mojaloop

DevSecOps Improvement Update

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

mojaloop

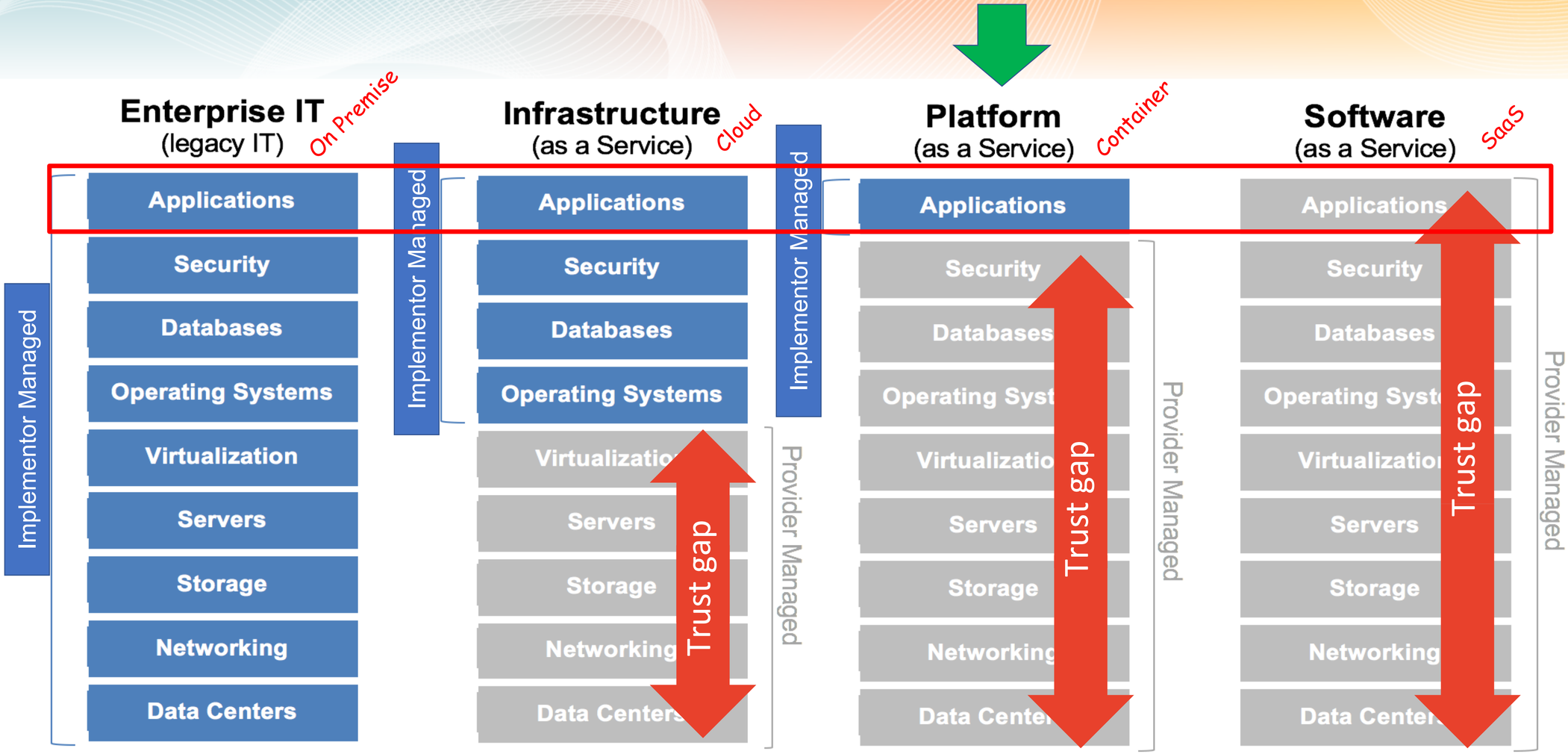
DevSecOps Initiative Overview

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:

- Statement of Responsibility – A summary of all security measures undertaken in building the Mojaloop Platform
- Flexibility to deploy across various cloud platforms and cloud native technologies

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 Convention (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 (Multi Cloud Security Standard)
- Epic 8: Mojaloop DevSecOps Model (Responsibility Statement)

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

Container Security & Open Source Security - Tools Integration Update

By Lewis & Victor

mojaloop

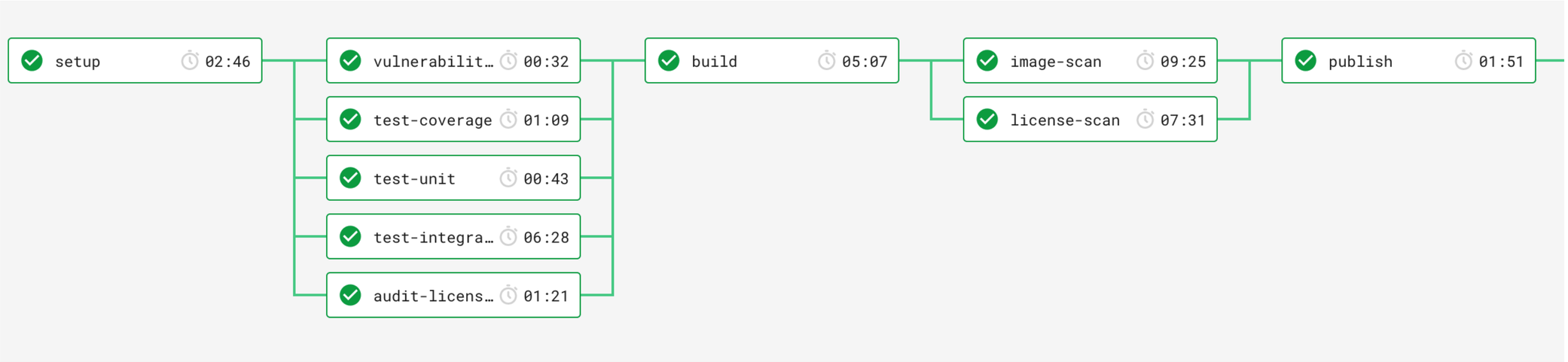
Epic 3: Open Source Quality & Security
#1154 license-scanner updates

- Existing license-scanner work
- Change from blacklist to whitelist

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		(including 10 internal repos which are referenced in different projects)
Total module references (in package-lock.json files, all nested dependencies)				
Total module dependencies:	16,758	15,813		
Unique module dependencies:	1567	1457		

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
- Work included typing together vulnerability reports in summary:

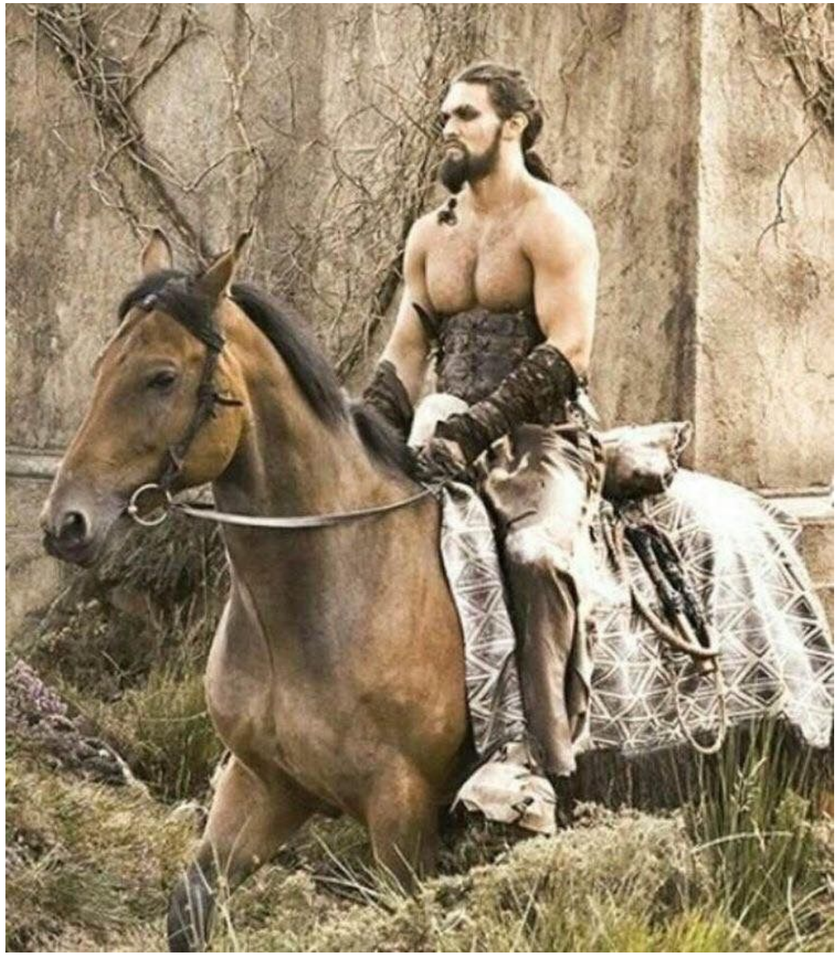
	bulk-api-adapter	central-event-processor	central-settlement	email-notifier	ml-api-adapter	mojaloop-simulator	quoting-service
Critical	0	0	0	0	0	2	0
High	4	4	4	4	4	20	4
Medium	6	6	9	5	5	9	6
Low	2	2	2	2	2	4	2

WARNING:

JSON file snippets ahead.

```
{
    "feed": "vulnerabilities",
    "feed_group": "alpine:3.9",
    "fix": "1.1.1d-r0",
    "nvd_data": [
        {
            "cvss_v2": {
                "base_score": 1.9,
                "exploitability_score": 3.4,
                "impact_score": 2.9
            },
            "cvss_v3": {
                "base_score": -1.0,
                "exploitability_score": -1.0,
                "impact_score": -1.0
            },
            "id": "CVE-2019-1547"
        }
    ],
    "package": "libcrypto1.1-1.1.1b-r1",
    "package_cpe": "None",
    "package_cpe23": "None",
    "package_name": "libcrypto1.1",
    "package_path": "None",
    "package_type": "APKG",
    "package_version": "1.1.1b-r1",
    "severity": "Low",
    "url": "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1547",
    "vendor_data": [],
    "vuln": "CVE-2019-1547"
},
```


mojaloop-simulator_v0.0.3-snapshot-vuln.json



momoa_horseback_jason.png

```
"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_v0.0.3-snapshot-content-files.json

momoa_frangapani_jason.jpeg

mojaloop

Thank You

Questions?