745f6-nvtz8_docker_97fb646d-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_POD_coredns-6dcc67dcbc-vt5kh_kube-system_87125631-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_POD_coredns-6dcc67dcbc-4trll_kube-system_870becbd-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_POD_kube-proxy-lxb2h_kube-system_870bffa0-1038-11ea-812f-00155d0b0118_2
[WARN]      * No AppArmorProfile Found: k8s_kube-scheduler_kube-scheduler-docker-desktop_kube-system_ef4d089e81b94aa15841e51ed8c41712_10
[WARN]      * No AppArmorProfile Found: k8s_etcd_etcd-docker-desktop_kube-system_3773efb8e009876ddfa2c10173dba95e_2
```

Epic 3: Open Source Quality & Security
AppArmor runtime security

- AppArmor (Application Armor) is a Linux security module that protects an operating system and its applications from **runtime** security threats.
- Docker expects to find an AppArmor policy loaded and enforced. It automatically generates and loads a default profile for containers named docker-default.
- Profiles can allow capabilities like network access, raw socket access, and the permission to read, write, or execute files on matching paths.

```
profile docker-nginx flags=(attach_disconnected,mediate_deleted) {
  #include <abstractions/base>

  network inet tcp,
  network inet udp,
  network inet icmp,

  deny network raw,

  deny network packet,

  file,
  umount,

  deny /bin/** wl,
  deny /boot/** wl,
  deny /dev/** wl,
  deny /etc/** wl,
  deny /home/** wl,
  deny /lib/** wl,
  deny /lib64/** wl,
  deny /media/** wl,
  deny /mnt/** wl,
  deny /opt/** wl,
  deny /proc/** wl,
  deny /root/** wl,
  deny /sbin/** wl,
  deny /srv/** wl,
  deny /tmp/** wl,
  deny /sys/** wl,
  deny /usr/** wl,

  audit /** w,

  /var/run/nginx.pid w,

  /usr/sbin/nginx ix,
```

Challenges / Next Steps

- Continuous monitoring of the threat landscape – Including public concerns on Mojaloop Security.
- Hold formal feedback sessions with implementers.
- Safely navigate through a large landscape of open source security tools.
- Continuous tool update without impacting the CI/CD workflow process.
- Keep compliance initiatives use case driven.

mojaloop

More coffee stains

Thank You

Questions?

Oh no! A spill!

mojaloop

Appendix

Epic 1: Javascript to Typescript Conversion

Typescript Pros

- Type checking makes it easier to find bugs that usually get caught only at runtime (no test substitute)
- OOP allows for "interface oriented development" which is an enabler of Single Responsibility Principle - which leads to scalable code and dependency management
- Easier to refactor when code gets bigger
- TS and JS can co-exist on the same project, no all of nothing approach required
- A significant number of large JS libraries and frameworks are already TS

Epic 1: Javascript to Typescript Conversion

Typescript Cons

- Additional dev tools/steps - more setup time
- Devs have to learn TS
- TS on its own is no silver bullet - bad developers can still produce bad TS code
- Might detract JS purists from contributing - not true anymore since the majority of JS devs can do TS (source https://stackshare.io/typescript)

Epic 1: Javascript to Typescript Conversion

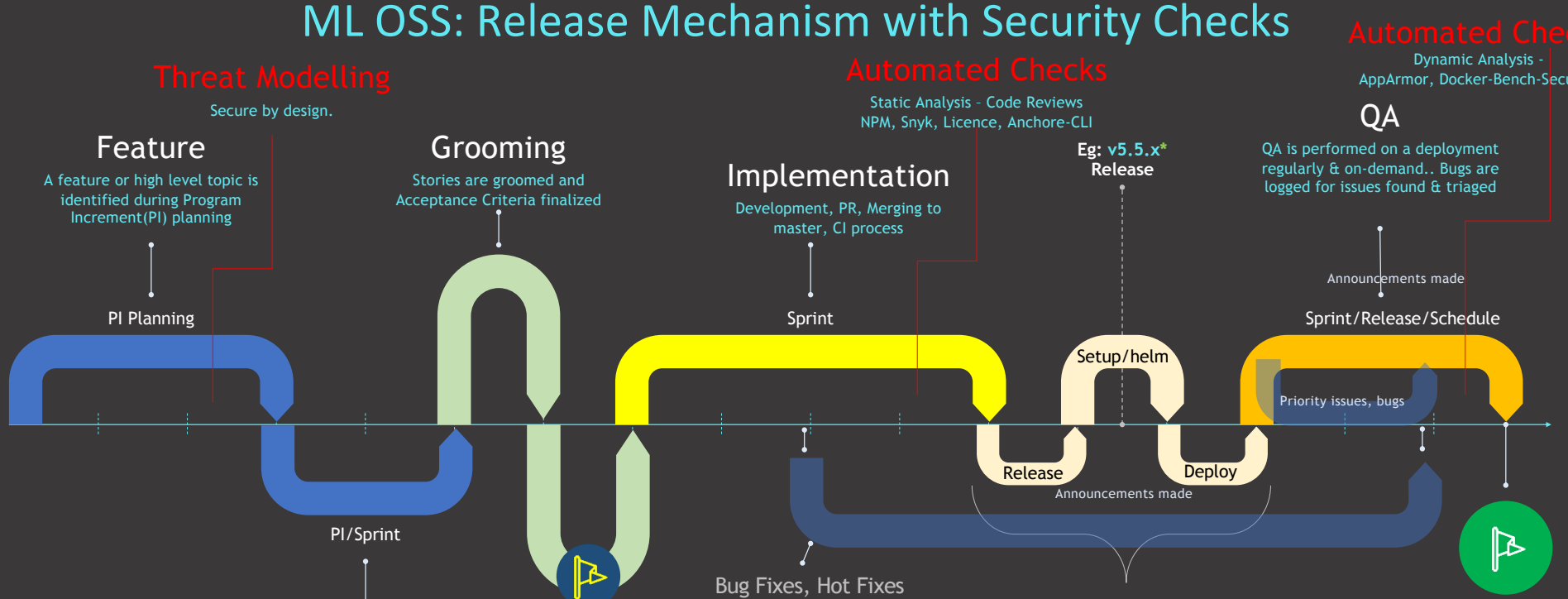
Typescript Fallacies

- Development takes longer
  - Cost of software is in maintaining it, not the initial code - TS can improve maintainability of the code
- Prevent recruiting good JS people
  - “good JS” often translates to hard to maintain procedural code.
  - Plus, good developers can use many tools, including many languages.

Recommendation

- Plan the update of core and shared repos to Typescript
  - Start with shared libraries first, then move on to
- Enforce new core and shared repos to use Typescript

ML OSS: Release Mechanism with Security Checks



* Inspired by SemVer; x.y.z – where 'x' is the PI number, 'x.y' is the Sprint number and 'z' is the number of release in a particular sprint

Note: This depicts a single iteration that happens multiple times over the course of a PI

ModusBox for BMGF